TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

Implementace skeneru zranitelností do datového centra

Bakalářská práce

Studijní program: B2612 – Elektrotechnika a informatika
Studijní obor: 1802R022 – Informatika a logistika

Autor práce: **Michal Miklánek**
Vedoucí práce: **Doc. RNDr. Pavel Satrapa, Ph.D.**

Liberec 2017

Technická univerzita v Liberci
Fakulta mechatroniky, informatiky a mezioborových studií
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michal Miklánek**
Osobní číslo:	**M14000242**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Informatika a logistika**
Název tématu:	**Implementace skeneru zranitelností do datového centra**
Zadávající katedra:	**Ústav nových technologií a aplikované informatiky**

Zásady pro vypracování:

1. Proveďte rešerši současného stavu skenování zranitelnosti informační infrastruktury včetně dopadů Zákona o kybernetické bezpečnosti.
2. Vyberte několik produktů z této oblasti a porovnejte je.
3. Navrhněte nasazení vybraného produktu do prostředí datového centra České pošty a vytvořte skenovací politiky.
4. Navržené řešení otestujte a vyhodnoťte výsledky.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **40 - 60 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. V Tribunu EU vyd. 1. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.
[2] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.
[3] LYON, Gordon Fyodor. Nmap network scanning: official Nmap project guide to network discovery and security scanning. 1st ed. Sunnyvale, CA: Insecure.Com, LLC, c2008. ISBN 0979958717.
[4] KIM, Peter. Hacking: praktický průvodce penetračním testováním. Vydání první. Přeložil Jan POKORNÝ. Brno: Zoner Press, 2015. Encyklopedie Zoner Press. ISBN 978-80-7413-313-8.
[5] DRASTICH, Martin. Systém managementu bezpečnosti informací. 1. vyd. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.
[6] WILEY, John & Sons, Ltd. Vulnerability Management For Dummies, 2nd Edition. Southern Gate, Chichester, West Sussex, PO19 8SQ, England: The Atrium, 2015. ISBN 978-1-119-13150-2.

Vedoucí bakalářské práce: **doc. RNDr. Pavel Satrapa, Ph.D.**
Ústav nových technologií a aplikované informatiky

Datum zadání bakalářské práce: **20. října 2016**

Termín odevzdání bakalářské práce: **15. května 2017**

prof. Ing. Zdeněk Plíva, Ph.D.
děkan

L.S.

prof. Dr. Ing. Jiří Maryška, CSc.
vedoucí ústavu

V Liberci dne 20. října 2016

Děkuji vedoucímu bakalářské práce doc. RNDr. Pavlu Satrapovi, Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce. Dále bych rád poděkoval za odborné konzultace Michalu Moučkovi, M.Sc. z firmy Risk Analysis Consultants, s.r.o. Za spolupráci a podporu děkuji svým kolegům z odd. BICT České pošty a za pomoc při jazykové korektuře práce a velké podpoře po celou dobu studia děkuji své manželce Mgr. Vlastě Miklánkové.

Čestné prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum: 9.5.2017

Podpis:

Abstrakt

Tato práce řeší zprovoznění skeneru zranitelností v datových centrech reálné firmy v návaznosti na zákon o kybernetické bezpečnosti. Cílem práce je porovnání konkurenčních produktů v oblasti skenování zranitelností, popis výchozího způsobu použití skeneru zranitelností a návrh na implementaci do běžného provozu datového centra.

Výstupem je sada otestovaných skenovacích politik a připravené šablony reportů. Vzorově jsem napojil na skener jeden systém na platformě UNIX a jeden na platformě Windows s popsanými postupy. Přednostně se jedná o systémy spadající do kritické informační infrastruktury. Porovnání konkurenčních produktů jsem provedl z uživatelského hlediska s důrazem na sadu kritérií, kterou jsem v kontextu znalosti prostředí a vlastních požadavků považoval za klíčovou. Z provedených testů vyplynulo, že z největší části vyhovují dva produkty výrobců Tenable a Qualys.

Podle mého návrhu se podařilo zprovoznit skenery Tenable Nessus ve všech třech datových centrech. Připravené skenovací politiky tvoří sadu určenou pro rutinní použití napříč platformami. Krom doplňkových politik, které slouží např. k testování, zda se skener dokázal přihlásit ke skenovanému aktivu s dostatečným oprávněním, je zásadní politika provádějící v pravidelných intervalech audit instalovaných opravných balíků operačních systémů a aplikací tzv. patch audit sken s výstupem do reportů z připravených šablon.

Práce může být vodítkem pro další instituce, které tuto problematiku dříve či později budou řešit.

Klíčová slova

Informační bezpečnost, Zranitelnost, Skener zranitelností, Kritická informační infrastruktura

Abstract

This dissertation addresses the launch of a vulnerability scanner in the data centers of a real firm, in line with the Cyber Security Act. The aim of the dissertation is to compare competing products in the area of vulnerability scanning, to describe the default way of using a vulnerability scanner and to propose its implementation into the normal operation of the data center.

The output is a set of tested scan policies and prepared report templates. As a sample, I connected one system based on the UNIX platform and one based on the Windows platform to the scanner and described the procedures. It regards preferentially critical information infrastructure systems. I compared the competing products from the user perspective with a focus on a set of criteria that I considered crucial according to my knowledge of the environment and my own requirements. Realized tests have shown the highest compliance by two products made by producers Tenable and Qualys.

Following my proposal, two Tenable Nessus scanners have been successfully launched in all three data centers. The prepared scan policies represent a set designed for routine cross-platform use. In addition to complementary policies, which serve for example to test whether the scanner was able to log into the scanned asset with sufficient rights, the policy performing regularly an audit of the installed patches of operating systems and applications , the so-called patch audit scan, with an output to the reports from the prepared templates is essential.

This work may serve as guideline for other institutions that will deal with this issue sooner or later.

Keywords

Information security, Vulnerability, Vulnerability scanner, Critical information infrastructure

Obsah

Seznam použitých zkratek

AR	Analýza rizik
ČP	Česká pošta, s.p.
DC	Datové centrum
DSČP	Datová síť České pošty
GPO	Group Policy
HTTP(S)	Hyper Text Terminal Protocol (Secured)
HW	Hardware
ICT	Informační a komunikační technologie
IP	Internet Protocol
ISZS ČP	Informační systém základních služeb ČP
KII	Kritická informační infrastruktura
OBM	Out of Band Management
OS	Operační systém
SC	Security center
SIEM	Security Information and Event Management
SSH	Secure Shell
SUDO	Substitute user do
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ZKB	Zákon o kybernetické bezpečnosti

1 Úvod a cíl práce

1.1 Úvod

Tato práce se zabývá návrhem implementace skeneru zranitelností do datového centra velkého podniku. Tímto podnikem je Česká pošta, s.p. Datová síť České pošty (DSČP) čítá několik tisíc koncových stanic, mnoho set serverů na různých platformách, desítky lokalit a vlastní datové centrum (DC). S postupnou digitalizací této tradiční firmy vznikla přirozeně nutnost řídit také informační rizika, tedy hodnotit aktiva, definovat hrozby, analyzovat rizika, zavádět vhodná opatření ke snížení zranitelností, zkrátka dělat vše pro to, aby informace v elektronické podobě putovaly datovou sítí bezpečně, zároveň dostupně a se zaručenou integritou. S rozvojem výpočetní techniky jsou postupně i na oblast informační bezpečnosti kladeny stále větší nároky, a to nejen z pohledu konkurenceschopnosti podniku, ale i přímo ze zákonů přijatých Parlamentem České republiky. Zákon o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) účinný od 1. 1. 2015 společně s vyhláškou o kybernetické bezpečnosti pracuje s pojmem kritická informační infrastruktura (KII). Dle tohoto zákona musí KII splňovat určitá kritéria. Vzhledem k tomu, že Česká pošta provozuje informační systémy spadající do KII, vzniká zde nutnost a potřeba zákon naplnit. I z tohoto důvodu je v prostředí České pošty projekt implementace skeneru zranitelností aktuální, se zaměřením v první řadě na servery v kategorii KII.

Tlak ze strany zákona nicméně nebyl primárním popudem k nasazení této bezpečnostní technologie. Česká pošta pořídila skener zranitelností již v roce 2012, avšak jeho implementace byla omezena pouze na úroveň příležitostného skenování lokalit, nikoliv datového centra. Implementace skeneru do DC a vytvoření skenovacích politik je předmětem právě této bakalářské práce. Její téma jsem si zvolil, protože pro Českou poštu pracuji na pozici bezpečnostního analytika v odd. Bezpečnost ICT sedmým rokem a tento projekt je zároveň mou aktuální hlavní pracovní náplní.

Skener zranitelností je pouze střípek z celé mozaiky odvětví informační bezpečnosti. Jedná se o jednu z řady technologií, které při správném použití pomáhají firmě chránit aktiva a včas reagovat na případné pokusy o jejich zneužití. V případě skeneru zranitelností jde o to včas odhalit slabá místa, kudy je možné na informační systém zaútočit, a na základě těchto zjištění slabá místa posílit, např. doinstalováním nejnovějších aktualizací. I ta nejlepší implementace skeneru bude vždy pouze vodítkem pro bezpečnostní administrátory, kteří z výsledků testů a za pomoci dobře nastavených procesů dokáží zajistit co nejméně zranitelné operační systémy a aplikace běžící v produkčním prostředí.

1.2 Cíl práce

Cílem této práce je navrhnout a popsat kompletní nasazení technologie skeneru zranitelností do datového centra včetně vzorového napojení dvou informačních systémů (platforma Windows a UNIX) na skener. Primární okruh zařízení, která budou skenována, spadá do prvků kritické informační infrastruktury ve smyslu ZKB. Nasazením technologie je myšleno vytvoření návrhu umístění skenerů v rámci datové sítě České pošty, následné zajištění instalace SW a zprovoznění skenerů. Důležitou částí práce je navržení skenovacích politik pro použití na centrálních systémech, navržení jejich konfigurací a časového plánu pravidelného spouštění skenů. Pro přehlednost a čitelnost budou skenovací politiky přepsány do textové podoby a v podobě tabulek budou přílohou této práce.

Vzhledem k tomu, že se některá schémata a výstupy budou vztahovat k produkčnímu prostředí reálné firmy, dojde k minimální nutné anonymizaci citlivých dat (např. IP adres) tak, aby bylo možné tento dokument zveřejnit.

2 Teoretická část

2.1 Definice pojmů

Mám-li popisovat možnosti implementace skeneru zranitelností, ať současné či budoucí, považuji za důležité hned na začátku sjednotit terminologii a stručně popsat obecný význam technologií zmiňovaných v této práci. Obecné pojmy jsou výstižně vysvětleny v knize Josefa Požára *Informační bezpečnost* [1], ze které tuto kapitolu cituji s výjimkou pojmu informační systém, jejž lépe vystihl prof. Molnár v knize *Podnikové informační systémy*. [2]

- **Aktivum** (*Asset*). Aktiva jsou všechny hmotné i nehmotné statky, vše, co má pro majitele informačního systému jistou hodnotu. Za nejcennější aktiva se považují peníze, majetek a především data a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo osobě způsobily určitou ztrátu.
- **Bezpečnost** (*Security*). Pod pojmem bezpečnost chápeme vlastnost nějakého objektu nebo subjektu (informačního systému či technologie), která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám.
- **Hrozba** (*Threat*) je skutečnost, událost, síla nebo osoby, jejichž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost (např. přírodní katastrofa, hacker, zaměstnanec aj.).
- **Informační systém** je soubor lidí, technických prostředků a metod (programů), zabezpečujících sběr, přenos, zpracování, uchování dat, za účelem prezentace informací pro potřeby uživatelů činných v systémech řízení. [2]
- **Riziko** (*Risk*) je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva.
- **Ocenění rizik** (*Risk Assessment*) je proces vyhodnocení hrozeb, které působí na informační systém s cílem definovat úroveň rizika, kterému je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň.

- **Útokem**, který nazýváme rovněž **bezpečnostní incident**, rozumíme buďto úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech.
- **Zranitelnost** (*Vulnerability*) je nedostatek nebo slabina bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv. Každé aktivum je zranitelné, protože jeho hodnotu ohrožují různé vlivy.

2.2 Řízení informačních rizik

Podobně jako se využití internetu šířilo od technologických nadšenců k široké veřejnosti, dalo by se říci, že povědomí o informačních rizicích se postupně šíří od úzce specializovaných bezpečnostních komunit k běžným uživatelům informačních technologií. Ačkoliv zástupci laické veřejnosti nemusí tušit, co je kupříkladu DDoS útok, dvouhodinová nedostupnost oblíbeného internetového portálu, obchodu, nebo webové aplikace elektronického bankovnictví, se spolehlivě dostane na titulní stranu novin.

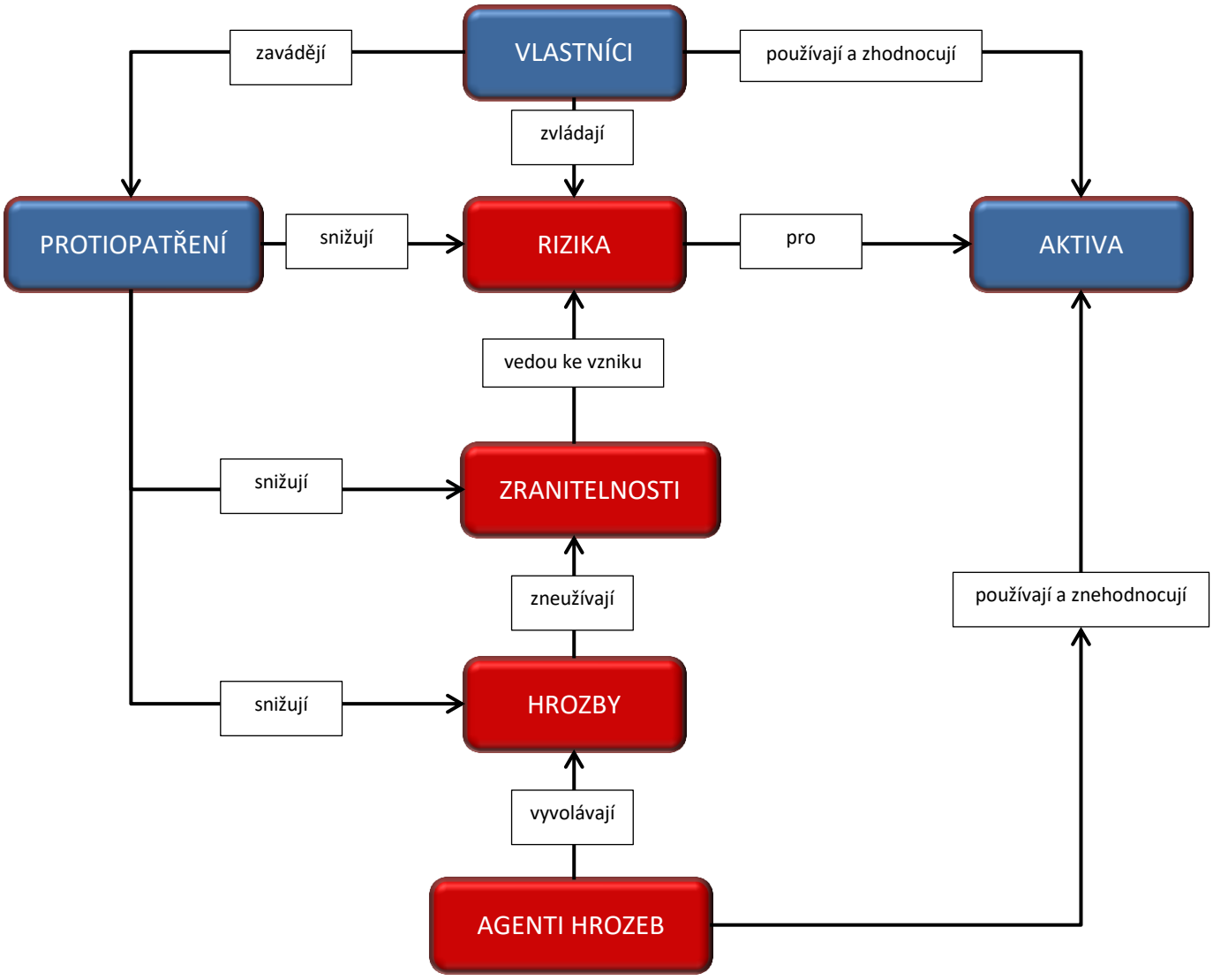
Zájem o zabezpečení informačních systémů firem i soukromých zařízení postupně roste s tím, jak podobných útoků přibývá. Týmy IT bezpečnosti (pokud ve firmách existují) se pomalu a postupně přesouvají z pozice „nutné zlo“ (a to v lepším případě, v horším případě „zbytečný a obtěžující“) do role plnohodnotné součásti analytických a projektových týmů. Má to svou logiku, pokud existuje pouze malý předpoklad výskytu negativních důsledků, riziko je malé a nemá význam se jím příliš zabývat. Dobře to vystihuje analytické vyjádření rizika R vzorcem [3]:

$$R = \frac{P.D}{O}.E$$

kde P je pravděpodobnost vzniku události, D je následek události, E je četnost (expozice) události. Všechny tyto tři veličiny výsledné riziko zvyšují. Naopak snížení rizika dosáhneme zavedením opatření O. Čím více je společnost závislá na informačních technologiích, tím se fakticky zvyšují reálné dopady, následky kybernetických útoků. Přesouváním stále většího objemu dat, aplikací a ve svém

důsledku peněz do prostředí veřejného internetu, roste zájem méně poctivé části lidstva se těchto prostředků zmocnit, nebo například vyřadit kritický systém z provozu. Úměrně s tím také roste i pravděpodobnost, že k takovým událostem bude docházet, a nepochybně stále častěji. Význam zavádění opatření snižující riziko je v tomto kontextu zřetelný.

V oblasti řízení informačních rizik se nejčastěji uvádí definice, která riziko popisuje jako možnost, že specifická hrozba využije specifickou zranitelnost systému, překoná stávající opatření a způsobí narušení důvěrnosti, integrity nebo dostupnosti aktiva a to povede ke vzniku škody. Mechanismus uplatnění rizika probíhá tak, jak výstižně znázornil Miroslav Čermák ve své knize Řízení informačních rizik v praxi. [4] (viz *Obrázek 1 - Mechanismus uplatnění rizika*)

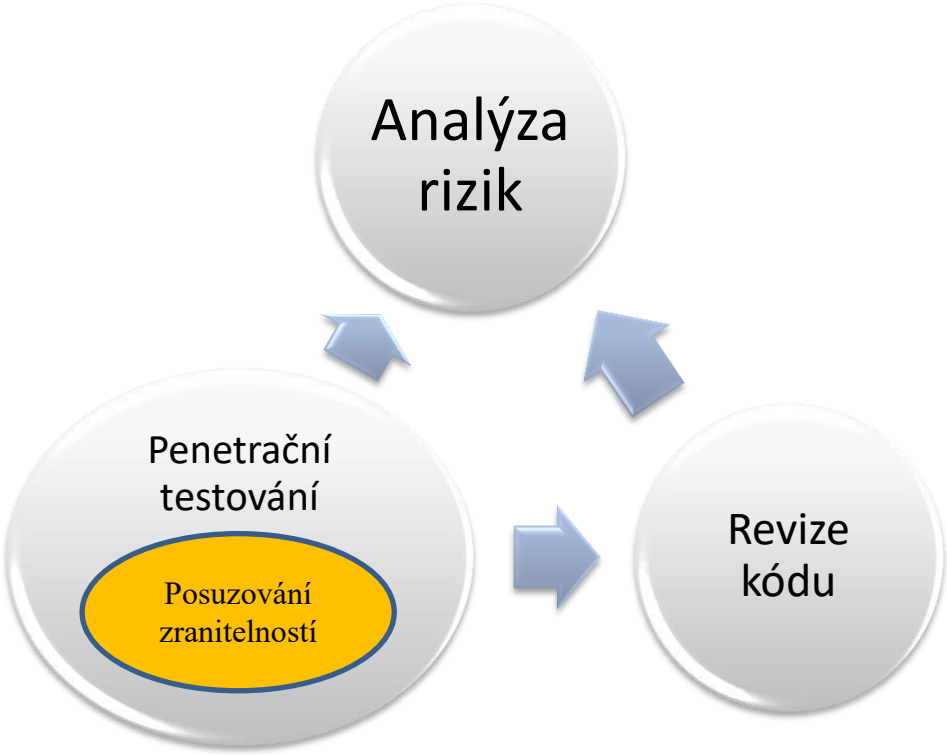


Obrázek 1 - Mechanismus uplatnění rizika [4]

2.3 Sken zranitelností

„Cílem skenování zranitelností, v zahraniční literatuře označované jako *vulnerability scan*, je nalezení známých zranitelností v systému, databázi, aplikaci nebo síťovém prvku. Za tímto účelem se používají automatizované nástroje jako je Nessus, Nexpose nebo Qualys, které disponují rozsáhlou databází operačních systémů a zranitelností a jsou schopny po zadání IP adresy nebo IP adresního rozsahu dané systémy oskenovat a zobrazit známé zranitelnosti včetně odkazu, kde jsou uvedeny detailní informace včetně návodu jak danou zranitelnost odstranit. Přístup do systému zpravidla není nutný.“ [5] Tak definuje Miroslav Čermák sken zranitelností na webu Sart&Clever. Pravdou je, že přístup do systému není nutný, ale vlastní praxe ukázala diametrální rozdíly ve výsledcích skenování s přístupem a bez něj.

Skenování zranitelností je zpravidla součástí širšího procesu analýzy rizik (AR) a výsledky skenování jsou jedním ze zdrojů AR, jak je naznačeno na obrázku (viz *Obrázek 2 - Analýza rizik* [5])



Obrázek 2 - Analýza rizik [5]

2.4 Důvody pro hledání zranitelností

Obecná snaha o nalezení zranitelností v systému může mít různou motivaci. Nejčastěji to však budou tyto důvody:

- odhalení vlastních zranitelností
- odhalení cizích zranitelností – penetrační testování
- využití nalezených zranitelností, útok na cizí cíle – hacking

Z uvedených motivací plyne, že vlastník aktiv i útočník mohou ve výsledku používat stejný nástroj pro zjištění zranitelností. Jeden však ve snaze zranitelnosti najít a odstranit, druhý ve snaze zranitelnosti najít a zneužít ve svůj prospěch. V této práci se budeme zabývat variantou první, tedy hledáním zranitelností proto, aby byly co nejdříve odstraněny a vlastní aktiva byla méně zranitelná.

2.5 Typy skenování

Skenery zranitelností obvykle nabízí více typů prováděných skenů. V této kapitole jsou krátce popsány obecné způsoby a možnosti provádění skenů. Z pohledu směru použití se dají definovat dva způsoby skenování - „externí sken“ a „interní sken“.

- Externí sken
    - Při externím skenování je skener používán tak, abychom o skenovaném cíli zjistili co nejvíce, aniž bychom znali síťové prostředí, přihlašovací údaje k operačním systémům či aplikacím. Tento způsob může být využit v síti, o které mnoho nevíme, a potřebujeme zjistit, co se v dané síti nachází. Půjde převážně o skenování portů, případně zkoušení spuštění skriptů na webových formulářích atd. Využití najde takový způsob rovněž pro systémy vystavené přímo do internetu, a to např. v podobě penetračních testů. Způsob provedení testu může být i velice invazivní a při nešetrném nastavení může dojít k pádu nebo poškození skenovaného systému. Skenování vlastní sítě bez autentizace může být užitečné pro zjištění, zda např. skutečný stav odpovídá stavu popsanému v dokumentaci. Je tak možné poměrně snadno odhalit chybné konfigurace.

- Interní sken
  - Interní sken definuji jako cílené skenování zranitelností konkrétních systémů, ke kterým je umožněn ideálně plný přístup. Pokud je splněn předpoklad přihlášení s plným oprávněním k danému OS, není např. žádoucí na takovém systému pravidelně skenovat porty. Skener zjistí informaci jednoduše (např. v CentOS příkazem *netstat –a*). Po přihlášení na daný systém je sken zaměřen na hledání zranitelností např. v podobě chybějících opravných balíků pro OS, neaktualizovaných aplikací atd.

Z pohledu využití lze skeny dělit následovně:

- Síťové skenování portů
  - Skenování portů je proces, při kterém se zjišťuje, jaké služby poskytuje dané síťové zařízení na otevřených, tím pádem potencionálně zneužitelných portech. Nejčastěji se používá metoda tzv. SYN skenu. Tu popisuje Margaret Rouse na webu *techtarget.com* takto: „Při SYN skenu se klient pokouší navázat TCP/IP spojení na každém dostupném portu. To je realizováno posíláním SYN (synchronization) paketů, jako kdyby chtěl navázat třícestný handshake na každém portu." [6].
- Lokální skenování portů
  - Lokální skenování portů rovněž zjišťuje, jaké služby poskytuje dané síťové zařízení, avšak po přihlášení k cílovému systému metodou *netstat*.
- Hledání zranitelností operačních systémů a aplikací
  - Bez přihlášení
    - Skener v této variantě nemá přístup ke všem službám, běžícím procesům atd. V této variantě lze pouze hledat otevřené porty a služby na nich běžící. O verzi operačního systému a instalovaných záplatách OS se zpravidla nedozvíme mnoho. Téměř nic se také nedozvíme o instalovaných aplikacích a jejich verzích. Tento typ skenů se hodí pro skenování cizích systémů, ke kterým nemáme přístupové údaje.

  - S přihlášením
    - Z pohledu kompletnosti testů a relevantnosti výsledků je ideální přihlášení na účet root (administrátor). To však z mnoha jiných (provozních či bezpečnostních) důvodů nemusí být v produkční síti povoleno. Řešením může být použití oddělených rolí pro správu přihlašovacích údajů privilegovaného účtu. Zranitelnosti v OS nejlépe odhalíme tímto typem skenování.
- Skenování webových aplikací
  - Hledání zranitelností aplikací s otevřeným rozhraním do internetu. Obvyklé známé zranitelnosti jsou např. XSS (Cross-site scripting) nebo SQL Injection.
- Skenování operačního systému – shoda s auditní politikou
  - Auditní politika je v podstatě předem definovaná šablona obsahující dílčí kontroly. Každá kontrola je reprezentována krátkým kusem kódu, např. pro zjištění běžící služby OS či přítomnosti souboru indikujícího verzi SW apod.
  - Příklad kódu jedné auditní kontroly pro OS SLES v 10 [7]:

```
#
# ID108 - zapnuti systemoveho auditu
#
echo "##################### ID107 ####################"
echo ""
echo "---"
echo "Kontrola behu auditd"
echo "---"
echo ""
audit=`ps -ef |grep -w auditd |grep -v grep`
if [ -z "$audit" ]; then
    echo " Audit demon neni spusten"
else
    echo $audit
fi
echo ""
echo "---"
echo "Existuji soubory /etc/audit"
echo "---"
ls -la /etc/audit
echo ""
echo "---"
echo "Existuje log soubor /var/log/audit/audit.log"
echo "zkontrolujte prava na 600 a vlastnictvi root:root:"
echo "---"
ls -la /var/log/audit/audit.log
echo ""
```

2.6 Obecně platné standardy pro popis zranitelností

Jak již bylo uvedeno, zranitelnost je nějaké slabé místo zneužitelné útočníkem nebo škodlivým SW. V praxi se jedná např. o odhalenou chybu v kódu aplikace, či operačního systému. S neustálým vývojem SW produktů v kombinaci s lidskou nedokonalostí lze téměř s jistotou říct, že zranitelnosti vznikají dnes a denně a bude tomu tak do té doby, dokud bude nějaký vývoj probíhat. S touto skutečností vznikl na druhé straně požadavek a potřeba tyto slabiny nejen odhalovat, ale také popsat jakýmsi jednotným jazykem tak, aby bylo možno tuto obecně platnou terminologii univerzálně využít. Nespornou výhodou přesných názvů zranitelností je jejich využití např. v informačních systémech, které mají za úkol nějakým automatizovaným způsobem na zjištěné zranitelnosti reagovat.

O sjednocení názvů veřejně známých zranitelností se stará komunita CVE (Common Vulnerabilities and Exposures) sponzorovaná US-CERT (United States Computer Emergency Readiness Team). CVE komunita např. definuje formát, jak jsou zranitelnosti nazývány a popisovány, ale hlavně udržuje samotné CVE, tedy databázi veřejně známých zranitelností. Jedná se o soubor dostupný v různých formátech (CVRF, XML, HTML, CSV, TXT). Ten lze použít jako zdrojový soubor pro technologie využívající soupis zranitelností.

Aby bylo možné s jednotlivými zranitelnostmi relevantně pracovat a porovnávat je, je nutné mít také k dispozici nástroj jak závažnost zranitelností měřit. V odvětví síťové bezpečnosti pro to existuje standard, jenž umí změřit závažnost zranitelných míst systémů. Tento standard se nazývá Common Vulnerability Scoring System (CVSS, společný systém hodnocení zranitelností). Metodika CVSS je implementována do veřejně dostupného kalkulátoru, pomocí něhož lze vypočítat výsledné riziko.

Prohledávání databáze CVE je rovněž možné přes webové stránky NVD (National Vulnerability Database). V době psaní této práce je v databázi 80827 známých zranitelností.

2.7 Návaznost na zákon o kybernetické bezpečnosti (ZKB)

Od 1. 1. 2015 je účinný zákon o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) společně s vyhláškou o kybernetické bezpečnosti. (vyhláška č. 316/2014 Sb.). Tento zákon v paragrafu 3 vymezuje orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti. Dále existuje nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury. Paragraf 1 uvádí tato průřezová kritéria:

Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,
b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob. [8]

Toto nařízení má rovněž svou přílohu, kde jsou vyjmenována kritéria podle odvětví. Je zmiňována např. energetika, vodní hospodářství, zdravotnictví a mnohé další. V kategorii VI. KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY je odrážka:

E. Technologické prvky pro poštovní služby:

a) centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,
b) sběrný přepravní uzel,
c) řídící a mezinárodní pošta,
d) poštovní dopravní infrastruktura. [8]

Vyhláška č. 316/2014 Sb. v paragrafu 15 odstavci 3 zmiňuje automatizovaný nástroj pro kontrolu zranitelností systémů kritické informační infrastruktury (KII) takto: „Orgán a osoba uvedená v paragrafu 3 písm. c) a d) zákona dále pro informační systém kritické informační infrastruktury a komunikační systém kritické informační infrastruktury provádí kontrolu zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocení a reaguje na zjištěné zranitelnosti.“ [9] Použití skeneru zranitelností na systémy spadající do KII v ČP je tedy de facto přikazováno zákonným opatřením.

2.7.1 Kritická infrastruktura

„Definice kritické infrastruktury říká, že kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva. Z definice vyplývá, že úkolem společnosti je tedy kritickou infrastrukturu chránit tak, aby fungovala za běžných, mimořádných i krizových situací. Z tohoto je možno vyvodit, že ochrana kritické infrastruktury je proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování kritické infrastruktury.“ [7] Tak se vyjadřuje o kritické infrastruktuře kniha Ochrana kritické infrastruktury autorské trojice Šenovský M., Šenovský P., Adamec. Nástroj pro vyhledávání zranitelností včetně procesu odstraňování nalezených zranitelností je z tohoto pohledu jednou ze složek ochrany informační infrastruktury, v první řadě té kritické.

2.7.2 Systémy kritické informační infrastruktury v České poště

V rámci datové sítě České pošty bylo nutné definovat systémy spadající pod ZKB a tvořící kritickou informační infrastrukturu. V rámci této bakalářské práce budou právě tyto systémy prioritně zařazeny do pravidelného skenování a vyhodnocování nalezených zranitelností u jednotlivých serverů těchto informačních systémů. Jedná se obecně o rozsáhlé informační systémy, které pracují například s finančními údaji nebo citlivými daty. Pro potřeby implementace skeneru zranitelností budou systémy KII reprezentovány IP adresou nebo IP adresním rozsahem.

Česká pošta pro systémy spadající do kategorie KII zavádí vlastní termín „Informační systém základních služeb ČP“ (dále ISZS ČP). Zkratku KII a ISZS budu v této práci považovat za ekvivalent.

3 Definice požadavků a srovnání produktů

3.1 Požadavky na skener zranitelností pro implementaci do prostředí České pošty

Výběr finálně implementovaného produktu je závislý na řadě faktorů. V této kapitole shrneme klíčové vlastnosti, které od nástroje budeme očekávat.
Klíčové požadavky jsou následující:

- Plná kontrola nad HW i SW (tzv. On-Premise řešení)
- Skenování sítě na portech TCP/UDP
- Skenování zranitelností operačních systémů (Linux, Solaris, Windows)
- Kontrola OS na shodu s auditní politikou
- Možnost vytváření vlastních auditních politik
- Možnost skenování OS s přihlášením
- Oddělení rolí pro správu přístupových údajů privilegovaného účtu skeneru
- Centrální management
- Reportovací nástroj
- Skenování webových aplikací

3.2 Vybrané produkty k porovnání

Z poměrně velkého množství dostupných skenovacích nástrojů jsem vybral pět zástupců.

- NMap
- Nexpose (společnost Rapid7)
- Qualys Enterprise Suite
- Tenable SecurityCenter
- Acunetix

Pro možnost otestování produktů Nexpose, Qualys a Acunetix jsem oslovil jejich výrobce, kteří mi velmi ochotně poskytli 30denní zkušební licence na enterprise verze. NMap je zdarma a licence Tanable SecurityCenter byly v ČP k dispozici. (viz *kapitola 4.1*).

3.3 Porovnání a vyhodnocení

I když se ve všech případech jedná o produkty určené ke skenování, jejich porovnání není snadné. Při detailnějším zkoumání má každé řešení svá specifika a těžko hledat na trhu dvě stejná, která by bylo možné porovnat 1:1. V tabulce (*Tabulka 1 - Srovnání produktů*) je naznačeno, jakým způsobem jednotlivé produkty splňují zadaná kritéria.

Tabulka 1 - Srovnání produktů

	NMap	Nexpose	Qualys	Tenable	Acunetix
Verze	6.40	6.4.22	VM	SC	11
On-Premise řešení	✔	✔	✘	✔	✔
Skenování sítě na portech TCP/UDP	✔	✔	✔	✔	✘
Skenování zranitelností OS (Linux, Solaris, Windows)	✘	✔	✔	✔	✘
Kontrola OS na shodu s auditní politikou	✘	✘	✔	✔	✘
Vytváření vlastních auditních politik	✘	✘	✘	✔	✘
Možnost skenování s přihlášením	✘	✔	✔	✔	✔
Oddělení rolí pro správu přístupových údajů privilegovaného účtu skeneru	✘	✘	✔	✔	✘
Skenování webových aplikací	✘	✔	✔	✔	✔
Centrální management	✘	✘	✔	✔	✘
Reportovací nástroj	✘	✔	✔	✔	✘

3.3.1 NMap

NMap je považován za jakýsi prazáklad skenerů sítě. Jedná se o konzolovou aplikaci na platformě UNIX, která slouží ke skenování portů v síti. Její výhody jsou ve snadném ovládání, pokročilých možnostech nastavení, rychlosti a dostupnosti (bývá součástí Linuxových distribucí). Nástroj je velmi dobře využitelný pro rychlé zjištění aktiv v neznámé síti. Nejedná se o skener zranitelností, ale např. Tenable Nessus využívá NMap jako svou vestavěnou funkci.

3.3.2 Nexpose

Produkt firmy Rapid7 se snaží přiblížit komplexním řešením, která nabízí např. Tenable či Qualys. Při testování jsem ocenil snadnost instalace a poměrně intuitivní ovládání. Nexpose používá pro hledání zranitelností SW Metasploit, což ho zásadně odlišuje od ostatních skenerů. V součtu vrací nejméně výsledků (viz Tabulka *3 - Počty nalezených zranitelností při testování skenerů*). Zcela postrádá některé zásadní funkce (viz *Tabulka 1 - Srovnání produktů*). Obecně jde o levnější variantu řešení, nicméně celkem dobře použitelnou.

3.3.3 Qualys versus Tenable

Skutečné srovnání snesou produkty společnosti Qualys a Tenable. Jedná se o rozsáhlé systémy s mnoha moduly, které jsou v případě Qualys volitelné, v případě Tenable obsažené v rámci produktu SecurityCenter. Obsahují pokročilé funkce jak samotného skenování, tak reportingu a celkové správy. Ačkoliv mají rozdílný přístup počínaje grafickým rozhraním a konče způsobem licencování, vykazují obdobně pokročilé možnosti skenování a řízení zranitelností. Obecně jsou produkty Qualys a Tenable považovány za špičky na trhu v této kategorii, což potvrdily i prováděné testy v rámci této práce. Zásadní rozdíl je způsob umístění celého systému, kdy Qualys jde cestou tzv. cloudového (on-line) řešení (systém je provozován na straně výrobce) a Tenable se drží On-premise instalací (zákazník má HW i SW plně pod kontrolou). Oba způsoby jistě najdou své zastánce. V rámci ČP nejsou cloudová řešení zatím příliš preferována. (Dle dalších zjištění Qualys nabízí i tzv. privátní Cloud, ovšem za poměrně nevýhodných finančních podmínek.) Detailnější porovnání produktů Tenable a Qualys jsem v rámci možností provedl v tabulce (*Tabulka 2 - Porovnání Tenable a Qualys*). Při použití obou nástrojů jsem nacházel určité funkce či vlastnosti, které se u obou produktů určitým způsobem lišily. Na škále 1–10 (1 splňuje nejméně, 10 splňuje nejlépe) jsem se pokusil srovnat některé z nich. Jedná se o subjektivní hodnocení z uživatelského pohledu.

Tabulka 2 - Porovnání Tenable a Qualys

	Qualys	Tenable
On-Premise řešení	1	10
Skenování webových aplikací	10	7
Množství přednastavených reportů	9	10
Použitelnost přednastavených reportů	9	7
Možnosti editace šablon reportů	4	9
Modul pro skenování mobilních zařízení	ne	ano
Ovládání přes jedno okno prohlížeče	ne	ano

3.3.4 Acunetix

Pro doplnění portfolia produktů ke srovnání jsem v testovacím prostředí vyzkoušel i skener zaměřený čistě na webové aplikace. Snadná instalace i ovládání je příjemný benefit. Úzce zaměřený produkt však nesplňuje potřebné parametry k použití v tomto projektu.

3.3.5 Srovnání výsledků ze tří skenerů zranitelností

Pro otestování toho, jaké zranitelnosti jednotlivé skenery najdou či nenajdou na operačních systémech, bylo použito pět virtuálních strojů v testovacím prostředí, na něž byly naistalovány různé operační systémy v minimálních konfiguracích a bez instalace jakýchkoliv opravných balíků.

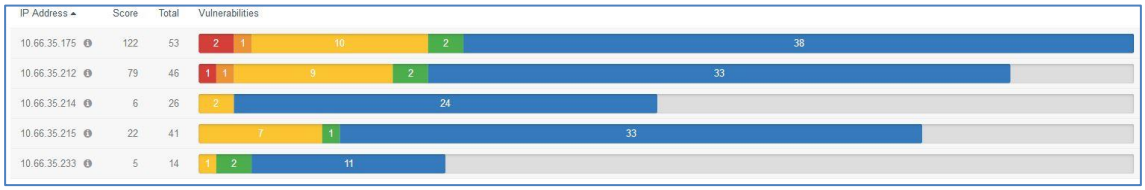
a) WindowsServer 2008 R2
b) CentOS 7
c) Windows 7 Professional
d) WindowsServer 2012 R2 Core
e) WindowsServer 2012 R2

Politiky skenování byly vybrány výchozí typu „full audit“, tedy od výrobce přednastavené, použitelné bez větších uživatelských zásahů. Skeny byly provedeny s autentizací pod účtem s plným oprávněním. Pro srovnání jsem spustil identické skeny i bez autentizace. Přehled počtů nalezených zranitelností je uveden v tabulce (*Tabulka 3 - Počty nalezených zranitelností při testování skenerů*). Z výsledků lze

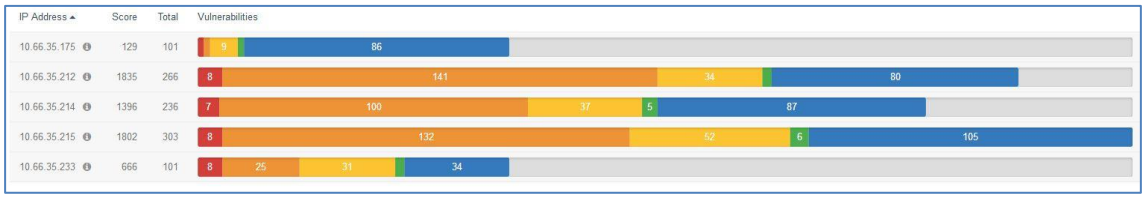
sledovat schopnosti jednotlivých produktů. Na jednotlivých platformách výsledky poměrně kolísají, ale při celkovém součtu nalezených zranitelností napříč platformami Tenable nalezl zranitelností nejvíce, velmi podobně jako Qualys. Nexpose cca o ¼ méně. Zásadní rozdíl, který jsem předpokládal, je v účinnosti skenů provedených s přihlášení, proti skenům bez přihlášení. Bez přihlášení byla nalezena zhruba desetina zranitelností, oproti skenování s přihlášením. Rozložení závažností nalezených zranitelností skenerem Nessus na pěti testovacích stanicích s přihlášením a bez přihlášení je znázorněno v grafech *Obrázek 3 - Sken bez autentizace (Tenable Nessus)* a *Obrázek 4 - Sken s autentizací (Tenable Nessus).*

Tabulka 3 - Počty nalezených zranitelností při testování skenerů

		Počty celkem nalezených zranitelností					
		Tenable		Qualys		Nexpose	
	IP adresa	s přihlášením	bez přihlášení	s přihlášením	bez přihlášení	s přihlášením	bez přihlášení
WindowsServer 2008 R2	10.66.35.212	270	31	302	29	148	9
	čas [h:m:s]	0:05:00	0:28:00	0:18:13	0:18:13	0:07:00	0:06:00
CentOS 7	10.66.35.233	101	14	113	14	131	2
	čas [h:m:s]	0:01:00	0:13:00	0:15:32	0:15:14	0:01:00	0:01:00
Windows 7 Professional	10.66.35.175	101	53	82	32	110	12
	čas [h:m:s]	0:02:00	0:02:00	0:04:55	0:04:55	0:06:00	0:05:00
WindowsServer 2012 R2 Core	10.66.35.214	236	18	276	19	162	5
	čas [h:m:s]	0:07:00	0:02:00	0:04:43	0:04:39	0:02:00	0:02:00
WindowsServer 2012 R2	10.66.35.215	303	32	233	30	221	12
	čas [h:m:s]	0:04:00	0:02:00	0:04:48	0:04:44	0:08:00	0:07:00
	suma počtu zranitelností	1011	148	1006	124	772	40
	Rozdíl výsledků skenování bez přihlášení, proti skenu s přihlášením v [%]		14,6%		12,3%		5,2%



Obrázek 3 - Sken bez autentizace (Tenable Nessus)



Obrázek 4 - Sken s autentizací (Tenable Nessus)

Legenda zjištěných zranitelností dle barev

- Kritická
- Vysoká
- Střední
- Nízká
- Informativní

3.3.6 Reportovací možnosti porovnávaných nástrojů

Samostatnou kategorií při hodnocení skenerů jsou možnosti práce s reporty. Výstupy ze skenů jsou pro řízení zranitelností klíčové. Samotné nalezení zranitelností je teprve začátek složité cesty k jejich odstranění. O výsledcích skenů je nutno vhodným způsobem informovat jednak vedoucí pracovníky a jednak administrátory daných systémů. Stejné výsledky se tedy interpretují v různé míře detailu (podrobnější report z jedné běžné stanice může vytvořit bez problému soubor ve formátu PDF o 500 stranách) různými způsoby a testované nástroje poskytovaly různou úroveň a komfort při přizpůsobování výsledných reportů. Subjektivní porovnání grafické i informační stránky reportů lze provést v přílohách (*Příloha č. 1, Příloha č. 2, Příloha č. 3*). V možnostech a snadnosti ovládání rozhraní pro tvorbu reportů z mého pohledu vychází nejlépe Tenable SecurityCenter. Na druhou stranu použitelnost již předpřipravených reportů od výrobce jsem shledal lepší u QualysGuard, kde byl bez problémů použitelný přímo výsledek skenu.

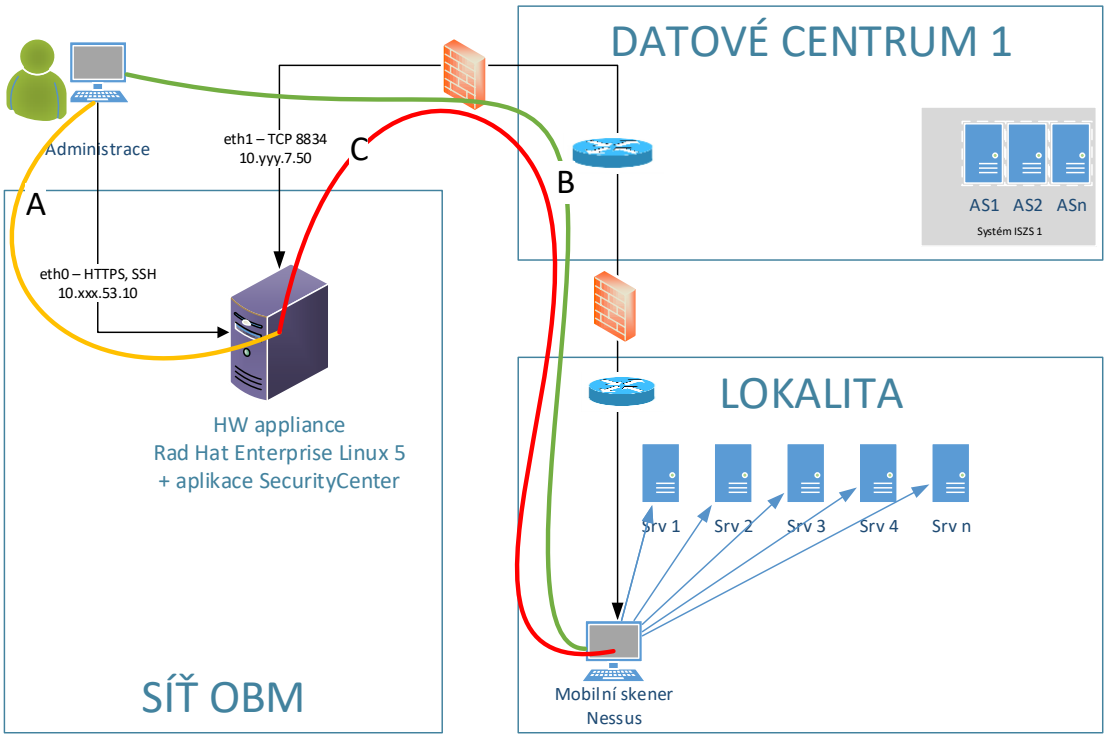
3.3.7 Závěr porovnání

Ze zjištěných výsledků a zkušeností získaných testováním pěti různých produktů lze konstatovat, že zadané požadavky splňují nejlépe produkty výrobců Qualys a Tenable. Jedním z klíčových požadavků bylo on-premise řešení a Tenable je z tohoto pohledu tedy nejlepší volbou. Pokud se koncový uživatel řešení smíří s tím, že výsostně citlivá data o zranitelnostech kritických systémů budou pravidelně (byť šifrovaně) putovat internetem na vzdálené servery zaoceánské firmy, lze doporučit obě zmíněné varianty.

4 Návrh implementace

4.1 Popis výchozího stavu

V roce 2012 byl v prostředí České pošty implementován skener zranitelností Tenable Nessus s řídící službou Tenable SecurityCenter 4 (SC4). SC4 byl nainstalován na HW platformu DELL PowerEdge R310. Administrační rozhraní bylo umístěno do sítě OBM, tedy oddělené sítě určené pro administraci systémů. Dále byl instalován tzv. „mobilní skener zranitelností Nessus“. Jedná se o skener zranitelností nainstalovaný na běžný notebook. Skener Tenable Nessus je v současné době využíván pouze pro skenování zranitelností operačních systémů a aplikací. Frekvence použití není nijak pravidelná, jedná se o vytipované kontroly v jednotlivých lokalitách. V roce 2012 byla zakoupena licence umožňující skenovat 500 IP adres, což pro potřeby příležitostného skenování lokalit dostačuje.



Obrázek 5 - Současný stav zapojení v ČP

Praktické využití skeneru probíhá tak, že do kontrolované lokality je umístěn mobilní skener, tedy notebook s instalací aplikace Tenable Nessus, případně virtuální stroj, který zastává stejnou funkci. Aby byly výsledky skenování

relevantní, je vždy nutné zajistit povolení potřebné síťové komunikace. (Základní politika síťové komunikace je v DSČP nastavena způsobem „co není povoleno, je zakázáno“.)

- Permanentně povolený přístup ke správě SC4 je znázorněn písmenem A (viz *Obrázek 5 - Současný stav zapojení v ČP*), a to ve směru ze stanice administrátora SC4 na SC4 na TCP porty 22 a 443. Kde TCP port 22 je použit pro administraci OS pomocí SSH, TCP port 443 je použit pro administraci aplikace SC4 pomocí protokolu HTTPS.
- Povolení přístupu ke správě mobilního skeneru je znázorněno jako komunikace B, je variabilní a povoluje se či zakazuje operativně pouze na základě žádosti pracovníka, který aktuální skenování provádí. Požadavek na porty je shodný s komunikací A.
- Povolení komunikace C na TCP portu 8834, na kterém naslouchá skener Nessus a komunikuje s SC4. Tato komunikace se povoluje či zakazuje operativně pouze na základě žádosti pracovníka obsluhujícího skener.

Aktuální matice povolení síťové komunikace vypadá tak, jak je uvedeno v tabulce (*Tabulka 4 - Matice pro povolení komunikace v síti*). Po dokončení skenování je nutné stejné rozsahy IP adres zakázat, resp. vrátit do původního stavu.

Tabulka 4 - Matice pro povolení komunikace v síti

Zdroj/ IP	Porty zdroje	Cíl/IP	Porty cíle
SC4/10.xxx.53.10	TCP All	Nessus/?	TCP 8834
Nessus/?	TCP All	LAN segment ?*	TCP All
Nessus/?	UDP All	LAN segment ?*	UDP All
Servis/IP administrátora	TCP All	Nessus/?	TCP 22
NTB Mobilní skener/?	TCP All	SC4/10.xxx.53.10	TCP 443

Výsledek spuštěného testu je uložen do SC4. Zjištěné zranitelnosti operačních systémů a aplikací jsou pak manuálně vyhodnoceny pracovníkem, který skenování provádí. Při zjištění konkrétní zranitelnosti je kontaktován administrátor systému

a je vyzván k nápravě. Po odstranění zranitelností (instalace opravných SW balíků, upgrade SW, atd.) je proveden kontrolní test.

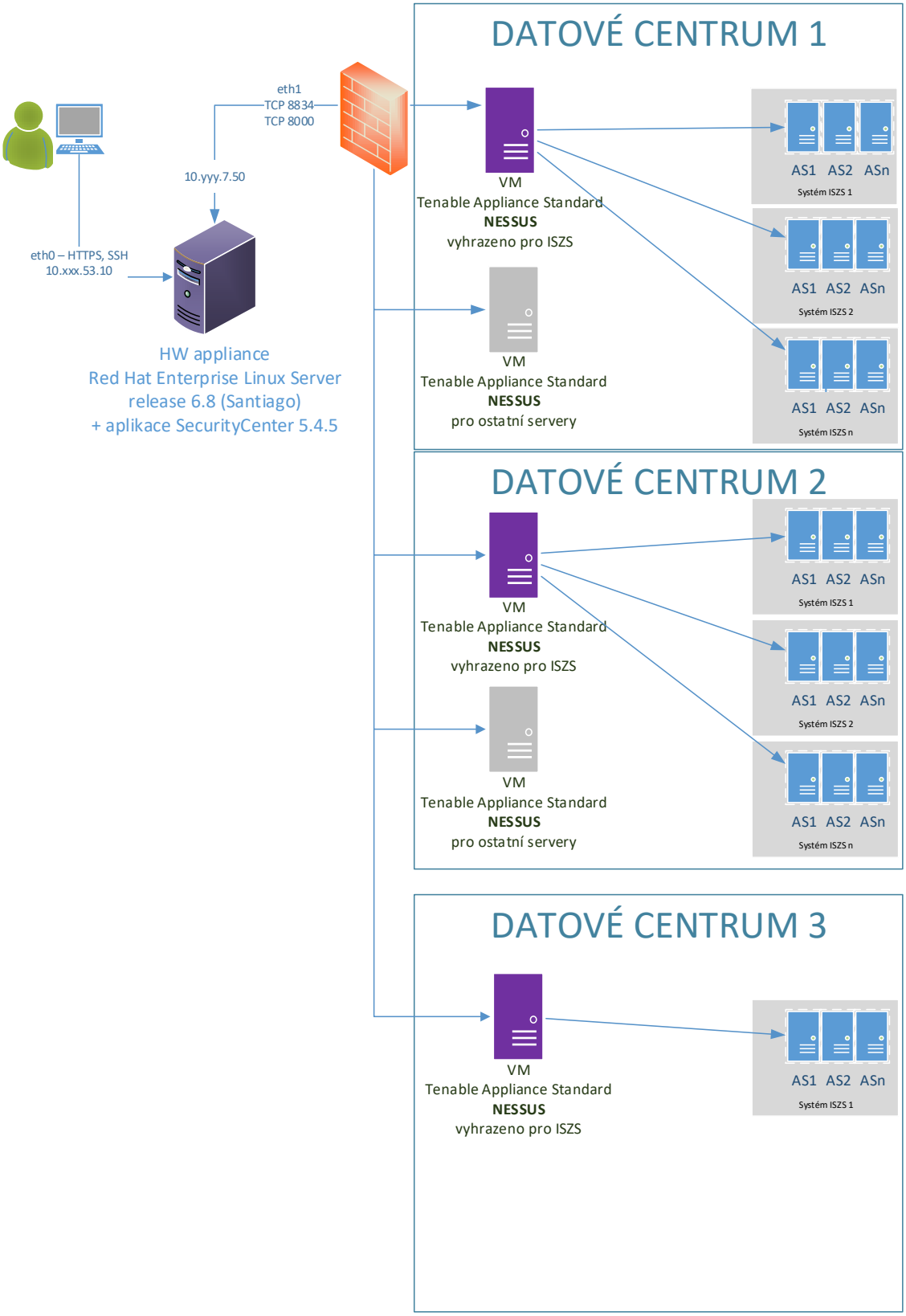
4.2 Návrh nasazení Tenable Nessus do datového centra

V roce 2016 ČP rozšířila počet licencí skeneru zranitelností Tenable Nessus o 200. Celkem je možné skenovat až 700 IP adres. Důvodem rozšíření byl záměr skenování systémů KII. Informační systémy spadající v ČP do kategorie KII, jsou umístěny celkem ve třech datových centrech České pošty. Z povahy samotné technologie skeneru zranitelností vyplývá, že mezi skenerem a skenovaným systémem by se neměly nacházet další síťové prvky jako např. firewally nebo IPS sondy. Skener by taková zařízení zbytečně zatěžoval a velmi pravděpodobně by generoval řadu falešně pozitivních událostí. Skener proto umístíme přímo do sítí v datových centrech, kde jsou provozovány servery, které plánujeme skenovat.

Pro centrální řízení skenů bude použita stávající instalace Tenable SecurityCenter (SC4). Tento server poskytuje uživatelské webové rozhraní, přes které probíhá veškeré nastavování samotného centra i koncových skenerů. Součástí mých implementačních prací bude kompletní konfigurace tohoto prostředí, tzn.:

- rekonfigurace uživatelských oprávnění a rolí
- konfigurace úložiště - *Repositories* (databáze pro ukládání výsledků skenů)
- konfigurace zón – *Scan Zones* (zóna je rozsah síťových adres, na něž může být sken aplikován)
- připojení a konfigurace nově nainstalovaných skenerů
- nastavení skenovacích politik
- nastavení pravidelného spouštění skenů
- konfigurace reportů.

Pro skenování zranitelností bude tedy v každém datovém centru instalován nejméně jeden skener zranitelností. Schéma síťového uspořádání je znázorněno na obrázku (*Obrázek 6 - Schéma návrhu implementace Tenable Nessus do DC*).



Obrázek 6 - Schéma návrhu implementace Tenable Nessus do DC

4.2.1 Možnosti instalace skeneru Tenable Nessus

Výrobce SW Tenable Nessus nabízí dvě varianty, jak skener instalovat.

- První varianta je použití vlastního operačního systému, na který je následně instalována aplikace Tenable Nessus. Jedná se o variantu pracnější, operační systém je nutno průběžně udržovat. Výhodou je plná kontrola nad OS, přístup k OS přes SSH a např. pokročilejší možnosti ladění auditních politik. Při instalaci OS je také možné nastavit vlastní velikost použitého diskového prostoru.

  Požadavky na HW:

  - CPU: 1 dual-core 2 GHz
  - Paměť: 4 GB RAM
  - Diskový prostor: 30 GB
- Druhou variantou je výrobcem dodávaná tzv. appliance. Jedná se o instalační balík (formát OVA pro vmvaare ESXi) obsahující operační systém i aplikaci. Jde o velice rychlou a snadnou instalaci. Po instalaci se provede pouze konfigurace sítě a aplikace je zprovozněna. Ovládání appliance probíhá přes webové rozhraní na portu 8000 (administrace appliance) a 8834 (aplikace Nessus) protokolem HTTPS (přístup na konzoli OS po portu 22 je uzavřen). Nevýhodou, na kterou jsme při testování narazili, je absence možnosti ovlivnit, kolik diskového prostoru si appliance alokuje. 20GB pro OS, 30GB pro data a 8GB RAM, je o něco více, než kolik je udáváno výrobcem jako minimální konfigurace HW pro skener.

  Zjištěné požadavky na HW (alokované přednastaveným inst. balíkem OVA)

  - CPU: 1 dual-core 2 GHz
  - Paměť: 8 GB RAM
  - Diskový prostor: 50 GB

Po zvážení všech pro a proti zvítězila varianta instalování skenerů jako appliance.

4.2.2 Instalované skenery

Jména a IP adresy instalovaných skenerů vycházejí ze zaběhnuté jmenné konvence používané v rámci podniku a budou následující:

- ISZS
    - sc4-cs1 - 10.xxx.244.132
    - sc4-cs2 - 10.zzz.240.68
    - sc4-cs3 - 10.yyy.5.228
- OSTATNÍ
    - sc4-cs4 - 10.xxx.244.133
    - sc4-cs5 - 10.yyy.5.229

4.2.3 Instalace a nastavení appliance Nessus Scanner

Instalace do virtuálního prostředí proběhla bez potíží. Na jednotlivých skenerech byla nastavena IP adresa, přes webové rozhraní pak proběhlo vytvoření administrátorského účtu.

Každý skener je propojen s konzolí SecurityCenter, čímž jsou mimo jiné zajištěny pravidelné aktualizace zásuvných modulů.
Na každém novém skeneru (administrace applianace) je nastaveno toto:

- Synchronizace času NTP:
    - NTP Local Reference Clock: *Off*
    - Ignore NTP Requests: *On*
    - Custom NTP server(s): (*dle umístění skeneru*)
- Přesměrování logů ze skeneru do dohledového nástroje SIEM
    - pomocí definice: *.info @*ipadresa_siem* - zajišťuje odesílání logů s prioritou *info* a vyšší ve formátu syslog do SIEM.
- Nastavení přístupu přes PROXY do internetu ze skenerů na doménu **.tenable.com* pro možnost stahování aktualizací OS appliance.
- Pravidelná kontrola aktualizací OS
    - denně ve 4:30h

4.3 Konfigurace uživatelských oprávnění a rolí

Jak jsem již naznačil v kapitole 2.5, skenování zranitelností operačních systémů na serverech v datovém centru má význam pouze v případě, že se skener může ke všem skenovaným stanicím přihlásit privilegovaným účtem (root/administrator).

Proto bude aplikace Tenable Nessus pro skenování používat účet (s oprávněním root/administrator) vytvořený na skenovaném operačním systému a tento účet bude určen pouze k účelu skenování. Aby nemohl být tento privilegovaný účet použit/zneužit pro přihlašování na koncové systémy, umožňuje SecurityCenter spravovat přístupové údaje k tomuto účtu jinou osobou, než tou, která spravuje samotný skener zranitelností. Ta se v aplikaci SecurityCenter přihlásí s rolí „*Credential Manager*“. Tato role dovoluje pouze spravovat přihlašovací údaje, jež jsou následně využity při skenování koncových systémů.

4.3.1 Účet pro sken s přihlášením – platforma UNIX

Účet určený pro skenování s přihlášením se bude jmenovat *nessus_u* (povoleno je max. 8 znaků). Přístupy jsou v ČP na platformě UNIX řízeny pomocí SUDO. Na každém serveru bude tedy v souboru */etc/sudoers* záznam:

```
nessus_u <jméno_serveru>=NOPASSWD: ALL
```

Přihlášení na účet *nessus_u* bude možné pouze pomocí SSH klíče. SSH klíč bude generován pod dohledem „čtyř očí“. (Detailněji je toto popsáno v kapitole 4.3.3.) Následně bude pomocí role *Credential Manager* importován do Tenable SecurityCenter a sdílen k použití při skenování. Soubor se soukromým klíčem bude poté smazán ze stanice, kde byl vygenerován.

4.3.2 Účet pro sken s přihlášením – platforma Windows

Pro platformu Microsoft Windows bude vytvořen účet v ActiveDirectory. Pomocí globálních politik bude tomuto účtu povoleno přihlásit se na konkrétní servery s právy lokálního administrátora. Po analýze rizik při použití takového účtu jsme rozhodli použít pro každou aplikaci/systém zvláštní účet ve jmenné konvenci *nessus_ZkratkaAplikace*. K tomu, aby mohl být jen jeden účet napříč všemi systémy v DSČP při zachování dostatečného zabezpečení, nabízí se možnost využít přihlašování pomocí Kerberos tiketů. Tato varianta však bude vyžadovat hlubší studii proveditelnosti a rozsáhlejší testování. Pokud proběhnou, tak v rámci dalšího rozvoje, nikoliv v první fázi implementace.

Aby se skener mohl ke skenovanému serveru přihlásit, je od výrobce doporučeno povolit na lokálním firewallu operačního systému porty pro SMB a WMI. Pro konkrétní nastavení portů proběhla řada testů k odladění globální politiky. Výsledná a zároveň vzorová globální politika GPO slouží k povolení prostupů ze skenerů na skenovaná aktiva, přiřazení uživatele do skupiny lokálních administrátorů atd. V textové formě je tato politika k dispozici mezi přílohami pod názvem *BICT_Nessus_ips_c.* Pro každý další systém bude zkopírováním vytvořena další ve jmenné konvenci *BICT_Nessus_ZkratkaSystému_c.*

4.3.3 Postup pro vytvoření skenovacích účtů

Pro vytvoření účtu byl navržen pracovní postup, který má zajistit to, aby účet *nessus* bylo možné použít pouze při skenování.

- Na straně Tenable SecurityCenter
  - vytvoření účtu pro pracovníka provozu centrálních systémů (PCS) s rolí „Credential Manager“
- Na straně produkčního serveru
  - vytvoření účtu „nessus“ s potřebným oprávněním
- Pod dohledem „4 očí“ pracovníků BCIT s PCS
  - vytvoření přihlašovacích údajů, 8 znaků hesla zadá odd. PCS a 8 znaků zadá odd. BICT
- Na straně Tenable SecurityCenter
  - import neveřejné části klíče do SecurityCenter pod účtem s rolí „Credential Manager“
  - sdílení přístupových údajů uživatelům SecurityCenter, kteří jsou ve skupině BICT
- Pod dohledem „4 očí“
  - smazání neveřejné části klíče ze systému, kde byl generován

Přihlášení na všechny účty používané ke skenování bude monitorováno přes dohledový nástroj SIEM.

4.3.4 Dohled účtu pro skenování přes SIEM

Úvodní prerekvizitou pro přidání každého nového systému pod skener zranitelností je zasílání logů operačního systému do centrálního SIEM. Jakkoliv by to mělo být jednou ze základních konfigurací operačních systémů, praxe ukázala, že tomu tak ve skutečnosti není. Abychom měli logy s jistotou k dispozici, je nutné u každého přidávaného aktiva toto nastavení prověřit. Na vyhodnocení logů z operačních systémů je postaveno následující pravidlo.

Pro eliminaci rizika zneužití účtu *nessus_u* bylo v dohledovém nástroji SIEM navrženo pravidlo, které koreluje událost s popisem „*accepted password*“ a uživatelské jméno „*nessus_u*“. Log s těmito parametry by z produkčních serverů dorazil pouze tehdy, pokud by proběhlo přihlášení na účet *nessus_u* pomocí hesla. Takový případ bude generovat bezpečnostní incident. Definice pravidla vypadá takto:

```
SELECT * FROM Event(
(event_desc .toLowerCase() IN ( 'accepted password' ) AND user_dst
toLowerCase() IN ( 'nessus_u' ))
```

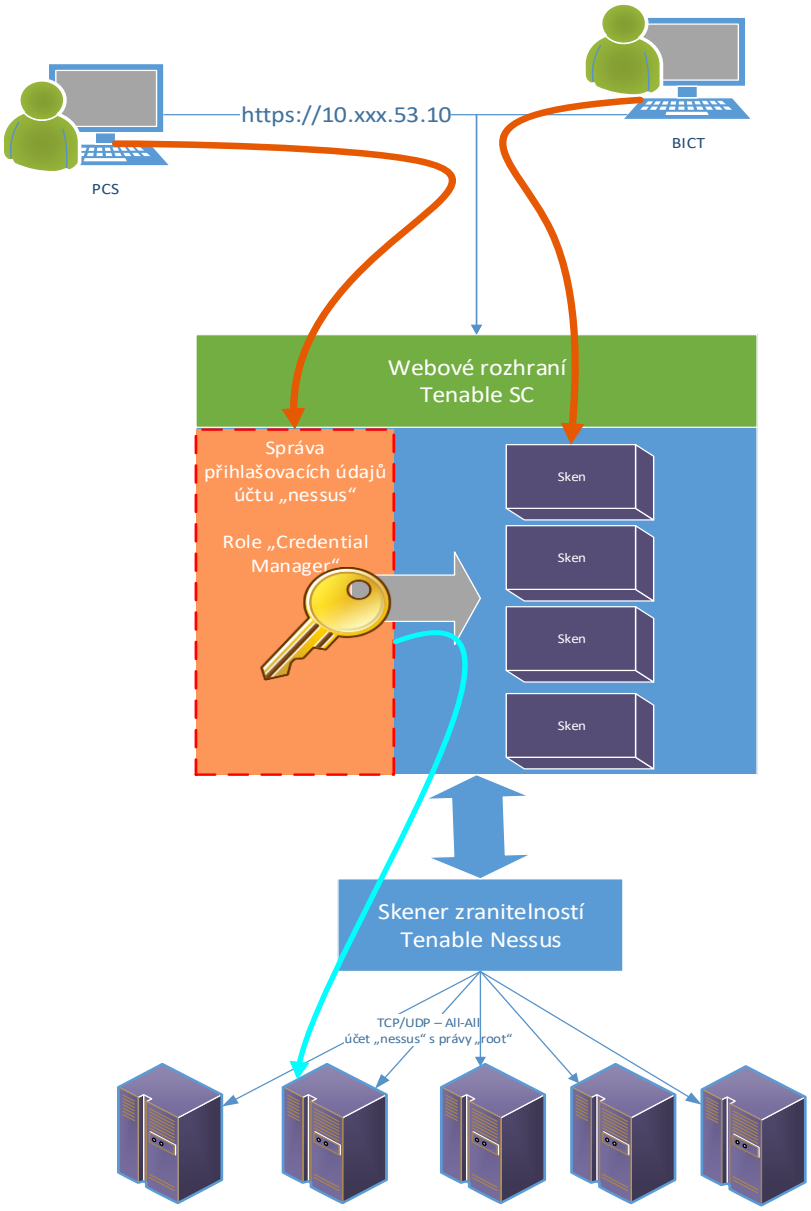
Ve standardní situaci se vyskytuje log, kde je v kombinaci s uživatelským jménem „*nessus_u*“ popis události „*Accepted publickey*“, přičemž tajný klíč je k dispozici pouze aplikaci SecurityCenter.

4.3.5 Rozdělení rolí na úrovni SecurityCenter

Rozdělení rolí bude vypadat takto:

- BICT administruje SC, spravuje lokální účty na SC
- BICT řídí a spravuje skenery, skeny a reporty ze skenů
- Pracovník odd. PCS má přidělen lokální účet do SecurityCenter
- Pracovník PCS zadává pod svým účtem v SC přihlašovací údaje k účtu „nessus“

Graficky je tento model znázorněn na obrázku (*Obrázek 7 - Použití účtu pro skenování*)



Obrázek 7 - Použití účtu pro skenování

4.4 Konfigurace úložiště skenů

Výsledky provedených skenů jsou ukládány v databázi na straně SecurityCenter. Definice těchto databází se provádí v centrální konzoli SecurityCenter v nabídce *Repositories* (Úložiště). Pro každé úložiště je nutné definovat rozsah IP adres, ze kterých bude možné výsledky skenů do úložiště uložit.

4.4.1 Úložiště v prostředí České pošty

Pro přehlednost použití nadefinujeme pro každý použitý skener vždy jedno úložiště. Jména úložišť a síťové rozsahy v úložištích akceptované budou tedy následující:

- DC_1_ISZS 10.xxx.0.0/16
- DC_1 10.xxx.0.0/16
- DC_2_ISZS 10.yyy.0.0/16
- DC_2 10.yyy.0. 0/16
- DC_3_ISZC 10.zzz.224.0/19

V případě budoucího rozvoje (např. přidání skeneru do vnějšího perimetru sítě) bude přidáno další úložiště např. s názvem:

- DMZ_1

4.5 Konfigurace skenovacích zón

Dále je nutné definovat tzv. skenovací zóny. Skenovací zónou definujeme jednotlivé podsítě, které mohou být skenovány vybraným skenerem/skenery. Pro každý informační systém budeme vytvářet oddělenou zónu.

4.5.1 Zóny v prostředí ČP

Jmenná konvence zón bude „ZKRATKA_Název_systému“.

Příklad:

- NDS_Důchodová_služba 10.xxx.79.0/24
- T&T_Tracing&Tracking 10.xxx.116.0/24,10.xxx.139.0/24

4.6 Skenovací politiky

Jádro problematiky skenování zranitelností spočívá ve správné konfiguraci skenovacích politik, respektive jejich nastavení tak, aby vyhovovaly zamýšleným cílům. Bez nich nelze očekávat relevantní výsledky skenů. Konkrétním politikám se budu věnovat v této kapitole.

Skenovací politika je v případě Tenable Nessus reprezentována textovým souborem ve formátu XML, kde jsou jednotlivé volby v převážné většině nastavitelné do hodnot „yes“ / „no“, případně „endabled“ / „disabled“. Příklad zápisu jedné volby:

```
<preference>
        <name>stop_scan_on_disconnect</name>
        <value>yes</value>
</preference>
```

Některé položky očekávají číselný vstup, např. výčet skenovaných portů. Pro uživatele je k dispozici grafické rozhraní, které nabízí poněkud přehlednější správu tohoto souboru, jenž má více než 1000 řádků. Jednotlivé volby jsou převedeny na grafická tlačítka. Ani jedna z těchto variant nemá takovou vypovídající hodnotu, aby vhodně a přehledně ukázala rozdíly jednotlivých politik, proto jsem zvolil formát tabulkový. Každá volba bude reprezentována originálním textem z grafického rozhraní, originálním popisem volby z manuálu výrobce, jeho českým překladem a polem s nastavenou hodnotou. Výsledné politiky budou vytištěny v přílohách a jejich PDF verze uloženy na přiloženém CD.

Účelem sady čtyř politik, které jsem navrhl, je získat přehled o síti, v níž je systém provozován, ověření správné autentizace skeneru a možnosti auditovat stav zranitelnosti operačního systému.

4.6.1 PING sken sítě pro objevení nových IP adres

Název politiky: PING_sken

První politika, kterou jsem připravil ke spuštění, je tzv. „Discovery scan“ nebo také „Ping scan“. Jde o sken, kdy se programem PING (anglicky **P**acket **I**nter**N**et **G**roper) dotazují IP adresy v síti a čeká se, zda z nich přijde odpověď. Tento typ skenu je

spouštěn pouze na vyžádání v případě, že je potřeba zjistit, jaká zařízení se nacházejí v dané síti. Typická situace využití této politiky nastává při úvodním napojení konkrétních systémů na skener zranitelností (viz *kapitola 4.7*) pro ověření běžících aktiv v dané síti. Jedná se o základní sken sítě, který se dá též vykonat pomocí aplikace NMap, jak již bylo zmíněno v kapitole 3.3.1. Tento sken by měl být rychlý, ale zároveň spolehlivý. Nebude využívat žádné zásuvné moduly a ze základních funkcí bude využívat PING s metodami ARP, TCP a ICMP.

4.6.2 AUTH sken pro ověření autentizace skeneru

Název politiky: AUTH_sken

Abychom si byli jisti, že se skener dokázal správně autentizovat a mohl pak přistoupit na dané aktivum s dostatečným oprávněním, je dobré toto nějakým způsobem (lépe více způsoby) ověřit. Jako základní kontrola mohou sloužit logy z operačního systému zachycené v dohledovém nástroji SIEM. Zde však poznáme pouze úspěšné či neúspěšné přihlášení, nikoliv zda kontroly proběhly s oprávněním administrátora. Od výrobce Tenable existuje několik zásuvných modulů (pluginů), které poměrně přehledně sdělí, do jaké míry se autentizace podařila, a zda sken proběhl s dostatečnými právy. Vytvoříme proto speciální politiku, jež bude všechny tyto kontroly obsahovat.

Výčet použitých zásuvných modulů:

Skupina zásuvných modulů: Settings

ID	Název zásuvného modulu
12634	Authenticated Check : OS Name and Installed Package Enumeration
21745	Authentication Failure - Local Checks Not Run
19506	Nessus Scan Information
24786	Nessus Windows Scan Not Performed with Admin Privileges

Skupina zásuvných modulů: Windows

ID	Název zásuvného modulu
10394	Microsoft Windows SMB Log In Possible
26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
10428	Microsoft Windows SMB Registry Not Fully Accessible Detection

Skupina zásuvných modulů: Windows : User management

ID	Název zásuvného modulu
10910	Microsoft Windows Local User Information

Dobrá kontrola na to, zda se skeneru podařilo přihlásit, je také zapnutí funkce port-skenu. Pokud proběhne lokálně (pomocí WMI netstat nebo SSH netsat), indikuje to úspěšné přihlášení do OS. Zapnutí volby „*Only run network port scanners if local port enumeration failed*“ zajistí, že se síťový port-sken spustí jen tehdy, pokud se nepodaří vyčíst stav portů lokálně. Síťový port-sken bude v této politice orientován na rychlost a šetrnost. Použil jsem tedy metodu SYN (poloviční TCP handshake) na prvních 100 portů, což je rychlé a zároveň plně vypovídající.

4.6.3 PATCH AUDIT sken operačních systémů

Název politiky: PATCH_AUDIT_sken

Tato politika vychází z předpokladu, že známe konkrétní seznam aktiv (aktiva jsou reprezentována IP adresou), na která budeme směrovat sken s touto politikou. Dále předpokládáme, že se na skenované aktivum podařilo úspěšně přihlásit s dostatečným oprávněním, a tím pádem mohou správně proběhnout všechny kontroly. V záložce nastavení zásuvných modulů (Plugins) budou zapnuty všechny moduly ze všech skupin, které jsou k dispozici. Nessus v první řadě zjišťuje, o jaký operační systém se jedná, a následně používá jen relevantní kontroly pro zjištěný systém.

4.6.4 PORT sken

Název politiky: PORT_sken

Z mnoha důvodů nás může zajímat, jaké porty jsou na konkrétním aktivu otevřené pro přístup „z venku“, tedy nikoliv metodou *netstat* po přihlášení do OS. Půjde tedy o sken, který nebude využívat přihlašovací údaje. Ačkoliv na skenovaném aktivu mohou být porty otevřené, existuje mnoho dalších možností (firewally síťové, firewally v OS), které mohou ve skutečnosti tytéž porty blokovat. Tímto skenem lze zjistit skutečný stav dostupných otevřených portů.

4.7 Postup při napojení produkčního systému

Pro napojení produkčního systému na skenování zranitelností je třeba provést následující kroky v uvedeném pořadí. Platformy UNIX a Windows se drobně liší.

4.7.1 platforma UNIX

- Zjištění počtu produkčních a testovacích serverů systému a jejich IP adres
- Zjištění segmentace sítě, ve které je systém umístěn
- Spuštění PING skenu na síť x.x.x.0/x, ve které se systém nachází
- Porovnání výsledků PING skenu s prvním bodem a vyrovnání nesrovnalostí
- Zajištění síťových prostupů mezi skenerem a skenovanou sítí
- Ověření, zda jsou logy OS odesílány do SIEM
- Na základě IP adres určení skeneru a úložiště
- Vytvoření nové skenovací zóny v SecurityCenter
- Vytvoření účtu *nesssus_u* na všech serverech systému
- Spuštění AUTH skenu a ověření výsledků
- Definování časových oken pro pravidelné skenování na produkčních serverech
- Spuštění PATCH AUDIT skenu na testovacích serverech
- Spuštění PATCH AUDIT skenu na produkční servery v časovém okně
- Po prvním spuštění vyhodnocení výsledků
- Nastavení pravidelného spouštění skenu

4.7.2 platforma Windows

1. Zjištění počtu produkčních a testovacích serverů systému a jejich IP adres
2. Zjištění segmentace sítě, ve které je systém umístěn
3. Spuštění PING skenu na síť x.x.x.0/x, ve které se systém nachází
4. Porovnání výsledků PING skenu s prvním bodem a vyrovnání nesrovnalostí
5. Zajištění síťových prostupů mezi skenerem a skenovanou sítí
6. Ověření, zda jsou logy OS odesílány do SIEM
7. Na základě IP adres určení skeneru a úložiště
8. Vytvoření nové skenovací zóny v SecurityCenter
9. Vytvoření účtu *nesssus_ZkratkaAplikace* v Active Directory
10. Implementace GPO politiky na testovací servery skenovaného systému
11. Spuštění AUTH skenu – ověření, že jsou politiky GPO plně funkční
12. Definování časových oken pro pravidelné skenování na produkčních serverech
13. Implementace GPO politiky na produkční servery skenovaného systému
14. Spuštění PATCH AUDIT skenu na testovacích serverech
15. Spuštění PATCH AUDIT skenu na produkční servery v časovém okně
16. Po prvním spuštění vyhodnocení výsledků
17. Nastavení pravidelného spouštění skenu

5 Implementace a testování

5.1 Popis mé role při implementaci

Celý proces implementace probíhal prakticky ve tříčlenném týmu. Projektový manažer nebyl na tento úkol vyčleněn, tudíž jedna z podstatných rolí, kterou jsem pod vedením svých nadřízených zastával, byla právě tato. Projektové řízení obnášelo veškeré organizační záležitosti pro zajištění dostatečné komunikace mezi všemi zúčastněnými organizačními jednotkami, koordinaci dílčích činností a hlídání termínů. Mí dva týmoví kolegové mi byli nápomocni nejvíce ve dvou oblastech. První kolega odvedl velký kus práce při tvorbě a otestování GPO politiky pro platformu Windows, bez níž by nebylo možné zajistit přihlašování skeneru na servery s OS Windows. Druhý kolega zajišťoval část testovacích prací a převážnou část exekutivní činnosti, tedy komunikaci s administrátory systémů pro získání všech potřebných podkladů (ověření seznamu serverů, distribuci uživatelského účtu atd.). Mou rolí pak byla koordinace všech kroků, administrace samotné aplikace SecurityCenter včetně skenerů Nessus, návrh implementace a skenovacích politik, testování a rutinní nasazení skenovacích politik, stejně tak příprava a testování šablon reportů.

V přípravné fázi jsme strávili několik týdnů testováním technologie ve vlastním testovacím prostředí (VMWare), kde jsme se dostatečně seznámili s možnostmi zvolené technologie. V rámci příprav jsem také provedl otestování a porovnání konkurenčních produktů (viz *kapitola 3*).

5.2 Vznik návrhu implementace a skenovacích politik

Následně jsem zkompletoval strategii rozmístění a použití skenerů v datových centrech. Do každého datového centra jsem navrhl umístit jeden skener pro systémy ISZS a druhý pro ostatní systémy (pokud v DC jiné systémy jsou) viz *kapitola 4.2*. Politiky, které jsem připravil a popsal v *kapitole 4.6,* jsou kompletní sadou použitelnou nezávisle na platformách. Účelem bylo připravit vše tak, aby bylo kdykoliv jednoduše zjistitelné, zda se skener dokáže správně autentizovat na skenovaný operační systém. K tomuto účelu slouží jedna z politik (AUT sken) a ta

je zároveň klíčová při napojení skeneru na nový systém. Díky výsledkům z „AUTH skenu“ si totiž snadno ověříme, že přihlašovací údaje byly nastaveny správně, že přihlašovací metody procházejí bezchybně, a že tím pádem má skener možnost spolehlivě zkontrolovat všechny zranitelnosti skenovaného operačního systému.

5.3 Průběh implementace

Po provedených přípravách bylo mým úkolem kontaktovat oddělení Enterprise architektury (EA). Od EA bylo nutné získat standardní zpracování softwarové architektury na základě našich podkladů tak, abychom zpět obdrželi instalační formuláře. S instalačními formuláři jsem mohl pokračovat na oddělení Provozu centrálních systémů (PCS). Na základě instalačních formulářů byla provedena instalace skenerů na virtuální servery.

Jakmile jsem měl k dispozici čisté instalace skenerů, provedl jsem jejich konfiguraci, napojil je na SecurityCenter, dále přes PROXY do internetu pro stahování aktualizací a zároveň také na SIEM kvůli sběru systémových logů. Další konfigurace (přípravu úložišť a skenovacích zón, tvorbu politik a reportů) jsem prováděl již na úrovni SecurityCenter.

Aby bylo možné rutinně připojovat různé systémy (primárně spadající pod ZKB) na skener zranitelností, bylo mým cílem vzorové napojení jednoho systému z platformy UNIX a jednoho z platformy Windows. Tím jsem zároveň prověřil, že mnou navržené postupy jsou zcela funkční.

Ve spolupráci s administrátorem odd. PCS jsem vytvořil uživatelské účty pro skenování a vložil přihlašovací údaje do SecurityCenter. Na konkrétních dvou systémech jsem prošel celý proces napojení až po nastavení pravidelných kontrol a vyladění finálních reportů. Součástí postupu pro napojení jsou testovací skeny. Reporty z těchto skenů jsou k dispozici mezi přílohami této práce.

Nezanedbatelnou část práce zabralo odladění GPO politik pro OS Windows. GPO upravují nastavení firewallu na OS, definují umístění uživatele do skupiny atd.

Ve výsledku se implementačnímu týmu ve spolupráci s odd. PCS podařilo vytvořit GPO politiku (viz příloha GPO *BICT_Nessus_ips_c*), která povoluje jen to nejnutnější a nevytváří zbytečné prostupy, jež by samotné zabezpečení Windows serveru naopak snižovaly.

5.4 Testování

Testování probíhalo v podstatě kontinuálně ve všech fázích projektu. V úvodní fázi bylo zaměřeno na samotnou instalaci Nessus skeneru a obsluhu SecurityCenter. Následovalo testování navržených skenovacích politik a způsobu použití přihlašovacích metod skeneru k OS a s tím souvisejících GPO politik pro Windows, podobně jako nastavení SUDO v UNIX systémech.

Nejvíce testů proběhlo v oblasti přihlašování skeneru ke skenovaným operačním systémům. K testování jsem používal již vytvořenou skenovací politiku „AUTH sken“ z jejíchž výsledků bylo zřetelné, zda se skeneru podařilo dostat do operačního systému se správným oprávněním. Důvodů, proč se tak nemusí stát, je dlouhá řada. Kladné výsledky testů v testovacím prostředí nám nijak nezaručily, že stejných výsledků dosáhneme v prostředí produkčním. To ovlivňují různé další omezující faktory (firewally, access listy na síťových prvcích apod.) a je tedy znovu zapotřebí analyzovat a zajišťovat opatření pro hladký chod skeneru.

Samotný skener je však ze své podstaty velkým pomocníkem při odhalování důvodů neúspěšných stavů. Dokáže kupříkladu testovat a reportovat seznam otevřených portů na cílovém aktivu, což jsme s výhodou používali pomocí naší skenovací politiky „PORT sken“.

5.5 Časový rozvrh implementace

Časový odhad implementace počítal s obdobím 01-04/2017. Reálně jsme se do cílového stavu dobrali s cca měsíčním zpožděním, což je vzhledem k rozsahu prací a velikosti organizační struktury podniku přijatelný skluz. Reálný časový rozvrh pak vypadal zhruba takto:

- Příprava, testování a seznámení s produktem 11/2016-01/2017
- Návrh implementace 01/2017
- Příprava a testování skenovacích politik 02/2017
- SW architektura + instalace skenerů 02/2017
- Konfigurace skenerů, příprava uživatelských účtů „nessus“ 03/2017
- Ladění GPO politik a přihlášení přes SUDO pro účet „neesus“ 04/2017
- Vzorové napojení prvních dvou produkčních systémů ISZS 04-05/2017
- Rutinní připojení dalších systémů ISZS 05-06/2017

5.6 Kalendářní plán skenů

V době dokončení této práce jsou pravidelně skenovány dva informační systémy, jeden (PPS) běžící na platformě UNIX (umístěn ve dvou DC), druhý (IPS) běžící na platformě Windows. Od administrátorů byla zjištěna časová okna, kdy je možné systémy skenovat, aniž by docházelo k nevhodné zátěži produkčního prostředí. Časový plán testů tedy vypadá takto:

Tabulka 5 - Kalendářní plán skenů

Jméno skenu	Politika	Čas startu	Kalendářní plán
IPS	PATCH_AUDIT_sken	Apr 29, 2017 23:00	Every week on Sat at 23:00 +02:00
PPS_1	PATCH_AUDIT_sken	Apr 30, 2017 03:00	Every week on Sun at 03:00 +02:00
PPS_2	PATCH_AUDIT_sken	Apr 30, 2017 03:00	Every week on Sun at 03:00 +02:00

5.7 Nalezené zranitelnosti

První ostrý sken proběhl v nočních hodinách posledního dubnového víkendu. Skenery pracovaly bezchybně a skeny proběhly tak, jak bylo očekáváno. Výsledky úvodních skenů na prvních dvou produkčních informačních systémech ukázaly poměrně zásadní nedostatky, zvláště v UNIX prostředí. Valnou většinu kritických zranitelností představovala verze operačního systému (Solaris 10). Dle dostupných informací paralelně běží projekt migrace operačních systémů na podporované verze. Tím pádem by se tento trend měl velice brzy na výsledcích projevit a po upgrade OS by mělo zranitelností výrazně ubývat. Nicméně úvodní report lze uvést jako exemplární odstrašující příklad kriticky zranitelného informačního systému.

Souhrn

Tento report ukazuje výsledku skenu zranitelností na níže uvedených aktivech. Jednalo se o tzv. PATCH_AUDIT sken operačního systému.

Cílem takového skenu je zjištění, které opravné balíky na daném aktivu chybí. Tento report vypisuje chybějící patche se závažností CRITICAL a HIGH.

Přehled zranitelností na skenovaných aktivech

Critical	222	14.56%
High	476	31.21%
Medium	289	18.95%
Low	68	4.46%
Info	470	30.82%

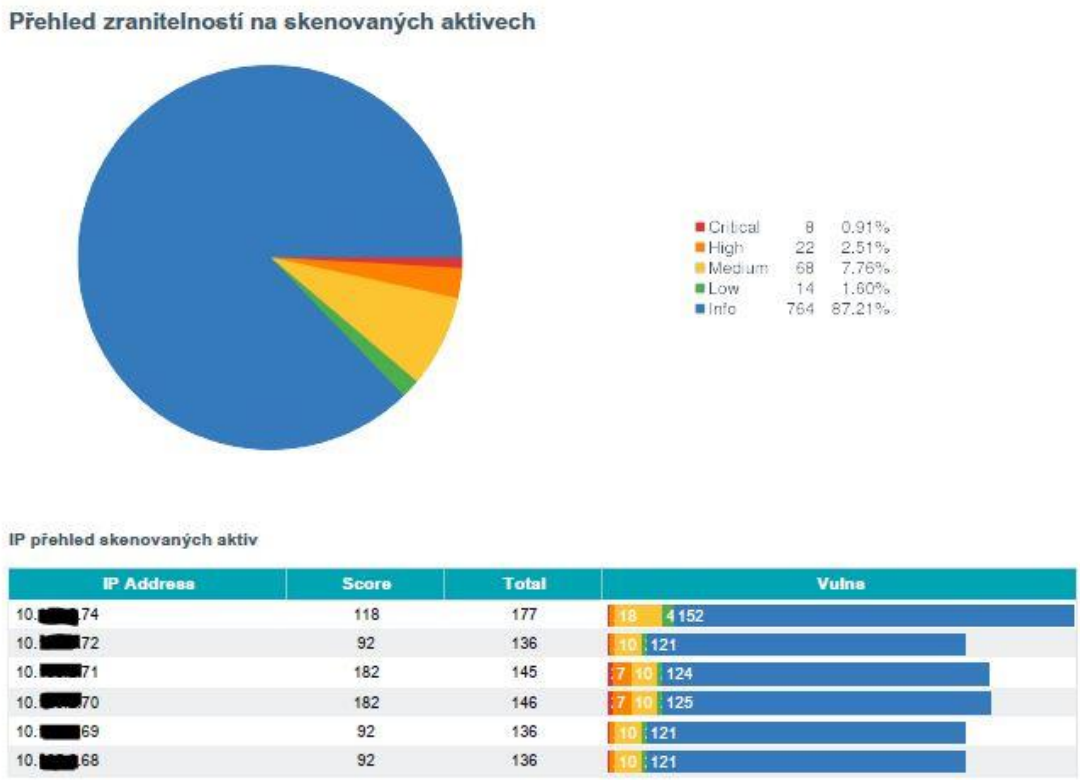
IP přehled skenovaných aktiv

IP Address	Score	Total	Vulns
10.[redacted]91	1745	174	26 58 39 8 43
10.[redacted]80	843	104	15 21 10 55
10.[redacted].76	1745	174	26 58 39 8 43
10.[redacted].49	843	106	15 21 10 57
10.[redacted].48	843	106	15 21 10 57
10.[redacted].36	1745	174	26 58 39 8 43
10.[redacted].35	1867	191	27 65 43 8 48
10.[redacted].31	1648	166	24 58 33 9 42
10.[redacted].21	1648	166	24 58 33 9 42
10.[redacted].19	1648	164	24 58 33 9 40

Obrázek 8 - Výsledek skenu z produkčního ISZS systému na platformě UNIX

Souhrnné výsledky těchto skenů jsou k nahlédnutí ve formě screenshotů z výsledných repotů. (*Obrázek 8 - Výsledek skenu z produkčního ISZS systému na platformě UNIX* a *Obrázek 9 - Výsledek skenu z produkčního ISZS systému na platformě W*)

Vzhledem k tomu, že se jedná o produkční systémy, IP adresy jsou z bezpečnostních důvodů maskovány. U systému v UNIX prostředí dosahují zranitelnosti v kategorii kritické a vysoké téměř 50% ze všech nalezených zranitelností, což je velmi vysoké číslo. U systému provozovaného v prostředí Windows jde o 3,5%.



Obrázek 9 - Výsledek skenu z produkčního ISZS systému na platformě Windows

6 Závěr

Implementaci skeneru zranitelností do datových center se podařilo v řádném termínu dostat do fáze, kdy jsou důkladně popsány veškeré potřebné pracovní postupy, jsou vytvořeny potřebné politiky a šablony reportů a minimálně dva vzorové systémy jsou pravidelně skenovány. Tím je vše připraveno k tomu, aby mohlo následovat napojování libovolného počtu dalších informačních systémů bez větších potíží. Z prvních výsledků testů produkčních systémů je zřetelné, že počty nalezených zranitelností nejsou zanedbatelné a nasazení skeneru není pouze formalita.

Návrh implementace byl akceptován všemi zúčastněnými organizačními jednotkami a postupně realizován. Za klíčovou podmínku úspěšné realizace bych označil podporu ze strany vedoucího pracovníka oddělení PCS (Provoz centrálních systémů). Pokud by z této pozice neexistovala aktivní součinnost, tlak na podřízené administrátory a souznění s celým projektem, troufám si tvrdit, že by za takových okolností byl tento projekt v podniku velikosti ČP nerealizovatelný.

Po technické stránce samotná instalace skenerů probíhala bez větších komplikací. Potíže, které bylo nutno velice intenzivně řešit, se nakumulovaly až ve finální fázi. To, aby se skener skutečně dokázal na konkrétní produkční server přihlásit s plnými právy, se ukázalo jako ne zcela triviální úkol a následně to obnášelo řadu ověřování nastavení jak na síťové úrovni, tak na úrovni operačních systémů. Samotné SecurityCenter nabízí mnoho kombinací, jak tuto funkci použít, ale větší detail bohužel není v dokumentaci k produktu příliš zachycen, ačkoliv jinak samotná dokumentace od Tenable patří k těm povedenějším.

Po odhalení a vyřešení těchto drobností je skener funkční tak, jak bylo navrženo a požadováno. Směr, kterým se bude vyvíjet rozvoj skenování, bude zařazení tzv. „COMPLIANCE SKEN“. To však obnáší přípravu auditních politik pro jednotlivé operační systémy a poměrně rozsáhlé testování.

Nyní zbývá to poslední – přijmout taková opatření, aby byly nalezené zranitelnosti v co nejkratší možné době odstraněny.

Bibliografie

[1] **POŽÁR, Josef.** *Informační bezpečnost.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 8086898385.
[2] **Ing.Prof., MOLNÁR Zdeněk.** *Podnikové informační systémy.* Praha : České vysoké učení technické v Praze, 2009. 9788001043806.
[3] **pplk. prof. Ing. David VALIŠ, Ph.D. et Ph.D.** *Hodnocení rizika.* místo neznámé : Skripta k předmětu HRI ve formátu PDF, 2016.
[4] **ČERMÁK, Miroslav.** *Řízení informačních rizik v praxi.* místo neznámé : Tribun EU, 2009. 978-80-7399-731-1.
[5] —. CLEVER AND SMART. *www.cleverandsmart.cz.* [Online] 18. 1. 2016. [Citace: 28. 12. 2016.] http://www.cleverandsmart.cz/audit-proverka-konfigurace-skenovani-zranitelnosti-penetracni-test-a-analyza-rizik/.
[6] **ROUSE, Margaret.** TechTarget Searchnetworking. *TechTarget.* [Online] TechTarget, 2000-2017. [Citace: 7. 4. 2017.] http://searchnetworking.techtarget.com/definition/SYN-scanning.
[7] **VOBRUBA, Tomáš.** *auditni script pro politiku Linuxu SLES a SUSE/OpenSUSE.* [textový soubor] Praha : Cleverlance, 2016.
[8] **NEČAS, Petr.** nařízení vlády č. 432/2010 Sb. *Zákony pro lidi.* [Online] AION CS, s.r.o., 2010. [Citace: 15. 04 2017.] https://www.zakonyprolidi.cz/cs/2010-432.
[9] **NBU.** Vyhláška č. 316/2014 Sb. *Zákon pro lidi.* [Online] AION CS, s.r.o., 2014. [Citace: 15. 4. 2017.] https://www.zakonyprolidi.cz/cs/2014-316.
[10] **ŠENOVSKÝ, M., ADAMEC, V. a ŠENOVSKÝ, P.** *Ochrana kritické infrastruktury.* Ostrava : Edice SPBI Spektrum, 2007. 978-80-7385-025-8.
[11] **Ministerstvo vnitra.** *Sbírka zákonů 2014.* Praha : Tiskárna Ministerstva vnitra, 2014. ISSN 1211-1244.

Seznam obrázků

Přílohy

Příloha č. 1.

Porovnání výsledků a reportů skenů

Skenovaný operační systém: a) Windows Server 2008 R2

Stav operačního systému: bez aktualizací

Použité skenery:

a) Tenable Nessus – sken s autentizací
b) QualysGuard – sken s autentizací
c) QualysGuard – sken bez autentizace
d) Nexpose – sken s autentizací

SecurityCenter™

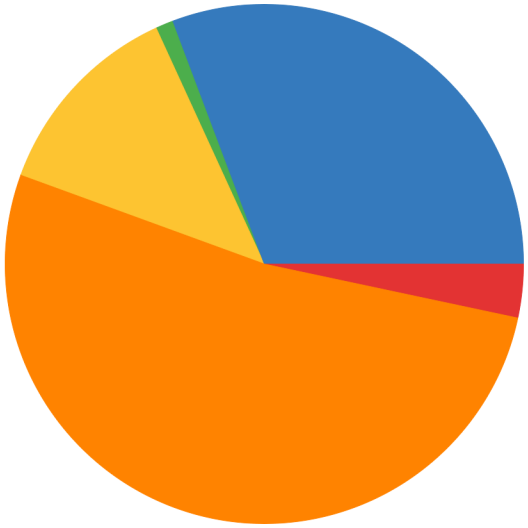
Win_2008_auth_10.66.35.212

March 9, 2017 at 10:43am CET

Michal Miklánek [mimiu]
CESKA POSTA S. P.

Souhrn

Přehled závažnosti všech zranitelností



Critical	9	3.33%
High	141	52.22%
Medium	34	12.59%
Low	3	1.11%
Info	83	30.74%

IP přehled

IP Address	DNS Name	Score	Total	Vulns
10.66.35.212	42ghj2js.ad.cpost.cz	1875	270	9 141 34 83

Přehled portů

Port	Info	Low	Med.	High	Crit.	Total
0	30	0	0	0	0	30
123	2	0	0	0	0	2
135	3	0	0	0	0	3
137	2	0	0	0	0	2
138	2	0	0	0	0	2
445	27	1	26	140	8	202
3389	10	2	8	1	1	22
5355	2	0	0	0	0	2
49152	1	0	0	0	0	1
49153	1	0	0	0	0	1
49154	1	0	0	0	0	1
49155	1	0	0	0	0	1
49156	1	0	0	0	0	1

Zranitelnosti - výčet

10.66.35.212

IP Address: 10.66.35.212
NetBIOS Name: WIN-5JUHIB97UQI\WIN-5JUHIB97UQI
DNS Name: 42ghj2js.ad.cpost.cz
OS CPE: cpe:/o:microsoft:windows_server_2008:r2:gold
MAC Address: 00:0c:29:eb:a2:df
Score: 1881
Repository: Test polygon BICT Olsanska

Počty zranitelností dle závažnosti

Severity	Count
Critical	9
High	141
Medium	34
Low	3
Info	83

Výpis zranitelností závažnosti: Critical, High

Plugin	Plugin Name	Severity
22024	Microsoft Internet Explorer Unsupported Version Detection	Critical
26921	Windows Service Pack Out-of-Date	Critical
44422	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Critical
48291	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical
53377	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical
56736	MS11-083: Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)	Critical
61529	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical
63419	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Critical
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Critical
42110	MS09-054: Cumulative Security Update for Internet Explorer (974455)	High
42115	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467)	High
43064	MS09-072: Cumulative Security Update for Internet Explorer (976325)	High
43865	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)	High
44110	MS10-002: Cumulative Security Update for Internet Explorer (978207)	High
44416	MS10-006: Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)	High
44423	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)	High
45378	MS10-018: Cumulative Security Update for Internet Explorer (980182)	High
45506	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution (981210)	High
45507	MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	High
45509	MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)	High
46312	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)	High
46839	MS10-032: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)	High
46840	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)	High
46842	MS10-035: Cumulative Security Update for Internet Explorer (982381)	High
47711	MS10-043: Vulnerability in Canonical Display Driver Could Allow Remote Code Execution (2032276)	High
47750	MS KB2286198: Windows Shell Shortcut Icon Parsing Arbitrary Code Execution	High
48216	MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)	High
48284	MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	High
48285	MS10-048: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	High

Plugin	Plugin Name	Severity
48286	MS10-049: Vulnerabilities in SChannel could allow Remote Code Execution (980436)	High
48288	MS10-051: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)	High
48290	MS10-053: Cumulative Security Update for Internet Explorer (2183461)	High
48295	MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)	High
48296	MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799)	High
48297	MS10-060: Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)	High
48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution	High
49219	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)	High
49948	MS10-071: Cumulative Security Update for Internet Explorer (2360131)	High
49950	MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)	High
49951	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)	High
49953	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)	High
49958	MS10-081: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)	High
49960	MS10-083: Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)	High
49962	MS10-085: Vulnerability in SChannel Could Allow Denial of Service (2207566)	High
51162	MS10-090: Cumulative Security Update for Internet Explorer (2416400)	High
51163	MS10-091: Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199)	High
51164	MS10-092: Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)	High
51167	MS10-095: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)	High
51168	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)	High
51170	MS10-098: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	High
51172	MS10-100: Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)	High
51455	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)	High
51587	MS KB2488013: Internet Explorer CSS Import Rule Processing Arbitrary Code Execution	High
51903	MS11-003: Cumulative Security Update for Internet Explorer (2482017)	High
51907	MS11-007: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)	High
51911	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)	High
51912	MS11-012: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)	High

Plugin	Plugin Name	Severity
51913	MS11-013: Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)	High
52585	MS11-017: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (2508062)	High
53375	MS11-018: Cumulative Security Update for Internet Explorer (2497640)	High
53376	MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)	High
53381	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)	High
53385	MS11-028: Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015)	High
53387	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)	High
53389	MS11-032: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618)	High
53391	MS11-034: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)	High
55118	MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490)	High
55119	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)	High
55121	MS11-041: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)	High
55122	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512)	High
55123	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution (2536276)	High
55124	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)	High
55126	MS11-046: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665)	High
55128	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275)	High
55130	MS11-050: Cumulative Security Update for Internet Explorer (2530548)	High
55132	MS11-052: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521)	High
55286	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275) (remote check)	High
55570	MS11-054: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)	High
55787	MS11-057: Critical Cumulative Security Update for Internet Explorer (2559049)	High
55793	MS11-063: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)	High
55794	MS11-064: Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)	High
55798	MS11-068: Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)	High
56174	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)	High
56449	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)	High
56451	MS11-077: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)	High

Plugin	Plugin Name	Severity
56452	MS11-078: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)	High
56455	MS11-081: Critical Cumulative Security Update for Internet Explorer (2586448)	High
56737	MS11-084: Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)	High
56738	MS11-085: Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)	High
56824	MS KB2506014: Update for the Windows Operating System Loader	High
57273	MS11-087: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)	High
57276	MS11-090: Cumulative Security Update of ActiveX Kill Bits (2618451)	High
57283	MS11-097: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712)	High
57285	MS11-099: Cumulative Security Update for Internet Explorer (2618444)	High
57414	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)	High
57469	MS12-001: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)	High
57472	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)	High
57473	MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)	High
57942	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)	High
57943	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)	High
57944	MS12-010: Cumulative Security Update for Internet Explorer (2647516)	High
57946	MS12-012: Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)	High
57947	MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)	High
57950	MS12-016: Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)	High
58332	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	High
58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High
58655	MS12-023: Cumulative Security Update for Internet Explorer (2675157)	High
58656	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution (2653956)	High
58657	MS12-025: Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)	High
59042	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)	High
59043	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)	High
59044	MS 2695962: Update Rollup for ActiveX Kill Bits (2695962)	High
59454	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)	High
59455	MS12-037: Cumulative Security Update for Internet Explorer (2699988)	High
59456	MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)	High

Plugin	Plugin Name	Severity
59459	MS12-041: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)	High
59460	MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)	High
59906	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)	High
59908	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)	High
59910	MS12-047: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)	High
59911	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)	High
61527	MS12-052: Cumulative Security Update for Internet Explorer (2722913)	High
61530	MS12-055: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)	High
61531	MS12-056: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2706045)	High
62045	MS 2736233: Update Rollup for ActiveX Kill Bits (2736233)	High
62223	MS12-063: Cumulative Security Update for Internet Explorer (2744842)	High
62463	MS12-068: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197)	High
62906	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2745030)	High
62907	MS12-075: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)	High
63224	MS12-077: Cumulative Security Update for Internet Explorer (2761465)	High
63225	MS12-078: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)	High
63228	MS12-081: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)	High
63229	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution (2770660)	High
63420	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)	High
63422	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324)	High
63423	MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)	High
63522	MS13-008: Security Update for Internet Explorer (2799329)	High
64570	MS13-009: Security Update for Internet Explorer (2792100)	High
64571	MS13-010: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2797052)	High
64576	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2800277)	High
64577	MS13-016: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778344)	High
64578	MS13-017: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2799494)	High
64579	MS13-018: Vulnerability in TCP/IP Could Allow Denial of Service (2790655)	High
64580	MS13-019: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)	High
65210	MS13-021: Security Update for Internet Explorer (2809289)	High

Plugin	Plugin Name	Severity
65215	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)	High
65875	MS13-028: Security Update for Internet Explorer (2817183)	High
65876	MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2828223)	High
65878	MS13-031: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2813170)	High
65883	MS13-036: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2829996)	High

QUALYSGUARD® ENTERPRISE SUITE

Scan Results

March 14, 2017

This report was generated with an evaluation version of Qualys

Michal Miklanek
ceska5mm
Manager

Ceska Posta s.p.
olšanská
Prague 13000
Czech Republic

03/14/2017 at 11:10:02 (GMT+0100)

Report Summary

Launch Date:	03/08/2017 at 09:31:23 (GMT+0100)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1488961744.33017
Scanner Appliances:	Miklanek (Scanner 9.1.27-1, Vulnerability Signatures 2.3.558-2)
Duration:	00:18:13
Authentication:	Windows authentication was successful for 1 host
Title:	Win_2008_auth - 20170308
Network:	Global Default Network
Asset Groups:	-
IPs:	10.66.35.212
Excluded IPs:	-
Option Profile:	Initial Options_Miklanek

Summary of Vulnerabilities

Total: 302 Security Risk (Avg): 5.0

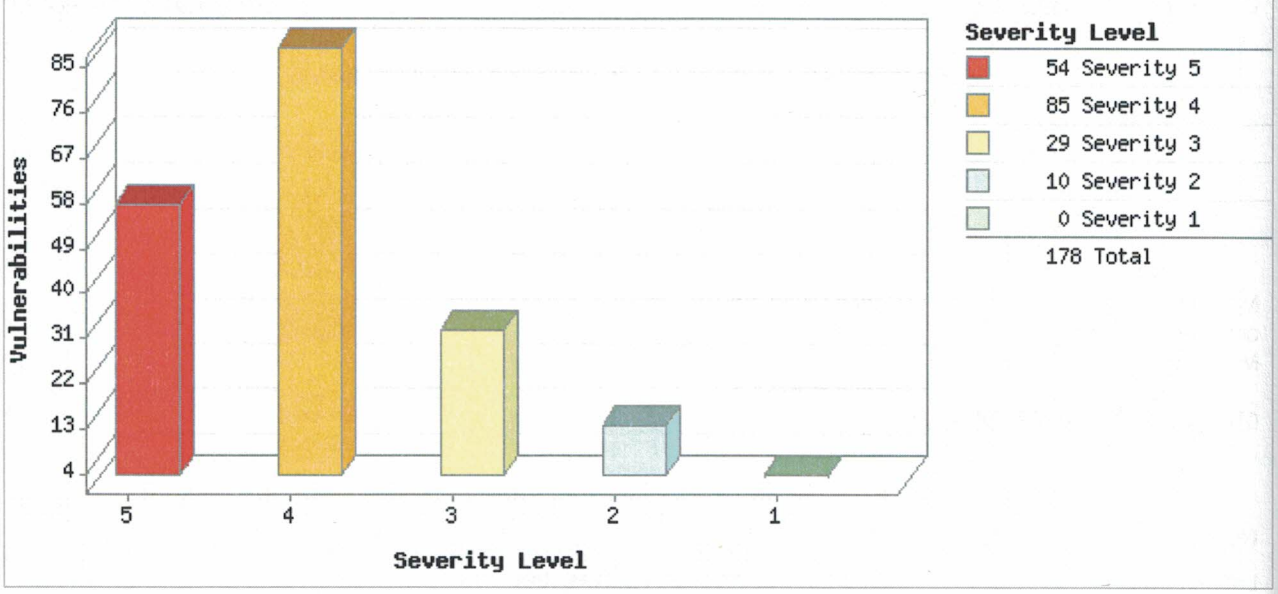
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	54	0	0	54
4	85	0	0	85
3	29	2	8	39
2	10	3	47	60
1	0	1	63	64
Total	**178**	**6**	**118**	**302**

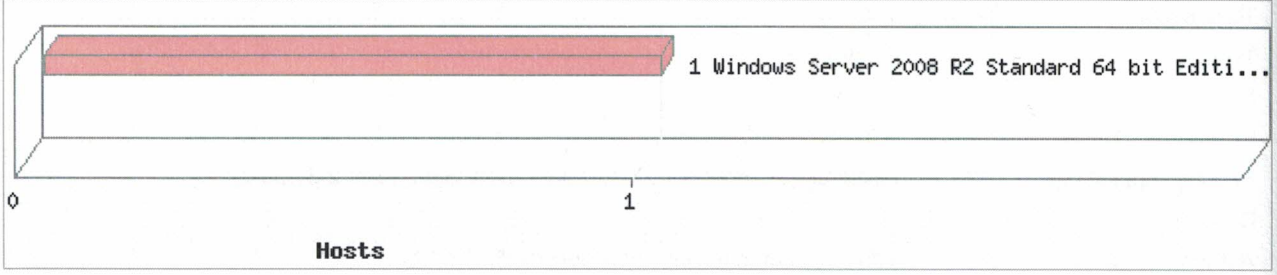
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Windows	130	4	22	156
Security Policy	5	1	58	64
Internet Explorer	33	0	0	33
Information gathering	0	1	18	19
General remote services	4	0	6	10
Total	**172**	**6**	**104**	**282**

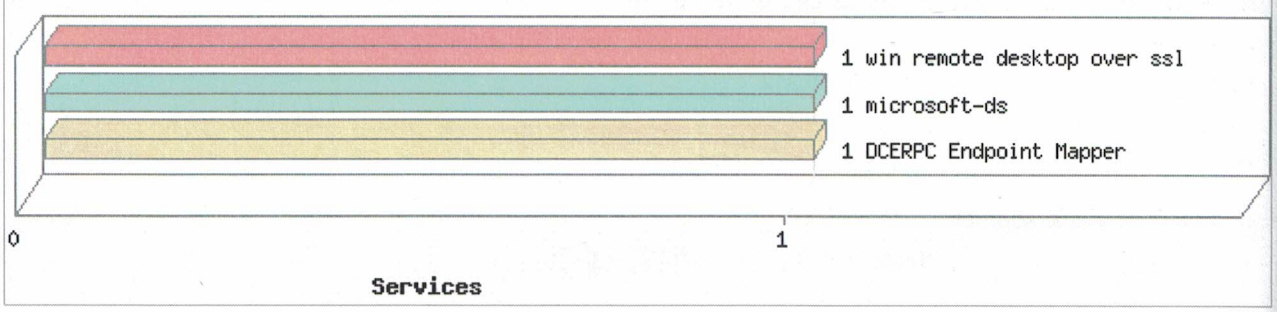
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

▼ 10.66.35.212 (win-5juhib97uqi, WIN-5JUHIB97UQI) - Global Default Network — Windows Server 2008 R2 Standard 64 bit Edition

▼ Vulnerabilities (178) ⊞⊟

▶ 5 Microsoft Embedded OpenType Font Engine Remote Code Execution Vulnerability (MS10-001)

- 5 Microsoft SMB Client Remote Code Execution Vulnerability (MS10-006)
- 5 Microsoft SMB Server Remote Code Execution Vulnerability (MS10-012)
- 5 Microsoft DirectShow Remote Code Execution Vulnerability (MS10-013)
- 5 Microsoft Windows Remote Code Execution Vulnerability (MS10-019)
- 5 Microsoft Windows Canonical Display Driver Remote Code Execution Vulnerability (MS10-043 and Microsoft Security Advisory 2028859)
- 5 Microsoft Media Decompression Remote Code Execution Vulnerability (MS10-033)
- 5 Microsoft Windows Shell Remote Code Execution Vulnerability (MS10-046 and KB2286198)
- 5 Microsoft Windows XML Core Services Remote Code Execution Vulnerability (MS10-051)
- 5 Microsoft OpenType Font Driver Remote Code Execution Vulnerability (MS10-091)
- 5 Microsoft Data Access Components Remote Code Execution Vulnerability (MS11-002)
- 5 Microsoft OpenType Compact Font Format (CFF) Driver Remote Code Execution Vulnerability (MS11-007)
- 5 Microsoft Windows Cumulative Security Update of ActiveX Kill Bits (MS11-027)
- 5 Microsoft OpenType Compact Font Format (CFF) Driver Remote Code Execution Vulnerability (MS11-032)
- 5 Microsoft SMB Server Remote Code Execution Vulnerability (MS11-020)
- 5 Microsoft JScript and VBScript Scripting Engines Remote Code Execution Vulnerability (MS11-031)
- 5 Microsoft Distributed File System Remote Code Execution Vulnerability (MS11-042)
- 5 Microsoft Windows SMB Client Remote Code Execution (MS11-043)
- 5 Microsoft OLE Automation Remote Code Execution Vulnerability (MS11-038)
- 5 Microsoft Windows 2008 R2 Service Pack 1 Not Installed
- 5 Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (MS11-083)
- 5 Microsoft Cumulative Security Update of ActiveX Kill Bits (MS11-090)
- 5 Microsoft Windows C Run-Time Library Remote Code Execution Vulnerability (MS12-013)
- 5 Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerability (MS12-008)
- 5 Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- 5 Microsoft Windows Remote Code Execution Vulnerability (MS12-024)
- 5 Microsoft Combined Security Update for Microsoft Office, Windows, .NET Framework and Silverlight (MS12-034)
- 5 Microsoft Windows Unauthorized Digital Certificates Spoofing Vulnerability (KB2718704)
- 5 Microsoft Remote Desktop Remote Code Execution Vulnerability (MS12-036)
- 5 Microsoft Data Access Components Remote Code Execution Vulnerability (MS12-045)
- 5 Microsoft Windows Print Spooler Components Remote Code Execution Vulnerability (MS13-001)
- 5 Microsoft Windows Client-Server Runtime Subsystem Elevation of Privilege Vulnerability (MS13-019)
- 5 Microsoft Windows Kernel-Mode Driver Elevation of Privilege Vulnerability (MS13-027)
- 5 Microsoft Windows Remote Desktop Client Remote Code Execution Vulnerability (MS13-029)
- 5 Microsoft Windows Kernel Multiple Elevation of Privilege Vulnerabilities (MS13-031)
- 5 Microsoft Internet Explorer Cumulative Security Update (MS10-002 and KB979352)
- 5 Microsoft Internet Explorer Cumulative Security Update (MS10-018 and KB981374)
- 5 Microsoft Cumulative Security Update for Internet Explorer (MS10-071)
- 5 Microsoft Internet Explorer Vector Markup Language Remote Code Execution Vulnerability (MS11-052)
- 5 Microsoft Internet Explorer Cumulative Security Update (MS11-050)
- 5 Microsoft Internet Explorer Cumulative Security Update (MS11-057)
- 5 Microsoft Internet Explorer Cumulative Security Update (MS11-081)

- 5 Microsoft Internet Explorer Cumulative Security Update (MS12-023)
- 5 Microsoft Internet Explorer Cumulative Security Update (MS12-063) (SA2757760)
- 5 Microsoft Internet Explorer Cumulative Security Update (MS12-077)
- 5 Microsoft Internet Explorer Remote Code Execution Vulnerability (MS13-008 and KB2794220)
- 5 Microsoft Internet Explorer Remote Code Execution Vulnerability (MS13-009)
- 5 Microsoft Vector Markup Language Remote Code Execution Vulnerability (MS13-010)
- 5 Microsoft Internet Explorer Multiple Remote Code Execution Vulnerabilities (MS13-021)
- 5 Microsoft Internet Explorer Multiple Remote Code Execution Vulnerabilities (MS13-028)
- 5 EOL/Obsolete Operating System: Microsoft Windows Server 2008 R2 RTM Detected
- 5 EOL/Obsolete Software: Microsoft Internet Explorer 8 Detected
- 5 Microsoft Internet Explorer Time2 Element Behavior Use-After-Free Vulnerability (MS11-050)
- 5 Microsoft Kernel-Mode Drivers Remote Code Execution Vulnerability (MS11-087 and KB2639658)
- 4 Microsoft Cumulative Security Update for ActiveX Kill Bits (MS09-055)
- 4 Microsoft Windows CryptoAPI Spoofing Vulnerability (MS09-056)
- 4 Microsoft Windows Cumulative Security Update of ActiveX Kill Bits (MS10-008)
- 4 Microsoft VBScript Remote Code Execution Vulnerability (MS10-022 and KB981169)
- 4 Microsoft SMB Client Remote Code Execution Vulnerability (MS10-020)
- 4 Microsoft Windows Kernel Elevation Privilege Vulnerability (MS10-021)
- 4 Microsoft Outlook Express and Windows Mail Remote Code Execution Vulnerability (MS10-030)
- 4 Microsoft Windows Cumulative Security Update of ActiveX Kill Bits (MS10-034)
- 4 Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerabilities (MS10-032)
- 4 Microsoft .NET Framework Tampering Vulnerability (MS10-041)
- 4 Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (MS10-073)
- 4 Microsoft Windows MFC Remote Code Execution Vulnerability (MS10-074)
- 4 Microsoft Windows Kernel Elevation of Privilege Vulnerability (MS10-047)
- 4 Microsoft Windows TCP/IP Elevation of Privilege Vulnerability (MS10-058)
- 4 Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (MS10-048)
- 4 Microsoft Windows Print Spooler Remote Code Execution Vulnerability (MS10-061)
- 4 Microsoft Embedded OpenType Font Engine Remote Code Execution Vulnerability (MS10-076)
- 4 Microsoft Windows Common Control Library Remote Code Execution Vulnerability (MS10-081)
- 4 Microsoft Windows Shell and WordPad COM Validation Remote Code Execution Vulnerability (MS10-083)
- 4 Microsoft Windows Task Scheduler Privilege Escalation Vulnerability (MS10-092)
- 4 Microsoft Windows Kernel Elevation of Privilege Vulnerabilities (MS11-011)
- 4 Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerabilities (MS10-098)
- 4 Microsoft Consent User Interface Elevation of Privilege Vulnerability (MS10-100)
- 4 Microsoft Windows Address Book Remote Code Execution Vulnerability (MS10-096)
- 4 Microsoft JScript and VBScript Scripting Engines Information Disclosure Vulnerability (MS11-009)
- 4 Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerability (MS11-012)
- 4 Microsoft Windows Kerberos Elevation of Privilege Vulnerability (MS11-013)
- 4 Microsoft Windows Remote Desktop Client Remote Code Execution Vulnerability (MS11-017)
- 4 Microsoft SMB Client Remote Code Execution Vulnerability (MS11-019)
- 4 Microsoft DNS Resolution Remote Code Execution Vulnerability (MS11-030)

- 4 Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerability (MS11-034)
- 4 Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerability (MS11-041)
- 4 Microsoft SMB Server Denial of Service Vulnerability (MS11-048)
- 4 Microsoft MHTML Information Disclosure Vulnerability (MS11-037)
- 4 Microsoft Ancillary Function Driver Elevation of Privileges Vulnerability (MS11-046)
- 4 Microsoft Windows Kernel Mode Drivers Elevation of Privilege (MS11-054)
- 4 Microsoft Windows Client/Server Runtime Subsystem Elevation of Privilege Vulnerability (MS11-056)
- 4 Microsoft Windows Client/Server Run-time Subsystem Elevation of Privilege Vulnerability (MS11-063)
- 4 Microsoft Data Access Components Remote Code Execution Vulnerability (MS11-059)
- 4 Microsoft Windows Kernel Denial of Service Vulnerability (MS11-068)
- 4 Microsoft Windows Components Remote Code Execution Vulnerability (MS11-071)
- 4 Microsoft Active Accessibility Remote Code Execution Vulnerability (MS11-075)
- 4 Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerability (MS11-077)
- 4 Microsoft Windows Mail and Windows Meeting Space Remote Code Execution Vulnerability (MS11-085)
- 4 Microsoft Windows Kernel Security Feature Bypass Vulnerability (MS12-001)
- 4 Microsoft Windows Media Remote Code Execution Vulnerability (MS12-004)
- 4 Microsoft Windows Remote Code Execution Vulnerability (MS12-005)
- 4 Microsoft Windows Color Control Panel Remote Code Execution Vulnerability (MS12-012)
- 4 Microsoft Ancillary Function Driver Elevation of Privilege (MS12-009)
- 4 Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerability (MS12-018)
- 4 Microsoft Windows Partition Manager Elevation of Privilege Vulnerability (MS12-033)
- 4 Microsoft Windows TCP/IP Elevation of Privilege Vulnerability (MS12-032)
- 4 Microsoft Windows Kernel-Mode Drivers Elevation of Privileges Vulnerability (MS12-041)
- 4 Microsoft Windows Kernel Privilege Escalation Vulnerability (MS12-042)
- 4 Microsoft XML Core Services Remote Code Execution Vulnerability (MS12-043 and KB2719615)
- 4 Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerability (MS12-047)
- 4 Microsoft Windows Shell Remote Code Execution Vulnerability (MS12-048)
- 4 Microsoft Windows Unauthorized Digital Certificates Spoofing Vulnerability (KB2728973)
- 4 Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerability (MS12-055)
- 4 Microsoft JScript and VBScript Scripting Engines Remote Code Execution Vulnerability (MS12-056)
- 4 Windows Networking Components Could Allow Remote Code Execution (MS12-054)
- 4 Microsoft Windows Kernel Privilege Escalation Vulnerability (MS12-068)
- 4 Microsoft .NET Framework Remote Code Execution Vulnerability (MS12-074)
- 4 Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerability (MS12-075)
- 4 Microsoft Windows IP-HTTPS Component Security Feature Bypass Vulnerability (MS12-083)
- 4 Windows File Handling Component Remote Code Execution Vulnerability (MS12-081)
- 4 Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerability (MS12-078)
- 4 Microsoft Fraudulent Digital Certificates Spoofing Vulnerability (KB2798897)
- 4 Microsoft XML Core Services Remote Code Execution Vulnerability (MS13-002)
- 4 Windows Kernel-Mode Driver Elevation of Privilege (MS13-005)
- 4 Microsoft .NET Framework Elevation of Privilege (MS13-004)
- 4 Microsoft Windows Kernel Multiple Elevation of Privilege Vulnerabilities (MS13-017)
- 4 Microsoft Windows Kernel-Mode Driver Elevation of Privilege Vulnerability (MS13-016)
- 4 Microsoft .Net Framework Elevation of Privilege Vulnerability (MS13-015)

4	Microsoft Windows Kernel-Mode Driver Elevation of Privilege Vulnerability (MS13-036)		
4	Microsoft Internet Explorer "onreadystatechange" Use After Free Vulnerability (MS10-018)		
4	Microsoft Internet Explorer Cumulative Security Update (MS10-053)		
4	Microsoft Internet Explorer CSS Style Table Layout Uninitialized Memory Vulnerability (MS10-090)		
4	Microsoft Internet Explorer Remote Code Execution Vulnerability (MS10-090)		
4	Microsoft Internet Explorer Remote Code Execution Vulnerability (MS11-003 and KB2488013)		
4	Microsoft Internet Explorer Cross-Zone Local Cookie File Access Security Bypass Vulnerability (MS11-057)		
4	Microsoft Cumulative Security Update for Internet Explorer (MS11-099)		
4	Microsoft Cumulative Security Update for Internet Explorer (MS12-010)		
4	Microsoft Internet Explorer Cumulative Security Update (MS12-037)		
4	Microsoft Internet Explorer Cumulative Security Update (MS12-052)		
3	Microsoft Windows Local Security Authority Subsystem Service Denial of Service Vulnerability (MS09-059)		
3	Microsoft Windows 7 and Windows Server 2008 R2 Remote SMB Denial of Service Vulnerability (MS10-020 and KB977544)		
3	Microsoft Windows OpenType Compact Font Format (CFF) Driver Elevation of Privilege Vulnerability (MS10-037)		
3	Microsoft Windows win32k.sys Driver "CreateDIBPalette()" Buffer Overflow Vulnerability (MS10-098)		
3	Microsoft Windows SChannel Remote Code Execution Vulnerability (MS10-049)		
3	Microsoft Windows SMB Server Remote Code Execution Vulnerability (MS10-054)		
3	Microsoft Windows Tracing Feature for Services Privilege Elevation Vulnerability (MS10-059)		
3	Microsoft MHTML Information Disclosure Vulnerability (KB2501696, MS11-026)		
3	Microsoft Windows TCP/IP Denial of Service Vulnerability (MS11-064)		
3	Microsoft Windows Kernel-Mode Drivers Denial of Service Vulnerability (MS11-084)		
3	Microsoft Windows Client/Server Run-time Subsystem Elevation of Privilege Vulnerability (MS11-097)		
3	Microsoft Windows DirectWrite Could Allow Denial of Service Vulnerability (MS12-019)		
3	Microsoft Minimum Certificate Key Length Update Not Installed (KB2661254)		
3	Microsoft Windows Kerberos Denial of Service Vulnerability (MS12-069)		
3	Microsoft Windows TCP/IP Denial of Service Vulnerability (MS13-018)		
3	Microsoft Internet Explorer Cumulative Security Update (MS10-035 and KB980088)		
3	Microsoft Internet Explorer XSS Filter "SCRIPT" Tag XSS Vulnerability (MS10-018)		
3	Microsoft Internet Explorer CSS "expression" Remote Denial of Service Vulnerability - Zero Day		
3	Microsoft Internet Explorer MSHTML Findtext Processing Vulnerability - Zero Day		
3	Microsoft Internet Explorer Mouse Tracking Events Design Error Vulnerability		
3	Microsoft Internet Explorer Stack Exhaustion Denial of Service Vulnerability		
3	Built-in Guest Account Not Renamed at Windows Target System		
3	Microsoft Windows "RunAs" Password Length Local Information Disclosure - Zero Day		
3	Microsoft Internet Explorer File Download Denial of Service Vulnerability - Zero Day		
3	Hotfix KB2264107 (DLL hijacking) Not Installed / Not Configured		
3	Microsoft Windows IPv6 Protocol Stack Network Discovery Design Error Vulnerability (KB2750841)		
3	SSL/TLS use of weak RC4 cipher	port 3389/tcp over SSL	
3	SSL/TLS Server supports TLSv1.0	port 3389/tcp over SSL	
3	Windows Remote Desktop Protocol Weak Encryption Method Allowed	port 3389/tcp over SSL	
2	Enabled Cached Logon Credential		

2	Allowed Null Session		
2	Default Windows Administrator Account Name Present		
2	Microsoft Windows Service Isolation Bypass Privilege Escalation Vulnerability (KB2264072)		
2	Microsoft Internet Explorer Print Handler Vulnerability		
2	Microsoft Internet Explorer Cache Objects History Enumeration Vulnerability - Zero Day		
2	Microsoft Windows Explorer AutoPlay Not Disabled		
2	Windows Explorer Autoplay Not Disabled for Default User		
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 3389/tcp over SSL	
2	SSL Certificate - Signature Verification Failed Vulnerability	port 3389/tcp over SSL	

Potential Vulnerabilities (6)

Information Gathered (118)

Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

10.66.35.212

Target distribution across scanner appliances

Miklanek : 10.66.35.212

Windows authentication was successful for these hosts (1)

Instance os:
10.66.35.212

Options Profile

Initial Options_Miklanek

Scan Settings	
Ports	-
Scanned TCP Ports	Standard Scan
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Perform 3-way Handshake	Off
Vulnerability Detection	Complete
Password Brute Forcing	-
System	Disabled
Custom	Disabled
Authentication	-
Windows	Enabled

Unix/Cisco	Enabled
Oracle	Disabled
Oracle Listener	Disabled
SNMP	Disabled
VMware	Disabled
DB2	Disabled
HTTP	Disabled
MySQL	Disabled
Overall Performance	Normal
Additional Certificate Detection	Normal
Authenticated Scan Certificate Discovery	Disabled
Hosts to Scan in Parallel	-
Use Appliance Parallel ML Scaling	Off
External Scanners	15
Scanner Appliances	30
Processes to Run in Parallel	-
Total Processes	10
HTTP Processes	10
Packet (Burst) Delay	Medium
Port Scanning and Host Discovery	-
Intensity	Normal
Dissolvable Agent	-
Dissolvable Agent (for this profile)	Disabled
Windows Share Enumeration	Disabled
Windows Directory Search	Disabled
Lite OS Discovery	Disabled
Advanced Settings	
Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Packet Options	-
Ignore firewall-generated TCP RST packets	Off
Ignore all TCP RST packets	Off
Ignore firewall-generated TCP SYN-ACK packets	Off
Do not send TCP ACK or SYN-ACK packets during host discovery	Off

▸ Report Legend

This report was generated with an evaluation version of Qualys

The correctness and completeness of your vulnerability reports is very important to us. If you believe our system made an error in your report, please notify us and we will contact you immediately for clarification.

QUALYSGUARD® ENTERPRISE SUITE

Scan Results

March 14, 2017

This report was generated with an evaluation version of Qualys

Michal Miklanek
ceska5mm
Manager

Ceska Posta s.p.
olšanská
Prague 13000
Czech Republic

03/14/2017 at 11:14:42 (GMT+0100)

Report Summary

Launch Date:	03/08/2017 at 10:04:26 (GMT+0100)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1488963842.33018
Scanner Appliances:	Miklanek (Scanner 9.1.27-1, Vulnerability Signatures 2.3.558-3)
Duration:	00:18:13
Title:	Win_2008_neauth
Network:	Global Default Network
Asset Groups:	-
IPs:	10.66.35.212
Excluded IPs:	-
Option Profile:	Initial Options_Miklanek

Summary of Vulnerabilities

Total: 29 Security Risk (Avg): 5.0

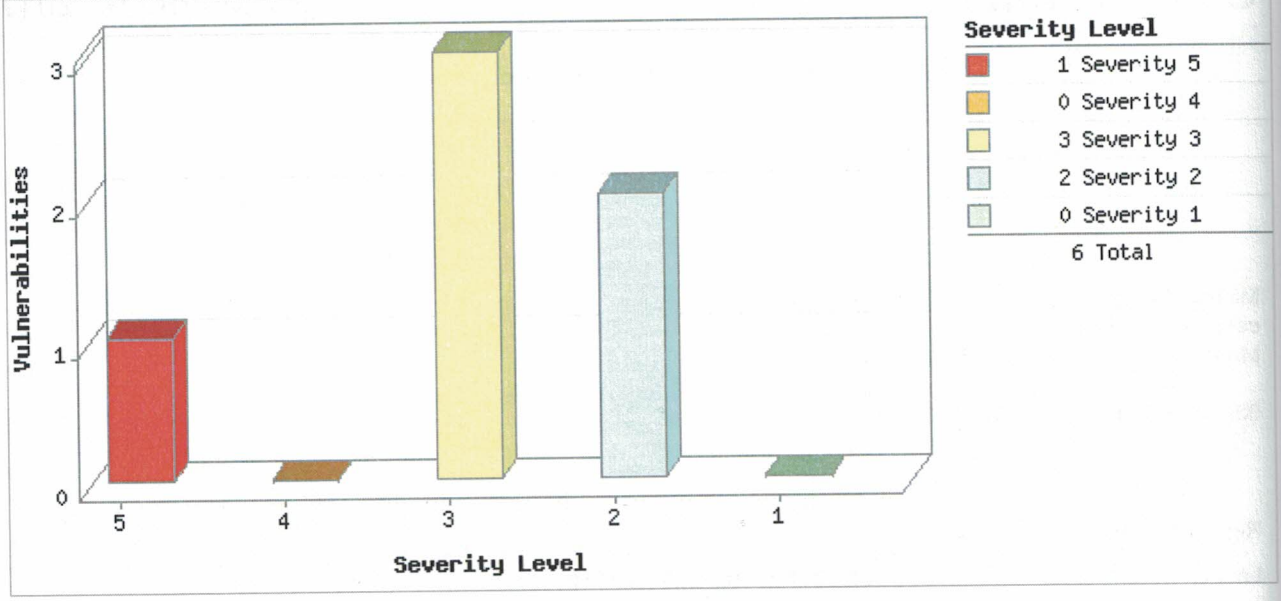
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	1	0	0	1
4	0	0	0	0
3	3	1	1	5
2	2	0	4	6
1	0	0	17	17
Total	**6**	**1**	**22**	**29**

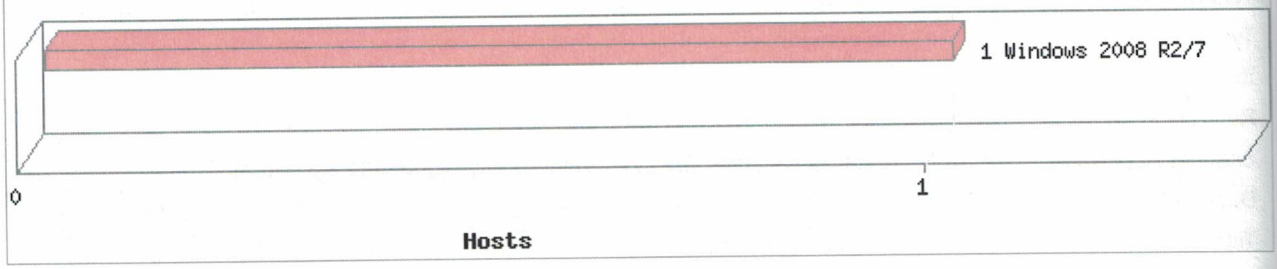
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	4	0	6	10
Windows	2	1	2	5
TCP/IP	0	0	5	5
Information gathering	0	0	4	4
SMB / NETBIOS	0	0	2	2
Total	**6**	**1**	**19**	**26**

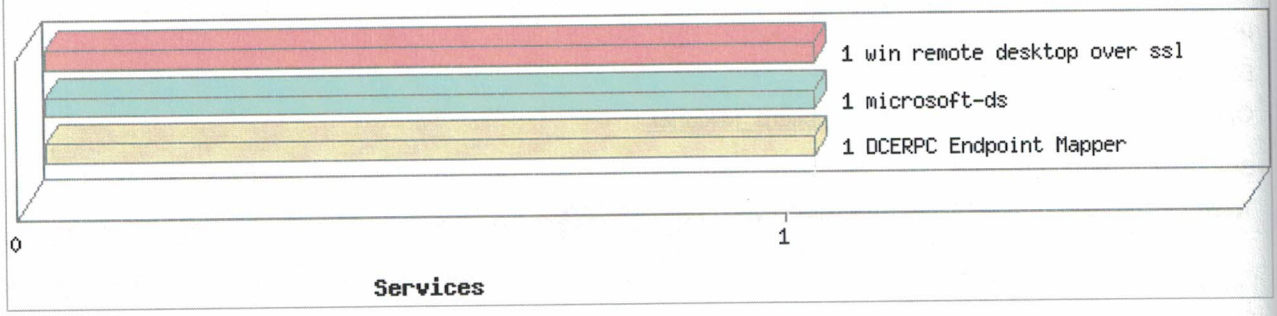
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

▼ 10.66.35.212 (win-5juhib97uqi, WIN-5JUHIB97UQI) Windows 2008 R2/7
- Global Default Network

▼ Vulnerabilities (6) ⊞⊟

▶ 5 Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)

▸	3	SSL/TLS use of weak RC4 cipher	port 3389/tcp over SSL
▸	3	SSL/TLS Server supports TLSv1.0	port 3389/tcp over SSL
▸	3	Windows Remote Desktop Protocol Weak Encryption Method Allowed	port 3389/tcp over SSL
▸	2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 3389/tcp over SSL
▸	2	SSL Certificate - Signature Verification Failed Vulnerability	port 3389/tcp over SSL

▸ Potential Vulnerabilities (1) ⊞⊟

▸ Information Gathered (22) ⊞⊟

▾ Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

10.66.35.212

Target distribution across scanner appliances

Miklanek : 10.66.35.212

Options Profile

Initial Options_Miklanek

Scan Settings	
Ports	-
Scanned TCP Ports	Standard Scan
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Perform 3-way Handshake	Off
Vulnerability Detection	Complete
Password Brute Forcing	-
System	Disabled
Custom	Disabled
Authentication	-
Windows	Enabled
Unix/Cisco	Enabled
Oracle	Disabled
Oracle Listener	Disabled
SNMP	Disabled
VMware	Disabled
DB2	Disabled
HTTP	Disabled
MySQL	Disabled

Overall Performance	Normal
Additional Certificate Detection	Normal
Authenticated Scan Certificate Discovery	Disabled
Hosts to Scan in Parallel	-
Use Appliance Parallel ML Scaling	Off
External Scanners	15
Scanner Appliances	30
Processes to Run in Parallel	-
Total Processes	10
HTTP Processes	10
Packet (Burst) Delay	Medium
Port Scanning and Host Discovery	-
Intensity	Normal
Dissolvable Agent	-
Dissolvable Agent (for this profile)	Disabled
Windows Share Enumeration	Disabled
Windows Directory Search	Disabled
Lite OS Discovery	Disabled
Advanced Settings	
Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Packet Options	-
Ignore firewall-generated TCP RST packets	Off
Ignore all TCP RST packets	Off
Ignore firewall-generated TCP SYN-ACK packets	Off
Do not send TCP ACK or SYN-ACK packets during host discovery	Off

▶ Report Legend

This report was generated with an evaluation version of Qualys

Highest Risk Vulnerabilities

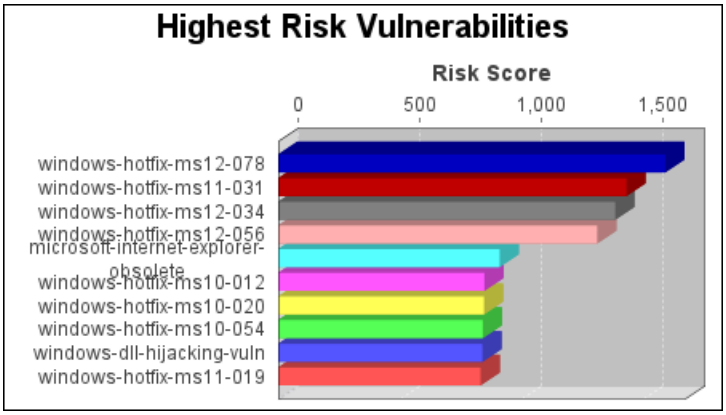
Asset report for 10.66.35.212

Audited on March 1, 2017

Reported on February 19, 2017

Table of Contents

1. Executive Overview



The windows-hotfix-ms12-078 vulnerability poses the highest risk to the organization with a risk score of 1,589. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

2. Highest Risk Vulnerability Details

2.1. MS12-078: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534) (windows-hotfix-ms12-078)

Category	Web, Mail, Microsoft, Browsers, Microsoft Patch, Microsoft Windows, Remote Execution
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	1,589
References	CERT: TA12-346A, CVE-2012-2556, CVE-2012-4786, MS12-078, MSKB: 2783534, OVAL: OVAL15845, OVAL: OVAL16067

2.2. MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666) (windows-hotfix-ms11-031)

Category	Web, Mail, Microsoft, Remote Execution, Microsoft Patch
CVSS score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Risk Score	1,430
References	BID: 47249, CERT: TA11-102A, CVE-2011-0663, MS11-031, MSKB: 2514666, OVAL: OVAL12673

2.3. MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578) (windows-hotfix-ms12-034)

Category	Mail, Microsoft, Microsoft .NET Framework, IAVM, Microsoft Office, Microsoft Windows, Remote Execution, Browsers, Microsoft Patch, Web
CVSS score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Risk Score	1,384
References	BID: 53335, BID: 53347, BID: 53351, BID: 53358, BID: 53360, BID: 53363, CERT: TA11-347A, CERT: TA12-129A, CERT: TA12-164A, CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848, DISA_SEVERITY: Category I, DISA_VMSKEY: V0032304, IAVM: 2012-A-0079, MS11-087, MS12-034, MS12-039, MSKB: 2681578, OVAL: OVAL13998, OVAL: OVAL14655, OVAL: OVAL15290, OVAL: OVAL15355, OVAL: OVAL15388, OVAL: OVAL15466, OVAL: OVAL15555, OVAL: OVAL15574, OVAL: OVAL15580, OVAL: OVAL15621, OVAL: OVAL15628, OVAL: OVAL15645, OVAL: OVAL15667

2.4. MS12-056: Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution (2706045) (windows-hotfix-ms12-056)

Category	Web, Mail, Microsoft, IAVM, Microsoft Windows, Remote Execution, Browsers, Microsoft Patch
CVSS score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

Risk Score	1,310
References	CERT: TA12-227A, CVE-2012-2523, DISA_SEVERITY: Category II, DISA_VMSKEY: V0033654, IAVM: 2012-A-0130, MS12-052, MS12-056, MSKB: 2706045, OVAL: OVAL15790

2.5. Obsolete Version of Microsoft Internet Explorer (microsoft-internet-explorer-obsolete)

Category	Microsoft Internet Explorer, Obsolete Software, Microsoft, Browsers
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	909
References	URL: https://support.microsoft.com/lifecycle#gp/Microsoft-Internet-Explorer

2.6. MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) (windows-hotfix-ms10-012)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	847
References	CERT: TA10-040A, CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231, MS10-012, MSKB: 971468, OVAL: OVAL7751, OVAL: OVAL8314, OVAL: OVAL8438, OVAL: OVAL8524

2.7. MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232) (windows-hotfix-ms10-020)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	845
References	BID: 39336, CERT: TA10-103A, CVE-2009-3676, CVE-2010-0269, CVE-2010-0270, CVE-2010-0476, CVE-2010-0477, MS10-020, MSKB: 980232, OVAL: OVAL6859, OVAL: OVAL6918, OVAL: OVAL7129, OVAL: OVAL7164, OVAL: OVAL7186

2.8. MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (windows-hotfix-ms10-054)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	840
References	CERT: TA10-222A, CVE-2010-2550, CVE-2010-2551, CVE-2010-2552, MS10-054, MSKB: 982214, OVAL: OVAL11106, OVAL: OVAL12015, OVAL: OVAL12072

2.9. Windows DLL Hijacking Vulnerability (windows-dll-hijacking-vuln)

Category	Microsoft
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	839
References	MSKB: 2264107, URL: http://www.microsoft.com/technet/security/advisory/2269637.mspx

2.10. MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455) (windows-hotfix-ms11-019)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	831
References	BID: 46360, BID: 47239, CERT: TA11-102A, CERT-VN: 323172, CVE-2011-0654, CVE-2011-0660, MS11-019, MSKB: 2511455, OVAL: OVAL11995, OVAL: OVAL12637, XF: 65376

Příloha č. 2.

Porovnání výsledků a reportů skenů

Skenovaný operační systém: CentOS 7

Stav operačního systému: bez aktualizací

Použité skenery:

a) Tenable Nessus – sken s autentizací
b) QualysGuard – sken s autentizací
c) Nexpose – sken s autentizací

SecurityCenter™

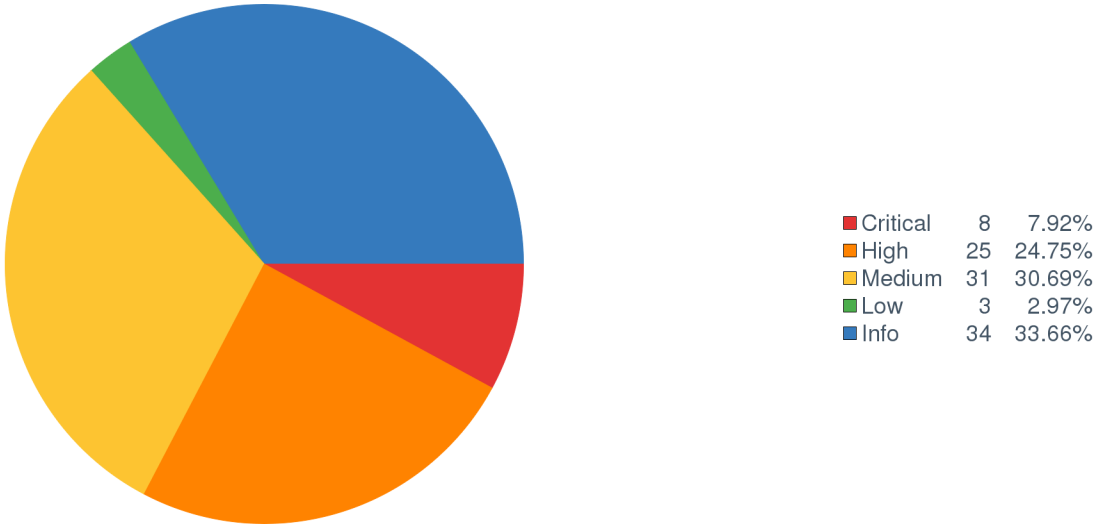
CentOS_7_auth_10.66.35.233

March 9, 2017 at 10:55am CET

Michal Miklánek [mimiu]
CESKA POSTA S. P.

Souhrn

Přehled závažnosti všech zranitelností



IP přehled

IP Address	DNS Name	Score	Total	Vulns
10.66.35.233		666	101	8 25 31 3 34

Přehled portů

Port	Info	Low	Med.	High	Crit.	Total
0	26	1	30	25	8	90
22	8	2	1	0	0	11

Zranitelnosti - výčet

10.66.35.233

IP Address: 10.66.35.233
OS CPE: cpe:/o:centos:centos:7:update2
MAC Address: 00:0c:29:5d:3c:38
Score: 666
Repository: Test_polygon_Olše_MIMI

Počty zranitelností dle závažnosti

Severity	Count
Critical	8
High	25
Medium	31
Low	3
Info	34

Výpis zranitelností závažnosti: Critical, High

Plugin	Plugin Name	Severity
88758	CentOS 7 : glibc (CESA-2016:0176)	Critical
89059	CentOS 6 / 7 : openssl (CESA-2016:0301) (DROWN)	Critical
91017	CentOS 7 : openssl (CESA-2016:0722)	Critical
91786	CentOS 6 / 7 : libxml2 (CESA-2016:1292)	Critical
95321	CentOS 7 : kernel (CESA-2016:2574)	Critical
95332	CentOS 7 : python (CESA-2016:2586)	Critical
95341	CentOS 7 : mariadb (CESA-2016:2595)	Critical
96633	CentOS 7 : kernel (CESA-2017:0086)	Critical
87139	CentOS 7 : glibc (CESA-2015:2172)	High
87224	CentOS 7 : libxml2 (CESA-2015:2550)	High
88148	CentOS 7 : kernel (CESA-2016:0064)	High
88759	CentOS 7 : kernel (CESA-2016:0185)	High
90276	CentOS 7 : mariadb (CESA-2016:0534)	High
90722	CentOS 7 : nspr / nss / nss-softokn / nss-util (CESA-2016:0685)	High
91104	CentOS 7 : pcre (CESA-2016:1025)	High
91105	CentOS 7 : kernel (CESA-2016:1033)	High
91785	CentOS 7 : kernel (CESA-2016:1277)	High
92702	CentOS 7 : kernel (CESA-2016:1539)	High
93594	CentOS 7 : kernel (CESA-2016:1847)	High
93777	CentOS 6 / 7 : openssl (CESA-2016:1940)	High
93779	CentOS 5 / 6 / 7 : bind (CESA-2016:1944)	High
93967	CentOS 7 : kernel (CESA-2016:2047)	High
94254	CentOS 7 : kernel (CESA-2016:2098) (Dirty COW)	High
94978	CentOS 6 / 7 : policycoreutils (CESA-2016:2702)	High
94981	CentOS 5 / 6 / 7 : nss / nss-util (CESA-2016:2779)	High
95329	CentOS 7 : nettle (CESA-2016:2582)	High
95334	CentOS 7 : openssh (CESA-2016:2588)	High
95336	CentOS 7 : dhcp (CESA-2016:2590)	High
95373	CentOS 6 / 7 : expat (CESA-2016:2824)	High
97194	CentOS 7 : bind (CESA-2017:0276)	High
97305	CentOS 6 / 7 : openssl (CESA-2017:0286)	High
97331	CentOS 7 : kernel (CESA-2017:0294)	High
97558	CentOS 7 : kernel (CESA-2017:0386)	High

QUALYSGUARD® ENTERPRISE SUITE

Scan Results

March 14, 2017

This report was generated with an evaluation version of Qualys

Michal Miklanek
ceska5mm
Manager

Ceska Posta s.p.
olšanská
Prague 13000
Czech Republic

03/14/2017 at 11:16:35 (GMT+0100)

Report Summary

Launch Date:	03/07/2017 at 15:09:23 (GMT+0100)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1488895738.32968
Scanner Appliances:	Miklanek (Scanner 9.1.27-1, Vulnerability Signatures 2.3.557-2)
Duration:	00:15:32
Authentication:	Unix/Cisco/Checkpoint Firewall authentication was successful for 1 host
Title:	CentOS_7_auth
Network:	Global Default Network
Asset Groups:	-
IPs:	10.66.35.233
Excluded IPs:	-
Option Profile:	Initial Options

Summary of Vulnerabilities

Total: 113 Security Risk (Avg): 5.0

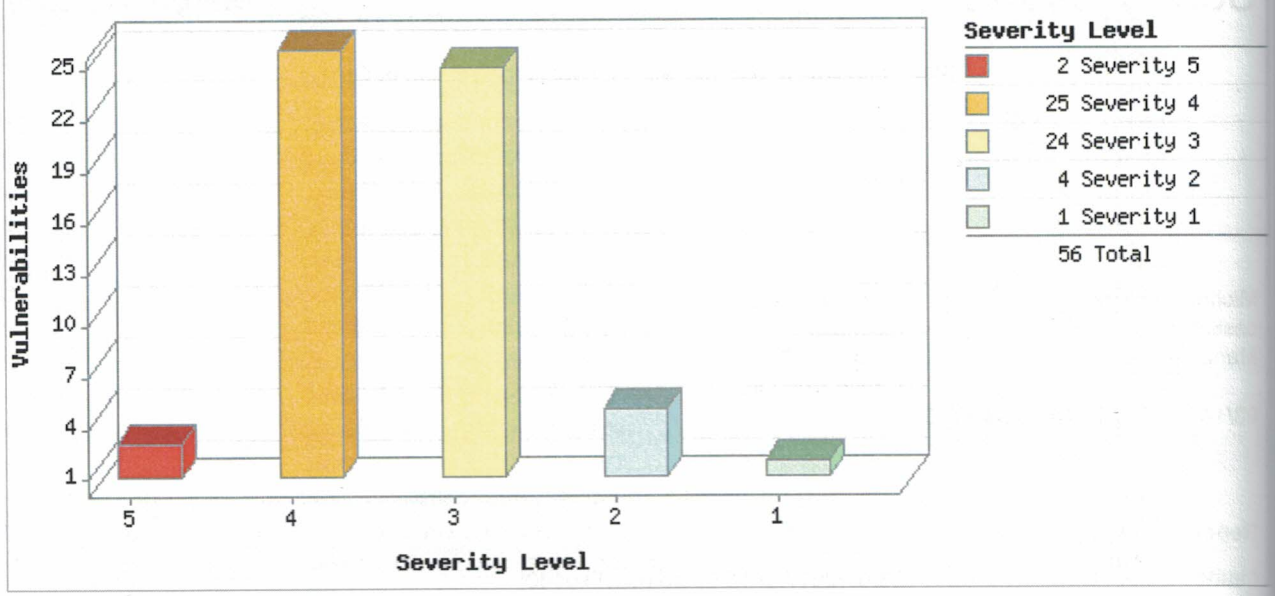
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	2	0	0	2
4	25	0	0	25
3	24	1	2	27
2	4	0	10	14
1	1	0	44	45
Total	**56**	**1**	**56**	**113**

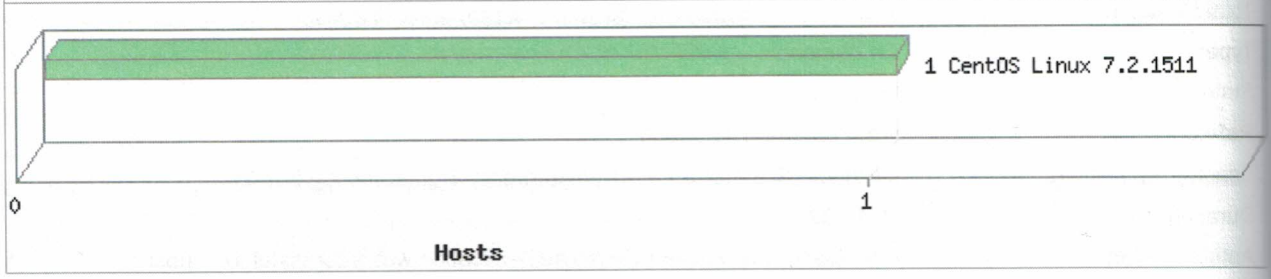
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Local	22	1	13	36
CentOS	33	0	0	33
Information gathering	0	0	19	19
Security Policy	1	0	11	12
TCP/IP	0	0	5	5
Total	**56**	**1**	**48**	**105**

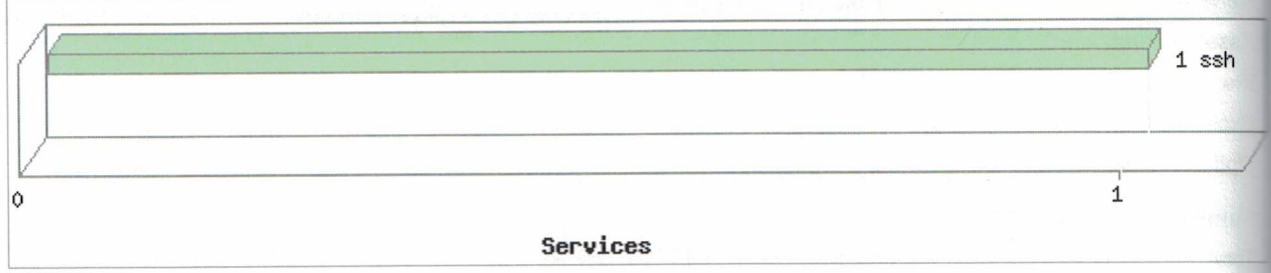
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

▼ 10.66.35.233 (-, -) - Global Default Network CentOS Linux 7.2.1511

▼ Vulnerabilities (56) ⊞⊟

- 5 CentOS Security Update for glibc (CESA-2016:0176)
- 5 CentOS Security Update for nss-util (CESA-2016:0370)
- 4 CentOS Security Update for bind (CESA-2015:2655)
- 4 CentOS Security Update for glibc (CESA-2015:2172)

- 4 CentOS Security Update for kernel (CESA-2015:2552)
- 4 CentOS Security Update for kernel Security Update (CESA-2016:0064)
- 4 CentOS Security Update for kernel (CESA-2016:0185)
- 4 CentOS Security Update for openssl (CESA-2016:0301)
- 4 CentOS Security Update for bind (CESA-2016:0459)
- 4 CentOS Security Update for openssl (CESA-2016:0722)
- 4 CentOS Security Update for kernel (CESA-2016:1033)
- 4 CentOS Security Update for pcre Security Update (CESA-2016:1025)
- 4 CentOS Security Update for kernel (CESA-2016:1277)
- 4 CentOS Security Update for kernel (CESA-2016:1539)
- 4 CentOS Security Update for mariadb (CESA-2016:1602)
- 4 CentOS Security Update for kernel (CESA-2016:1633)
- 4 CentOS Security Update for kernel (CESA-2016:1847)
- 4 CentOS Security Update for kernel (CESA-2016:2047)
- 4 CentOS Security Update for kernel (CESA-2016:2098) (Dirty Cow)
- 4 CentOS Security Update for policycoreutils (CESA-2016:2702)
- 4 CentOS Security Update for kernel (CESA-2016:2574)
- 4 CentOS Security Update for openssl (CESA-2016:1940)
- 4 CentOS Security Update for bind (CESA-2016:1944)
- 4 CentOS Security Update for mariadb (CESA-2016:2595)
- 4 CentOS Security Update for bind (CESA-2016:2615)
- 4 CentOS Security Update for bind (CESA-2017:0062)
- 4 CentOS Security Update for kernel (CESA-2017:0086)
- 3 CentOS Security Update for openssl (CESA-2015:2617)
- 3 CentOS Security Update for grub2 (CESA-2015:2653)
- 3 CentOS Security Update for libxml2 (CESA-2015:2550)
- 3 CentOS Security Update for nss (CESA-2016:0007)
- 3 CentOS Security Update for openssl (CESA-2016:0008)
- 3 CentOS Security Update for gnutls (CESA-2016:0012)
- 3 CentOS Security Update for openssh (CESA-2016:0043)
- 3 CentOS Security Update for bind Security Update (CESA-2016:0073)
- 3 CentOS Security Update for polkit (CESA-2016:0189)
- 3 CentOS Security Update for libssh2 (CESA-2016:0428)
- 3 CentOS Security Update for openssh (CESA-2016:0465)
- 3 CentOS Security Update for mariadb (CESA-2016:0534)
- 3 CentOS Security Update for krb5 (CESA-2016:0532)
- 3 CentOS Security Update for nss Security Update (CESA-2016:0685)
- 3 CentOS Security Update for libndp (CESA-2016:1086)
- 3 CentOS Security Update for python (CESA-2016:1626)
- 3 CentOS Security Update for nss (CESA-2016:2779)
- 3 CentOS Security Update for expat (CESA-2016:2824)
- 3 CentOS Security Update for nettle (CESA-2016:2582)
- 3 CentOS Security Update for curl (CESA-2016:2575)
- 3 CentOS Security Update for firewalld (CESA-2016:2597)
- 3 CentOS Security Update for sudo (CESA-2016:2872)
- 3 CentOS Security Update for vim (CESA-2016:2972)

- 3 CentOS Security Update for openssh (CESA-2016:2588)
- 2 CentOS Security Update for glibc (CESA-2016:2573)
- 2 CentOS Security Update for python (CESA-2016:2586)
- 2 CentOS Security Update for sudo (CESA-2016:2593)
- 2 CentOS Security Update for util-linux (CESA-2016:2605)
- 1 User Accounts With Password Aging Not Set

▸ Potential Vulnerabilities (1)

▸ Information Gathered (56)

▾ Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

10.66.35.233

Target distribution across scanner appliances

Miklanek : 10.66.35.233

Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts (1)

Instance os:
10.66.35.233

Options Profile

Initial Options

Scan Settings	
Ports	-
Scanned TCP Ports	Standard Scan
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Perform 3-way Handshake	Off
Vulnerability Detection	Complete
Password Brute Forcing	-
System	Disabled
Custom	Disabled
Authentication	-
Windows	Enabled
Unix/Cisco	Enabled
Oracle	Disabled
Oracle Listener	Disabled
SNMP	Disabled

VMware	Disabled
DB2	Disabled
HTTP	Disabled
MySQL	Disabled
Overall Performance	Normal
Additional Certificate Detection	Normal
Authenticated Scan Certificate Discovery	Disabled
Hosts to Scan in Parallel	-
Use Appliance Parallel ML Scaling	Off
External Scanners	15
Scanner Appliances	30
Processes to Run in Parallel	-
Total Processes	10
HTTP Processes	10
Packet (Burst) Delay	Medium
Port Scanning and Host Discovery	-
Intensity	Normal
Dissolvable Agent	-
Dissolvable Agent (for this profile)	Disabled
Windows Share Enumeration	Disabled
Windows Directory Search	Disabled
Lite OS Discovery	Disabled
Advanced Settings	
Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Packet Options	-
Ignore firewall-generated TCP RST packets	Off
Ignore all TCP RST packets	Off
Ignore firewall-generated TCP SYN-ACK packets	Off
Do not send TCP ACK or SYN-ACK packets during host discovery	Off

▸ Report Legend

This report was generated with an evaluation version of Qualys

Highest Risk Vulnerabilities

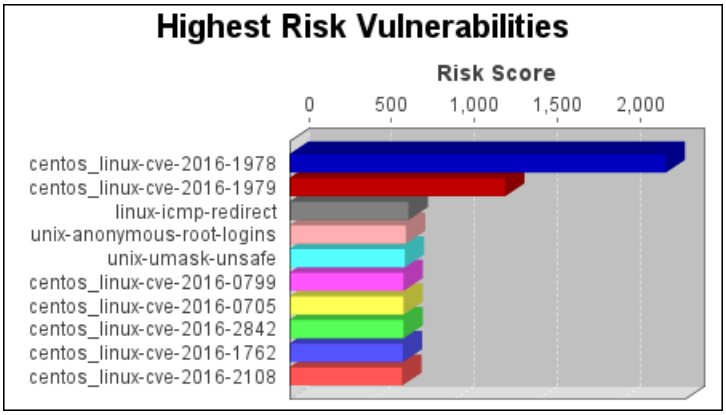
Asset report for 10.66.35.233

Audited on February 19, 2017

Reported on February 19, 2017

Table of Contents

1. Executive Overview



The centos_linux-cve-2016-1978 vulnerability poses the highest risk to the organization with a risk score of 2,271. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

2. Highest Risk Vulnerability Details

2.1. Cent OS: CVE-2016-1978: CESA-2016:0685 (nspr, nss-softokn, nss-util) (centos_linux-cve-2016-1978)

Category	CentOS, Denial of Service
CVSS score	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Risk Score	2,271
References	SUSE: SUSE-SU-2016:0727, SUSE: SUSE-SU-2016:0777, SUSE: SUSE-SU-2016:0820, SUSE: SUSE-SU-2016:0909, REDHAT: RHSA-2016:0591, REDHAT: RHSA-2016:0684, REDHAT: RHSA-2016:0685, BID: 84275, BID: 91787, SECTRACK: 1035258, UBUNTU: USN-2973-1, GENTOO: GLSA-201605-06, NVD: CVE-2016-1978, DEBIAN: DSA-3688

2.2. Cent OS: CVE-2016-1979: CESA-2016:0685 (nspr, nss-softokn, nss-util) (centos_linux-cve-2016-1979)

Category	CentOS, Denial of Service
CVSS score	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Risk Score	1,301
References	SUSE: SUSE-SU-2016:0727, SUSE: SUSE-SU-2016:0777, SUSE: SUSE-SU-2016:0820, SUSE: SUSE-SU-2016:0909, REDHAT: RHSA-2016:0591, REDHAT: RHSA-2016:0684, REDHAT: RHSA-2016:0685, DEBIAN: DSA-3576, DEBIAN: DSA-3688, BID: 84221, SECTRACK: 1035215, UBUNTU: USN-2973-1, GENTOO: GLSA-201605-06, NVD: CVE-2016-1979

2.3. ICMP redirection enabled (linux-icmp-redirect)

Category	UNIX
CVSS score	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Risk Score	719
References	BID: 6823, MSKB: 293626, XF: cisco-ios-icmp-redirect(11306)

2.4. Anonymous root login is allowed (unix-anonymous-root-logins)

Category	UNIX
CVSS score	6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)
Risk Score	703

2.5. User umask value is unsafe (unix-umask-unsafe)

Category	UNIX

CVSS score	4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)
Risk Score	697

2.6. Cent OS: CVE-2016-0799: CESA-2016:0722 (openssl) (centos_linux-cve-2016-0799)

Category	OpenSSL, CentOS, Denial of Service
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	688
References	SUSE: SUSE-SU-2016:0617, SUSE: SUSE-SU-2016:0620, SUSE: SUSE-SU-2016:0621, SUSE: SUSE-SU-2016:0624, SUSE: SUSE-SU-2016:0631, SUSE: SUSE-SU-2016:0641, SUSE: SUSE-SU-2016:0678, SUSE: SUSE-SU-2016:1057, REDHAT: RHSA-2016:0722, REDHAT: RHSA-2016:0996, DEBIAN: DSA-3500, BID: 83755, BID: 91787, UBUNTU: USN-2914-1, GENTOO: GLSA-201603-15, NVD: CVE-2016-0799

2.7. Cent OS: CVE-2016-0705: CESA-2016:0301 (openssl) (centos_linux-cve-2016-0705)

Category	OpenSSL, CentOS, Denial of Service
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	688
References	SUSE: SUSE-SU-2016:0617, SUSE: SUSE-SU-2016:0620, SUSE: SUSE-SU-2016:0621, SUSE: SUSE-SU-2016:0624, SUSE: SUSE-SU-2016:0631, SUSE: SUSE-SU-2016:1057, DEBIAN: DSA-3500, BID: 83754, BID: 91787, UBUNTU: USN-2914-1, GENTOO: GLSA-201603-15, NVD: CVE-2016-0705

2.8. Cent OS: CVE-2016-2842: CESA-2016:0722 (openssl) (centos_linux-cve-2016-2842)

Category	OpenSSL, CentOS, Denial of Service
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	688
References	REDHAT: RHSA-2016:0722, REDHAT: RHSA-2016:0996, BID: 84169, NVD: CVE-2016-2842, DEBIAN: DSA-3500

2.9. Cent OS: CVE-2016-1762: CESA-2016:1292 (libxml2) (centos_linux-cve-2016-1762)

Category	CentOS, Denial of Service
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	685
References	APPLE: APPLE-SA-2016-03-21-1, APPLE: APPLE-SA-2016-03-21-2, APPLE: APPLE-SA-2016-03-21-3, APPLE: APPLE-SA-2016-03-21-5, APPLE: APPLE-SA-2016-03-21-6, BID: 85059, SECTRACK: 1035353, UBUNTU: USN-2994-1, REDHAT: RHSA-2016:1292, DEBIAN: DSA-3593, NVD: CVE-2016-1762

2.10. Cent OS: CVE-2016-2108: CESA-2016:1137 (openssl) (centos_linux-cve-2016-2108)

Category	OpenSSL, Remote Execution, CentOS, Denial of Service

CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	680
References	APPLE: APPLE-SA-2016-07-18-1, SUSE: SUSE-SU-2016:1206, SUSE: SUSE-SU-2016:1228, SUSE: SUSE-SU-2016:1231, SUSE: SUSE-SU-2016:1233, SUSE: SUSE-SU-2016:1267, SUSE: SUSE-SU-2016:1290, SUSE: SUSE-SU-2016:1360, REDHAT: RHSA-2016:0722, REDHAT: RHSA-2016:0996, REDHAT: RHSA-2016:1137, DEBIAN: DSA-3566, BID: 89752, BID: 91787, SECTRACK: 1035721, UBUNTU: USN-2959-1, GENTOO: GLSA-201612-16, NVD: CVE-2016-2108

Příloha č. 3.

Porovnání výsledků a reportů skenů

Skenovaný operační systém: Windows 7 Professional

Použité skenery:

a) Tenable Nessus – sken s autentizací
b) QualysGuard – sken s autentizací
c) Nexpose – sken s autentizací

SecurityCenter™

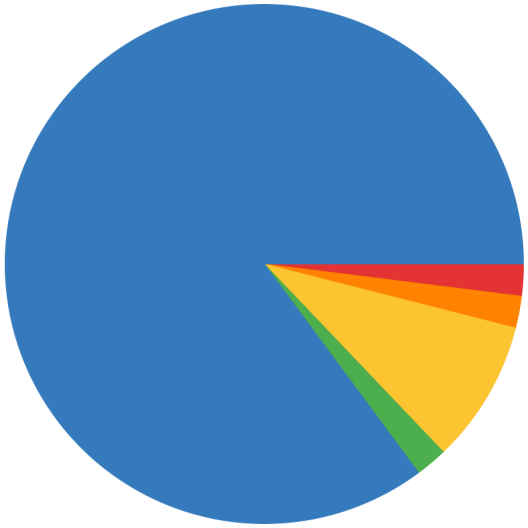
Win_7_auth_10.66.35.175

March 13, 2017 at 4:30pm CET

Michal Miklánek [mimiu]
CESKA POSTA S. P.

Souhrn

Přehled závažnosti všech zranitelností



Critical	2	1.98%
High	2	1.98%
Medium	9	8.91%
Low	2	1.98%
Info	86	85.15%

IP přehled

IP Address	DNS Name	Score	Total	Vulns
10.66.35.175	windows-test.ad.cpost.cz	129	101	29 86

Přehled portů

Port	Info	Low	Med.	High	Crit.	Total
0	34	0	0	0	0	34
123	2	0	0	0	0	2
135	2	0	0	0	0	2
137	3	0	0	0	0	3
138	2	0	0	0	0	2
139	2	0	0	0	0	2
445	15	0	1	1	0	17
500	2	0	0	0	0	2
1900	2	0	0	0	0	2
3389	9	2	8	1	1	21
3702	2	0	0	0	0	2
4500	2	0	0	0	0	2
5355	3	0	0	0	1	4
49152	1	0	0	0	0	1
49153	1	0	0	0	0	1
49154	1	0	0	0	0	1
49155	1	0	0	0	0	1
49156	1	0	0	0	0	1
49158	1	0	0	0	0	1

Zranitelnosti - výčet

10.66.35.175

IP Address: 10.66.35.175
NetBIOS Name: WORKGROUP\WINDOWS-TEST
DNS Name: windows-test.ad.cpost.cz
OS CPE: cpe:/o:microsoft:windows_7:::professional
MAC Address: 00:0c:29:6f:0b:be
Score: 132
Repository: Test_polygon_Olše_MIMI

Počty zranitelností dle závažnosti

Severity	Count
Critical	2
High	2
Medium	9
Low	2
Info	86

Výpis zranitelností závažnosti: Critical, High

Plugin	Plugin Name	Severity
53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Critical
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Critical
55286	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275) (remote check)	High
58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High

QUALYSGUARD® ENTERPRISE SUITE

Scan Results

March 14, 2017

This report was generated with an evaluation version of Qualys

Michal Miklanek
ceska5mm
Manager

Ceska Posta s.p.
olšanská
Prague 13000
Czech Republic

03/14/2017 at 11:26:52 (GMT+0100)

Report Summary

Launch Date:	03/07/2017 at 13:48:16 (GMT+0100)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1488890713.32963
Scanner Appliances:	Miklanek (Scanner 9.1.27-1, Vulnerability Signatures 2.3.557-2)
Duration:	00:04:55
Authentication:	Windows authentication was successful for 1 host
Title:	Win_7_auth
Network:	Global Default Network
Asset Groups:	-
IPs:	10.66.35.175
Excluded IPs:	-
Option Profile:	Initial Options

Summary of Vulnerabilities

Total: 82 Security Risk (Avg): 5.0

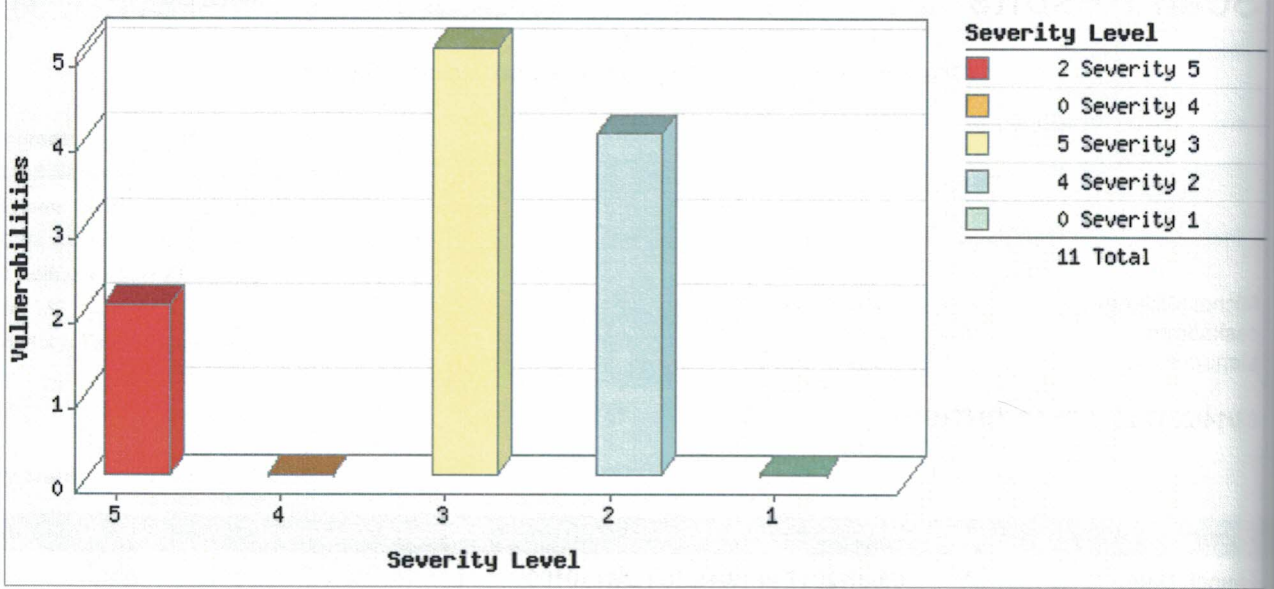
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	2	0	0	2
4	0	0	0	0
3	5	1	4	10
2	4	2	39	45
1	0	0	25	25
Total	**11**	**3**	**68**	**82**

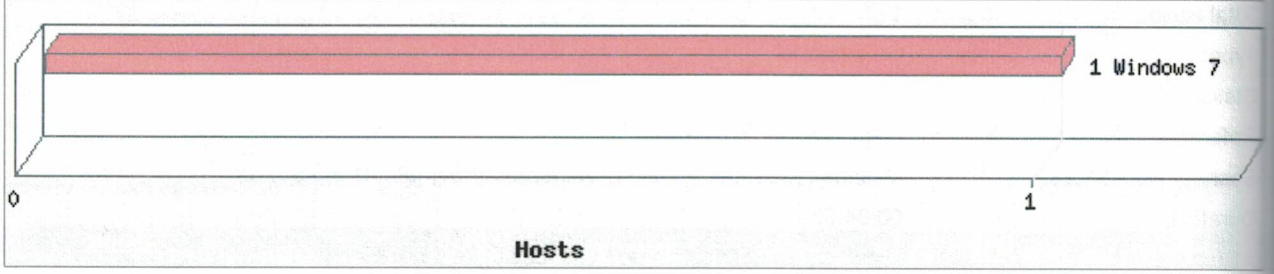
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Security Policy	2	1	32	35
Windows	4	1	5	10
Information gathering	0	1	9	10
General remote services	4	0	6	10
TCP/IP	0	0	8	8
Total	**10**	**3**	**60**	**73**

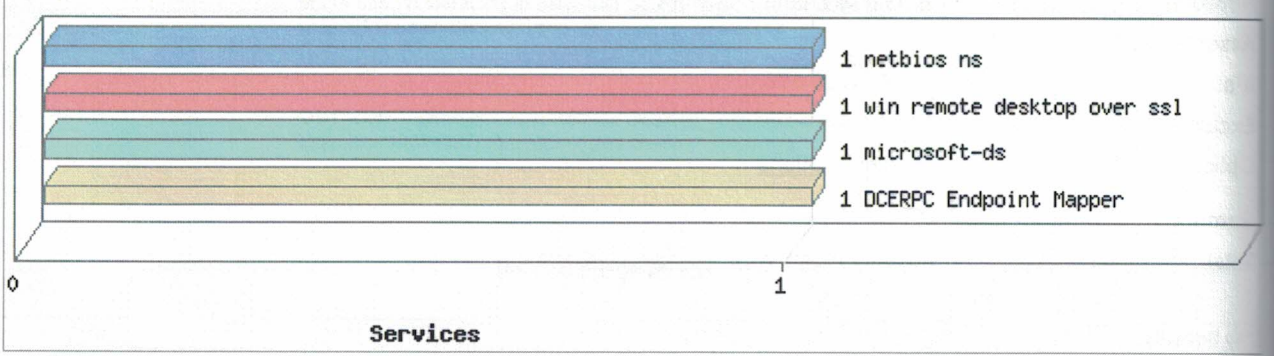
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

▼ 10.66.35.175 (windows-test, WINDOWS-TEST) - Global Default Network — Windows 7

▼ Vulnerabilities (11) ⊞⊟

▶ 5 Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability

		(MS12-020)	
▸	5	EOL/Obsolete Operating System: Microsoft Windows 7 RTM Detected	
▸	3	Administrator Account's Password Does Not Expire	
▸	3	Built-in Guest Account Not Renamed at Windows Target System	
▸	3	SSL/TLS use of weak RC4 cipher	port 3389/tcp over SSL
▸	3	SSL/TLS Server supports TLSv1.0	port 3389/tcp over SSL
▸	3	Windows Remote Desktop Protocol Weak Encryption Method Allowed	port 3389/tcp over SSL
▸	2	NetBIOS Name Accessible	
▸	2	Default Windows Administrator Account Name Present	
▸	2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 3389/tcp over SSL
▸	2	SSL Certificate - Signature Verification Failed Vulnerability	port 3389/tcp over SSL

▸ Potential Vulnerabilities (3) ⊞⊟

▸ Information Gathered (68) ⊞⊟

▾ Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

10.66.35.175

Target distribution across scanner appliances

Miklanek : 10.66.35.175

Windows authentication was successful for these hosts (1)

Instance os:
10.66.35.175

Options Profile

Initial Options

Scan Settings	
Ports	-
Scanned TCP Ports	Standard Scan
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Perform 3-way Handshake	Off
Vulnerability Detection	Complete
Password Brute Forcing	-
System	Disabled
Custom	Disabled
Authentication	-

Windows	Enabled
Unix/Cisco	Enabled
Oracle	Disabled
Oracle Listener	Disabled
SNMP	Disabled
VMware	Disabled
DB2	Disabled
HTTP	Disabled
MySQL	Disabled
Overall Performance	Normal
Additional Certificate Detection	Normal
Authenticated Scan Certificate Discovery	Disabled
Hosts to Scan in Parallel	-
Use Appliance Parallel ML Scaling	Off
External Scanners	15
Scanner Appliances	30
Processes to Run in Parallel	-
Total Processes	10
HTTP Processes	10
Packet (Burst) Delay	Medium
Port Scanning and Host Discovery	-
Intensity	Normal
Dissolvable Agent	-
Dissolvable Agent (for this profile)	Disabled
Windows Share Enumeration	Disabled
Windows Directory Search	Disabled
Lite OS Discovery	Disabled
Advanced Settings	
Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Packet Options	-
Ignore firewall-generated TCP RST packets	Off
Ignore all TCP RST packets	Off
Ignore firewall-generated TCP SYN-ACK packets	Off
Do not send TCP ACK or SYN-ACK packets during host discovery	Off

▸ Report Legend

This report was generated with an evaluation version of Qualys

Highest Risk Vulnerabilities

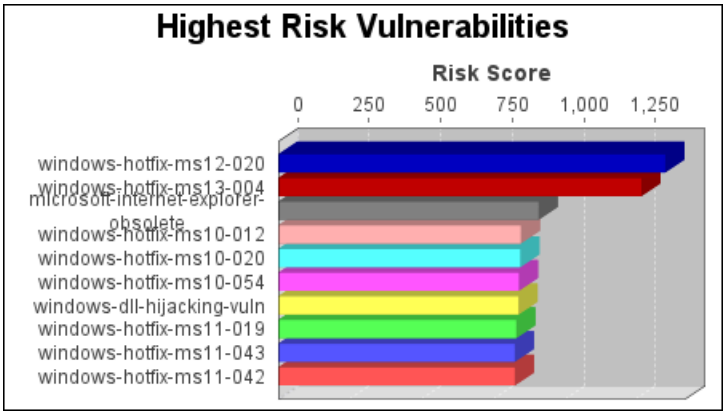
Asset report for 10.66.35.175

Audited on March 1, 2017

Reported on February 19, 2017

Table of Contents

1. Executive Overview



The windows-hotfix-ms12-020 vulnerability poses the highest risk to the organization with a risk score of 1,351. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

2. Highest Risk Vulnerability Details

2.1. MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (windows-hotfix-ms12-020)

Category	Microsoft, Microsoft Windows, Remote Execution, IAVM, Microsoft Patch
CVSS score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Risk Score	1,351
References	CERT: TA12-073A, CVE-2012-0002, CVE-2012-0152, DISA_SEVERITY: Category I, DISA_VMSKEY: V0031885, IAVM: 2012-A-0039, MS12-020, MSKB: 2671387, OVAL: OVAL14623, OVAL: OVAL14626

2.2. MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324) (windows-hotfix-ms13-004)

Category	Web, Microsoft, Microsoft .NET Framework, IAVM, Privilege Escalation, Microsoft Windows, Browsers, Microsoft Patch
CVSS score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Risk Score	1,268
References	CERT: TA13-008A, CVE-2013-0001, CVE-2013-0002, CVE-2013-0003, CVE-2013-0004, DISA_SEVERITY: Category I, DISA_VMSKEY: V0036453, IAVM: 2013-A-0006, MS13-004, MSKB: 2769324, OVAL: OVAL15814, OVAL: OVAL16339, OVAL: OVAL16343, OVAL: OVAL16381

2.3. Obsolete Version of Microsoft Internet Explorer (microsoft-internet-explorer-obsolete)

Category	Microsoft Internet Explorer, Obsolete Software, Microsoft, Browsers
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	909
References	URL: https://support.microsoft.com/lifecycle#gp/Microsoft-Internet-Explorer

2.4. MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) (windows-hotfix-ms10-012)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	847
References	CERT: TA10-040A, CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231, MS10-012, MSKB: 971468, OVAL: OVAL7751, OVAL: OVAL8314, OVAL: OVAL8438, OVAL: OVAL8524

2.5. MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232) (windows-hotfix-ms10-020)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	845
References	BID: 39336, CERT: TA10-103A, CVE-2009-3676, CVE-2010-0269, CVE-2010-0270, CVE-2010-0476, CVE-2010-0477, MS10-020, MSKB: 980232, OVAL: OVAL6859, OVAL: OVAL6918, OVAL: OVAL7129, OVAL: OVAL7164, OVAL: OVAL7186

2.6. MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (windows-hotfix-ms10-054)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	840
References	CERT: TA10-222A, CVE-2010-2550, CVE-2010-2551, CVE-2010-2552, MS10-054, MSKB: 982214, OVAL: OVAL11106, OVAL: OVAL12015, OVAL: OVAL12072

2.7. Windows DLL Hijacking Vulnerability (windows-dll-hijacking-vuln)

Category	Microsoft
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	839
References	MSKB: 2264107, URL: http://www.microsoft.com/technet/security/advisory/2269637.mspx

2.8. MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455) (windows-hotfix-ms11-019)

Category	Microsoft, Microsoft Windows, Remote Execution, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	831
References	BID: 46360, BID: 47239, CERT: TA11-102A, CERT-VN: 323172, CVE-2011-0654, CVE-2011-0660, MS11-019, MSKB: 2511455, OVAL: OVAL11995, OVAL: OVAL12637, XF: 65376

2.9. MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution (2536276) (windows-hotfix-ms11-043)

Category	Microsoft, Microsoft Windows, Remote Execution, IAVM, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Risk Score	826
References	CVE-2011-1268, DISA_SEVERITY: Category II, DISA_VMSKEY: V0028592, IAVM: 2011-A-0079, MS11-043, MSKB: 2536276, OVAL: OVAL12746

2.10. MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512) (windows-hotfix-ms11-042)

Category	Microsoft, Remote Execution, IAVM, Microsoft Patch
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	826
References	BID: 48180, BID: 48187, CVE-2011-1868, CVE-2011-1869, DISA_SEVERITY: Category I, DISA_VMSKEY: V0028593, IAVM: 2011-A-0087, MS11-042, MSKB: 2535512, OVAL: OVAL11758, OVAL: OVAL12640, XF: 67726, XF: 67727

Příloha č. 4.

Skenovací politika „PING sken“

PING SKEN

Název politiky: PING_sken

Ping sken slouží ke zjištění fakticky běžících aktiv v konkrétní síti.

Scan Options

Ovládání obecných pokročilých možností skeneru

General Settings

Enable Safe Checks	Nessus attempts to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When **Enable Safe Checks** is enabled, the second step is skipped. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.	✔
	Nessus se pokouší identifikovat vzdálené zranitelnosti na základě inforamcí z banerů a zkouší vykonat zranitelnost. Pokud je volba "Enable Safe Checks" zaputa, druhý krok je přeskočen. Není to tak spolehlivé, ale pro cílové aktivum je to přívětivější.	

Stop scanning hosts that become unresponsive during the scan	During a scan hosts may become unresponsive after a period of time. Enabling this setting stops scan attempts against hosts that stop sending results.	✔
	Během skenování se může stát, že po nějaké době přestane aktivum odpovídat. Při zaškrtnutí této volby bude skenování takového aktiva zastaveno.	

Performance Options

Slow down the scan when network congestion is detected	When Nessus detects congestion during a scan, it will slow the speed of the scan in an attempt to ease the burden on the affected segment(s).	✔
	Při zjištění přetížení během skenování zpomalí rychlost skenování.	

Use Linux kernel congestion detection	Use Linux kernel congestion detection during the scan to help alleviate system lockups on the Nessus scanner server.	⃠
	Použije detekci přetížení pro Linux kernel.	

Network Timeout (in seconds)	Determines the amount of time, in seconds, to determine if there is an issue communicating over the network.	5
	Určení doby v sekundách pro zjištění problému v síťové komunikaci.	

Max Simultaneous Checks Per Host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.	5
	Nastavení maximálního počtu kontrol puštěných na jedno aktivum.	

Max Simultaneous Hosts Per Scan	This setting limits the maximum number of hosts that a single Nessus scanner will scan at the same time. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the Max Hosts Per Scan option. For example, if the Max Simultaneous Hosts Per Scan is set to 5 and there are five scanners per zone, each scanner will accept five hosts to scan, allowing a total of 25 hosts to be scanned between the five scanners.	30
	Nastavení maximálního počtu počítačů, které bude jeden skener skenovat v jednom čase.	

Max number of concurrent TCP sessions per host	This setting limits the maximum number of TCP sessions established by any of the active scanners while scanning a single host.	⃠
	Maximální počet TCP spojení sestavených aktivním skenerem během skenování jednoho aktiva.	

Max number of concurrent TCP sessions per scan	This setting limits the maximum number of TCP sessions established by any of the active scanners during a scan.	unlimited
	Maximální počet TCP spojení sestavených jakýmkoliv z aktivních skenerů během skenování.	

Host Discovery

Nastavení možností "Discovery" skenu. (PING sken)		
Ping the remote host	When enabled, Nessus attempts to ping the hosts in the scan to determine if the host is alive or not.	✔
	Pokud je povoleno, Nessus zkouší *ping* , aby zjistil zda je aktivum naživu.	
General Settings (available when Ping the remote host is enabled)		
Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.	⃠
	Tato volba umožňuje zahrnout nebo vyloučit ze skenování vlastní stanici (Nessus skener). To se používá, pokud je Nessus skener umístěn ve stejné síti jako skenovaná aktiva.	
Use Fast Network Discovery	When Nessus "pings" a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1 - 65535 even when there is no service behind the device). Such checks can take some time, especially if the remote host is firewalled. If the "Use Fast Network Discovery" option is enabled, Nessus will not perform these checks.	✔
	Pokud Nessus "pingá" na vzdálenou IP adresu a obdrží odpověď, provede další extra kontrolu, aby se ujistil, že se nejedná o transparentní proxy nebo loadbalancer, který nevrací relevantní odpověď. Pokud je cíl za firewalem, můžou takové kontroly zabrat hodně času. Tato volba takové kontroly zakáže.	
Ping Methods (available when Ping the remote host is enabled)		
ARP	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.	✔
	Ping na MAC adresy. Použitelné pouze v lokální síti.	
TCP	Ping a host using TCP.	✔
	Ping pomocí protokolu TCP.	
Destination ports	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting on **built-in**.	built-in
	Je možné definovat specifické porty pro TCP ping. Pro výchozí nastavení je určena volna **built-in**	
ICMP	Ping a host using the Internet Control Message Protocol (ICMP).	✔
	Ping pomocí protokolu ICMP.	
Assume ICMP unreachable means the host is down	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When enabled, this option will consider this to mean the host is dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.	✔
	Pokud je ping poslán na aktivum, které je vypnuté, jeho brána může vrátit ICMP zprávu o nedostupnosti. To pomáhá urychlit rychlost objevování stanic v některých sítích. Při zaškrtnutí této volby bude obdržení "ICMP unreachable" vyhodnoceno jako nedostupné aktivum. Stejné chování však mohou vykazovat některé firewally nebo paketové filtry. Pak se některé stanice mohou chovat jako nedostupné, ačkoliv jsou zapnuté.	
Maximum Number of Retries (ICMP enable)	Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.	2
	Volba umožňuje specifikovat počet pokusů, kolikrát bude *ping* poslán na cílové aktivum. Výchozí hodnota je 2.	
UDP	Ping a host using the User Datagram Protocol (UDP). Tip: UDP is a "stateless" protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.	⃠
	Ping pomocí protokolu UDP. Tip: UDP je nestavový protokol, což znamená, že komunikace není prováděna pomocí "handshake" dialogu. Komunikace na bázi UDP není vždy spolehlivá. Z podstaty UDP nejsou služby a skenované zařízení vždy na dálku spolehlivě zjistitelné.	
Fragile Devices		
Scan Network Printers	Instructs the Nessus scanner not to scan network printers if unselected. Since many printers are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal síťové tiskárny, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tiskárny, které již jednou identifikoval. To je doporučeno v produkčních sítích.	
Scan Novell Netware Hosts	Instructs the Nessus scanner not to scan Novel Netware hosts if unselected. Since many Novell Netware hosts are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal Novel Netware stroje, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tato zařízení, které již jednou identifikoval. To je doporučeno v produkčních sítích.	
Wake-on-LAN		
List of MAC addresses	Wake on Lan (WOL) packets will be sent to the hosts listed, one on each line, in an attempt to wake the specified host(s) during a scan.	⃠
	Skener může během skenování pomocí WOL paketů vzbudit síťová zařízení, která budou uvedena zde na seznamu.	
Boot time wait (in minutes)	The number of minutes Nessus will wait to attempt a scan of hosts sent a WOL packet.	⃠
	Nastavení počtu minut, jak dlouho má skener čekat po poslání WOL paketu.	
Network Type		
Network Type	Allows you to specify if you are using publicly routable IPs, private non-Internet routable IPs or a mix of these. Select "Mixed" if you are using RFC 1918 addresses and have multiple routers within your network.	mix
	Dovoluje specifikovat typ sítě LAN WAN MIX	

Port Scanning

Nastavení možností port skenu

Ports

Consider Unscanned Ports as Closed	If a port is not scanned with a selected port scanner (e.g., out of the range specified), The scanner will consider it closed.	⃠
	Při této volbě budou neoskenované porty považovány za zavřené.	

Port scan range	Directs the scanner to target a specific range of ports. Accepts "default" (a list of approximately 4,790 common ports found in the nessus-services file), "all" (scans all ports from 0-65535), or a custom list of ports specified by the user. The custom list may contain individual ports and ranges; for example, "21,23,25,80,110" and "1-1024,8080,9000-9200" are valid values. Specifying "1-65535" will scan all ports.	⃠
	Specifikace portů, které mají být skenovány. - "default" - Výchozí nastavení je 4790 běžných portů definovaných v servisních souborech Nessus. - "all" - všechny porty 0-65535 - vlastní definice (viz uvedené příklady)	

Local Port Enumerators

SSH (netstat)	This option uses netstat to check for open ports on the target host. It relies on the netstat command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.	⃠
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes SSH spojení na skenovaném aktivu. Tento sken je zamýšlený pro UNIXové systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	

WMI (netstat)	This option uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials	⃠
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes WMI spojení na skenovaném aktivu. Tento sken je zamýšlený pro Windows systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	

SNMP	Direct Nessus to scan targets for a SNMP service. Nessus will guess relevant SNMP settings during a scan. If the settings are provided by the user under "Preferences", this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.	⃠
	Nasměruje Nessus na služby SNMP u skenovaných aktiv. Nessus se pokusí odhadnout SNMP nastavení během skenování. Pokud jsou nastavení poskytnuta uživatelem s vyšším oprávněním, umožní to skeneru lépe otestovat vzdálené aktivum a zajistí lepší a detailnější výsledky. Existuje mnoho kontrol pro Cisco routery, které určují přítomnost zranitelností na základě vráceného SNMP řetězce.	

Only run network port scanners if local port enumeration failed	Rely on local port enumeration first before relying on network port scans.	⃠
	V první řadě se skener pokusí vyčíst porty lokálně, před tím než začne porty na aktivu skenovat.	

Verify open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).	⃠
	Pokud výčet lokálních portů najde otevřený port, Nessus si ověří, zda je otevřen i na dálku. Pomůže to určit, zda je použita nějaká forma řízení přístupu (např. TCP wrappers, firewall)	

Network Port Scanners

TCP	Use Nessus' built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features. **Note:** On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner instead.	⃠
	Použije Nessus vestavěný TCP skener pro zjištění otevřených TCP portů na cílovém aktivu. Tento skener je optimalizován a má určité samoladící funkce. Poznámka: Pokud na některých platformách (např. Windows, MacOS) TCP skener způsobí vážné problémy s výkonem, Nessus místo něj zahájí SYN skener.	

SYN	Use Nessus' built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and then determines port state based on a reply – or lack of.	⃠
	Použije Nessus vestavěný SYN skener pro identifikaci TCP portů na cílovém aktivu. SYN sken je oblíbená metoda pro provádění skenování portů a obecně je považována za méně rušivou než TCP sken. Skener posílá SYN pakety na port a čeká na SYN-ACK odpověď a podle odpovědi určí stav portu.	

Override automatic firewall detection	Automatic (normal) Do not detect RST rate limitation (soft) Ignore closed ports (agressive) Disabled (softer)	normal
	Míra potlačení automatické detekce firewallu.	

UDP	This option engages Nessus' built-in UDP scanner to identify open UDP ports on the targets. **Tip:** UDP is a "stateless" protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable. Utilizing the UDP scanner will noticeably increase scanning time.	⃠
	Tato volba se zabývá vestavěným Nessus UDP skenerem pro identifikaci otevřených UDP portů na skenovaném aktivu. **Tip:** UDP je nestavový protokol, komunikace tedy není prováděna přes "handshake" dialog. Komunikace založená na UDP není spolehlivá a vzhledem k povaze UDP služeb není vždy vzdáleně zjistitelná. Využití UDP skeneru výrazně zvýší čas skenování.	

Service Discovery

Nastavení možností skenování běžících služeb na cílových portech		
Probe all ports to find services	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.	
	Pokusy o mapování každého otevřeného portu se službou, která běží na tomto portu. Pamatujte, že ve výjimečných případech to může narušit některé služby a způsobit vedlejší účinky.	
Search for SSL based services	Controls how Nessus will test SSL based services: known SSL ports (e.g., 443), all ports, or none. Testing for SSL capability on all ports may be disruptive for the tested host.	
	Určuje, jak bude Nessus testovat služby založené na protokolu SSL: Známé SSL porty (například 443), všechny porty, nebo žádné. Testování na schopnost SSL na všech portech může být rušivé pro testované aktivum.	
Search for SSL on	If selected, choose between Known SSL ports (e.g., 443) and All ports. Testing for SSL capability on all ports may be disruptive for the tested host.	
	Výběr mezi známými porty (např. 443) a všemi porty.	
Identify certificates expiring within x days	Identifies SSL certificates that will expire within the specified timeframe. Enter a value to set a timeframe (in days).	
	Identifikuje SSL certifikáty, které expirují během specifikovaného časového úseku. Vložte hodnotu časového úseku ve dnech.	
Enumerate all SSL ciphers	When SecurityCenter performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.	
	Pokud skener provádí SSL sken pokusí se zjistit SSL šifru použitou na skenovaném aktivu tak, že se pokusí sestavit spojení různými dokumentovanými SSL šiframi, bez ohledu na to, co dává skenované aktivum k dispozici.	
Enable CRL checking (connects to the Internet)	Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL). Enabling this option will make a connection and query one or more servers on the internet.	
	Kontrola SSL certifikátů proti CRL v internetu.	

Values for Assessment Options

Možnosti vyhodnocování informací získaných během skenování

Accuracy

Override normal accuracy	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to “Paranoid” then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of “Avoid false alarms” will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not changing from “Normal” is a middle ground between these two settings.	normal
	V některých případech Nessus nemůže určit, zda je přítomna vada, či nikoliv. Nastavení "Paranoid" zajistí reportování i v tom případě, pokud existují pochybnosti o výsledku. Naopak volba "Avoid false alarms" (vyhnout se falešným poplachům) způsobí, že Nessus nebude hlásit žádnou chybu, pokud existuje náznak nejistoty.Výchozí volba "Normal" je střední cesta mezi těmito dvěma volbami.	

Perform thorough tests (may disrupt your network or impact scan speed)	Causes various plugins to use more aggressive settings. For example, when looking through SMB file shares, a plugin can analyze 3 directory levels deep instead of its default of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially providing better audit results.	⃠
	Volba způsobí více agresivní nastavení pluginů. Například při hledání SMB sdílení souborů může plugin analyzovat 3 úrovně adresářů místo výchozí hodnoty 1. To může mít za důsledek větší provoz v síti. Sken bude více rušivý, ale bude poskytovat lepší hodnoty výsledku.	

Antivirus

Antivirus definition grace period (in days)	This option determines the delay in the number of days of reporting the software as being outdated. The valid values are between 0 (no delay, default) and 7.	⃠
	Tato volba určuje zpoždění v počtu dnů od nahlášení zastaralého software. Hodnoty se pohybují od 0 (žádná prodleva, výchozí) do 7	

SMTP

Third Party Domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.	⃠
	Nessus se pokusí posílat spam skrz každé SMTP zařízení na adresu vepsanou do tohoto pole. Doménové adresa třetí strany musí být mimo síť, která je skenována. V opačném případě může test poškodit SMTP server.	

From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.	⃠
	Testovací zprávy poslané na server SMTP se budou jevit jako poslané z této adresy.	

To Address	Nessus will attempt to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.	⃠
	Nessus se pokusí posílat zprávy na adresu uvedenou v tomto poli. "postmaster" je výchozí hodnota, protože je platná na většině poštovních serverů.	

Values for Brute Force Options

Řízení skenování hrubou silou, možnosti použití nástroje Hydra

General Settings

Only use credentials provided by the user	In some cases, Nessus can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Nessus from performing these tests.	
	V některých případech může Nessus vyzkoušet výchozí účty a jejich známá výchozí hesla. To může způsobit zamčení účtu, pokud vznikne mnoho po sobě jdoucích neplatných pokusů o přihlášení. Ve výchozím nastavení má Nessus tyto testy zakázány.	⃠

Oracle Database

Test default Oracle accounts (slow)	Test for known default accounts in Oracle software.	
	Test na přítomnost známých stadardních účtů v software Oracle.	⃠

Hydra

Always enable Hydra (slow)	Enables Hydra whenever the scan is performed.	
	Umožňuje použít nástroj Hydra (prolamovač hesel) kdykoliv je provedena kontrola.	⃠
Logins file	A file that contains user names that Hydra will use during the scan.	
	Soubor obsahující uživatelská jména, která použije nástroj Hydra.	⃠
Passwords file	A file that contains passwords for user accounts that Hydra will use during the scan.	
	Soubor obsahující hesla, která použije nástroj Hydra.	⃠
Number of parallel tasks	The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.	
	Počet současných Hydra testů. Výchozí nastavení je 16.	⃠
Timeout (in seconds)	The number of seconds per logon attempt.	
	Počet sekund na přihlašovací pokus.	⃠
Try empty passwords	If enabled, Hydra will additionally try user names without using a password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také prázdné heslo.	⃠
Try login as password	If enabled, Hydra will additionally try a user name as the corresponding password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také stejné heslo jako uživatelské jméno.	⃠
Stop brute forcing after the first success	If enabled, Hydra will stop brute forcing user accounts after the first time an account is successfully accessed.	
	Pokud bude tato volba zaškrtnuta, Hydra zastaví prolamování hesla po prvním úspěšném přístupu.	⃠
Add accounts found by other plugins to the login file	If disabled, only the user names specified in the logins file will be used for the scan. Otherwise, additional user names discovered by other plugins will be added to the logins file and used for the scan.	
	Při zakázání této volby budou použita jen uživatelská jména specifikovaná v souboru se jmény. Při povolení této volby budou přidána uživatelská jména nalezená ostatními pluginy.	⃠
PostgreSQL database name	The database that you want Hydra to test.	
	Jméno databáze pro Hydra test.	⃠
SAP R/3 Client ID (0 - 99)	The ID of the SAP R/3 client that you want Hydra to test.	
	SAP R/3 klient pro Hydra test.	⃠
Windows accounts to test	Can be set to *Local accounts* , *Domain Accounts* , or *Either* .	
	Může být nastaveno *Local accounts* , *Domain Accounts* , nebo *Either* .	⃠
Interpret passwords as NTLM hashes	If enabled, Hydra will interpret passwords as NTLM hashes.	
	Pokud je povoleno, Hydra bude interpretovat hesla jako NTLM hash.	⃠
Cisco login password	This password is used to login to a Cisco system before brute forcing enable passwords. If no password is provided here, Hydra will attempt to login using credentials that were successfully brute forced earlier in the scan.	
	Toto heslo je použito pro přihlášení na Cisco systémy před zkušením hesla hrubou silou. Pokud tu není žádné heslo poskytnuto, Hydra bude zkoušet přihlašovací údaje, které zjistila v předchozích skenech.	⃠
Web page to brute force	Enter a web page that is protected by HTTP basic or digest authentication. If a web page is not provided here, Hydra will attempt to brute force a page discovered by the Nessus web crawler that requires HTTP authentication.	
	Webová stránka pro útok hrubou silou nástrojem Hydra.	⃠
HTTP proxy test website	If Hydra successfully brute forces an HTTP proxy, it will attempt to access the website provided here via the brute forced proxy.	
	Pokud Hydra úspěšně prolomí proxy, bude zkoušet přistoupit na tuto HTTP stránku přes proxy.	⃠
LDAP DN	The LDAP Distinguish Name scope that Hydra will authenticate against.	
	LDAP DN jméno, proti kterému se bude Hydra autentizovat.	⃠

Settings/Assessment/Malware

Nastavení možností testování na Malware, použití známých MD5 hash

General Settings

Disable DNS Resolution	Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.	
	Tato volba zabrání Nessus skeneru používat cloud pro porovnávání nálezů skenu proti známému škodlivému softwaru. Výchozí stav je vypnuto - tedy hledání v cloudu povoleno.	

Hash and Whitelist Files

Provide your own list of known bad MD5 hashes	Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash the description will show up in the scan results.	
	Další známé špatné MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Provide your own list of known good MD5 hashes	Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description will show up in the scan results.	
	Další známé dobré MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Hosts file whitelist	Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check). This option allows you to upload a file containing a list of IPs and hostnames that will be ignored by Nessus during a scan. Include one IP and hostname (formatted identically to your hosts file on the target) per line in a regular text file.	
	Tato možnost vám umožní nahrát soubor obsahující seznam IP adres a aktiv, které budou během skenování skenerem ignorovány. Soubor musí obsahovat jednu IP a hostname na řádek v běžném textovém souboru.	

File System Scanning

Možnosti nastavení skenování souborového systému		
File System Scanning		
Scan File System	Turning on this option allows you to scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.	
	Zapnutí této volby umožňuje skenovat systémové adresáře a soubory na skenovaném aktivu. Upozornění: Povolení tohoto nastavení při zacílení na 10 a více hostů může snížit výkon.	
Directories		
Scan %Systemroot%	Enable file system scanning to scan %Systemroot%	
	Povolí skenovat %Systemroot%	
Scan %ProgramFiles%	Enable file system scanning to scan %ProgramFiles%	
	Povolí skenovat %ProgramFiles%	
Scan %ProgramFiles(x86)%	Enable file system scanning to scan %ProgramFiles(x86)%	
	Povolí skenovat %ProgramFiles(x86)%	
Scan %ProgramData%	Enable file system scanning to scan %ProgramData%	
	Povolí skenovat %ProgramData%	
Scan User Profiles	Enable file system scanning to scan user profiles	
	Povolí skenovat uživatelské profily	
Custom Filescan Directories	Add File Add a custom file that list directories for malware file scanning. List each each directory on one line. **Caution:** Root directories such as 'C:\' or 'D:\' are not accepted.	
	Je možné přidat vlastní adresáře pro skenování na malware. Do textového souboru je napsán každý adresář na jeden řádek. Kořenové adresáře jako C:\ nejsou akceptovány.	
Yara Rules Files		
	Nástroj na identifikaci a klasfikaci malware	

Values for SCADA Options

Tato volba umožňuje ovlivnit možnosti skenování průmyslových SCADA zařízení.		
Modbus/TCP Coil Access		
Start at register End at register	These options are available for commercial users. This drop-down menu item is dynamically generated by the SCADA plugins available with the commercial version of Nessus. Modbus uses a function code of 1 to read "coils" in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a "write coil" message. The defaults for this are "0" for the "Start reg" and "16" for the "End reg".	
ICCP/COTP TSAP Addressing Weakness		
Start COTP TSAP Stop COTP TSAP	The "ICCP/COTP TSAP Addressing" menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to "8" by default.	

Values for Web Applications Options

Nastavení skenování webových aplikací

Web Application Settings

Scan web applications	Enables the **General Settings**, **Web Crawler**, and **Application Test** Settings sections.	
	Zapnutí skenování webových aplikací.	

General Settings

Use a custom User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.	
	Určuje, za jaký typ internetového prohlížeče se bude Nessus vydávat.	

Web Crawler

Start crawling from	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., "/:/php4:/base").	
	Adresa URL, která bude první testována. Pokud je potřeba více stránek, použijte jako oddělaovač dvojtečku (např. /:/php4:/base)	

Excluded pages (regex)	Enable exclusion of portions of the web site from being crawled. For example, to exclude the "/manual" directory and all Perl CGI, set this field to: (^/manual)|(\.pl(\?.*)?$). Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).	
	Dovoluje vyloučit části webu, kterými skener prochází. Například pro vyloučení adresáře "/manual" a všech Perl CGI nastavte do tohoto pole (^/manual)|(\.pl(\?.*)?$). Nessus podporuje regulární výrazy POSIX stejně jako Perl regulární výrazy PCRE.	

Maximum pages to crawl	The maximum number of pages to crawl.	
	Maximální počet stránek, které se mají procházet.	

Maximum depth to crawl	Limit the number of links Nessus will follow for each start page.	
	Omezení počtu odkazů, které bude Nessus následovat za každou úvodní stránkou.	

Follow dynamic pages	If selected, Nessus will follow dynamic links and may exceed the parameters set above.	
	Pokud je zaškrtnuto, Nessus bude následovat dynamické vazby a může přesáhnout parametry uvedené výše.	

Application Test Settings

Enable generic web application tests	Enables the options listed below.	
	Povolí aplikační testy vypsané dále.	

Abort web application tests if HTTP login fails	If Nessus cannot login to the target via HTTP, then do not run any web application tests.	
	Pokud se Nessus nemůže přihlásit k aktivu přes HTTP, pak nepustí žádné další aplikační testy.	

Try all HTTP Methods	This option will instruct Nessus to also use "POST requests" for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Nessus will test each script/variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.	
	Nessus bude krom GET požadavků (výchozí nastavení) zkoušet také POST požadavky. Obecně platí, že složitější aplikace používají metody POST pro posílání uživatelských dat do aplikace. Toto nastavení poskytuje důkladnější testování, ale může značně navýšit potřebný čas. Pokud je toto zaškrtnuto, Nessus bude testovat každou proměnnou, kterou najde ve skriptu na obě metody GET i POST.	

Attempt HTTP Parameter Pollution	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like "/target.cgi?a='&b=2". With HTTP Parameter Pollution (HPP) enabled, the request may look like "/target.cgi?a='&a=1&b=2".	
	Při provádění testů webových aplikací zkouší obejít filtrovací mechanismy vkládáním obsahu do proměnných a zároveň poskytuje stejné proměnné se správným obsahem. Například normální SQL-injection test může vypadat takto: "/target.cgi?a='&b=2" S volbou HTTP Parameter Pollution může vypadat takto: "/target.cgi?a='&a=1&b=2"	

Test embedded web servers	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.	
	Vestavěné webové servery jsou často statické a neobsahují nastavitelné CGI skripty. Krom toho mohou být náchylné k selhání nebo přestanou reagovat během skenování. Proto Tenable doporučuje skenování vestavěných web serverů odděleně od ostatních webů pomocí této volby.	

Test more than one parameter at a time per form	This option manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This drop-down has five options: One value - This tests one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. Some pairs – This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters. All pairs (slower but efficient) – This form of testing is slightly slower but more efficient than the "one value" test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt "/test.php?a=XSS&b=1&c=1&d=1" and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for "/test.php?a=XSS&b=3&c=3&d=3" when the first value of each variable is "1". Some combinations – This form of testing will randomly check a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time. All combinations (extremely slow) – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where "All-pairs" testing seeks to create a smaller data set as a tradeoff for speed, "all combinations" makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.	
	Tato volba řídí kombinaci hodnot argumentu použitých v HTTP dotazu. Výchozí stav (bez hodnoty) testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Toto rozbalovací pole má pět voleb: One Value - testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Some pairs - Tato forma testování bude náhodně kontrolovat kombinace náhodných párů parametrů. Toto je nejrychlejší cesta, jak otestovat více parametrů. All pairs - (pomalejší, ale efektivnější, než volba "One Value") Some combinations - tato forma testování bude náhodně zkoušet kombinaci tří nebo více parametrů. Bude to trvat déle. All combinations (extrémně pomalé) - Tato metoda bude zkoušet naprosto všechny možné kombinace útočných řetězců s platným vstupem do proměnných. Tento zůsob může trvat velice dlouho.	

Do not stop after the first flaw is found per web page	This option determines when a new flaw is targeted. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless "thorough tests" is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack. The drop-down has four options: Per CGI – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option. Per port (quicker) – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. Per parameter (slow) – As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server. Look for all flaws (slower) – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.	
	Tato volba určuje, kdy je nová chyba zaměřena. To platí na úrovni skriptu. Nalezení XSS chyby nezakáže hledání po SQL-injection nebo "header injection", ale budete mít nanejvýš jednu zprávu pro každý typ na daném portu. Toto pole má čtyři možnosti: Per CGI - Jakmile je skriptem nalezena chyba na CGI, Nessus přepne na další známé CGI na stejném serveru, nebo pokud není jiné CGI, tak na další port/službu. Toto je výchozí volba. Per port (rychlejší) - Jakmile je skriptem nalezena chyba na weobvé službě, Nessus zastaví a přepne se na jinou webovou službu na jiném portu. Per parameter (pomalé) - Jakmile je jeden typ chyby nalezen v parametru CGI (např. XSS) Nessus se přepne na další parametr ze stejné CGI nebo další známou CGI, nebo další port/službu. Look for all flaws (pomalejší) - Provede rozsáhlé testy bez ohledu na zjištěné chyby, Tato volba může vyprodukovat velice obsáhlý a upovídaný report. Tato volba není ve většině případů doporučována.	

URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.	
	URL adresa pro RFI. Zde se specifikuje souboru pro Remote File Inclusion. Ve výchozím nastavení Nessus použije bezpečný soubor hostovaný u výrobce pro RFI testování. Pokud není dostupný internet, bude použit lokální soubor, který určen pro přesnější testování RFI.	

Maximum run time (minutes_)	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.	
	Tato volba řídí množství času v minutách strávených prováděním testů webových aplikací. Standardně je nastavneno na 60minut a platí pro všechny porty a CGI pro dané webové stránky. Skenování v lokálních sítích s malými webovými aplikacemi bude obvykle dokončena za méně než hodinu, nicméně webové stránky s velkými aplikacemi mohou pžadovat vyšší hodnotu.	

Values for Windows Scan Options

Základní nastavení pro Windows

General Setting

Request information about the SMB Domain	If the option Request information about the domain is set, then domain users will be queried instead of local users. Pokud je volba zaškrtnuta, budou dotazování doménoví uživatelé místo lokálních.	

Enumerate Domain User

Start UID	1000
End UID	1200

Enumerate Local User

Start UID	1000
End UID	1200

Values for Scan Report Options

Nastavení možností reportování		
Processing		
Report Verbosity	Determines the verbosity of the detail in the output of the scan results as Normal, Quiet, or Verbose.	normal
	Určuje míru detailu výstupu skenů. K dispozci jsou tři volby "Normal", "Quite", "Verbose"	
Show missing patches that have been superseded	Show patches in the report that have not been applied but have been superseded by a newer patch if enabled.	✔
	Pokud je volba zapnutá, zobrazí v reportu záplaty, které nebyly aplikovány, ale byly nahrazeny novější záplatou.	
Hide results from plugins initiated as a dependency	If a plugin is only run due to it being a dependency of a selected plugin, hide the results if enabled.	✔
	Skryje výsledky z pluginů, které jsou spuštěny v závislosti na jiných.	
Output		
Designate hosts by their DNS name	When possible, designate hosts by their DNS name rather than IP address in the reports.	✔
	Pokud je to možné, určit aktivum podle DNS jména, nikoliv podle IP adresy.	
Display hosts that respond to ping	When enabled, show a list of hosts that respond to pings sent as part of the scan.	✔
	Pokud je povoleno, zobrazí seznam aktiv, které odpoví na PING jako součást skenu.	
Display unreachable hosts	Display a list of hosts within the scan range that were not able to be reached during the scan, if enabled.	⃠
	Pokud je povoleno, zobrazí seznam aktiv, které jsou během skenu nedostupné.	
Generate SCAP XML Results	Generate a SCAP XML results file as a part of the report output for the scan.	⃠
	Generovat SCAP XML souboru jako součást skenu.	

Value for Authentication Options

Nastavení možností autentizace použité během skenování		
Authentication	When added, authentication methods may be used to login to the scan target machines to gather more complete results of the host's status. The authentication types include host, database, miscellaneous, plaintext authentication, and patch management. For each type, various relevant options are presented such as SNMPv3, MongoDB, VMWare APIs, and similar.	
	Možnost přidání další vlastní autentizační metody.	⃠
SNMP		
UDP Port	This is the UDP port that will be used when performing certain SNMP scans. Up to four different ports may be configured, with the default port being 161.	
	UDP port pro provádění SNMP skenů. Až čtyři různé porty mohou být definovány.	161
SSH		
known_hosts file	If an SSH known_hosts file is provided for the scan policy in the "known_hosts file" field, Nessus will only attempt to log in to hosts defined in this file. This helps to ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.	
	Pokud je skenovací politice poskytnut soubor "known_hosts", Nessus se bude pokoušet hlásit jen na aktiva uvedená v tomto souboru. (v souboru "know_hosts" budou uvedeny veřejné klíče - SSH fingerprinty - těchto aktiv). To pomáhá zajistit, že přihlašovací údaje, které používáte na své známé SSH servery nebudou použity k pokusu o přihlášení do systému, který nemusí být pod Vaší kontrolou. (např. honeypoty).	⃠
Preferred port	This option is set to direct the scan to connect to a specific port if SSH is known to be listening on a port other than the default of 22.	
	Pokud by SSH naslouchalo na jiném než standardním portu, pak by se jiný port nastavil zde.	22
Client Version	Specifies which type of SSH client to impersonate while performing scans.	
	Specifikuje, jaký typ SSH klienta bude během skenu představen.	OpenSSH_5.0
Windows		
Never send credentials in the clear	By default, Windows credentials are not sent to the target host in the clear.	
	Ve výchozím nastavení (zaškrtnuto) nejsou posílány přihlašovací údaje do Windows v otevřeném tvaru.	✔
Do not use NTLMv1 authentication	If the "Do not use NTLMv1 authentication" option is disabled, then it is theoretically possible to trick Nessus into attempting to log in to a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a "hash" obtained from Nessus. This "hash" can be potentially cracked to reveal a username or password. It may also be used to directly log in to other servers. Because NTLMv1 is an insecure protocol this option is enabled by default.	
	Pokud je volba ""Do not use NTLMv1 authentication" zakázána, je teoreticky možné přimět Nessus, aby se pokusil přihlásit k Windows serveru s doménovými přihlašovacími údaji pomocí NTLM verze 1. To poskytuje vzdálenému útočníkovi možnost použít "hash" obdržený z Nessus. Tento "hash" může být potencionálně zneužit jako jméno a heslo. Též to může být použito k přímému přihlášení na další servery. Protože je NTLM v. 1 nebezpečný protokol, je tato volba ve výchozím stavu povolena.	✔
Start the Remote Registry service during the scan	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.	
	Tato volba říká Nessusu, aby nastartoval službu Vzdálený registr (Remote Registry service) na skenovaném aktivu, pokud tato služba neběží. Tato služba je nezbytná pro vykonání některých Windows kontrol.	✔
Enable administrative shares during the scan	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.	
	Tato volba dovolí skeneru přistoupit k určitým položkám v registru, které lze číst je s oprávněním správce.	✔
Plaintext Authentication		
Perform patch audits over telnet	When enabled, patch audits will be permitted over a telnet connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	
	Pokud je toto povoleno, bude sken povolen přes TELNET spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	⃠
Perform patch audits over rsh	When enabled, patch audits will be permitted over a rsh connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	
	Pokud je toto povoleno, bude sken povolen přes RSH spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	⃠
Perform patch audits over rexec	When enabled, patch audits will be permitted over a rexec connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	
	Pokud je toto povoleno, bude sken povolen přes REXEC spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	⃠
HTTP		
Login method	Specify if the login action is performed via a GET or POST request.	
	Speifikace přihlašovací metody pro HTTP (GET/POST)	POST
Re-authenticate delay (seconds)	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.	
	Časová prodleva mezi pokusy o přihlášení. Tato volba je použitelná při obcházení zamykacího mechanismu.	0
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.	
		0
Invert authenticated regex	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., "Authentication failed!").	
	Na přihlašovací stránce bude Nessus hledat řetězec o neúspěšném přihlášení. (např. Authentication failed).	⃠
Use authenticated regex on HTTP headers	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.	
	Hledání výsledku autentizace v HTTP hlavičce.	⃠
Case insensitive authenticated regex	The regex searches are case sensitive by default. This instructs Nessus to ignore case.	
		⃠

Plugins

Skenovací zásuvné moduly nebo-li "pluginy" jsou jednotlivé dílčí kontroly prováděné během skenu. Jsou řazeny do skupin (family) podle platformy.
Pokud jsou vybrány všechny kontroly, Nessus na skenované aktivum aplikuje jen ty kontroly, které odpovídají danému operačnímu systému.
Pokud chceme získat výsledky pouze z některých konkrétních kontrol, označíme jen ty, které se mají během skenu vykonat.

Zapnuty všechny	⃠
Vypnuty všechny	✔
Specifický vběr	⃠

Plugin ID	Plugin Family	Název

Compliance

Tzv. "Compliance" skeny umožňují importovat vlastní auditní soubor, který definuje další jednotlivé kontroly, které např. vychází z vlastních bezpečnostních politik, nebo např. z obecně platného standardu CIS.

Použití auditního souboru		⃠

Příloha č. 5.

Skenovací politika „AUTH sken“

AUTH SKEN

Název politiky: AUTH_sken

Auth sken slouží ke kontrole, zda se podařilo skeneru přihlásit na cílové aktivum s dostatečným oprávněním.

Scan Options

Ovládání obecných pokročilých možností skeneru

General Settings

Enable Safe Checks	Nessus attempts to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When **Enable Safe Checks** is enabled, the second step is skipped. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.	✔
	Nessus se pokouší identifikovat vzdálené zranitelnosti na základě inforamcí z banerů a zkouší vykonat zranitelnost. Pokud je volba "Enable Safe Checks" zaputa, druhý krok je přeskočen. Není to tak spolehlivé, ale pro cílové aktivum je to přívětivější.	

Stop scanning hosts that become unresponsive during the scan	During a scan hosts may become unresponsive after a period of time. Enabling this setting stops scan attempts against hosts that stop sending results.	⃠
	Během skenování se může stát, že po nějaké době přestane aktivum odpovídat. Při zaškrtnutí této volby bude skenování takového aktiva zastaveno.	

Performance Options

Slow down the scan when network congestion is detected	When Nessus detects congestion during a scan, it will slow the speed of the scan in an attempt to ease the burden on the affected segment(s).	⃠
	Při zjištění přetížení během skenování zpomalí rychlost skenování.	

Use Linux kernel congestion detection	Use Linux kernel congestion detection during the scan to help alleviate system lockups on the Nessus scanner server.	⃠
	Použije detekci přetížení pro Linux kernel.	

Network Timeout (in seconds)	Determines the amount of time, in seconds, to determine if there is an issue communicating over the network.	5
	Určení doby v sekundách pro zjištění problému v síťové komunikaci.	

Max Simultaneous Checks Per Host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.	5
	Nastavení maximálního počtu kontrol puštěných na jedno aktivum.	

Max Simultaneous Hosts Per Scan	This setting limits the maximum number of hosts that a single Nessus scanner will scan at the same time. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the Max Hosts Per Scan option. For example, if the Max Simultaneous Hosts Per Scan is set to 5 and there are five scanners per zone, each scanner will accept five hosts to scan, allowing a total of 25 hosts to be scanned between the five scanners.	30
	Nastavení maximálního počtu počítačů, které bude jeden skener skenovat v jednom čase.	

Max number of concurrent TCP sessions per host	This setting limits the maximum number of TCP sessions established by any of the active scanners while scanning a single host.	
	Maximální počet TCP spojení sestavených aktivním skenerem během skenování jednoho aktiva.	

Max number of concurrent TCP sessions per scan	This setting limits the maximum number of TCP sessions established by any of the active scanners during a scan.	unlimited
	Maximální počet TCP spojení sestavených jakýmkoliv z aktivních skenerů během skenování.	

Host Discovery

Nastavení možností "Discovery" skenu. (PING sken)		
Ping the remote host	When enabled, Nessus attempts to ping the hosts in the scan to determine if the host is alive or not.	✔
	Pokud je povoleno, Nessus zkouší *ping* , aby zjistil zda je aktivum naživu.	

General Settings (available when Ping the remote host is enabled)		
Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.	⃠
	Tato volba umožňuje zahrnout nebo vyloučit ze skenování vlastní stanici (Nessus skener). To se používá, pokud je Nessus skener umístěn ve stejné síti jako skenovaná aktiva.	

Use Fast Network Discovery	When Nessus "pings" a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1 - 65535 even when there is no service behind the device). Such checks can take some time, especially if the remote host is firewalled. If the "Use Fast Network Discovery" option is enabled, Nessus will not perform these checks.	✔
	Pokud Nessus "pingá" na vzdálenou IP adresu a obdrží odpověď, provede další extra kontrolu, aby se ujistil, že se nejedná o transparentní proxy nebo loadbalancer, který nevrací relevantní odpověď. Pokud je cíl za firewalem, můžou takové kontroly zabrat hodně času. Tato volba takové kontroly zakáže.	

Ping Methods (available when Ping the remote host is enabled)		
ARP	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.	✔
	Ping na MAC adresy. Použitelné pouze v lokální síti.	

TCP	Ping a host using TCP.	✔
	Ping pomocí protokolu TCP.	

Destination ports	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting on **built-in**.	built-in
	Je možné definovat specifické porty pro TCP ping. Pro výchozí nastavení je určena volna **built-in**	

ICMP	Ping a host using the Internet Control Message Protocol (ICMP).	✔
	Ping pomocí protokolu ICMP.	

Assume ICMP unreachable means the host is down	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When enabled, this option will consider this to mean the host is dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.	⃠
	Pokud je ping poslán na aktivum, které je vypnuté, jeho brána může vrátit ICMP zprávu o nedostupnosti. To pomáhá urychlit rychlost objevování stanic v některých sítích. Při zaškrtnutí této volby bude obdržení "ICMP unreachable" vyhodnoceno jako nedostupné aktivum. Stejné chování však mohou vykazovat některé firewally nebo paketové filtry. Pak se některé stanice mohou chovat jako nedostupné, ačkoliv jsou zapnuté.	

Maximum Number of Retries (ICMP enable)	Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.	2
	Volba umožňuje specifikovat počet pokusů, kolikrát bude *ping* poslán na cílové aktivum. Výchozí hodnota je 2.	

UDP	Ping a host using the User Datagram Protocol (UDP). Tip: UDP is a "stateless" protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.	⃠
	Ping pomocí protokolu UDP. Tip: UDP je nestavový protokol, což znamená, že komunikace není prováděna pomocí "handshake" dialogu. Komunikace na bázi UDP není vždy spolehlivá. Z podstaty UDP nejsou služby a skenované zařízení vždy na dálku spolehlivě zjistitelné.	

Fragile Devices		
Scan Network Printers	Instructs the Nessus scanner not to scan network printers if unselected. Since many printers are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal síťové tiskárny, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tiskárny, které již jednou identifikoval. To je doporučeno v produkčních sítích.	

Scan Novell Netware Hosts	Instructs the Nessus scanner not to scan Novel Netware hosts if unselected. Since many Novell Netware hosts are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal Novel Netware stroje, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tato zařízení, které již jednou identifikoval. To je doporučeno v produkčních sítích.	

Wake-on-LAN		
List of MAC addresses	Wake on Lan (WOL) packets will be sent to the hosts listed, one on each line, in an attempt to wake the specified host(s) during a scan.	⃠
	Skener může během skenování pomocí WOL paketů vzbudit síťová zařízení, která budou uvedena zde na seznamu.	

Boot time wait (in minutes)	The number of minutes Nessus will wait to attempt a scan of hosts sent a WOL packet.	⃠
	Nastavení počtu minut, jak dlouho má skener čekat po poslání WOL paketu.	

Network Type		
Network Type	Allows you to specify if you are using publicly routable IPs, private non-Internet routable IPs or a mix of these. Select "Mixed" if you are using RFC 1918 addresses and have multiple routers within your network.	mix
	Dovoluje specifikovat typ sítě LAN WAN MIX	

Port Scanning

Nastavení možností port skenu

Ports

Consider Unscanned Ports as Closed	If a port is not scanned with a selected port scanner (e.g., out of the range specified), The scanner will consider it closed.	⊘
	Při této volbě budou neoskenované porty považovány za zavřené.	

Port scan range	Directs the scanner to target a specific range of ports. Accepts "default" (a list of approximately 4,790 common ports found in the nessus-services file), "all" (scans all ports from 0-65535), or a custom list of ports specified by the user. The custom list may contain individual ports and ranges; for example, "21,23,25,80,110" and "1-1024,8080,9000-9200" are valid values. Specifying "1-65535" will scan all ports.	
	Specifikace portů, které mají být skenovány. - "default" - Výchozí nastavení je 4790 běžných portů definovaných v servisních souborech Nessus. - "all" - všechny porty 0-65535 - vlastní definice (viz uvedené příklady)	1-100

Local Port Enumerators

SSH (netstat)	This option uses netstat to check for open ports on the target host. It relies on the netstat command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.	
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes SSH spojení na skenovaném aktivu. Tento sken je zamýšlený pro UNIXové systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	✔

WMI (netstat)	This option uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials	
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes WMI spojení na skenovaném aktivu. Tento sken je zamýšlený pro Windows systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	✔

SNMP	Direct Nessus to scan targets for a SNMP service. Nessus will guess relevant SNMP settings during a scan. If the settings are provided by the user under "Preferences", this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.	
	Nasměruje Nessus na služby SNMP u skenovaných aktiv. Nessus se pokusí odhadnout SNMP nastavení během skenování. Pokud jsou nastavení poskytnuta uživatelem s vyšším oprávněním, umožní to skeneru lépe otestovat vzdálené aktivum a zajistí lepší a detailnější výsledky. Existuje mnoho kontrol pro Cisco routery, které určují přítomnost zranitelností na základě vráceného SNMP řetězce.	✔

Only run network port scanners if local port enumeration failed	Rely on local port enumeration first before relying on network port scans.	✔
	V první řadě se skener pokusí vyčíst porty lokálně, před tím než začne porty na aktivu skenovat.	

Verify open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).	⊘
	Pokud výčet lokálních portů najde otevřený port, Nessus si ověří, zda je otevřen i na dálku. Pomůže to určit, zda je použita nějaká forma řízení přístupu (např. TCP wrappers, firewall)	

Network Port Scanners

TCP	Use Nessus' built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features. **Note:** On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner instead.	
	Použije Nessus vestavěný TCP skener pro zjištění otevřených TCP portů na cílovém aktivu. Tento skener je optimalizován a má určité samoladící funkce. Poznámka: Pokud na některých platformách (např. Windows, MacOS) TCP skener způsobí vážné problémy s výkonem, Nessus místo něj zahájí SYN skener.	⊘

SYN	Use Nessus' built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and then determines port state based on a reply – or lack of.	
	Použije Nessus vestavěný SYN skener pro identifikaci TCP portů na cílovém aktivu. SYN sken je oblíbená metoda pro provádění skenování portů a obecně je považována za méně rušivou než TCP sken. Skener posílá SYN pakety na port a čeká na SYN-ACK odpověď a podle odpovědi určí stav portu.	✔

Override automatic firewall detection	Automatic (normal) Do not detect RST rate limitation (soft) Ignore closed ports (agressive) Disabled (softer)	normal
	Míra potlačení automatické detekce firewallu.	

UDP	This option engages Nessus' built-in UDP scanner to identify open UDP ports on the targets. **Tip:** UDP is a "stateless" protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable. Utilizing the UDP scanner will noticeably increase scanning time.	
	Tato volba se zabývá vestavěným Nessus UDP skenerem pro identifikaci otevřených UDP portů na skenovaném aktivu. **Tip:** UDP je nestavový protokol, komunikace tedy není prováděna přes "handshake" dialog. Komunikace založená na UDP není spolehlivá a vzhledem k povaze UDP služeb není vždy vzdáleně zjistitelná. Využití UDP skeneru výrazně zvýší čas skenování.	⊘

Service Discovery

Nastavení možností skenování běžících služeb na cílových portech		
Probe all ports to find services	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.	
	Pokusy o mapování každého otevřeného portu se službou, která běží na tomto portu. Pamatujte, že ve výjimečných případech to může narušit některé služby a způsobit vedlejší účinky.	
Search for SSL based services	Controls how Nessus will test SSL based services: known SSL ports (e.g., 443), all ports, or none. Testing for SSL capability on all ports may be disruptive for the tested host.	
	Určuje, jak bude Nessus testovat služby založené na protokolu SSL: Známé SSL porty (například 443), všechny porty, nebo žádné. Testování na schopnost SSL na všech portech může být rušivé pro testované aktivum.	
Search for SSL on	If selected, choose between Known SSL ports (e.g., 443) and All ports. Testing for SSL capability on all ports may be disruptive for the tested host.	
	Výběr mezi známými porty (např. 443) a všemi porty.	
Identify certificates expiring within x days	Identifies SSL certificates that will expire within the specified timeframe. Enter a value to set a timeframe (in days).	
	Identifikuje SSL certifikáty, které expirují během specifikovaného časového úseku. Vložte hodnotu časového úseku ve dnech.	
Enumerate all SSL ciphers	When SecurityCenter performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.	
	Pokud skener provádí SSL sken pokusí se zjistit SSL šifru použitou na skenovaném aktivu tak, že se pokusí sestavit spojení různými dokumentovanými SSL šiframi, bez ohledu na to, co dává skenované aktivum k dispozici.	
Enable CRL checking (connects to the Internet)	Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL). Enabling this option will make a connection and query one or more servers on the internet.	
	Kontrola SSL certifikátů proti CRL v internetu.	

Values for Assessment Options

Možnosti vyhodnocování informací získaných během skenování

Accuracy

Override normal accuracy	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to “Paranoid” then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of “Avoid false alarms” will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not changing from “Normal” is a middle ground between these two settings.	normal
	V některých případech Nessus nemůže určit, zda je přítomna vada, či nikoliv. Nastavení "Paranoid" zajistí reportování i v tom případě, pokud existují pochybnosti o výsledku. Naopak volba "Avoid false alarms" (vyhnout se falešným poplachům) způsobí, že Nessus nebude hlásit žádnou chybu, pokud existuje náznak nejistoty.Výchozí volba "Normal" je střední cesta mezi těmito dvěma volbami.	

Perform thorough tests (may disrupt your network or impact scan speed)	Causes various plugins to use more aggressive settings. For example, when looking through SMB file shares, a plugin can analyze 3 directory levels deep instead of its default of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially providing better audit results.	⃠
	Volba způsobí více agresivní nastavení pluginů. Například při hledání SMB sdílení souborů může plugin analyzovat 3 úrovně adresářů místo výchozí hodnoty 1. To může mít za důsledek větší provoz v síti. Sken bude více rušivý, ale bude poskytovat lepší hodnoty výsledku.	

Antivirus

Antivirus definition grace period (in days)	This option determines the delay in the number of days of reporting the software as being outdated. The valid values are between 0 (no delay, default) and 7.	⃠
	Tato volba určuje zpoždění v počtu dnů od nahlášení zastaralého software. Hodnoty se pohybují od 0 (žádná prodleva, výchozí) do 7	

SMTP

Third Party Domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.	⃠
	Nessus se pokusí posílat spam skrz každé SMTP zařízení na adresu vepsanou do tohoto pole. Doménové adresa třetí strany musí být mimo síť, která je skenována. V opačném případě může test poškodit SMTP server.	

From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.	⃠
	Testovací zprávy poslané na server SMTP se budou jevit jako poslané z této adresy.	

To Address	Nessus will attempt to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.	⃠
	Nessus se pokusí posílat zprávy na adresu uvedenou v tomto poli. "postmaster" je výchozí hodnota, protože je platná na většině poštovních serverů.	

Values for Brute Force Options

Řízení skenování hrubou silou, možnosti použití nástroje Hydra

General Settings

Only use credentials provided by the user	In some cases, Nessus can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Nessus from performing these tests.	
	V některých případech může Nessus vyzkoušet výchozí účty a jejich známá výchozí hesla. To může způsobit zamčení účtu, pokud vznikne mnoho po sobě jdoucích neplatných pokusů o přihlášení. Ve výchozím nastavení má Nessus tyto testy zakázány.	⃠

Oracle Database

Test default Oracle accounts (slow)	Test for known default accounts in Oracle software.	
	Test na přítomnost známých stadardních účtů v software Oracle.	⃠

Hydra

Always enable Hydra (slow)	Enables Hydra whenever the scan is performed.	
	Umožňuje použít nástroj Hydra (prolamovač hesel) kdykoliv je provedena kontrola.	⃠
Logins file	A file that contains user names that Hydra will use during the scan.	
	Soubor obsahující uživatelská jména, která použije nástroj Hydra.	⃠
Passwords file	A file that contains passwords for user accounts that Hydra will use during the scan.	
	Soubor obsahující hesla, která použije nástroj Hydra.	⃠
Number of parallel tasks	The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.	
	Počet současných Hydra testů. Výchozí nastavení je 16.	⃠
Timeout (in seconds)	The number of seconds per logon attempt.	
	Počet sekund na přihlašovací pokus.	⃠
Try empty passwords	If enabled, Hydra will additionally try user names without using a password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také prázdné heslo.	⃠
Try login as password	If enabled, Hydra will additionally try a user name as the corresponding password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také stejné heslo jako uživatelské jméno.	⃠
Stop brute forcing after the first success	If enabled, Hydra will stop brute forcing user accounts after the first time an account is successfully accessed.	
	Pokud bude tato volba zaškrtnuta, Hydra zastaví prolamování hesla po prvním úspěšném přístupu.	⃠
Add accounts found by other plugins to the login file	If disabled, only the user names specified in the logins file will be used for the scan. Otherwise, additional user names discovered by other plugins will be added to the logins file and used for the scan.	
	Při zakázání této volby budou použita jen uživatelská jména specifikovaná v souboru se jmény. Při povolení této volby budou přidána uživatelská jména nalezená ostatními pluginy.	⃠
PostgreSQL database name	The database that you want Hydra to test.	
	Jméno databáze pro Hydra test.	⃠
SAP R/3 Client ID (0 - 99)	The ID of the SAP R/3 client that you want Hydra to test.	
	SAP R/3 klient pro Hydra test.	⃠
Windows accounts to test	Can be set to *Local accounts* , *Domain Accounts* , or *Either* .	
	Může být nastaveno *Local accounts* , *Domain Accounts* , nebo *Either* .	⃠
Interpret passwords as NTLM hashes	If enabled, Hydra will interpret passwords as NTLM hashes.	
	Pokud je povoleno, Hydra bude interpretovat hesla jako NTLM hash.	⃠
Cisco login password	This password is used to login to a Cisco system before brute forcing enable passwords. If no password is provided here, Hydra will attempt to login using credentials that were successfully brute forced earlier in the scan.	
	Toto heslo je použito pro přihlášení na Cisco systémy před zkušením hesla hrubou silou. Pokud tu není žádné heslo poskytnuto, Hydra bude zkoušet přihlašovací údaje, které zjistila v předchozích skenech.	⃠
Web page to brute force	Enter a web page that is protected by HTTP basic or digest authentication. If a web page is not provided here, Hydra will attempt to brute force a page discovered by the Nessus web crawler that requires HTTP authentication.	
	Webová stránka pro útok hrubou silou nástrojem Hydra.	⃠
HTTP proxy test website	If Hydra successfully brute forces an HTTP proxy, it will attempt to access the website provided here via the brute forced proxy.	
	Pokud Hydra úspěšně prolomí proxy, bude zkoušet přistoupit na tuto HTTP stránku přes proxy.	⃠
LDAP DN	The LDAP Distinguish Name scope that Hydra will authenticate against.	
	LDAP DN jméno, proti kterému se bude Hydra autentizovat.	⃠

Settings/Assessment/Malware

Nastavení možností testování na Malware, použití známých MD5 hash

General Settings

Disable DNS Resolution	Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.	⃠
	Tato volba zabrání Nessus skeneru používat cloud pro porovnávání nálezů skenu proti známému škodlivému softwaru. Výchozí stav je vypnuto - tedy hledání v cloudu povoleno.	

Hash and Whitelist Files

Provide your own list of known bad MD5 hashes	Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash the description will show up in the scan results.	⃠
	Další známé špatné MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Provide your own list of known good MD5 hashes	Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description will show up in the scan results.	⃠
	Další známé dobré MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Hosts file whitelist	Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check). This option allows you to upload a file containing a list of IPs and hostnames that will be ignored by Nessus during a scan. Include one IP and hostname (formatted identically to your hosts file on the target) per line in a regular text file.	⃠
	Tato možnost vám umožní nahrát soubor obsahující seznam IP adres a aktiv, které budou během skenování skenerem ignorovány. Soubor musí obsahovat jednu IP a hostname na řádek v běžném textovém souboru.	

File System Scanning

Možnosti nastavení skenování souborového systému		
File System Scanning		
Scan File System	Turning on this option allows you to scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.	⃠
	Zapnutí této volby umožňuje skenovat systémové adresáře a soubory na skenovaném aktivu. Upozornění: Povolení tohoto nastavení při zacílení na 10 a více hostů může snížit výkon.	
Directories		
Scan %Systemroot%	Enable file system scanning to scan %Systemroot%	⃠
	Povolí skenovat %Systemroot%	
Scan %ProgramFiles%	Enable file system scanning to scan %ProgramFiles%	⃠
	Povolí skenovat %ProgramFiles%	
Scan %ProgramFiles(x86)%	Enable file system scanning to scan %ProgramFiles(x86)%	⃠
	Povolí skenovat %ProgramFiles(x86)%	
Scan %ProgramData%	Enable file system scanning to scan %ProgramData%	⃠
	Povolí skenovat %ProgramData%	
Scan User Profiles	Enable file system scanning to scan user profiles	⃠
	Povolí skenovat uživatelské profily	
Custom Filescan Directories	Add File Add a custom file that list directories for malware file scanning. List each each directory on one line. **Caution:** Root directories such as 'C:\' or 'D:\' are not accepted.	⃠
	Je možné přidat vlastní adresáře pro skenování na malware. Do textového souboru je napsán každý adresář na jeden řádek. Kořenové adresáře jako C:\ nejsou akceptovány.	
Yara Rules Files		⃠
	Nástroj na identifikaci a klasfikaci malware	

Values for SCADA Options

Tato volba umožňuje ovlivnit možnosti skenování průmyslových SCADA zařízení.		
Modbus/TCP Coil Access		
Start at register End at register	These options are available for commercial users. This drop-down menu item is dynamically generated by the SCADA plugins available with the commercial version of Nessus. Modbus uses a function code of 1 to read "coils" in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a "write coil" message. The defaults for this are "0" for the "Start reg" and "16" for the "End reg".	
ICCP/COTP TSAP Addressing Weakness		
Start COTP TSAP Stop COTP TSAP	The "ICCP/COTP TSAP Addressing" menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to "8" by default.	

Values for Web Applications Options

Nastavení skenování webových aplikací

Web Application Settings

Scan web applications	Enables the **General Settings**, **Web Crawler**, and **Application Test** Settings sections.	
	Zapnutí skenování webových aplikací.	

General Settings

Use a custom User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.	
	Určuje, za jaký typ internetového prohlížeče se bude Nessus vydávat.	

Web Crawler

Start crawling from	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., "/:/php4:/base").	
	Adresa URL, která bude první testována. Pokud je potřeba více stránek, použijte jako oddělaovač dvojtečku (např. /:/php4:/base)	

Excluded pages (regex)	Enable exclusion of portions of the web site from being crawled. For example, to exclude the "/manual" directory and all Perl CGI, set this field to: (^/manual)|(\.pl(\?.*)?$). Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).	
	Dovoluje vyloučit části webu, kterými skener prochází. Například pro vyoloučení adresáře "/manual" a všech Perl CGI nastavte do tohoto pole (^/manual)|(\.pl(\?.*)?$). Nessus podporuje regulární výrazy POSIX stejně jako Perl regulární výrazy PCRE.	

Maximum pages to crawl	The maximum number of pages to crawl.	
	Maximální počet stránek, které se mají procházet.	

Maximum depth to crawl	Limit the number of links Nessus will follow for each start page.	
	Omezení počtu odkazů, které bude Nessus následovat za každou úvodní stránkou.	

Follow dynamic pages	If selected, Nessus will follow dynamic links and may exceed the parameters set above.	
	Pokud je zaškrtnuto, Nessus bude následovat dynamické vazby a může přesáhnout parametry uvedené výše.	

Application Test Settings

Enable generic web application tests	Enables the options listed below.	
	Povolí aplikační testy vypsané dále.	

Abort web application tests if HTTP login fails	If Nessus cannot login to the target via HTTP, then do not run any web application tests.	
	Pokud se Nessus nemůže přihlásit k aktivu přes HTTP, pak nepustí žádné další aplikační testy.	

Try all HTTP Methods	This option will instruct Nessus to also use "POST requests" for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Nessus will test each script/variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.	
	Nessus bude krom GET požadavků (výchozí nastavení) zkoušet také POST požadavky. Obecně platí, že složitější aplikace používají metody POST pro posílání uživatelských dat do aplikace. Toto nastavení poskytuje důkladnější testování, ale může značně navýšit potřebný čas. Pokud je toto zaškrtnuto, Nessus bude testovat každou proměnnou, kterou najde ve skriptu na obě metody GET i POST.	

Attempt HTTP Parameter Pollution	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like "/target.cgi?a='&b=2". With HTTP Parameter Pollution (HPP) enabled, the request may look like "/target.cgi?a='&a=1&b=2".	
	Při provádění testů webových aplikací zkouší obejít filtrovací mechanismy vkládáním obsahu do proměnných a zároveň poskytuje stejné proměnné se správným obsahem. Například normální SQL-injection test může vypadat takto: "/target.cgi?a='&b=2" S volbou HTTP Parameter Pollution může vypadat takto: "/target.cgi?a='&a=1&b=2"	

Test embedded web servers	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.	
	Vestavěné webové servery jsou často statické a neobsahují nastavitelné CGI skripty. Krom toho mohou být náchylné k selhání nebo přestanou reagovat během skenování. Proto Tenable doporučuje skenování vestavěných web serverů odděleně od ostatních webů pomocí této volby.	

Test more than one parameter at a time per form	This option manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This drop-down has five options: One value - This tests one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. Some pairs – This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters. All pairs (slower but efficient) – This form of testing is slightly slower but more efficient than the "one value" test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt "/test.php?a=XSS&b=1&c=1&d=1" and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for "/test.php?a=XSS&b=3&c=3&d=3" when the first value of each variable is "1". Some combinations – This form of testing will randomly check a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time. All combinations (extremely slow) – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where "All-pairs" testing seeks to create a smaller data set as a tradeoff for speed, "all combinations" makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.	
	Tato volba řídí kombinaci hodnot argumentu použitých v HTTP dotazu. Výchozí stav (bez hodnoty) testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Toto rozbalovací pole má pět voleb: One Value - testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Some pairs - Tato forma testování bude náhodně kontrolovat kombinace náhodných párů parametrů. Toto je nejrychlejší cesta, jak otestovat více parametrů. All pairs - (pomalejší, ale efektivnější, než volba "One Value") Some combinations - tato forma testování bude náhodně zkoušet kombinaci tří nebo více parametrů. Bude to trvat déle. All combinations (extrémně pomalé) - Tato metoda bude zkoušet naprosto všechny možné kombinace útočných řetězců s platným vstupem do proměnných. Tento zůsob může trvat velice dlouho.	

Do not stop after the first flaw is found per web page	This option determines when a new flaw is targeted. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless "thorough tests" is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack. The drop-down has four options: Per CGI – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option. Per port (quicker) – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. Per parameter (slow) – As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server. Look for all flaws (slower) – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.	
	Tato volba určuje, kdy je nová chyba zaměřena. To platí na úrovni skriptu. Nalezení XSS chyby nezakáže hledání po SQL-injection nebo "header injection", ale budete mít nanejvýš jednu zprávu pro každý typ na daném portu. Toto pole má čtyři možnosti: Per CGI - Jakmile je skriptem nalezena chyba na CGI, Nessus přepne na další známé CGI na stejném serveru, nebo pokud není jiné CGI, tak na další port/službu. Toto je výchozí volba. Per port (rychlejší) - Jakmile je skriptem nalezena chyba na weobvé službě, Nessus zastaví a přepne se na jinou webovou službu na jiném portu. Per parameter (pomalé) - Jakmile je jeden typ chyby nalezen v parametru CGI (např. XSS) Nessus se přepne na další parametr ze stejné CGI nebo další známou CGI, nebo další port/službu. Look for all flaws (pomalejší) - Provede rozsáhlé testy bez ohledu na zjištěné chyby, Tato volba může vyprodukovat velice obsáhlý a upovídaný report. Tato volba není ve většině případů doporučována.	

URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.	
	URL adresa pro RFI. Zde se specifikuje souboru pro Remote File Inclusion. Ve výchozím nastavení Nessus použije bezpečný soubor hostovaný u výrobce pro RFI testování. Pokud není dostupný internet, bude použit lokální soubor, který určen pro přesnější testování RFI.	

Maximum run time (minutes_)	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.	
	Tato volba řídí množství času v minutách strávených prováděním testů webových aplikací. Standardně je nastavneno na 60minut a platí pro všechny porty a CGI pro dané webové stránky. Skenování v lokálních sítích s malými webovými aplikacemi bude obvykle dokončena za méně než hodinu, nicméně webové stránky s velkými aplikacemi mohou pžadovat vyšší hodnotu.	

Values for Windows Scan Options

Základní nastavení pro Windows		
General Setting		
Request information about the SMB Domain	If the option Request information about the domain is set, then domain users will be queried instead of local users.	✔
	Pokud je volba zaškrtnuta, budou dotazování doménoví uživatelé místo lokálních.	
Enumerate Domain User		
Start UID	1000	✔
End UID	1200	
Enumerate Local User		
Start UID	1000	✔
End UID	1200	

Values for Scan Report Options

Nastavení možností reportování		
Processing		
Report Verbosity	Determines the verbosity of the detail in the output of the scan results as Normal, Quiet, or Verbose.	normal
	Určuje míru detailu výstupu skenů. K dispozci jsou tři volby "Normal", "Quite", "Verbose"	
Show missing patches that have been superseded	Show patches in the report that have not been applied but have been superseded by a newer patch if enabled.	✔
	Pokud je volba zapnutá, zobrazí v reportu záplaty, které nebyly aplikovány, ale byly nahrazeny novější záplatou.	
Hide results from plugins initiated as a dependency	If a plugin is only run due to it being a dependency of a selected plugin, hide the results if enabled.	✔
	Skryje výsledky z pluginů, které jsou spuštěny v závislosti na jiných.	
Output		
Designate hosts by their DNS name	When possible, designate hosts by their DNS name rather than IP address in the reports.	✔
	Pokud je to možné, určit aktivum podle DNS jména, nikoliv podle IP adresy.	
Display hosts that respond to ping	When enabled, show a list of hosts that respond to pings sent as part of the scan.	✔
	Pokud je povoleno, zobrazí seznam aktiv, které odpoví na PING jako součást skenu.	
Display unreachable hosts	Display a list of hosts within the scan range that were not able to be reached during the scan, if enabled.	⃠
	Pokud je povoleno, zobrazí seznam aktiv, které jsou během skenu nedostupné.	
Generate SCAP XML Results	Generate a SCAP XML results file as a part of the report output for the scan.	⃠
	Generovat SCAP XML souboru jako součást skenu.	

Value for Authentication Options

Nastavení možností autentizace použité během skenování		
Authentication	When added, authentication methods may be used to login to the scan target machines to gather more complete results of the host's status. The authentication types include host, database, miscellaneous, plaintext authentication, and patch management. For each type, various relevant options are presented such as SNMPv3, MongoDB, VMWare APIs, and similar.	⊘
	Možnost přidání další vlastní autentizační metody.	
SNMP		
UDP Port	This is the UDP port that will be used when performing certain SNMP scans. Up to four different ports may be configured, with the default port being 161.	161
	UDP port pro provádění SNMP skenů. Až čtyři různé porty mohou být definovány.	
SSH		
known_hosts file	If an SSH known_hosts file is provided for the scan policy in the "known_hosts file" field, Nessus will only attempt to log in to hosts defined in this file. This helps to ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.	⊘
	Pokud je skenovací politice poskytnut soubor "known_hosts", Nessus se bude pokoušet hlásit jen na aktiva uvedená v tomto souboru. (v souboru "know_hosts" budou uvedeny veřejné klíče - SSH fingerprinty - těchto aktiv). To pomáhá zajistit, že přihlašovací údaje, které používáte na své známé SSH servery nebudou použity k pokusu o přihlášení do systému, který nemusí být pod Vaší kontrolou. (např. honeypoty).	
Preferred port	This option is set to direct the scan to connect to a specific port if SSH is known to be listening on a port other than the default of 22.	22
	Pokud by SSH naslouchalo na jiném než standardním portu, pak by se jiný port nastavil zde.	
Client Version	Specifies which type of SSH client to impersonate while performing scans.	OpenSSH_5.0
	Specifikuje, jaký typ SSH klienta bude během skenu představen.	
Windows		
Never send credentials in the clear	By default, Windows credentials are not sent to the target host in the clear.	✔
	Ve výchozím nastavení (zaškrtnuto) nejsou posílány přihlašovací údaje do Windows v otevřeném tvaru.	
Do not use NTLMv1 authentication	If the "Do not use NTLMv1 authentication" option is disabled, then it is theoretically possible to trick Nessus into attempting to log in to a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a "hash" obtained from Nessus. This "hash" can be potentially cracked to reveal a username or password. It may also be used to directly log in to other servers. Because NTLMv1 is an insecure protocol this option is enabled by default.	✔
	Pokud je volba ""Do not use NTLMv1 authentication" zakázána, je teoreticky možné přimět Nessus, aby se pokusil přihlásit k Windows serveru s doménovými přihlašovacími údaji pomocí NTLM verze 1. To poskytuje vzdálenému útočníkovi možnost použít "hash" obdržený z Nessus. Tento "hash" může být potencionálně zneužit jako jméno a heslo. Též to může být použito k přímému přihlášení na další servery. Protože je NTLM v. 1 nebezpečný protokol, je tato volba ve výchozím stavu povolena.	
Start the Remote Registry service during the scan	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.	✔
	Tato volba říká Nessusu, aby nastartoval službu Vzdálený registr (Remote Registry service) na skenovaném aktivu, pokud tato služba neběží. Tato služba je nezbytná pro vykonání některých Windows kontrol.	
Enable administrative shares during the scan	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.	✔
	Tato volba dovolí skeneru přistoupit k určitým položkám v registru, které lze číst je s oprávněním správce.	
Plaintext Authentication		
Perform patch audits over telnet	When enabled, patch audits will be permitted over a telnet connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	⊘
	Pokud je toto povoleno, bude sken povolen přes TELNET spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	
Perform patch audits over rsh	When enabled, patch audits will be permitted over a rsh connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	⊘
	Pokud je toto povoleno, bude sken povolen přes RSH spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	
Perform patch audits over rexec	When enabled, patch audits will be permitted over a rexec connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	⊘
	Pokud je toto povoleno, bude sken povolen přes REXEC spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	
HTTP		
Login method	Specify if the login action is performed via a GET or POST request.	POST
	Speifikace přihlašovací metody pro HTTP (GET/POST)	
Re-authenticate delay (seconds)	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.	0
	Časová prodleva mezi pokusy o přihlášení. Tato volba je použitelná při obcházení zamykacího mechanismu.	
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.	0
Invert authenticated regex	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., "Authentication failed!").	⊘
	Na přihlašovací stránce bude Nessus hledat řetězec o neúspěšném přihlášení. (např. Authentication failed).	
Use authenticated regex on HTTP headers	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.	⊘
	Hledání výsledku autentizace v HTTP hlavičce.	
Case insensitive authenticated regex	The regex searches are case sensitive by default. This instructs Nessus to ignore case.	⊘

Plugins

Skenovací zásuvné moduly nebo-li "pluginy" jsou jednotlivé dílčí kontroly prováděné během skenu. Jsou řazeny do skupin (family) podle platformy.
Pokud jsou vybrány všechny kontroly, Nessus na skenované aktivum aplikuje jen ty kontroly, které odpovídají danému operačnímu systému.
Pokud chceme získat výsledky pouze z některých konkrétních kontrol, označíme jen ty, které se mají během skenu vykonat.

Zapnuty všechny	⃠
Vypnuty všechny	⃠
Specifický vběr	✔

Plugin ID	Plugin Family	Název
12634	Settings	Authenticated Check : OS Name and Installed Package Enumeration
21745	Settings	Authentication Failure - Local Checks Not Run
19506	Settings	Nessus Scan Information
24786	Settings	Nessus Windows Scan Not Performed with Admin Privileges
10394	Windows	Microsoft Windows SMB Log In Possible
26917	Windows	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
10428	Windows	Microsoft Windows SMB Registry Not Fully Accessible Detection
10910	Windows : User management	Microsoft Windows Local User Information

Compliance

Tzv. "Compliance" skeny umožňují importovat vlastní auditní soubor, který definuje další jednotlivé kontroly, které např. vychází z vlastních bezpečnostních politik, nebo např. z obecně platného standardu CIS.

Použití auditního souboru		⃠

Příloha č. 6.

Skenovací politika „PATCH AUDIT sken“

PATCH AUDIT SKEN

Název politiky: PATCH_AUDIT_sken

PATCH_AUDIT_sken slouží ke zjištění zranitelností operačního systému.
Předpokladem je úspěšné přihlášení do OS pod privilegovaným uživatelem. síti.

Scan Options

Ovládání obecných pokročilých možností skeneru

General Settings

Enable Safe Checks	Nessus attempts to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When **Enable Safe Checks** is enabled, the second step is skipped. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.	
	Nessus se pokouší identifikovat vzdálené zranitelnosti na základě inforamcí z banerů a zkouší vykonat zranitelnost. Pokud je volba "Enable Safe Checks" zaputa, druhý krok je přeskočen. Není to tak spolehlivé, ale pro cílové aktivum je to přívětivější.	✔

Stop scanning hosts that become unresponsive during the scan	During a scan hosts may become unresponsive after a period of time. Enabling this setting stops scan attempts against hosts that stop sending results.	
	Během skenování se může stát, že po nějaké době přestane aktivum odpovídat. Při zaškrtnutí této volby bude skenování takového aktiva zastaveno.	✔

Performance Options

Slow down the scan when network congestion is detected	When Nessus detects congestion during a scan, it will slow the speed of the scan in an attempt to ease the burden on the affected segment(s).	
	Při zjištění přetížení během skenování zpomalí rychlost skenování.	✔

Use Linux kernel congestion detection	Use Linux kernel congestion detection during the scan to help alleviate system lockups on the Nessus scanner server.	
	Použije detekci přetížení pro Linux kernel.	✔

Network Timeout (in seconds)	Determines the amount of time, in seconds, to determine if there is an issue communicating over the network.	
	Určení doby v sekundách pro zjištění problému v síťové komunikaci.	5

Max Simultaneous Checks Per Host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.	
	Nastavení maximálního počtu kontrol puštěných na jedno aktivum.	5

Max Simultaneous Hosts Per Scan	This setting limits the maximum number of hosts that a single Nessus scanner will scan at the same time. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the Max Hosts Per Scan option. For example, if the Max Simultaneous Hosts Per Scan is set to 5 and there are five scanners per zone, each scanner will accept five hosts to scan, allowing a total of 25 hosts to be scanned between the five scanners.	
	Nastavení maximálního počtu počítačů, které bude jeden skener skenovat v jednom čase.	30

Max number of concurrent TCP sessions per host	This setting limits the maximum number of TCP sessions established by any of the active scanners while scanning a single host.	
	Maximální počet TCP spojení sestavených aktivním skenerem během skenování jednoho aktiva.	

Max number of concurrent TCP sessions per scan	This setting limits the maximum number of TCP sessions established by any of the active scanners during a scan.	unlimited
	Maximální počet TCP spojení sestavených jakýmkoliv z aktivních skenerů během skenování.	

Host Discovery

Nastavení možností "Discovery" skenu. (PING sken)		
Ping the remote host	When enabled, Nessus attempts to ping the hosts in the scan to determine if the host is alive or not.	✔
	Pokud je povoleno, Nessus zkouší *ping* , aby zjistil zda je aktivum naživu.	

General Settings (available when Ping the remote host is enabled)		
Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.	⃠
	Tato volba umožňuje zahrnout nebo vyloučit ze skenování vlastní stanici (Nessus skener). To se používá, pokud je Nessus skener umístěn ve stejné síti jako skenovaná aktiva.	

Use Fast Network Discovery	When Nessus "pings" a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1 - 65535 even when there is no service behind the device). Such checks can take some time, especially if the remote host is firewalled. If the "Use Fast Network Discovery" option is enabled, Nessus will not perform these checks.	✔
	Pokud Nessus "pingá" na vzdálenou IP adresu a obdrží odpověď, provede další extra kontrolu, aby se ujistil, že se nejedná o transparentní proxy nebo loadbalancer, který nevrací relevantní odpověď. Pokud je cíl za firewalem, můžou takové kontroly zabrat hodně času. Tato volba takové kontroly zakáže.	

Ping Methods (available when Ping the remote host is enabled)		
ARP	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.	✔
	Ping na MAC adresy. Použitelné pouze v lokální síti.	

TCP	Ping a host using TCP.	✔
	Ping pomocí protokolu TCP.	

Destination ports	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting on **built-in**.	built-in
	Je možné definovat specifické porty pro TCP ping. Pro výchozí nastavení je určena volna **built-in**	

ICMP	Ping a host using the Internet Control Message Protocol (ICMP).	⃠
	Ping pomocí protokolu ICMP.	

Assume ICMP unreachable means the host is down	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When enabled, this option will consider this to mean the host is dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.	⃠
	Pokud je ping poslán na aktivum, které je vypnuté, jeho brána může vrátit ICMP zprávu o nedostupnosti. To pomáhá urychlit rychlost objevování stanic v některých sítích. Při zaškrtnutí této volby bude obdržení "ICMP unreachable" vyhodnoceno jako nedostupné aktivum. Stejné chování však mohou vykazovat některé firewally nebo paketové filtry. Pak se některé stanice mohou chovat jako nedostupné, ačkoliv jsou zapnuté.	

Maximum Number of Retries (ICMP enable)	Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.	⃠
	Volba umožňuje specifikovat počet pokusů, kolikrát bude *ping* poslán na cílové aktivum. Výchozí hodnota je 2.	

UDP	Ping a host using the User Datagram Protocol (UDP). Tip: UDP is a "stateless" protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.	⃠
	Ping pomocí protokolu UDP. Tip: UDP je nestavový protokol, což znamená, že komunikace není prováděna pomocí "handshake" dialogu. Komunikace na bázi UDP není vždy spolehlivá. Z podstaty UDP nejsou služby a skenované zařízení vždy na dálku spolehlivě zjistitelné.	

Fragile Devices		
Scan Network Printers	Instructs the Nessus scanner not to scan network printers if unselected. Since many printers are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal síťové tiskárny, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tiskárny, které již jednou identifikoval. To je doporučeno v produkčních sítích.	

Scan Novell Netware Hosts	Instructs the Nessus scanner not to scan Novel Netware hosts if unselected. Since many Novell Netware hosts are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal Novel Netware stroje, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tato zařízení, které již jednou identifikoval. To je doporučeno v produkčních sítích.	

Wake-on-LAN		
List of MAC addresses	Wake on Lan (WOL) packets will be sent to the hosts listed, one on each line, in an attempt to wake the specified host(s) during a scan.	⃠
	Skener může během skenování pomocí WOL paketů vzbudit síťová zařízení, která budou uvedena zde na seznamu.	

Boot time wait (in minutes)	The number of minutes Nessus will wait to attempt a scan of hosts sent a WOL packet.	5
	Nastavení počtu minut, jak dlouho má skener čekat po poslání WOL paketu.	

Network Type		
Network Type	Allows you to specify if you are using publicly routable IPs, private non-Internet routable IPs or a mix of these. Select "Mixed" if you are using RFC 1918 addresses and have multiple routers within your network.	mix
	Dovoluje specifikovat typ sítě LAN WAN MIX	

Port Scanning

Nastavení možností port skenu

Ports

Consider Unscanned Ports as Closed	If a port is not scanned with a selected port scanner (e.g., out of the range specified), The scanner will consider it closed.	✔
	Při této volbě budou neoskenované porty považovány za zavřené.	

Port scan range	Directs the scanner to target a specific range of ports. Accepts "default" (a list of approximately 4,790 common ports found in the nessus-services file), "all" (scans all ports from 0-65535), or a custom list of ports specified by the user. The custom list may contain individual ports and ranges; for example, "21,23,25,80,110" and "1-1024,8080,9000-9200" are valid values. Specifying "1-65535" will scan all ports.	all
	Specifikace portů, které mají být skenovány. - "default" - Výchozí nastavení je 4790 běžných portů definovaných v servisních souborech Nessus. - "all" - všechny porty 0-65535 - vlastní definice (viz uvedené příklady)	

Local Port Enumerators

SSH (netstat)	This option uses netstat to check for open ports on the target host. It relies on the netstat command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.	✔
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes SSH spojení na skenovaném aktivu. Tento sken je zamýšlený pro UNIXové systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	

WMI (netstat)	This option uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials	✔
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes WMI spojení na skenovaném aktivu. Tento sken je zamýšlený pro Windows systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	

SNMP	Direct Nessus to scan targets for a SNMP service. Nessus will guess relevant SNMP settings during a scan. If the settings are provided by the user under "Preferences", this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.	✔
	Nasměruje Nessus na služby SNMP u skenovaných aktiv. Nessus se pokusí odhadnout SNMP nastavení během skenování. Pokud jsou nastavení poskytnuta uživatelem s vyšším oprávněním, umožní to skeneru lépe otestovat vzdálené aktivum a zajistí lepší a detailnější výsledky. Existuje mnoho kontrol pro Cisco routery, které určují přítomnost zranitelností na základě vráceného SNMP řetězce.	

Only run network port scanners if local port enumeration failed	Rely on local port enumeration first before relying on network port scans.	✔
	V první řadě se skener pokusí vyčíst porty lokálně, před tím než začne porty na aktivu skenovat.	

Verify open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).	✔
	Pokud výčet lokálních portů najde otevřený port, Nessus si ověří, zda je otevřen i na dálku. Pomůže to určit, zda je použita nějaká forma řízení přístupu (např. TCP wrappers, firewall)	

Network Port Scanners

TCP	Use Nessus' built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features. **Note:** On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner instead.	🚫
	Použije Nessus vestavěný TCP skener pro zjištění otevřených TCP portů na cílovém aktivu. Tento skener je optimalizován a má určité samoladící funkce. Poznámka: Pokud na některých platformách (např. Windows, MacOS) TCP skener způsobí vážné problémy s výkonem, Nessus místo něj zahájí SYN skener.	

SYN	Use Nessus' built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and then determines port state based on a reply – or lack of.	✔
	Použije Nessus vestavěný SYN skener pro identifikaci TCP portů na cílovém aktivu. SYN sken je oblíbená metoda pro provádění skenování portů a obecně je považována za méně rušivou než TCP sken. Skener posílá SYN pakety na port a čeká na SYN-ACK odpověď a podle odpovědi určí stav portu.	

Override automatic firewall detection	Automatic (normal) Do not detect RST rate limitation (soft) Ignore closed ports (agressive) Disabled (softer)	normal
	Míra potlačení automatické detekce firewallu.	

UDP	This option engages Nessus' built-in UDP scanner to identify open UDP ports on the targets. **Tip:** UDP is a "stateless" protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable. Utilizing the UDP scanner will noticeably increase scanning time.	🚫
	Tato volba se zabývá vestavěným Nessus UDP skenerem pro identifikaci otevřených UDP portů na skenovaném aktivu. **Tip:** UDP je nestavový protokol, komunikace tedy není prováděna přes "handshake" dialog. Komunikace založená na UDP není spolehlivá a vzhledem k povaze UDP služeb není vždy vzdáleně zjistitelná. Využití UDP skeneru výrazně zvýší čas skenování.	

Service Discovery

Nastavení možností skenování běžících služeb na cílových portech		
Probe all ports to find services	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.	⊘
	Pokusy o mapování každého otevřeného portu se službou, která běží na tomto portu. Pamatujte, že ve výjimečných případech to může narušit některé služby a způsobit vedlejší účinky.	
Search for SSL based services	Controls how Nessus will test SSL based services: known SSL ports (e.g., 443), all ports, or none. Testing for SSL capability on all ports may be disruptive for the tested host.	✔
	Určuje, jak bude Nessus testovat služby založené na protokolu SSL: Známé SSL porty (například 443), všechny porty, nebo žádné. Testování na schopnost SSL na všech portech může být rušivé pro testované aktivum.	
Search for SSL on	If selected, choose between Known SSL ports (e.g., 443) and All ports. Testing for SSL capability on all ports may be disruptive for the tested host.	known SSL ports
	Výběr mezi známými porty (např. 443) a všemi porty.	
Identify certificates expiring within x days	Identifies SSL certificates that will expire within the specified timeframe. Enter a value to set a timeframe (in days).	60
	Identifikuje SSL certifikáty, které expirují během specifikovaného časového úseku. Vložte hodnotu časového úseku ve dnech.	
Enumerate all SSL ciphers	When SecurityCenter performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.	✔
	Pokud skener provádí SSL sken pokusí se zjistit SSL šifru použitou na skenovaném aktivu tak, že se pokusí sestavit spojení různými dokumentovanými SSL šiframi, bez ohledu na to, co dává skenované aktivum k dispozici.	
Enable CRL checking (connects to the Internet)	Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL). Enabling this option will make a connection and query one or more servers on the internet.	⊘
	Kontrola SSL certifikátů proti CRL v internetu.	

Values for Assessment Options

Možnosti vyhodnocování informací získaných během skenování

Accuracy

Override normal accuracy	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to “Paranoid” then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of “Avoid false alarms” will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not changing from “Normal” is a middle ground between these two settings.	normal
	V některých případech Nessus nemůže určit, zda je přítomna vada, či nikoliv. Nastavení "Paranoid" zajistí reportování i v tom případě, pokud existují pochybnosti o výsledku. Naopak volba "Avoid false alarms" (vyhnout se falešným poplachům) způsobí, že Nessus nebude hlásit žádnou chybu, pokud existuje náznak nejistoty.Výchozí volba "Normal" je střední cesta mezi těmito dvěma volbami.	

Perform thorough tests (may disrupt your network or impact scan speed)	Causes various plugins to use more aggressive settings. For example, when looking through SMB file shares, a plugin can analyze 3 directory levels deep instead of its default of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially providing better audit results.	⃠
	Volba způsobí více agresivní nastavení pluginů. Například při hledání SMB sdílení souborů může plugin analyzovat 3 úrovně adresářů místo výchozí hodnoty 1. To může mít za důsledek větší provoz v síti. Sken bude více rušivý, ale bude poskytovat lepší hodnoty výsledku.	

Antivirus

Antivirus definition grace period (in days)	This option determines the delay in the number of days of reporting the software as being outdated. The valid values are between 0 (no delay, default) and 7.	⃠
	Tato volba určuje zpoždění v počtu dnů od nahlášení zastaralého software. Hodnoty se pohybují od 0 (žádná prodleva, výchozí) do 7	

SMTP

Third Party Domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.	⃠
	Nessus se pokusí posílat spam skrz každé SMTP zařízení na adresu vepsanou do tohoto pole. Doménové adresa třetí strany musí být mimo síť, která je skenována. V opačném případě může test poškodit SMTP server.	

From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.	⃠
	Testovací zprávy poslané na server SMTP se budou jevit jako poslané z této adresy.	

To Address	Nessus will attempt to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.	⃠
	Nessus se pokusí posílat zprávy na adresu uvedenou v tomto poli. "postmaster" je výchozí hodnota, protože je platná na většině poštovních serverů.	

Values for Brute Force Options

Řízení skenování hrubou silou, možnosti použití nástroje Hydra

General Settings

Only use credentials provided by the user	In some cases, Nessus can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Nessus from performing these tests.	
	V některých případech může Nessus vyzkoušet výchozí účty a jejich známá výchozí hesla. To může způsobit zamčení účtu, pokud vznikne mnoho po sobě jdoucích neplatných pokusů o přihlášení. Ve výchozím nastavení má Nessus tyto testy zakázány.	⃠

Oracle Database

Test default Oracle accounts (slow)	Test for known default accounts in Oracle software.	
	Test na přítomnost známých stadardních účtů v software Oracle.	⃠

Hydra

Always enable Hydra (slow)	Enables Hydra whenever the scan is performed.	
	Umožňuje použít nástroj Hydra (prolamovač hesel) kdykoliv je provedena kontrola.	⃠
Logins file	A file that contains user names that Hydra will use during the scan.	
	Soubor obsahující uživatelská jména, která použije nástroj Hydra.	⃠
Passwords file	A file that contains passwords for user accounts that Hydra will use during the scan.	
	Soubor obsahující hesla, která použije nástroj Hydra.	⃠
Number of parallel tasks	The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.	
	Počet současných Hydra testů. Výchozí nastavení je 16.	⃠
Timeout (in seconds)	The number of seconds per logon attempt.	
	Počet sekund na přihlašovací pokus.	⃠
Try empty passwords	If enabled, Hydra will additionally try user names without using a password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také prázdné heslo.	⃠
Try login as password	If enabled, Hydra will additionally try a user name as the corresponding password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také stejné heslo jako uživatelské jméno.	⃠
Stop brute forcing after the first success	If enabled, Hydra will stop brute forcing user accounts after the first time an account is successfully accessed.	
	Pokud bude tato volba zaškrtnuta, Hydra zastaví prolamování hesla po prvním úspěšném přístupu.	⃠
Add accounts found by other plugins to the login file	If disabled, only the user names specified in the logins file will be used for the scan. Otherwise, additional user names discovered by other plugins will be added to the logins file and used for the scan.	
	Při zakázání této volby budou použita jen uživatelská jména specifikovaná v souboru se jmény. Při povolení této volby budou přidána uživatelská jména nalezená ostatními pluginy.	⃠
PostgreSQL database name	The database that you want Hydra to test.	
	Jméno databáze pro Hydra test.	⃠
SAP R/3 Client ID (0 - 99)	The ID of the SAP R/3 client that you want Hydra to test.	
	SAP R/3 klient pro Hydra test.	⃠
Windows accounts to test	Can be set to *Local accounts* , *Domain Accounts* , or *Either* .	
	Může být nastaveno *Local accounts* , *Domain Accounts* , nebo *Either* .	⃠
Interpret passwords as NTLM hashes	If enabled, Hydra will interpret passwords as NTLM hashes.	
	Pokud je povoleno, Hydra bude interpretovat hesla jako NTLM hash.	⃠
Cisco login password	This password is used to login to a Cisco system before brute forcing enable passwords. If no password is provided here, Hydra will attempt to login using credentials that were successfully brute forced earlier in the scan.	
	Toto heslo je použito pro přihlášení na Cisco systémy před zkušením hesla hrubou silou. Pokud tu není žádné heslo poskytnuto, Hydra bude zkoušet přihlašovací údaje, které zjistila v předchozích skenech.	⃠
Web page to brute force	Enter a web page that is protected by HTTP basic or digest authentication. If a web page is not provided here, Hydra will attempt to brute force a page discovered by the Nessus web crawler that requires HTTP authentication.	
	Webová stránka pro útok hrubou silou nástrojem Hydra.	⃠
HTTP proxy test website	If Hydra successfully brute forces an HTTP proxy, it will attempt to access the website provided here via the brute forced proxy.	
	Pokud Hydra úspěšně prolomí proxy, bude zkoušet přistoupit na tuto HTTP stránku přes proxy.	⃠
LDAP DN	The LDAP Distinguish Name scope that Hydra will authenticate against.	
	LDAP DN jméno, proti kterému se bude Hydra autentizovat.	⃠

Settings/Assessment/Malware

Nastavení možností testování na Malware, použití známých MD5 hash

General Settings

Disable DNS Resolution	Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.	
	Tato volba zabrání Nessus skeneru používat cloud pro porovnávání nálezů skenu proti známému škodlivému softwaru. Výchozí stav je vypnuto - tedy hledání v cloudu povoleno.	

Hash and Whitelist Files

Provide your own list of known bad MD5 hashes	Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash the description will show up in the scan results.	
	Další známé špatné MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Provide your own list of known good MD5 hashes	Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description will show up in the scan results.	
	Další známé dobré MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Hosts file whitelist	Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check). This option allows you to upload a file containing a list of IPs and hostnames that will be ignored by Nessus during a scan. Include one IP and hostname (formatted identically to your hosts file on the target) per line in a regular text file.	
	Tato možnost vám umožní nahrát soubor obsahující seznam IP adres a aktiv, které budou během skenování skenerem ignorovány. Soubor musí obsahovat jednu IP a hostname na řádek v běžném textovém souboru.	

File System Scanning

Možnosti nastavení skenování souborového systému		
File System Scanning		
Scan File System	Turning on this option allows you to scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.	
	Zapnutí této volby umožňuje skenovat systémové adresáře a soubory na skenovaném aktivu. Upozornění: Povolení tohoto nastavení při zacílení na 10 a více hostů může snížit výkon.	
Directories		
Scan %Systemroot%	Enable file system scanning to scan %Systemroot%	
	Povolí skenovat %Systemroot%	
Scan %ProgramFiles%	Enable file system scanning to scan %ProgramFiles%	
	Povolí skenovat %ProgramFiles%	
Scan %ProgramFiles(x86)%	Enable file system scanning to scan %ProgramFiles(x86)%	
	Povolí skenovat %ProgramFiles(x86)%	
Scan %ProgramData%	Enable file system scanning to scan %ProgramData%	
	Povolí skenovat %ProgramData%	
Scan User Profiles	Enable file system scanning to scan user profiles	
	Povolí skenovat uživatelské profily	
Custom Filescan Directories	Add File Add a custom file that list directories for malware file scanning. List each each directory on one line. **Caution:** Root directories such as 'C:\' or 'D:\' are not accepted.	
	Je možné přidat vlastní adresáře pro skenování na malware. Do textového souboru je napsán každý adresář na jeden řádek. Kořenové adresáře jako C:\ nejsou akceptovány.	
Yara Rules Files		
	Nástroj na identifikaci a klasfikaci malware	

Values for SCADA Options

Tato volba umožňuje ovlivnit možnosti skenování průmyslových SCADA zařízení.		
Modbus/TCP Coil Access		
Start at register End at register	These options are available for commercial users. This drop-down menu item is dynamically generated by the SCADA plugins available with the commercial version of Nessus. Modbus uses a function code of 1 to read "coils" in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a "write coil" message. The defaults for this are "0" for the "Start reg" and "16" for the "End reg".	
ICCP/COTP TSAP Addressing Weakness		
Start COTP TSAP Stop COTP TSAP	The "ICCP/COTP TSAP Addressing" menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to "8" by default.	

Values for Web Applications Options

Nastavení skenování webových aplikací

Web Application Settings

Scan web applications	Enables the **General Settings**, **Web Crawler**, and **Application Test** Settings sections.	
	Zapnutí skenování webových aplikací.	

General Settings

Use a custom User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.	
	Určuje, za jaký typ internetového prohlížeče se bude Nessus vydávat.	

Web Crawler

Start crawling from	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., "/:/php4:/base").	
	Adresa URL, která bude první testována. Pokud je potřeba více stránek, použijte jako oddělaovač dvojtečku (např. /:/php4:/base)	

Excluded pages (regex)	Enable exclusion of portions of the web site from being crawled. For example, to exclude the "/manual" directory and all Perl CGI, set this field to: (^/manual)|(\.pl(\?.*)?$). Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).	
	Dovoluje vyloučit části webu, kterými skener prochází. Například pro vyloučení adresáře "/manual" a všech Perl CGI nastavte do tohoto pole (^/manual)|(\.pl(\?.*)?$). Nessus podporuje regulární výrazy POSIX stejně jako Perl regulární výrazy PCRE.	

Maximum pages to crawl	The maximum number of pages to crawl.	
	Maximální počet stránek, které se mají procházet.	

Maximum depth to crawl	Limit the number of links Nessus will follow for each start page.	
	Omezení počtu odkazů, které bude Nessus následovat za každou úvodní stránkou.	

Follow dynamic pages	If selected, Nessus will follow dynamic links and may exceed the parameters set above.	
	Pokud je zaškrtnuto, Nessus bude následovat dynamické vazby a může přesáhnout parametry uvedené výše.	

Application Test Settings

Enable generic web application tests	Enables the options listed below.	
	Povolí aplikační testy vypsané dále.	

Abort web application tests if HTTP login fails	If Nessus cannot login to the target via HTTP, then do not run any web application tests.	
	Pokud se Nessus nemůže přihlásit k aktivu přes HTTP, pak nepustí žádné další aplikační testy.	

Try all HTTP Methods	This option will instruct Nessus to also use "POST requests" for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Nessus will test each script/variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.	
	Nessus bude krom GET požadavků (výchozí nastavení) zkoušet také POST požadavky. Obecně platí, že složitější aplikace používají metody POST pro posílání uživatelských dat do aplikace. Toto nastavení poskytuje důkladnější testování, ale může značně navýšit potřebný čas. Pokud je toto zaškrtnuto, Nessus bude testovat každou proměnnou, kterou najde ve skriptu na obě metody GET i POST.	

Attempt HTTP Parameter Pollution	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like "/target.cgi?a='&b=2". With HTTP Parameter Pollution (HPP) enabled, the request may look like "/target.cgi?a='&a=1&b=2".	
	Při provádění testů webových aplikací zkouší obejít filtrovací mechanismy vkládáním obsahu do proměnných a zároveň poskytuje stejné proměnné se správným obsahem. Například normální SQL-injection test může vypadat takto: "/target.cgi?a='&b=2" S volbou HTTP Parameter Pollution může vypadat takto: "/target.cgi?a='&a=1&b=2"	

Test embedded web servers	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.	
	Vestavěné webové servery jsou často statické a neobsahují nastavitelné CGI skripty. Krom toho mohou být náchylné k selhání nebo přestanou reagovat během skenování. Proto Tenable doporučuje skenování vestavěných web serverů odděleně od ostatních webů pomocí této volby.	

Test more than one parameter at a time per form	This option manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This drop-down has five options: One value - This tests one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. Some pairs – This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters. All pairs (slower but efficient) – This form of testing is slightly slower but more efficient than the "one value" test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt "/test.php?a=XSS&b=1&c=1&d=1" and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for "/test.php?a=XSS&b=3&c=3&d=3" when the first value of each variable is "1". Some combinations – This form of testing will randomly check a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time. All combinations (extremely slow) – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where "All-pairs" testing seeks to create a smaller data set as a tradeoff for speed, "all combinations" makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.	
	Tato volba řídí kombinaci hodnot argumentu použitých v HTTP dotazu. Výchozí stav (bez hodnoty) testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Toto rozbalovací pole má pět voleb: One Value - testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Some pairs - Tato forma testování bude náhodně kontrolovat kombinace náhodných párů parametrů. Toto je nejrychlejší cesta, jak otestovat více parametrů. All pairs - (pomalejší, ale efektivnější, než volba "One Value") Some combinations - tato forma testování bude náhodně zkoušet kombinaci tří nebo více parametrů. Bude to trvat déle. All combinations (extrémně pomalé) - Tato metoda bude zkoušet naprosto všechny možné kombinace útočných řetězců s platným vstupem do proměnných. Tento zůsob může trvat velice dlouho.	

Do not stop after the first flaw is found per web page	This option determines when a new flaw is targeted. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless "thorough tests" is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack. The drop-down has four options: Per CGI – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option. Per port (quicker) – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. Per parameter (slow) – As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server. Look for all flaws (slower) – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.	
	Tato volba určuje, kdy je nová chyba zaměřena. To platí na úrovni skriptu. Nalezení XSS chyby nezakáže hledání po SQL-injection nebo "header injection", ale budete mít nanejvýš jednu zprávu pro každý typ na daném portu. Toto pole má čtyři možnosti: Per CGI - Jakmile je skriptem nalezena chyba na CGI, Nessus přepne na další známé CGI na stejném serveru, nebo pokud není jiné CGI, tak na další port/službu. Toto je výchozí volba. Per port (rychlejší) - Jakmile je skriptem nalezena chyba na weobvé službě, Nessus zastaví a přepne se na jinou webovou službu na jiném portu. Per parameter (pomalé) - Jakmile je jeden typ chyby nalezen v parametru CGI (např. XSS) Nessus se přepne na další parametr ze stejné CGI nebo další známou CGI, nebo další port/službu. Look for all flaws (pomalejší) - Provede rozsáhlé testy bez ohledu na zjištěné chyby, Tato volba může vyprodukovat velice obsáhlý a upovídaný report. Tato volba není ve většině případů doporučována.	

URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.	
	URL adresa pro RFI. Zde se specifikuje souboru pro Remote File Inclusion. Ve výchozím nastavení Nessus použije bezpečný soubor hostovaný u výrobce pro RFI testování. Pokud není dostupný internet, bude použit lokální soubor, který určen pro přesnější testování RFI.	

Maximum run time (minutes_)	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.	
	Tato volba řídí množství času v minutách strávených prováděním testů webových aplikací. Standardně je nastavneno na 60minut a platí pro všechny porty a CGI pro dané webové stránky. Skenování v lokálních sítích s malými webovými aplikacemi bude obvykle dokončena za méně než hodinu, nicméně webové stránky s velkými aplikacemi mohou pžadovat vyšší hodnotu.	

Values for Windows Scan Options

Zákadní nastavení pro Windows		
General Setting		
Request information about the SMB Domain	If the option Request information about the domain is set, then domain users will be queried instead of local users.	✔
	Pokud je volba zaškrtnuta, budou dotazování doménoví uživatelé místo lokálních.	
Enumerate Domain User		
Start UID	1000	✔
End UID	1200	
Enumerate Local User		
Start UID	1000	✔
End UID	1200	

Values for Scan Report Options

Nastavení možností reportování		
Processing		
Report Verbosity	Determines the verbosity of the detail in the output of the scan results as Normal, Quiet, or Verbose.	normal
	Určuje míru detailu výstupu skenů. K dispozci jsou tři volby "Normal", "Quite", "Verbose"	
Show missing patches that have been superseded	Show patches in the report that have not been applied but have been superseded by a newer patch if enabled.	✔
	Pokud je volba zapnutá, zobrazí v reportu záplaty, které nebyly aplikovány, ale byly nahrazeny novější záplatou.	
Hide results from plugins initiated as a dependency	If a plugin is only run due to it being a dependency of a selected plugin, hide the results if enabled.	✔
	Skryje výsledky z pluginů, které jsou spuštěny v závislosti na jiných.	
Output		
Designate hosts by their DNS name	When possible, designate hosts by their DNS name rather than IP address in the reports.	✔
	Pokud je to možné, určit aktivum podle DNS jména, nikoliv podle IP adresy.	
Display hosts that respond to ping	When enabled, show a list of hosts that respond to pings sent as part of the scan.	✔
	Pokud je povoleno, zobrazí seznam aktiv, které odpoví na PING jako součást skenu.	
Display unreachable hosts	Display a list of hosts within the scan range that were not able to be reached during the scan, if enabled.	⃠
	Pokud je povoleno, zobrazí seznam aktiv, které jsou během skenu nedostupné.	
Generate SCAP XML Results	Generate a SCAP XML results file as a part of the report output for the scan.	⃠
	Generovat SCAP XML souboru jako součást skenu.	

Value for Authentication Options

Nastavení možností autentizace použité během skenování		
Authentication	When added, authentication methods may be used to login to the scan target machines to gather more complete results of the host's status. The authentication types include host, database, miscellaneous, plaintext authentication, and patch management. For each type, various relevant options are presented such as SNMPv3, MongoDB, VMWare APIs, and similar.	⊘
	Možnost přidání další vlastní autentizační metody.	
SNMP		
UDP Port	This is the UDP port that will be used when performing certain SNMP scans. Up to four different ports may be configured, with the default port being 161.	161
	UDP port pro provádění SNMP skenů. Až čtyři různé porty mohou být definovány.	
SSH		
known_hosts file	If an SSH known_hosts file is provided for the scan policy in the "known_hosts file" field, Nessus will only attempt to log in to hosts defined in this file. This helps to ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.	⊘
	Pokud je skenovací politice poskytnut soubor "known_hosts", Nessus se bude pokoušet hlásit jen na aktiva uvedená v tomto souboru. (v souboru "know_hosts" budou uvedeny veřejné klíče - SSH fingerprinty - těchto aktiv). To pomáhá zajistit, že přihlašovací údaje, které používáte na své známé SSH servery nebudou použity k pokusu o přihlášení do systému, který nemusí být pod Vaší kontrolou. (např. honeypoty).	
Preferred port	This option is set to direct the scan to connect to a specific port if SSH is known to be listening on a port other than the default of 22.	22
	Pokud by SSH naslouchalo na jiném než standardním portu, pak by se jiný port nastavil zde.	
Client Version	Specifies which type of SSH client to impersonate while performing scans.	OpenSSH_5.0
	Specifikuje, jaký typ SSH klienta bude během skenu představen.	
Windows		
Never send credentials in the clear	By default, Windows credentials are not sent to the target host in the clear.	✔
	Ve výchozím nastavení (zaškrtnuto) nejsou posílány přihlašovací údaje do Windows v otevřeném tvaru.	
Do not use NTLMv1 authentication	If the "Do not use NTLMv1 authentication" option is disabled, then it is theoretically possible to trick Nessus into attempting to log in to a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a "hash" obtained from Nessus. This "hash" can be potentially cracked to reveal a username or password. It may also be used to directly log in to other servers. Because NTLMv1 is an insecure protocol this option is enabled by default.	✔
	Pokud je volba ""Do not use NTLMv1 authentication" zakázána, je teoreticky možné přimět Nessus, aby se pokusil přihlásit k Windows serveru s doménovými přihlašovacími údaji pomocí NTLM verze 1. To poskytuje vzdálenému útočníkovi možnost použít "hash" obdržený z Nessus. Tento "hash" může být potencionálně zneužit jako jméno a heslo. Též to může být použito k přímému přihlášení na další servery. Protože je NTLM v. 1 nebezpečný protokol, je tato volba ve výchozím stavu povolena.	
Start the Remote Registry service during the scan	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.	✔
	Tato volba říká Nessusu, aby nastartoval službu Vzdálený registr (Remote Registry service) na skenovaném aktivu, pokud tato služba neběží. Tato služba je nezbytná pro vykonání některých Windows kontrol.	
Enable administrative shares during the scan	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.	✔
	Tato volba dovolí skeneru přistoupit k určitým položkám v registru, které lze číst je s oprávněním správce.	
Plaintext Authentication		
Perform patch audits over telnet	When enabled, patch audits will be permitted over a telnet connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	⊘
	Pokud je toto povoleno, bude sken povolen přes TELNET spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	
Perform patch audits over rsh	When enabled, patch audits will be permitted over a rsh connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	⊘
	Pokud je toto povoleno, bude sken povolen přes RSH spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	
Perform patch audits over rexec	When enabled, patch audits will be permitted over a rexec connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	⊘
	Pokud je toto povoleno, bude sken povolen přes REXEC spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	
HTTP		
Login method	Specify if the login action is performed via a GET or POST request.	POST
	Speifikace přihlašovací metody pro HTTP (GET/POST)	
Re-authenticate delay (seconds)	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.	0
	Časová prodleva mezi pokusy o přihlášení. Tato volba je použitelná při obcházení zamykacího mechanismu.	
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.	0
Invert authenticated regex	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., "Authentication failed!").	⊘
	Na přihlašovací stránce bude Nessus hledat řetězec o neúspěšném přihlášení. (např. Authentication failed).	
Use authenticated regex on HTTP headers	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.	⊘
	Hledání výsledku autentizace v HTTP hlavičce.	
Case insensitive authenticated regex	The regex searches are case sensitive by default. This instructs Nessus to ignore case.	⊘

Plugins

Skenovací zásuvné moduly nebo-li "pluginy" jsou jednotlivé dílčí kontroly prováděné během skenu. Jsou řazeny do skupin (family) podle platformy.
Pokud jsou vybrány všechny kontroly, Nessus na skenované aktivum aplikuje jen ty kontroly, které odpovídají danému operačnímu systému.
Pokud chceme získat výsledky pouze z některých konkrétních kontrol, označíme jen ty, které se mají během skenu vykonat.

Zapnuty všechny	✔
Vypnuty všechny	🚫
Specifický vběr	🚫

Plugin ID	Plugin Family	Název

Compliance

Tzv. "Compliance" skeny umožňují importovat vlastní auditní soubor, který definuje další jednotlivé kontroly, které např. vychází z vlastních bezpečnostních politik, nebo např. z obecně platného standardu CIS.

Použití auditního souboru		⃠

Příloha č. 7.

Skenovací politika „PORT sken“

PORT SKEN

Název politiky: PORT_sken

Port sken slouží ke zjištění fakticky dostupných portů na konkrétním aktivu.

Scan Options

Ovládání obecných pokročilých možností skeneru

General Settings

Enable Safe Checks	Nessus attempts to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When **Enable Safe Checks** is enabled, the second step is skipped. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.	✔
	Nessus se pokouší identifikovat vzdálené zranitelnosti na základě inforamcí z banerů a zkouší vykonat zranitelnost. Pokud je volba "Enable Safe Checks" zaputa, druhý krok je přeskočen. Není to tak spolehlivé, ale pro cílové aktivum je to přívětivější.	

Stop scanning hosts that become unresponsive during the scan	During a scan hosts may become unresponsive after a period of time. Enabling this setting stops scan attempts against hosts that stop sending results.	⃠
	Během skenování se může stát, že po nějaké době přestane aktivum odpovídat. Při zaškrtnutí této volby bude skenování takového aktiva zastaveno.	

Performance Options

Slow down the scan when network congestion is detected	When Nessus detects congestion during a scan, it will slow the speed of the scan in an attempt to ease the burden on the affected segment(s).	⃠
	Při zjištění přetížení během skenování zpomalí rychlost skenování.	

Use Linux kernel congestion detection	Use Linux kernel congestion detection during the scan to help alleviate system lockups on the Nessus scanner server.	⃠
	Použije detekci přetížení pro Linux kernel.	

Network Timeout (in seconds)	Determines the amount of time, in seconds, to determine if there is an issue communicating over the network.	5
	Určení doby v sekundách pro zjištění problému v síťové komunikaci.	

Max Simultaneous Checks Per Host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.	5
	Nastavení maximálního počtu kontrol puštěných na jedno aktivum.	

Max Simultaneous Hosts Per Scan	This setting limits the maximum number of hosts that a single Nessus scanner will scan at the same time. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the Max Hosts Per Scan option. For example, if the Max Simultaneous Hosts Per Scan is set to 5 and there are five scanners per zone, each scanner will accept five hosts to scan, allowing a total of 25 hosts to be scanned between the five scanners.	30
	Nastavení maximálního počtu počítačů, které bude jeden skener skenovat v jednom čase.	

Max number of concurrent TCP sessions per host	This setting limits the maximum number of TCP sessions established by any of the active scanners while scanning a single host.	⃠
	Maximální počet TCP spojení sestavených aktivním skenerem během skenování jednoho aktiva.	

Max number of concurrent TCP sessions per scan	This setting limits the maximum number of TCP sessions established by any of the active scanners during a scan.	unlimited
	Maximální počet TCP spojení sestavených jakýmkoliv z aktivních skenerů během skenování.	

Host Discovery

Nastavení možností "Discovery" skenu. (PING sken)

Ping the remote host	When enabled, Nessus attempts to ping the hosts in the scan to determine if the host is alive or not.	✔
	Pokud je povoleno, Nessus zkouší *ping* , aby zjistil zda je aktivum naživu.	

General Settings (available when Ping the remote host is enabled)

Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.	⃠
	Tato volba umožňuje zahrnout nebo vyloučit ze skenování vlastní stanici (Nessus skener). To se používá, pokud je Nessus skener umístěn ve stejné síti jako skenovaná aktiva.	

Use Fast Network Discovery	When Nessus "pings" a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1 - 65535 even when there is no service behind the device). Such checks can take some time, especially if the remote host is firewalled. If the "Use Fast Network Discovery" option is enabled, Nessus will not perform these checks.	✔
	Pokud Nessus "pingá" na vzdálenou IP adresu a obdrží odpověď, provede další extra kontrolu, aby se ujistil, že se nejedná o transparentní proxy nebo loadbalancer, který nevrací relevantní odpověď. Pokud je cíl za firewalem, můžou takové kontroly zabrat hodně času. Tato volba takové kontroly zakáže.	

Ping Methods (available when Ping the remote host is enabled)

ARP	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.	✔
	Ping na MAC adresy. Použitelné pouze v lokální síti.	

TCP	Ping a host using TCP.	✔
	Ping pomocí protokolu TCP.	

Destination ports	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting on **built-in**.	built-in
	Je možné definovat specifické porty pro TCP ping. Pro výchozí nastavení je určena volna **built-in**	

ICMP	Ping a host using the Internet Control Message Protocol (ICMP).	✔
	Ping pomocí protokolu ICMP.	

Assume ICMP unreachable means the host is down	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When enabled, this option will consider this to mean the host is dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.	⃠
	Pokud je ping poslán na aktivum, které je vypnuté, jeho brána může vrátit ICMP zprávu o nedostupnosti. To pomáhá urychlit rychlost objevování stanic v některých sítích. Při zaškrtnutí této volby bude obdržení "ICMP unreachable" vyhodnoceno jako nedostupné aktivum. Stejné chování však mohou vykazovat některé firewally nebo paketové filtry. Pak se některé stanice mohou chovat jako nedostupné, ačkoliv jsou zapnuté.	

Maximum Number of Retries (ICMP enable)	Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.	2
	Volba umožňuje specifikovat počet pokusů, kolikrát bude *ping* poslán na cílové aktivum. Výchozí hodnota je 2.	

UDP	Ping a host using the User Datagram Protocol (UDP). Tip: UDP is a "stateless" protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.	⃠
	Ping pomocí protokolu UDP. Tip: UDP je nestavový protokol, což znamená, že komunikace není prováděna pomocí "handshake" dialogu. Komunikace na bázi UDP není vždy spolehlivá. Z podstaty UDP nejsou služby a skenované zařízení vždy na dálku spolehlivě zjistitelné.	

Fragile Devices

Scan Network Printers	Instructs the Nessus scanner not to scan network printers if unselected. Since many printers are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal síťové tiskárny, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tiskárny, které již jednou identifikoval. To je doporučeno v produkčních sítích.	

Scan Novell Netware Hosts	Instructs the Nessus scanner not to scan Novel Netware hosts if unselected. Since many Novell Netware hosts are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.	⃠
	Neoznačení této volby říká skeneru, aby vynechal Novel Netware stroje, které bývají na skenování citlivé. NE u této položky přimějou Nessus přeskočit tato zařízení, které již jednou identifikoval. To je doporučeno v produkčních sítích.	

Wake-on-LAN

List of MAC addresses	Wake on Lan (WOL) packets will be sent to the hosts listed, one on each line, in an attempt to wake the specified host(s) during a scan.	⃠
	Skener může během skenování pomocí WOL paketů vzbudit síťová zařízení, která budou uvedena zde na seznamu.	

Boot time wait (in minutes)	The number of minutes Nessus will wait to attempt a scan of hosts sent a WOL packet.	⃠
	Nastavení počtu minut, jak dlouho má skener čekat po poslání WOL paketu.	

Network Type

Network Type	Allows you to specify if you are using publicly routable IPs, private non-Internet routable IPs or a mix of these. Select "Mixed" if you are using RFC 1918 addresses and have multiple routers within your network.	mix
	Dovoluje specifikovat typ sítě LAN WAN MIX	

Port Scanning

Nastavení možností port skenu

Ports

Consider Unscanned Ports as Closed	If a port is not scanned with a selected port scanner (e.g., out of the range specified), The scanner will consider it closed.	⊘
	Při této volbě budou neoskenované porty považovány za zavřené.	

Port scan range	Directs the scanner to target a specific range of ports. Accepts "default" (a list of approximately 4,790 common ports found in the nessus-services file), "all" (scans all ports from 0-65535), or a custom list of ports specified by the user. The custom list may contain individual ports and ranges; for example, "21,23,25,80,110" and "1-1024,8080,9000-9200" are valid values. Specifying "1-65535" will scan all ports.	⊘
	Specifikace portů, které mají být skenovány. - "default" - Výchozí nastavení je 4790 běžných portů definovaných v servisních souborech Nessus. - "all" - všechny porty 0-65535 - vlastní definice (viz uvedené příklady)	

Local Port Enumerators

SSH (netstat)	This option uses netstat to check for open ports on the target host. It relies on the netstat command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.	⊘
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes SSH spojení na skenovaném aktivu. Tento sken je zamýšlený pro UNIXové systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	

WMI (netstat)	This option uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials	⊘
	Tato volba použije příkaz *netstat* pro zjištění otevřených portů na cílovém aktivu. Spoléhá se na příkaz *netstat* spuštěný přes WMI spojení na skenovaném aktivu. Tento sken je zamýšlený pro Windows systémy a vyžaduje přihlašovací údaje ke skenovanému aktivu.	

SNMP	Direct Nessus to scan targets for a SNMP service. Nessus will guess relevant SNMP settings during a scan. If the settings are provided by the user under "Preferences", this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.	⊘
	Nasměruje Nessus na služby SNMP u skenovaných aktiv. Nessus se pokusí odhadnout SNMP nastavení během skenování. Pokud jsou nastavení poskytnuta uživatelem s vyšším oprávněním, umožní to skeneru lépe otestovat vzdálené aktivum a zajistí lepší a detailnější výsledky. Existuje mnoho kontrol pro Cisco routery, které určují přítomnost zranitelností na základě vráceného SNMP řetězce.	

Only run network port scanners if local port enumeration failed	Rely on local port enumeration first before relying on network port scans.	⊘
	V první řadě se skener pokusí vyčíst porty lokálně, před tím než začne porty na aktivu skenovat.	

Verify open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).	⊘
	Pokud výčet lokálních portů najde otevřený port, Nessus si ověří, zda je otevřen i na dálku. Pomůže to určit, zda je použita nějaká forma řízení přístupu (např. TCP wrappers, firewall)	

Network Port Scanners

TCP	Use Nessus' built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features. **Note:** On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner instead.	✔
	Použije Nessus vestavěný TCP skener pro zjištění otevřených TCP portů na cílovém aktivu. Tento skener je optimalizován a má určité samoladící funkce. Poznámka: Pokud na některých platformách (např. Windows, MacOS) TCP skener způsobí vážné problémy s výkonem, Nessus místo něj zahájí SYN skener.	

SYN	Use Nessus' built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and then determines port state based on a reply – or lack of.	✔
	Použije Nessus vestavěný SYN skener pro identifikaci TCP portů na cílovém aktivu. SYN sken je oblíbená metoda pro provádění skenování portů a obecně je považována za méně rušivou než TCP sken. Skener posílá SYN pakety na port a čeká na SYN-ACK odpověď a podle odpovědi určí stav portu.	

Override automatic firewall detection	Automatic (normal) Do not detect RST rate limitation (soft) Ignore closed ports (agressive) Disabled (softer)	normal
	Míra potlačení automatické detekce firewallu.	

UDP	This option engages Nessus' built-in UDP scanner to identify open UDP ports on the targets. **Tip:** UDP is a "stateless" protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable. Utilizing the UDP scanner will noticeably increase scanning time.	⊘
	Tato volba se zabývá vestavěným Nessus UDP skenerem pro identifikaci otevřených UDP portů na skenovaném aktivu. **Tip:** UDP je nestavový protokol, komunikace tedy není prováděna přes "handshake" dialog. Komunikace založená na UDP není spolehlivá a vzhledem k povaze UDP služeb není vždy vzdáleně zjistitelná. Využití UDP skeneru výrazně zvýší čas skenování.	

Service Discovery

Nastavení možností skenování běžících služeb na cílových portech		
Probe all ports to find services	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.	
	Pokusy o mapování každého otevřeného portu se službou, která běží na tomto portu. Pamatujte, že ve výjimečných případech to může narušit některé služby a způsobit vedlejší účinky.	

Search for SSL based services	Controls how Nessus will test SSL based services: known SSL ports (e.g., 443), all ports, or none. Testing for SSL capability on all ports may be disruptive for the tested host.	
	Určuje, jak bude Nessus testovat služby založené na protokolu SSL: Známé SSL porty (například 443), všechny porty, nebo žádné. Testování na schopnost SSL na všech portech může být rušivé pro testované aktivum.	

Search for SSL on	If selected, choose between Known SSL ports (e.g., 443) and All ports. Testing for SSL capability on all ports may be disruptive for the tested host.	
	Výběr mezi známými porty (např. 443) a všemi porty.	

Identify certificates expiring within x days	Identifies SSL certificates that will expire within the specified timeframe. Enter a value to set a timeframe (in days).	
	Identifikuje SSL certifikáty, které expirují během specifikovaného časového úseku. Vložte hodnotu časového úseku ve dnech.	

Enumerate all SSL ciphers	When SecurityCenter performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.	
	Pokud skener provádí SSL sken pokusí se zjistit SSL šifru použitou na skenovaném aktivu tak, že se pokusí sestavit spojení různými dokumentovanými SSL šiframi, bez ohledu na to, co dává skenované aktivum k dispozici.	

Enable CRL checking (connects to the Internet)	Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL). Enabling this option will make a connection and query one or more servers on the internet.	
	Kontrola SSL certifikátů proti CRL v internetu.	

Values for Assessment Options

Možnosti vyhodnocování informací získaných během skenování

Accuracy		
Override normal accuracy	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to “Paranoid” then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of “Avoid false alarms” will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not changing from “Normal” is a middle ground between these two settings.	normal
	V některých případech Nessus nemůže určit, zda je přítomna vada, či nikoliv. Nastavení "Paranoid" zajistí reportování i v tom případě, pokud existují pochybnosti o výsledku. Naopak volba "Avoid false alarms" (vyhnout se falešným poplachům) způsobí, že Nessus nebude hlásit žádnou chybu, pokud existuje náznak nejistoty.Výchozí volba "Normal" je střední cesta mezi těmito dvěma volbami.	
Perform thorough tests (may disrupt your network or impact scan speed)	Causes various plugins to use more aggressive settings. For example, when looking through SMB file shares, a plugin can analyze 3 directory levels deep instead of its default of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially providing better audit results.	⃠
	Volba způsobí více agresivní nastavení pluginů. Například při hledání SMB sdílení souborů může plugin analyzovat 3 úrovně adresářů místo výchozí hodnoty 1. To může mít za důsledek větší provoz v síti. Sken bude více rušivý, ale bude poskytovat lepší hodnoty výsledku.	
Antivirus		
Antivirus definition grace period (in days)	This option determines the delay in the number of days of reporting the software as being outdated. The valid values are between 0 (no delay, default) and 7.	⃠
	Tato volba určuje zpoždění v počtu dnů od nahlášení zastaralého software. Hodnoty se pohybují od 0 (žádná prodleva, výchozí) do 7	
SMTP		
Third Party Domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.	⃠
	Nessus se pokusí posílat spam skrz každé SMTP zařízení na adresu vepsanou do tohoto pole. Doménové adresa třetí strany musí být mimo síť, která je skenována. V opačném případě může test poškodit SMTP server.	
From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.	⃠
	Testovací zprávy poslané na server SMTP se budou jevit jako poslané z této adresy.	
To Address	Nessus will attempt to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.	⃠
	Nessus se pokusí posílat zprávy na adresu uvedenou v tomto poli. "postmaster" je výchozí hodnota, protože je platná na většině poštovních serverů.	

Values for Brute Force Options

Řízení skenování hrubou silou, možnosti použití nástroje Hydra

General Settings

Only use credentials provided by the user	In some cases, Nessus can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Nessus from performing these tests.	
	V některých případech může Nessus vyzkoušet výchozí účty a jejich známá výchozí hesla. To může způsobit zamčení účtu, pokud vznikne mnoho po sobě jdoucích neplatných pokusů o přihlášení. Ve výchozím nastavení má Nessus tyto testy zakázány.	⃠

Oracle Database

Test default Oracle accounts (slow)	Test for known default accounts in Oracle software.	
	Test na přítomnost známých stadardních účtů v software Oracle.	⃠

Hydra

Always enable Hydra (slow)	Enables Hydra whenever the scan is performed.	
	Umožňuje použít nástroj Hydra (prolamovač hesel) kdykoliv je provedena kontrola.	⃠
Logins file	A file that contains user names that Hydra will use during the scan.	
	Soubor obsahující uživatelská jména, která použije nástroj Hydra.	⃠
Passwords file	A file that contains passwords for user accounts that Hydra will use during the scan.	
	Soubor obsahující hesla, která použije nástroj Hydra.	⃠
Number of parallel tasks	The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.	
	Počet současných Hydra testů. Výchozí nastavení je 16.	⃠
Timeout (in seconds)	The number of seconds per logon attempt.	
	Počet sekund na přihlašovací pokus.	⃠
Try empty passwords	If enabled, Hydra will additionally try user names without using a password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také prázdné heslo.	⃠
Try login as password	If enabled, Hydra will additionally try a user name as the corresponding password.	
	Pokud bude tato volba zaškrtnuta, Hydra použije také stejné heslo jako uživatelské jméno.	⃠
Stop brute forcing after the first success	If enabled, Hydra will stop brute forcing user accounts after the first time an account is successfully accessed.	
	Pokud bude tato volba zaškrtnuta, Hydra zastaví prolamování hesla po prvním úspěšném přístupu.	⃠
Add accounts found by other plugins to the login file	If disabled, only the user names specified in the logins file will be used for the scan. Otherwise, additional user names discovered by other plugins will be added to the logins file and used for the scan.	
	Při zakázání této volby budou použita jen uživatelská jména specifikovaná v souboru se jmény. Při povolení této volby budou přidána uživatelská jména nalezená ostatními pluginy.	⃠
PostgreSQL database name	The database that you want Hydra to test.	
	Jméno databáze pro Hydra test.	⃠
SAP R/3 Client ID (0 - 99)	The ID of the SAP R/3 client that you want Hydra to test.	
	SAP R/3 klient pro Hydra test.	⃠
Windows accounts to test	Can be set to *Local accounts* , *Domain Accounts* , or *Either* .	
	Může být nastaveno *Local accounts* , *Domain Accounts* , nebo *Either* .	⃠
Interpret passwords as NTLM hashes	If enabled, Hydra will interpret passwords as NTLM hashes.	
	Pokud je povoleno, Hydra bude interpretovat hesla jako NTLM hash.	⃠
Cisco login password	This password is used to login to a Cisco system before brute forcing enable passwords. If no password is provided here, Hydra will attempt to login using credentials that were successfully brute forced earlier in the scan.	
	Toto heslo je použito pro přihlášení na Cisco systémy před zkušením hesla hrubou silou. Pokud tu není žádné heslo poskytnuto, Hydra bude zkoušet přihlašovací údaje, které zjistila v předchozích skenech.	⃠
Web page to brute force	Enter a web page that is protected by HTTP basic or digest authentication. If a web page is not provided here, Hydra will attempt to brute force a page discovered by the Nessus web crawler that requires HTTP authentication.	
	Webová stránka pro útok hrubou silou nástrojem Hydra.	⃠
HTTP proxy test website	If Hydra successfully brute forces an HTTP proxy, it will attempt to access the website provided here via the brute forced proxy.	
	Pokud Hydra úspěšně prolomí proxy, bude zkoušet přistoupit na tuto HTTP stránku přes proxy.	⃠
LDAP DN	The LDAP Distinguish Name scope that Hydra will authenticate against.	
	LDAP DN jméno, proti kterému se bude Hydra autentizovat.	⃠

Settings/Assessment/Malware

Nastavení možností testování na Malware, použití známých MD5 hash

General Settings

Disable DNS Resolution	Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.	
	Tato volba zabrání Nessus skeneru používat cloud pro porovnávání nálezů skenu proti známému škodlivému softwaru. Výchozí stav je vypnuto - tedy hledání v cloudu povoleno.	

Hash and Whitelist Files

Provide your own list of known bad MD5 hashes	Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash the description will show up in the scan results.	
	Další známé špatné MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Provide your own list of known good MD5 hashes	Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description will show up in the scan results.	
	Další známé dobré MD5 hashe lze nahrát pomocí txt souboru, který bude obsahovat jeden MD5 hash na řádek. Volitelně je možné přidat popis ke každému hash. Popis se provede tak, že se napíše čárka za hash a pak následuje komentář. Pokud bude nějaký hash zachycen, popis se zobrazí ve výsledcích kontroly.	

Hosts file whitelist	Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check). This option allows you to upload a file containing a list of IPs and hostnames that will be ignored by Nessus during a scan. Include one IP and hostname (formatted identically to your hosts file on the target) per line in a regular text file.	
	Tato možnost vám umožní nahrát soubor obsahující seznam IP adres a aktiv, které budou během skenování skenerem ignorovány. Soubor musí obsahovat jednu IP a hostname na řádek v běžném textovém souboru.	

File System Scanning

Možnosti nastavení skenování souborového systému		
File System Scanning		
Scan File System	Turning on this option allows you to scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.	⃠
	Zapnutí této volby umožňuje skenovat systémové adresáře a soubory na skenovaném aktivu. Upozornění: Povolení tohoto nastavení při zacílení na 10 a více hostů může snížit výkon.	
Directories		
Scan %Systemroot%	Enable file system scanning to scan %Systemroot%	⃠
	Povolí skenovat %Systemroot%	
Scan %ProgramFiles%	Enable file system scanning to scan %ProgramFiles%	⃠
	Povolí skenovat %ProgramFiles%	
Scan %ProgramFiles(x86)%	Enable file system scanning to scan %ProgramFiles(x86)%	⃠
	Povolí skenovat %ProgramFiles(x86)%	
Scan %ProgramData%	Enable file system scanning to scan %ProgramData%	⃠
	Povolí skenovat %ProgramData%	
Scan User Profiles	Enable file system scanning to scan user profiles	⃠
	Povolí skenovat uživatelské profily	
Custom Filescan Directories	Add File Add a custom file that list directories for malware file scanning. List each each directory on one line. **Caution:** Root directories such as 'C:\' or 'D:\' are not accepted.	⃠
	Je možné přidat vlastní adresáře pro skenování na malware. Do textového souboru je napsán každý adresář na jeden řádek. Kořenové adresáře jako C:\ nejsou akceptovány.	
Yara Rules Files		⃠
	Nástroj na identifikaci a klasfikaci malware	

Values for SCADA Options

Tato volba umožňuje ovlivnit možnosti skenování průmyslových SCADA zařízení.		
Modbus/TCP Coil Access		
Start at register End at register	These options are available for commercial users. This drop-down menu item is dynamically generated by the SCADA plugins available with the commercial version of Nessus. Modbus uses a function code of 1 to read "coils" in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a "write coil" message. The defaults for this are "0" for the "Start reg" and "16" for the "End reg".	
ICCP/COTP TSAP Addressing Weakness		
Start COTP TSAP Stop COTP TSAP	The "ICCP/COTP TSAP Addressing" menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to "8" by default.	

Values for Web Applications Options

Nastavení skenování webových aplikací

Web Application Settings

Scan web applications	Enables the **General Settings**, **Web Crawler**, and **Application Test** Settings sections.	
	Zapnutí skenování webových aplikací.	

General Settings

Use a custom User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.	
	Určuje, za jaký typ internetového prohlížeče se bude Nessus vydávat.	

Web Crawler

Start crawling from	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., "/:/php4:/base").	
	Adresa URL, která bude první testována. Pokud je potřeba více stránek, použijte jako oddělaovač dvojtečku (např. /:/php4:/base)	

Excluded pages (regex)	Enable exclusion of portions of the web site from being crawled. For example, to exclude the "/manual" directory and all Perl CGI, set this field to: (^/manual)|(\.pl(\?.*)?$). Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).	
	Dovoluje vyloučit části webu, kterými skener prochází. Například pro vyloučení adresáře "/manual" a všech Perl CGI nastavte do tohoto pole (^/manual)|(\.pl(\?.*)?$). Nessus podporuje regulární výrazy POSIX stejně jako Perl regulární výrazy PCRE.	

Maximum pages to crawl	The maximum number of pages to crawl.	
	Maximální počet stránek, které se mají procházet.	

Maximum depth to crawl	Limit the number of links Nessus will follow for each start page.	
	Omezení počtu odkazů, které bude Nessus následovat za každou úvodní stránkou.	

Follow dynamic pages	If selected, Nessus will follow dynamic links and may exceed the parameters set above.	
	Pokud je zaškrtnuto, Nessus bude následovat dynamické vazby a může přesáhnout parametry uvedené výše.	

Application Test Settings

Enable generic web application tests	Enables the options listed below.	
	Povolí aplikační testy vypsané dále.	

Abort web application tests if HTTP login fails	If Nessus cannot login to the target via HTTP, then do not run any web application tests.	
	Pokud se Nessus nemůže přihlásit k aktivu přes HTTP, pak nepustí žádné další aplikační testy.	

Try all HTTP Methods	This option will instruct Nessus to also use "POST requests" for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Nessus will test each script/variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.	
	Nessus bude krom GET požadavků (výchozí nastavení) zkoušet také POST požadavky. Obecně platí, že složitější aplikace používají metody POST pro posílání uživatelských dat do aplikace. Toto nastavení poskytuje důkladnější testování, ale může značně navýšit potřebný čas. Pokud je toto zaškrtnuto, Nessus bude testovat každou proměnnou, kterou najde ve skriptu na obě metody GET i POST.	

Attempt HTTP Parameter Pollution	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like "/target.cgi?a='&b=2". With HTTP Parameter Pollution (HPP) enabled, the request may look like "/target.cgi?a='&a=1&b=2".	
	Při provádění testů webových aplikací zkouší obejít filtrovací mechanismy vkládáním obsahu do proměnných a zároveň poskytuje stejné proměnné se správným obsahem. Například normální SQL-injection test může vypadat takto: "/target.cgi?a='&b=2" S volbou HTTP Parameter Pollution může vypadat takto: "/target.cgi?a='&a=1&b=2"	

Test embedded web servers	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.	
	Vestavěné webové servery jsou často statické a neobsahují nastavitelné CGI skripty. Krom toho mohou být náchylné k selhání nebo přestanou reagovat během skenování. Proto Tenable doporučuje skenování vestavěných web serverů odděleně od ostatních webů pomocí této volby.	

Test more than one parameter at a time per form	This option manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This drop-down has five options: One value - This tests one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. Some pairs – This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters. All pairs (slower but efficient) – This form of testing is slightly slower but more efficient than the "one value" test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt "/test.php?a=XSS&b=1&c=1&d=1" and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for "/test.php?a=XSS&b=3&c=3&d=3" when the first value of each variable is "1". Some combinations – This form of testing will randomly check a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time. All combinations (extremely slow) – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where "All-pairs" testing seeks to create a smaller data set as a tradeoff for speed, "all combinations" makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.	
	Tato volba řídí kombinaci hodnot argumentu použitých v HTTP dotazu. Výchozí stav (bez hodnoty) testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Toto rozbalovací pole má pět voleb: One Value - testuje jeden parametr současně s útočícím řetězcem, bez zkoušení "non-attack" varinat pro další parametry. Jde o nejrychlejší variantu. Some pairs - Tato forma testování bude náhodně kontrolovat kombinace náhodných párů parametrů. Toto je nejrychlejší cesta, jak otestovat více parametrů. All pairs - (pomalejší, ale efektivnější, než volba "One Value") Some combinations - tato forma testování bude náhodně zkoušet kombinaci tří nebo více parametrů. Bude to trvat déle. All combinations (extrémně pomalé) - Tato metoda bude zkoušet naprosto všechny možné kombinace útočných řetězců s platným vstupem do proměnných. Tento zůsob může trvat velice dlouho.	

Do not stop after the first flaw is found per web page	This option determines when a new flaw is targeted. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless "thorough tests" is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack. The drop-down has four options: Per CGI – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option. Per port (quicker) – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. Per parameter (slow) – As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server. Look for all flaws (slower) – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.	
	Tato volba určuje, kdy je nová chyba zaměřena. To platí na úrovni skriptu. Nalezení XSS chyby nezakáže hledání po SQL-injection nebo "header injection", ale budete mít nanejvýš jednu zprávu pro každý typ na daném portu. Toto pole má čtyři možnosti: Per CGI - Jakmile je skriptem nalezena chyba na CGI, Nessus přepne na další známé CGI na stejném serveru, nebo pokud není jiné CGI, tak na další port/službu. Toto je výchozí volba. Per port (rychlejší) - Jakmile je skriptem nalezena chyba na weobvé službě, Nessus zastaví a přepne se na jinou webovou službu na jiném portu. Per parameter (pomalé) - Jakmile je jeden typ chyby nalezen v parametru CGI (např. XSS) Nessus se přepne na další parametr ze stejné CGI nebo další známou CGI, nebo další port/službu. Look for all flaws (pomalejší) - Provede rozsáhlé testy bez ohledu na zjištěné chyby, Tato volba může vyprodukovat velice obsáhlý a upovídaný report. Tato volba není ve většině případů doporučována.	

URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.	
	URL adresa pro RFI. Zde se specifikuje souboru pro Remote File Inclusion. Ve výchozím nastavení Nessus použije bezpečný soubor hostovaný u výrobce pro RFI testování. Pokud není dostupný internet, bude použit lokální soubor, který určen pro přesnější testování RFI.	

Maximum run time (minutes_)	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.	
	Tato volba řídí množství času v minutách strávených prováděním testů webových aplikací. Standardně je nastavneno na 60minut a platí pro všechny porty a CGI pro dané webové stránky. Skenování v lokálních sítích s malými webovými aplikacemi bude obvykle dokončena za méně než hodinu, nicméně webové stránky s velkými aplikacemi mohou pžadovat vyšší hodnotu.	

Values for Windows Scan Options

Základní nastavení pro Windows

General Setting

Request information about the SMB Domain	If the option Request information about the domain is set, then domain users will be queried instead of local users.	
	Pokud je volba zaškrtnuta, budou dotazování doménoví uživatelé místo lokálních.	

Enumerate Domain User

Start UID	1000	
End UID	1200	

Enumerate Local User

Start UID	1000	
End UID	1200	

Values for Scan Report Options

Nastavení možností reportování		
Processing		
Report Verbosity	Determines the verbosity of the detail in the output of the scan results as Normal, Quiet, or Verbose.	normal
	Určuje míru detailu výstupu skenů. K dispozci jsou tři volby "Normal", "Quite", "Verbose"	
Show missing patches that have been superseded	Show patches in the report that have not been applied but have been superseded by a newer patch if enabled.	✔
	Pokud je volba zapnutá, zobrazí v reportu záplaty, které nebyly aplikovány, ale byly nahrazeny novější záplatou.	
Hide results from plugins initiated as a dependency	If a plugin is only run due to it being a dependency of a selected plugin, hide the results if enabled.	✔
	Skryje výsledky z pluginů, které jsou spuštěny v závislosti na jiných.	
Output		
Designate hosts by their DNS name	When possible, designate hosts by their DNS name rather than IP address in the reports.	✔
	Pokud je to možné, určit aktivum podle DNS jména, nikoliv podle IP adresy.	
Display hosts that respond to ping	When enabled, show a list of hosts that respond to pings sent as part of the scan.	✔
	Pokud je povoleno, zobrazí seznam aktiv, které odpoví na PING jako součást skenu.	
Display unreachable hosts	Display a list of hosts within the scan range that were not able to be reached during the scan, if enabled.	⃠
	Pokud je povoleno, zobrazí seznam aktiv, které jsou během skenu nedostupné.	
Generate SCAP XML Results	Generate a SCAP XML results file as a part of the report output for the scan.	⃠
	Generovat SCAP XML souboru jako součást skenu.	

Value for Authentication Options

Nastavení možností autentizace použité během skenování		
Authentication	When added, authentication methods may be used to login to the scan target machines to gather more complete results of the host's status. The authentication types include host, database, miscellaneous, plaintext authentication, and patch management. For each type, various relevant options are presented such as SNMPv3, MongoDB, VMWare APIs, and similar.	
	Možnost přidání další vlastní autentizační metody.	⃠
SNMP		
UDP Port	This is the UDP port that will be used when performing certain SNMP scans. Up to four different ports may be configured, with the default port being 161.	
	UDP port pro provádění SNMP skenů. Až čtyři různé porty mohou být definovány.	161
SSH		
known_hosts file	If an SSH known_hosts file is provided for the scan policy in the "known_hosts file" field, Nessus will only attempt to log in to hosts defined in this file. This helps to ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.	
	Pokud je skenovací politice poskytnut soubor "known_hosts", Nessus se bude pokoušet hlásit jen na aktiva uvedená v tomto souboru. (v souboru "know_hosts" budou uvedeny veřejné klíče - SSH fingerprinty - těchto aktiv). To pomáhá zajistit, že přihlašovací údaje, které používáte na své známé SSH servery nebudou použity k pokusu o přihlášení do systému, který nemusí být pod Vaší kontrolou. (např. honeypoty).	⃠
Preferred port	This option is set to direct the scan to connect to a specific port if SSH is known to be listening on a port other than the default of 22.	
	Pokud by SSH naslouchalo na jiném než standardním portu, pak by se jiný port nastavil zde.	22
Client Version	Specifies which type of SSH client to impersonate while performing scans.	
	Specifikuje, jaký typ SSH klienta bude během skenu představen.	OpenSSH_5.0
Windows		
Never send credentials in the clear	By default, Windows credentials are not sent to the target host in the clear.	
	Ve výchozím nastavení (zaškrtnuto) nejsou posílány přihlašovací údaje do Windows v otevřeném tvaru.	✔
Do not use NTLMv1 authentication	If the "Do not use NTLMv1 authentication" option is disabled, then it is theoretically possible to trick Nessus into attempting to log in to a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a "hash" obtained from Nessus. This "hash" can be potentially cracked to reveal a username or password. It may also be used to directly log in to other servers. Because NTLMv1 is an insecure protocol this option is enabled by default.	
	Pokud je volba ""Do not use NTLMv1 authentication" zakázána, je teoreticky možné přimět Nessus, aby se pokusil přihlásit k Windows serveru s doménovými přihlašovacími údaji pomocí NTLM verze 1. To poskytuje vzdálenému útočníkovi možnost použít "hash" obdržený z Nessus. Tento "hash" může být potencionálně zneužit jako jméno a heslo. Též to může být použito k přímému přihlášení na další servery. Protože je NTLM v. 1 nebezpečný protokol, je tato volba ve výchozím stavu povolena.	✔
Start the Remote Registry service during the scan	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.	
	Tato volba říká Nessusu, aby nastartoval službu Vzdálený registr (Remote Registry service) na skenovaném aktivu, pokud tato služba neběží. Tato služba je nezbytná pro vykonání některých Windows kontrol.	⃠
Enable administrative shares during the scan	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.	
	Tato volba dovolí skeneru přistoupit k určitým položkám v registru, které lze číst je s oprávněním správce.	⃠
Plaintext Authentication		
Perform patch audits over telnet	When enabled, patch audits will be permitted over a telnet connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	
	Pokud je toto povoleno, bude sken povolen přes TELNET spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	⃠
Perform patch audits over rsh	When enabled, patch audits will be permitted over a rsh connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	
	Pokud je toto povoleno, bude sken povolen přes RSH spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	⃠
Perform patch audits over rexec	When enabled, patch audits will be permitted over a rexec connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.	
	Pokud je toto povoleno, bude sken povolen přes REXEC spojení. Tento protokol je však v prostém textu a jeména a hesla procházejí v nešifrované podobě a můžou být zachycena. Tato možnost je ve výchozím nastavení zakázána.	⃠
HTTP		
Login method	Specify if the login action is performed via a GET or POST request.	
	Speifikace přihlašovací metody pro HTTP (GET/POST)	POST
Re-authenticate delay (seconds)	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.	
	Časová prodleva mezi pokusy o přihlášení. Tato volba je použitelná při obcházení zamykacího mechanismu.	0
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.	
		0
Invert authenticated regex	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., "Authentication failed!").	
	Na přihlašovací stránce bude Nessus hledat řetězec o neúspěšném přihlášení. (např. Authentication failed).	⃠
Use authenticated regex on HTTP headers	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.	
	Hledání výsledku autentizace v HTTP hlavičce.	⃠
Case insensitive authenticated regex	The regex searches are case sensitive by default. This instructs Nessus to ignore case.	
		⃠

Plugins

Skenovací zásuvné moduly nebo-li "pluginy" jsou jednotlivé dílčí kontroly prováděné během skenu. Jsou řazeny do skupin (family) podle platformy.
Pokud jsou vybrány všechny kontroly, Nessus na skenované aktivum aplikuje jen ty kontroly, které odpovídají danému operačnímu systému.
Pokud chceme získat výsledky pouze z některých konkrétních kontrol, označíme jen ty, které se mají během skenu vykonat.

Zapnuty všechny	⃠
Vypnuty všechny	✔
Specifický vběr	⃠

Plugin ID	Plugin Family	Název

Compliance

Tzv. "Compliance" skeny umožňují importovat vlastní auditní soubor, který definuje další jednotlivé kontroly, které např. vychází z vlastních bezpečnostních politik, nebo např. z obecně platného standardu CIS.

Použití auditního souboru		⃠

Příloha č. 8.

GPO politika pro OS Windows

BICT_Nessus_ips_c

BICT_Nessus_ips_c

Data collected on: 13.4.2017 11:36:01
User Revisions: 3 (AD), 3 (sysvol)
Computer Revisions: 20 (AD), 20 (sysvol)

General

Details

Domain	ad.cpost.cz
Owner	AD\svcagpm
Created	13.4.2017 11:13:10
Modified	13.4.2017 11:26:36
User Revisions	3 (AD), 3 (sysvol)
Computer Revisions	20 (AD), 20 (sysvol)
Unique ID	{349C5679-2BFF-47B5-A899-9E217C6B23CC}
GPO Status	User settings disabled

Links

Location	Enforced	Link Status	Path
None			

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
AD\AD_Nessus_IPS_Test_G

WMI Filtering

WMI Filter Name	None
Description	Not applicable

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
AD\AD_Nessus_IPS_Test_G	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Deny log on as a service	AD\AD_Nessus_local_access_G
Deny log on locally	AD\AD_Nessus_local_access_G
Deny log on through Terminal Services	AD\AD_Nessus_local_access_G

Local Policies/Security Options

Network Access

Policy	Setting
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves

System Services

Remote Registry (Startup Mode: Automatic)

Permissions
No permissions specified

Auditing
No auditing specified

Windows Management Instrumentation (Startup Mode: Automatic)

Permissions
No permissions specified

Auditing
No auditing specified

Windows Firewall with Advanced Security

Global Settings

Policy	Setting
Policy version	2,26
Disable stateful FTP	Not configured
Disable stateful PPTP	Not configured
IPsec exempt	Not configured
IPsec through NAT	Not configured
Preshared key encoding	Not configured
SA idle time	Not configured
Strong CRL check	Not configured

Inbound Rules

Name	Description
CPOST_NESSUS_WMI (WMI-In)	Not configured

This rule may contain some elements that cannot be interpreted by current version of GPMC reporting module	
Enabled	True
Program	%systemroot%\system32\svchost.exe
Action	Allow
Authorized computers	Not configured
Authorized users	Not configured
Protocol	6
Local port	Any
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	10.xxx.xxx.132, 10.xxx.xxx.68, 10.xxx.xxx.228, 10.xxx.xxx.133, 10.
Profile	Domain
Network interface type	All
Service	winmgmt
Allow edge traversal	False
Group	Not configured

CPOST_NESSUS_ICMP	Not configured

This rule may contain some elements that cannot be interpreted by current version of GPMC reporting module	
Enabled	True
Program	Any
Action	Allow
Authorized computers	Not configured
Authorized users	Not configured
Protocol	1
Local port	Any
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	10.xxx.xxx.132, 10.xxx.xxx.68, 10.xxx.xxx.228, 10.xxx.xxx.133, 10.
Profile	Domain
Network interface type	All
Service	All programs and services
Allow edge traversal	False
Group	Not configured

CPOST_NESSUS_SMB	Not configured

This rule may contain some elements that cannot be interpreted by current version of GPMC reporting module	
Enabled	True
Program	system
Action	Allow
Authorized computers	Not configured
Authorized users	Not configured
Protocol	6
Local port	139, 445
Remote port	Any

ICMP settings	Any
Local scope	Any
Remote scope	10.xxx.xxx.132, 10.xxx.xxx.68, 10.xxx.xxx.228, 10.xxx.xxx.133, 10.
Profile	Domain
Network interface type	All
Service	All programs and services
Allow edge traversal	False
Group	Not configured

CPOST_NESSUS_WMI (ASync-In)	Not configured
This rule may contain some elements that cannot be interpreted by current version of GPMC reporting module	
Enabled	True
Program	%systemroot%\system32\wbem\unsecapp.exe
Action	Allow
Authorized computers	Not configured
Authorized users	Not configured
Protocol	6
Local port	Any
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	10.xxx.xxx.132, 10.xxx.xxx.68, 10.xxx.xxx.228, 10.xxx.xxx.133, 10.
Profile	Domain
Network interface type	All
Service	All programs and services
Allow edge traversal	False
Group	Not configured

CPOST_NESSUS_WMI (DCOM-In)	Not configured
This rule may contain some elements that cannot be interpreted by current version of GPMC reporting module	
Enabled	True
Program	%systemroot%\system32\svchost.exe
Action	Allow
Authorized computers	Not configured
Authorized users	Not configured
Protocol	6
Local port	135
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	10.xxx.xxx.132, 10.xxx.xxx.68, 10.xxx.xxx.228, 10.xxx.xxx.133, 10.
Profile	Domain
Network interface type	All
Service	All programs and services
Allow edge traversal	False
Group	Not configured

Preferences

Control Panel Settings

Local Users and Groups

Group (Name: Administrators (built-in))

Administrators (built-in) (Order: 1)

Local Group

Action	Update

Properties

Group name	Administrators (built-in)
Delete all member users	Disabled
Delete all member groups	Disabled

Add members

Name	Security Identifier (SID)
AD\svcSC4_Nessus_ips	S-1-5-21-3951749903-3806043176-1814297650-38302

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Disabled)

No settings defined.

Příloha č. 9.

Ukázka výsledného reportu ze skenu typu „PATCH AUDIT sken“

Sken testovacích serverů systému IPS

SecurityCenter™

CP_PATCH_sken_přehled_H.C. (Scan: IPS)

May 1, 2017 at 12:19pm CEST

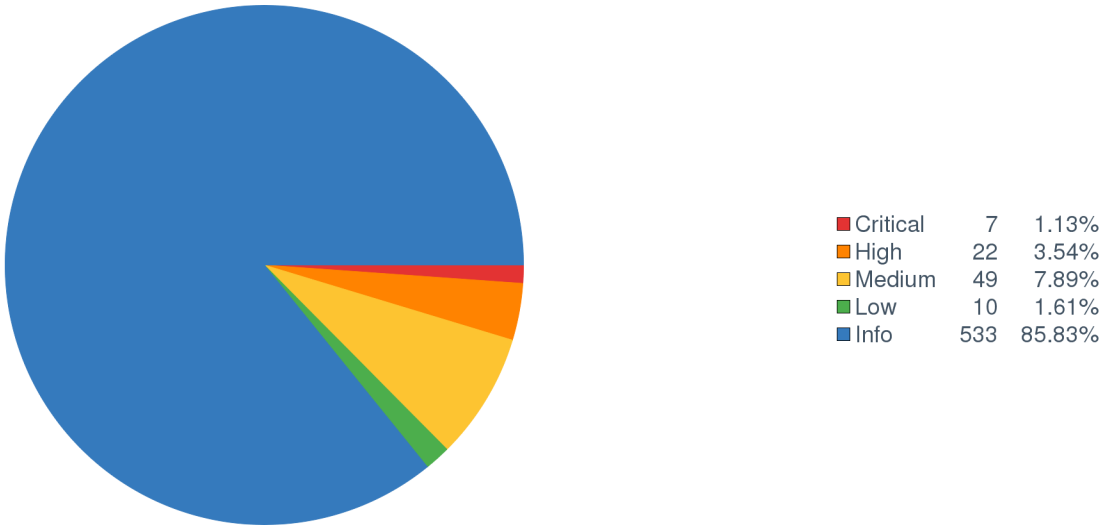
Michal Miklánek [mimiu]
CESKA POSTA S. P.

Souhrn

Tento report ukazuje výsledku skenu zranitelností na níže uvedených aktivech. Jednalo se o tzv. PATCH_AUDIT sken operačního systému.

Cílem takového skenu je zjištění, které opravné balíky na daném aktivu chybí. Tento report vypisuje chybějící patche se závažností CRITICAL a HIGH.

Přehled zranitelností na skenovaných aktivech



IP přehled skenovaných aktiv

IP Address	Score	Total	Vulns
10.165.2.87	183	144	8 7 125
10.165.2.86	251	161	9 13 134
10.165.2.85	118	177	18 4 152
10.165.2.84	105	139	11 122

Výčet zranitelností na jednotlivých aktivech

10.165.2.87

IP Address: 10.165.2.87
NetBIOS Name: AD\IPS5T-AS
DNS Name: ips5t-as.centrum.cpost.cz
OS CPE: cpe:/o:microsoft:windows_server_2012:r2:gold:x64-datacenter
MAC Address: 00:50:56:b3:33:86
Score: 183
Repository: DC_Malešice_ISZS

Počty zranitelností dle závažnosti HIGH a CRITICAL

Severity	Count
Critical	2
High	8

Výpis zranitelností závažnosti: Critical, High

Plugin	Plugin Name	Severity
72704	Microsoft .NET Framework Unsupported	Critical
92516	Oracle Java SE Multiple Vulnerabilities (July 2016 CPU)	Critical
81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)	High
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	High
90625	Oracle Java SE Multiple Vulnerabilities (April 2016 CPU)	High
90828	Oracle Java SE Hotspot JSR 292 Method Handles RCE	High
94138	Oracle Java SE Multiple Vulnerabilities (October 2016 CPU)	High
96628	Oracle Java SE Multiple Vulnerabilities (January 2017 CPU) (SWEET32)	High
99312	KB4015550: Windows 8.1 and Windows Server 2012 R2 April 2017 Cumulative Update	High
99588	Oracle Java SE Multiple Vulnerabilities (April 2017 CPU)	High

Výpis otevřených portů na skenovaném aktivu

Port	Info	Low	Med.	High	Crit.	Total
0	36	0	0	0	0	36
123	2	0	0	0	0	2
135	3	0	0	0	0	3
137	2	0	0	0	0	2
138	2	0	0	0	0	2
139	3	0	0	0	0	3
445	40	1	2	8	2	53
3389	12	1	5	0	0	18
5355	2	0	0	0	0	2
5985	2	0	0	0	0	2
49152	3	0	0	0	0	3
49153	3	0	0	0	0	3
49154	3	0	0	0	0	3
49155	3	0	0	0	0	3
49173	3	0	0	0	0	3
49196	3	0	0	0	0	3
49198	3	0	0	0	0	3

10.165.2.86

IP Address: 10.165.2.86
NetBIOS Name: AD\IPS4T-AS
DNS Name: ips4t-as.centrum.cpost.cz
OS CPE: cpe:/o:microsoft:windows_server_2012:r2:gold:x64-datacenter
MAC Address: 00:50:56:91:cd:e4
Score: 251
Repository: DC_Malešice_ISZS

Počty zranitelností dle závažnosti HIGH a CRITICAL

Severity	Count
Critical	3
High	9

Výpis zranitelností závažnosti: Critical, High

Plugin	Plugin Name	Severity
72704	Microsoft .NET Framework Unsupported	Critical
97737	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY)	Critical
97743	MS17-012: Security Update for Microsoft Windows (4013078)	Critical
81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)	High
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	High
97729	MS17-006: Cumulative Security Update for Internet Explorer (4013073)	High
97731	MS17-009: Security Update for Microsoft Windows PDF Library (4010319)	High
97732	MS17-011: Security Update for Microsoft Uniscribe (4013076)	High
97733	MS17-017: Security Update for Windows Kernel (4013081)	High
97738	MS17-018: Security Update for Windows Kernel-Mode Drivers (4013083)	High
97794	MS17-013: Security Update for Microsoft Graphics Component (4013075)	High
99312	KB4015550: Windows 8.1 and Windows Server 2012 R2 April 2017 Cumulative Update	High

Výpis otevřených portů na skenovaném aktivu

Port	Info	Low	Med.	High	Crit.	Total
0	37	0	0	0	0	37
123	2	0	0	0	0	2
135	3	0	0	0	0	3
137	2	0	0	0	0	2
138	2	0	0	0	0	2
139	3	0	0	0	0	3
445	37	1	8	9	3	58
3389	12	1	5	0	0	18
5355	2	0	0	0	0	2
5985	2	0	0	0	0	2
7937	2	0	0	0	0	2
7938	5	0	0	0	0	5
8648	2	0	0	0	0	2
9001	2	0	0	0	0	2
49152	3	0	0	0	0	3
49153	3	0	0	0	0	3
49154	3	0	0	0	0	3
49155	3	0	0	0	0	3
49168	3	0	0	0	0	3
49203	3	0	0	0	0	3
49204	3	0	0	0	0	3

10.165.2.85

IP Address: 10.165.2.85
NetBIOS Name: AD\IPS3T-DS
DNS Name: ips3t-ds.centrum.cpost.cz
OS CPE: cpe:/o:microsoft:windows_server_2012:r2:gold:x64-datacenter
MAC Address: 00:50:56:91:10:86
Score: 118
Repository: DC_Malešice_ISZS

Počty zranitelností dle závažnosti HIGH a CRITICAL

Severity	Count
Critical	1
High	2

Výpis zranitelností závažnosti: Critical, High

Plugin	Plugin Name	Severity
72704	Microsoft .NET Framework Unsupported	Critical
81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)	High
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	High

Výpis otevřených portů na skenovaném aktivu

Port	Info	Low	Med.	High	Crit.	Total
0	36	0	0	0	0	36
123	2	0	0	0	0	2
135	3	0	0	0	0	3
137	2	0	0	0	0	2
138	2	0	0	0	0	2
139	3	0	0	0	0	3
445	39	1	5	2	1	48
1433	11	2	8	0	0	21
3389	12	1	5	0	0	18
5355	2	0	0	0	0	2
5985	2	0	0	0	0	2
6728	2	0	0	0	0	2
7937	2	0	0	0	0	2
7938	5	0	0	0	0	5
8000	2	0	0	0	0	2
8464	2	0	0	0	0	2
9117	2	0	0	0	0	2
9443	2	0	0	0	0	2
49152	3	0	0	0	0	3
49153	3	0	0	0	0	3
49154	3	0	0	0	0	3
49155	3	0	0	0	0	3
49160	3	0	0	0	0	3
49188	3	0	0	0	0	3
49205	3	0	0	0	0	3

10.165.2.84

IP Address: 10.165.2.84
NetBIOS Name: AD\IPS3T-AS
DNS Name: ips3t-as.centrum.cpost.cz
OS CPE: cpe:/o:microsoft:windows_server_2012:r2:gold:x64-datacenter
MAC Address: 00:50:56:b3:5f:6e
Score: 327
Repository: DC_Malešice_ISZS

Počty zranitelností dle závažnosti HIGH a CRITICAL

Severity	Count
Critical	1
High	3

Výpis zranitelností závažnosti: Critical, High

Plugin	Plugin Name	Severity
72704	Microsoft .NET Framework Unsupported	Critical
81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)	High
85847	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)	High
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	High

Výpis otevřených portů na skenovaném aktivu

Port	Info	Low	Med.	High	Crit.	Total
0	36	0	0	0	0	36
123	2	0	0	0	0	2
135	3	0	0	0	0	3
137	2	0	0	0	0	2
138	2	0	0	0	0	2
139	3	0	0	0	0	3
445	37	1	6	3	1	48
3389	12	1	5	0	0	18
5355	2	0	0	0	0	2
5985	2	0	0	0	0	2
49152	3	0	0	0	0	3
49153	3	0	0	0	0	3
49154	3	0	0	0	0	3
49155	3	0	0	0	0	3
49163	3	0	0	0	0	3
49177	3	0	0	0	0	3
49178	3	0	0	0	0	3