UNICORN COLLEGE

Katedra informačních technologií

BAKALÁŘSKÁ PRÁCE

Bezpečnost a komunikace v síti obsahující Windows 10 a Windows Server 2012R2

Autor práce: Ladislav Nový

Vedoucí práce: Ing. David Hartman, Ph.D.

2018 Praha

UNICORN COLLEGE

Katedra Informačních technologií

Akademický rok 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení: Ladislav Nový

Studijní program: Systémové inženýrství a informatika

Studijní obor: Management ICT projektů

Název práce: Bezpečnost a komunikace v síti obsahující Windows 10 a Windows Server 2012R2

CÍL

Cílem práce je popsat a otestovat bezpečnost formou penetračního testování v síti obsahující Windows 10 a Windows 2012R2 a poukázat na časté problémy v bezpečnosti. Práce krom jiného popíše celý proces penetračního testovaní takového prostředí.

Cílem praktické části tedy bude připravit jak klientské prostředí Microsoft Windows 10 tak i serverové prostředí Windows 2012R2 společně s nutnými prvky AD a DNS a testovací stanici s nainstalovaným Kali Linuxem. Pro toto prostředí poté popsat způsob komunikace, ověření autentizace jednotlivých prvků systému a provést kontrolu zabezpečení systémů ve stávající konfiguraci za pomoci penetračních nástrojů a implementace best know-how ať již na základě best-practice tak i dle zjištěného stavu po kontrole.

OSNOVA

Úvod - Představení produktů a důležitost bezpečnosti.
1. Příprava prostředí
2. Komunikace a způsoby ověření v systémech (Kerberos, NTLM, Security auditing)
3. Kontrola zabezpečení - Kali Linux - Vulnerability scanning (Nessus), NMAP, Metasploit
4. Implementace best know-how (GPO, security nastavení)

Závěr - Shrnutí poznatků
Přílohy

DOPORUČENÁ LITERATURA

- Wiliam Panek.Microsoft Windows Server 2012R2 Installation and configuration. Sybex 1edition 2015. 978-1118870204
- Wiliam Panek.Microsoft Windows Server 2012R2 Administration Study Guide. Sybex 1edition 2015. 978-1118870181
- William Panek.Windows server 2012R2 Configurating Advanced Services. Sybex 1edition. 978-1118870129
- Michael G.Solomon. Security Strategies in Windows Platforms and Applications.Jones & Bartlett Learning 1 edition 2010.978-0763791933
-Wolf Halton, Bo Weaver.Kali Linux 2: Windows Penetration Testing.Packt Publishing 2016.1782168494

Vedoucí bakalářské práce:	David Hartman
Adresa pracoviště:	V Kapslovně 2767/2, 130 00 Praha 3
Datum zadání bakalářské práce:	11.10.2016
Termín odevzdání bakalářské práce:	04.05.2018

V Praze dne 04.05.2018

Unicorn College
UNICORN COLLEGE
V Kapslovně 2767/2, 130 00 Praha 3

.....
doc. Ing. Jan Čadil, Ph.D.
Rektor

Čestné prohlášení

Prohlašuji, že jsem svou bakalářskou práci na téma Bezpečnost a komunikace v síti obsahující Windows 10 a Windows Server 2012R2 vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím výhradně odborné literatury a dalších informačních zdrojů, které jsou v práci citovány a jsou také uvedeny v seznamu literatury a použitých zdrojů. Jako autor této bakalářské práce dále prohlašuji, že v souvislosti s jejím vytvořením jsem neporušil autorská práva třetích osob a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb.

V Praze dne 4.5.2018 ..... Ladislav Nový .....

(Ladislav Nový)

Poděkování

Děkuji vedoucímu bakalářské práce Ing. David Hartman Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

Bezpečnost a komunikace v síti obsahující Windows 10 a Windows Server 2012R2

Security and communication in a network based on Windows 10 and Windows Server 2012R2

UNICORN COLLEGE

Abstrakt

Cílem práce je popsat a otestovat bezpečnost formou penetračního testování v síti obsahující Windows 10 a Windows 2012R2 a poukázat na časté problémy v zabezpečení komunikace mezi prostředími. Práce krom jiného popíše celý proces penetračního testování takového prostředí. I přesto, že v současné době stále ve většině společností, podle zkušeností autora, převažuje klientský systém Microsoft Windows 7.

Cílem praktické části je tedy připravit jak klientské prostředí Microsoft Windows 10, tak i serverové prostředí Windows 2012R2 společně s nutnými prvky AD a DNS a testovací stanici s nainstalovaným Kali Linuxem. Následně popsat způsob komunikace klientské a serverového prostředí, ověření autentizace jednotlivých prvků systému a provést kontrolu zabezpečení systémů ve stávající konfiguraci za pomoci penetračního nástroje Kali Linux. V posledním kroku je implementováno best know-how ať již na základě best-practice, tak i dle zjištěného stavu po kontrole.

Klíčová slova:

Microsoft Windows 10, Microsoft Windows 2012R2, Kali Linux,
Penetrační testování

Abstract

The goal of this thesis is to test the security by running penetration tests in network that is based on Microsoft Windows 10 and Microsoft Windows 2012R2 systems. The focus is to point at common problems in security settings. Besides testing, the whole penetration process will also bes described.

In the practical part, servers and clients will be created. A client Microsoft Windows 10 station and Microsoft Windows 2012R2 as server based computer with AD, DNS services. Kali Linux distribution machine is deployed for penetrating testing. In addition process of communication, authentication and authorization between Microsoft based machines together with penetration scanning to uncover possible security misconfiguration will be described. At the end a best-practice document will be created based on actual test result.

Keywords:

Microsoft Windows 10, Microsoft Windows 2012R2, Kali Linux,
Penetration Testing

Obsah

Úvod

V současné době lze považovat bezpečnost v IT sektoru za jedno z nejdůležitějších témat. Společnosti musejí být připraveny čelit jak vnějším, tak i vnitřním útokům. Ve většině případů si firmy již začaly uvědomovat důležitost zabezpečení vůči vnějším útokům z internetu které jsou stále častější. V našem případě se jedná o téma, které není dle názoru autora až tolik diskutované, ale právě samotné ohrožení může být v některých případech mnohonásobně vyšší. Ve vnitřním prostředí sítě se může nacházet mnohem větší skrytá hrozba, která dokáže přinést firmě četné nepříjemnosti, ať už jde o únik informací týkajících se jednotlivých uživatelů, know-how společnosti, nebo poškození dobrého jména.

Útočníci, se snaží pronikat do počítačových sítí z mnoha důvodů. Dle autorů knihy [1] Smith Ben., Komar Brian je motivace útočníků dána několika faktory:

1. Proslulost, Přijetí a ego
2. Finanční zisk
3. Výzva
4. Aktivismus,
5. Pomsta
6. Špionáž
7. Informační válka

Může to být právě zaměstnanec, který není spokojen ve firmě, nudí se a rád by firmě touto cestou uškodil anebo získal informace, které by nadále mohl využít pro svůj prospěch.

Práce se snaží předvést jednotlivé scénáře, které by mohly v podnikovém prostředí nastat, popsat je a následně i navrhnout řešení jednotlivých nalezených problémů společně s dalšími příklady nastavení které mohou být použity.

[1] SMITH, Ben. a Brian KOMAR. *Zabezpečení systému a sítě Microsoft Windows*. Přeložil David KRÁSENSKÝ, přeložil Anna RYCHETSKÁ. Brno: Computer Press, 2006. ISBN 80-251-1260-8. Str. 49

Testovací platorma se skládá z klientského operačního systému Windows 10 společně se serverovou verzi operačního systému Windows Server 2012R2. Oba dva systémy v našem případě similují právě ono diskutované firemní prostředí, v kterém je klientská stanice součástí domény provozované na straně serverové. Pro možnost praktického předvedení jednotlivých útoků je v rámci testovací platformy přítomna i distribuce Kali Linux obsahující penetrační nástroje.

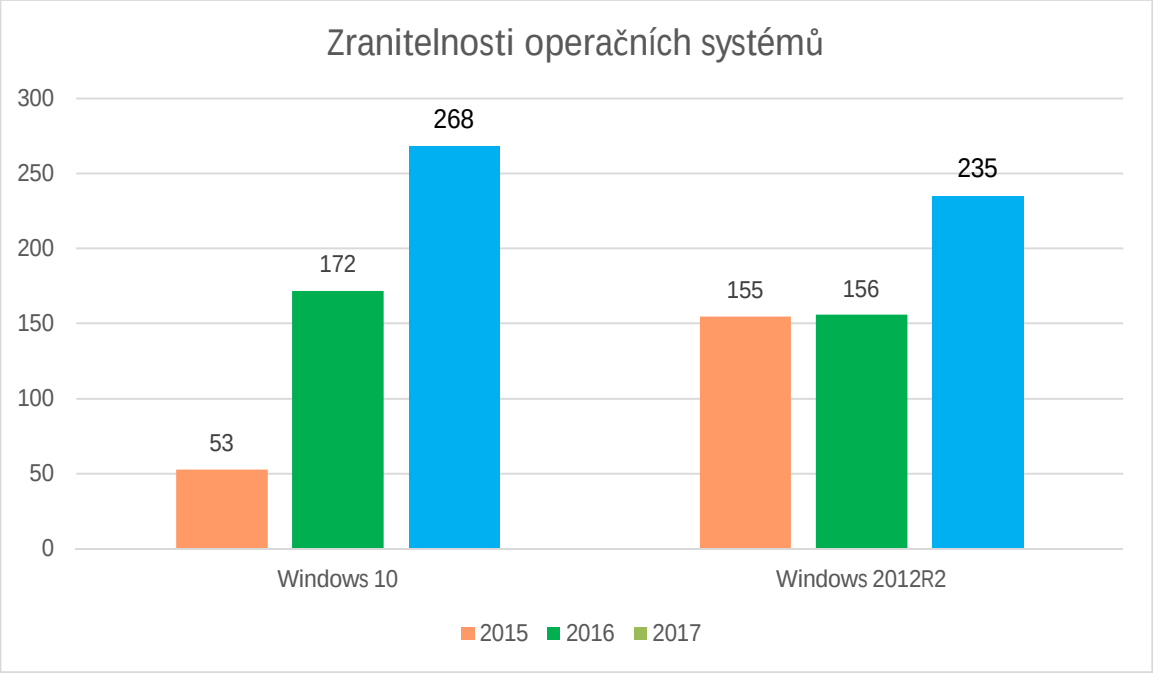
Pro ověřování bezpečnosti jednotlivých nastavení se používají zmíněné penetrační nástroje, které ověřují právě nastavení jednotlivých komponent proti jejich zneužití a následnému neautorizovanému přístupu do sítě.

Je důležité si také uvědomit, že pouhá instalace systému nezaručuje nejvyšší možnou bezpečnost systému samotného. Je proto vždy potřeba vyvážit nastavení samotného systému, jak z pohledu nastavení bezpečnosti, tak i uživatelské přívětivosti.

Dle statistik vyobrazených na [Graf 1], je možné vidět vzrůstající tendenci jednotlivých zranitelností nalezených v operačních systémech, které jsou každým rokem vyšší.

I přes četné aktualizace systému ze stran výrobce, dochází stále k nalézání nových hrozeb, a proto by každá společnost měla implementovat systém, který tuto skutečnost zohledňuje a proces zabezpečení se stane jedním z klíčových prvků.

Graf 1: Zranitelnosti operačních systémů Windows 10 a Windows Server 2012R2



Zdroj: [2,3]

Bakalářská práce v úvodu popisuje jednotlivé prvky systému Windows a přibližuje čtenáři jednotlivé komponenty, které jsou dále využívány. Součástí teoretické části je způsob komunikace mezi klientským a serverovým systémem společnosti Microsoft při jejich vzájemné interakci při ověřování a autentizaci, která probíhá při přihlašování v doménovém prostředí.

Před praktickou částí je popsán úvod do sítí TCP/IP, jako příprava pro následující část, která se zabývá jednotlivými scénáři, které mohou nastat.

Je nutno zmínit, že práce vysvětluje a ukazuje praktiky, které by bylo možné teoreticky dálé využít k získání neoprávněného přístupu k podobným druhům systémů. Nejedná se ale o návod pro čtenáře a autor se striktně vymezuje vůči podobnému smýšlení a orientuje prácí a její účel právě pro bezpečnost samotnou, která je zde v samostatné kapitole a řeší nalezené možnosti k průniku.

[2]CVE DETAILS–Vulnerability statistics [online].2016 [cit.2016.26.12] Dostupné z:http://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26.
[2]CVE DETAILS–Vulnerability statistics [online].2016 [cit.2016.26.12]Dostupné z:http://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26.

Nastavení testovacího prostředí

Práce samotná pro otestování bezpečnosti využívá penetrační nástroj Kali Linux aktualizovaný na poslední verzi vydanou vzhledem k datu instalace. Je třeba respektovat fakt, že útočníci vytvářející hrozby a napadají počítačové systémy. Jsou vždy o krok napřed, a proto je možné, že software samotný není schopen identifikovat všechny aktuální hrozby. Práce samotná si ani nedává za cíl zmapovat všechny druhy útoků, které je možné využít. Nezaměřuje se tedy na útoky typu DOS, MITM ani různé druhy sociálního inženýrství. Práce samotná se zaměřuje na otestování stávajícího prostředí z vnitřní sítě LAN, za pomoci penetračních nástrojů, kdy útočník působí v roli insidera a má tedy přístup k počítači zapojeného do sítě. Nepředpokládají se proto ani útoky z vnější sítě Internet.

1. Představení využívaného softwaru

Microsoft Windows 10 – samotný systém je postaven na jádru NT (New Technology) ve verzi 10.0. Systém je dostupný ve více edicích, které zpřístupňují a případně omezují jednotlivé funkcionality systému. V práci je využívána verze PRO[4] vzhledem k funkcionalitám umožňujícím kooperaci serverového systému Windows Server 2012R2 se systémem klientským, a to i pro jejich bezplatnou dostupnost přes portál Microsoft Imagine díky školnímu účtu Unicorn College S.R.O.

Tabulka 1: Minimální požadavky pro instalaci systému Microsoft Windows 10 -64bit

RAM	Disk	Procesor	Rozlišení
2GB	20GB	1GHz (64-bit)	VGA 800 x 600

Zdroj: Vlastní zpracování

Windows Server 2012R2 – postaven na jádru NT ve verzi 6.3. Systém je dostupný ve více verzích. Pro naši potřebu je využívána verze STANDARD[5] a to

[4]Microsoft: Windows 10 Compare Table document - [cit.2017.5.1]
Dostupné z http://wincom.blob.core.windows.net/documents/Win10CompareTable_FY17.pdf
[5]Microsoft: Windows Server 2012 R2 Products and Editions Comparison[cit.2017.5.1]

vzhledem k dostatečné funkčnosti v rámci práce a její snadné dostupnosti díky školnímu účtu v programu Microsoft Image dovolující bezplatné stažení systému.

Tabulka 2: Minimální požadavky pro instalaci systému Microsoft Windows Server 20012R2

RAM	Disk	Procesor	Rozlišení
512MB	32GB	1.4Ghz (64-bit)	VGA 800 x 600

Zdroj: Vlastní zpracování

Kali Linux – Jedná se o penetrační distribuci postavenou na operačním systému Linux, konkrétně na distribuci Debian. Operační systém Linux vznikl v roce 1991 jako osobní projekt Linusu Torvaldse, finského vysokoškolského studenta. [6]Postupem času se začaly vytvářet různé distribuce, které využívaly jádro systému Linux a nabízely dodatečnou funkčnost. Podobným způsobem vznikl i Kali Linux. Jako základ byla použita distribuce Debian, která byla modifikována dalšími rozšířeními používanými pro penetrační testování.

V bezpečnostní komunitě se na Kali Linux nahlíží jako na určitý standard, který obsahuje velké množství běžných nástrojů využívaných při penetračním testování. Bývá pravidlem, a to i přes to, že distribuce obsahuje velké množství nástrojů fakt, že většina penetračních testerů si distribuci přizpůsobuje dle svého uvážení dalšími rozšířeními.

2. Důležité komponenty testovaného systému

Pro porozumění dalším jevům, které budou zmíněné v dálších částech bakalářské práce, je zapotřebí si představit jednotlivé komponenty, které budou dále využívány.

Dostupné z:https://blogs.msdn.microsoft.com/robmar/2014/02/10/windows-server-2012-r2-products-and-editions-comparison/

[6] NEMETH, Evi, Garth SNYDER a Trent R. HEIN. Linux: kompletní příručka administrátora: 2. aktulizované vydání. 2008. ISBN 978-80-251-2410-9.Str. 43

2.1 Jádro systému Windows

Existují dvě základní varianty jader systému. Jádro monolitické a tzv. microkernel.

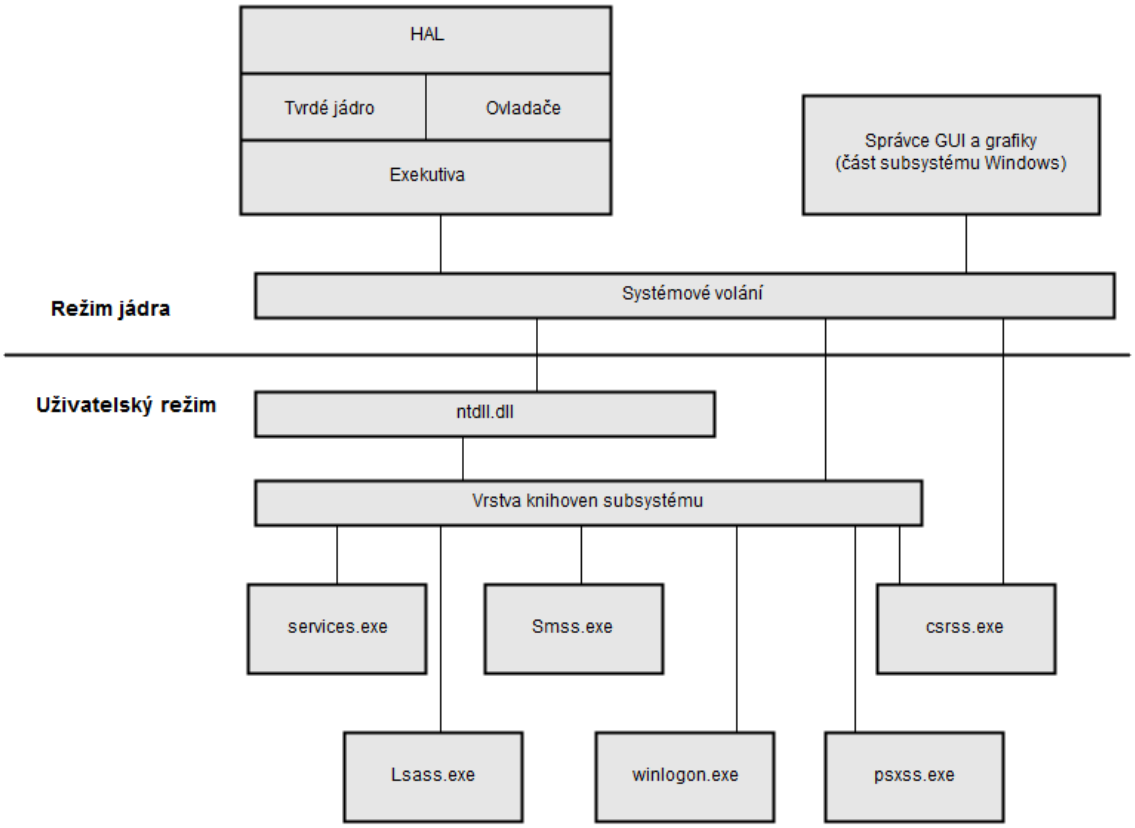
Jádro monolitické obsahuje většinu komponent nutných pro běh systému – souborové systémy, správu procesů, síťovou komunikaci nebo bezpečnostní model. Všechny tyto komponenty obvykle sdílejí jeden virtuální adresový prostor, díky kterému je umožněna rychlá komunikace mezi jednotlivými komponenty. Na stranu druhou může docházet k nechtěnému narušení datové struktury, nutné pro správné fungovaní jednotlivéch komponent, z kterých pak může vyústit pád celého systému.[7]

Jádro microkernel je opakem výše popsaného, zde samotné jádro vykonává pouze základní funkce typu: plánování vláken, předávání zpráv mezi procesy atp. Většina ostatních komponent se nachází mimo jádro samotné, ve formě modulů, zajišťujících ostatní funkčnosti.

Jádro systému Windows není striktně vymezeno, a proto využívá vlastnosti jak mikrokernalu, tak i jádra monolitického, z toho důvodu je nazýváno jádrem hybridním. Jádro se skládá ze dvou vrstev rozdělených podle úrovně oprávnění. Rozlišuje tzv. režim jádra (kernel mode), ve kterém se nachází většina základních funkcí a tzv. uživatelském řežimu (user mode), ve kterém se náchází ostatní komponenty.[7]

[7] **Dráb**, Martin. *Jádro systému Windows*,2011,472 s. ISBN: 978-80-251-2731-5. Str.47

Obrázek 1 - Jádro systému Windows NT



Zdroj: Vlastní zpracování s využitím [6, str.47]

2.2 Active Directory Domain Service

Jedná se o základní subsystém v síťovém prostředí s doménou. Funkcionalita doménové služby je klíčová v síťovém prostředí, pro přístup uživatelů k dalším zdrojům v síti. Ukládají se zde informace o uživatelích, jednotlivých zařízeních a dalších členech v rámci domény. Celkový koncept struktury by měl sloužit a umožnit snadnější organizaci a následnou orientaci v jednotlivých objektech a OU (Organization Unit).

Objekty samotné mohou být typu:

- Uživatel (User)
- Skupina (Group)
- Počítač (Computer)
- Tiskárna (Printer)
- Organizační jednotka (Organization Unit)

Jednotlivé objekty se mohou sdružovat do organizačních jednotek (OU), které dále vytvářejí celkovou strukturu a mohou mít následné potomky a tím umožnit administrátorům hierarchické roztřídění objektů dle jejich specifického zájmu.

V celkové struktuře se jedná o adresářový strom, který je úzce propojen s protokolem LDAP, který se stará o přístup k datům a jejich ukládání nebo vyhledávání jednotlivých informací. [8]

Logické seskupení objektů, umožňující jejich centrální správu, se označuje jako doména (domain)

Zmíněná doména je pouze jedním ze stavebních kamenů, které se implementují v rámci struktur Active Directory.

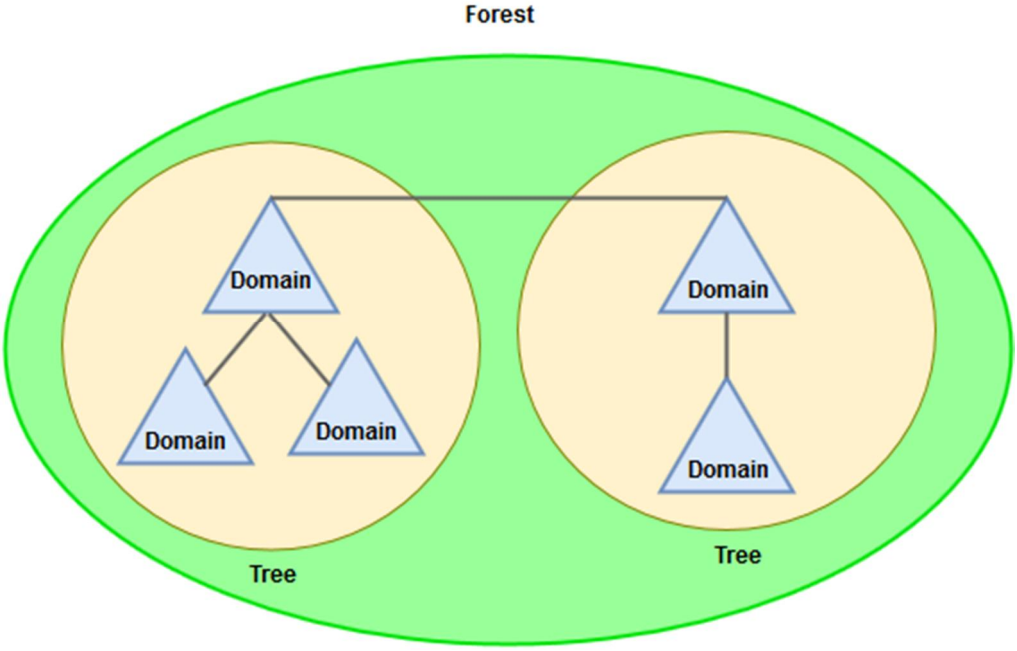
Stromy (Trees) služby Active Directory jsou logická seskupení domén. [8] Doménové struktury služby Active Directory jsou logická seskupení doménových stromů.

V doménovém stromu jde tedy o vztahy mezi nadřazenými a podřízenými doménami. Doména na vrcholu stromu se označuje jako kořenová doména (Root Domain). V praxi se první vytvořená doména v kořenovém stromu stává doménou kořenovou. Mezi jednotlivými stromy lze pak nastavovat vztahy důvěrnosti.

Stromy samotné jsou uspořádány v lese (Forest). V rámci lesa také existuje jako v případě stromů, jedna kořenová doména (Forest Root Domain).[9]

[8] William, R.Stanek. Mistrovství v Microsoft Windows Server 2008 – Kompletní informační zdroj pro profesionály,2009,1364 s. ISBN: 978-80-251-2158-0. Str. 955,956

Obrázek 2 - Active Directory – Forest, Tree, Domain



Zdroj: Vlastní zpracování s využitím [8]

Global Catalog (GC) je služba sloužící k indexaci všech objektů které jsou částí lesa. Global catalog je důležitý vzhledem ke skutečnosti, že doménový řadič (DC) má informace pouze o objektech, které jsou součástí jeho domény. Pokud chceme přistupovat k prvkům z jiné domény, je zapotřebí právě Global Catalog, který poskytne informace o tom, na kterém doménovém řadiči se objekt nachází.
Mezi hlavní využití doménové struktury je pak její propojení s GPO, které bude vysvětleno v následujícím odstavci. Každý objekt a organizační jednotka dovolují samostatné nastavení přístupových práv, díky kterým lze snadno řídit jejich další použití.[9]

V našem testovacím prostředí si vystačíme pouze s jednou kořenovou doménou, se kterou je nainstalována služba DNS sloužící k překladu IP adres na doménová jména a naopak.

[9] Samuraj-cz: Kerberos část 1 - Active Directory komponenty – [cit.2017.5.1]
Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-1-active-directory-komponenty/

2.3 Group policy objects (GPO)

Objekty slouží jako kontejnery pro konfiguraci zásad a jejího nastavení, které lze dále propojit se strukturou AD. Lze vytvořit velké množství jednotlivých skupin zásad, které pak lze dále navázat na uživatele nebo počítače ve struktuře AD. Tyto skupiny se dělí do dvou kategorií. První z nich je Computer Configuration a slouží k nastavení změn týkajících se počítače samotného a druhá skupina User Configuration zahrnuje nastavení spojené s konfigurací uživatelských účtů.
Každá z obou zmíněných kategorií obsahuje tři hlavní třídy nastavení.

- Software Settings - konfigurace softwaru počítače a správa instalací/odinstalací a oprav.
- Windows Settings – správa nastavení systému Windows jak samotného počítače, tak i uživatelského nastavení společně s možností skriptů a nastavení zabezpečení.
- Administrative Templates – slouží k řízení registru pro konfiguraci systému a jeho součástí. Šablony jsou přizpůsobeny konkrétní verzi operačního systému. Tyto šablony je možné importovat a tím si přizpůsobit nastavení dalších využívaných produktů. Jedná se o ADMX soubor, který je definován ve standardizovaném formátu XML.

Po založení domény jsou automaticky vytvořeny výchozí zásady řadiče domény (Default Domain Controllers Policy GPO) a object GPO výchozích zásad domény (Default Domain Policy GPO), které obsahují nastavení pro správu popsanou výše. Slouží pro prvotní výchozí nastavení zásad v doméně mimo jiné i například pro konfiguraci Kerberosu zmíněného níže.
Výchozí Objekt GPO spravuje oblasti zásad účtu. Kromě jiného lze nastavit zásady hesel, uzamykání uživatelského účtu nebo modul Kerberos, který aplikuje zásady protokolu samotného.[10]

[10] William, R.Stanek. Mistrovství v Microsoft Windows Server 2008 – Kompletní informační zdroj pro profesionály,2009,1364 s. ISBN: 978-80-251-2158-0. Str. 1165.
[9] Microsoft.com: Basic Concepts for the Kerberos Protocol – [cit.2017.11.27] Dostupné z https://technet.microsoft.com/en-us/library/cc961976.aspx

2.4 Kerberos

Názvem Kerberos byl v řecké mytologii označován trojhlavý hlavý pes u bran do podsvětí boha Hádese. V našem případě jde o technologii, která byla vyvinuta na univerzitě MIT v 80.letech známá jako project ATHENA. Důvod pro jméno Kerberos je právě kvůli jeho třem hlavám, kde každá z nich reprezentuje jednotlivý prvek. V našem případě tedy klienta, server a důvěrnou třetí stranu, tzv. KDC (Key Distribution Center), který nad nimi dohlíží.[11] Než si popíšeme, k čemu samotný Kerberos slouží, vymezíme si obecné pojmy, které jsou ve spojení s Kerberosem využívány.

Autentifikace (Authentication) – slouží k potvrzení identity daného subjektu.
Autorizace (Authorization) – slouží k získání přístupu ke zdrojům, ke kterým má držitel oprávnění přistupovat.

Pokud tedy aplikujeme výše dokumentované prvky na naše testovací prostředí, dochází z počátku k autentifikaci uživatele a dále pak k jeho autorizaci, která mu umožní přístup k pro něj privilegovaným zdrojům.

Kerberos je velmi komplexní síťový autentizační protokol využívající symetrickou kryptografii, sloužící k bezpečnému ověření identity komunikujících stran. Symetrická kryptografie, narozdíl od asymetrické se vyznačuje stejným klíčem, který se používá jak k dešifrování, tak i zašifrování přenášené informace. Standardně se protokol používá k autentizaci, ale Microsoft jej rozšířil o autorizační údaje, které přenášejí i seznam skupin, do kterých uživatel patří, a díky nim jsou nastavena jeho privilegia.

Je důležité zmínit, že výše popsaná autentifikační a autorizační funkčnost se týká jak samotných uživatelů, tak i jednotlivých počítačů, které jsou součástí procesu.

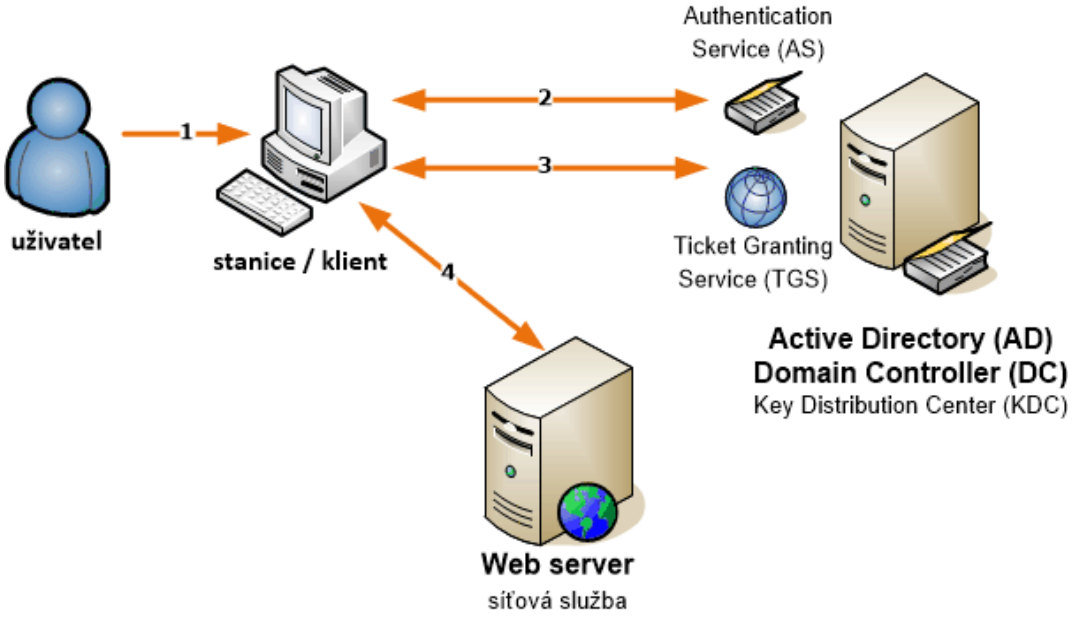
V našem prostředí založeném na Microsoft Windows produktech se používá Kerberos verze 5 ve spojení s SSO (Single Sign On), které umožnují tzv. „jednotné přihlášení“. Pod jednotným přihlášením rozumíme situaci, kdy se

uživatel přihlásí pouze jednou a o přihlášení do ostatních systémů se již nestará. Toto přihlášení je automaticky realizováno na pozadí.[12]

Vzhledem k tomu, že služba Kerberos je používaná jako defaulní služba pro autorizaci a autentifikaci v doménovém prostředí je zapotřebí důvěry (trust) mezi jednotlivými prvky, které komunikují v rámci dané domény. Z tohoto důvodu, každý počítač, který je přidán do dané domény a je tedy její součástí, má již zmíněnou důvěru od doménového kontroleru.

Specifikujme si níže jednotlivé prvky, které se samotného procesu účastní:

Obrázek 3 - Služby Kerberos v infrastruktuře



Zdroj: [11]

Uživatel – konkrétní klient, který se přihlašuje do systému případně přistupuje k určité síťové službě.

Cílová služba/počítač – služba, na kterou je vzdáleně klientem přistupováno.

Key Distribution Center (KDC) – důvěryhodná třetí strana, která se nachází na doménovém řadiči (DC) a obsahuje dvě nezávislé služby:

[10] Samuraj-cz: Kerberos část 3 – Single Sing-On a protokol Kerberos – [cit.2017.5.1] Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-3-single-sign-on-a-protokol-kerberos/

[11] Samuraj-cz: Kerberos část 4 – Hlavní termíny Kerberos protokolu – [cit.2017.5.1] Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-4-hlavni-terminy-kerberos-protokolu/

- Ticket Granting Service (TGS)[12]
- Authentication Service (AS)

Služba v prostředí Windows se jmenuje krbtgt a je spouštěna při startu jako podslužba LSASS (Local Security Authority Subsystem Service), která je zodpovědná za nastavení bezpečnostních pravidel v systému, kromě jiného také např. zapisuje do Windows logu v části Security. [13]

Kerberos ticket – hlavní doménou Kerberosu je vydávání ticketů a to dvou typů:

- TGT ticket za který je zodpovědná služba Authentification service
- Servisní ticket pro službu Ticket-granting Service

TGT ticket – zašifrovaný soubor za pomoci klíče služby KDC, obsahuje informace o tom kdo vyžádal tento ticket a pro koho je vyžádán (SPN), SPN doménové jméno, validitu samotného ticketu, service name – v tomto případě služba krbtgt. Klient samotný nedokáže číst tyto tickety, slouží pouze pro KDC jeho součástí je Session Key.[14]

Ticket se využívá:

- Při prvotním kontaktu s uživatelem pro zabezpečený přenos informací.
- Pro vyžádání servisních ticketů.

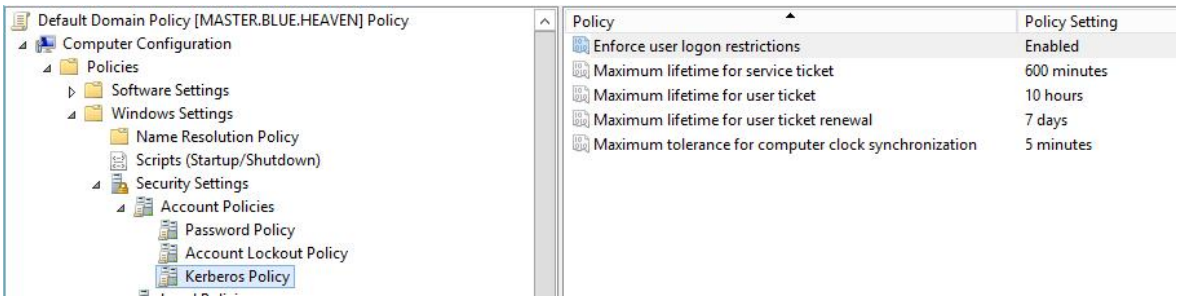
Informace o všech TGT ticketech, které jsou vydány pro konkretní stroj a službu pro kterou je uživatel autentifikován lze zjistit lokálně za pomoci příkazu klist.

[12] https://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service
How the Kerberos Version 5 Authentication Protocol Works https://technet.microsoft.com/en-us/library/cc772815(v=ws.10).aspx

Výchozí doba životnosti ticketu je 10 hodin, ticket může být obnovován maximálně po dobu 7 dní

Secret Key – vzniká za pomoci uživatelského hesla v textové formě společně s uživatelským jménem a doménou na které se provede jednosměrná hashovací funkce.
UPN – User Principle Name – uživatelské jméno svázané s doménou (doména se někdy též označuje jako realm)
SPN – Service Principle Name – unikátní identifikátor služby, která je nadále využívána Kerberosem při autentifikaci.
Session Key – využíván službou TGT a servisními tickety pro zabezpečení komunikace.

Obrázek 4 - Výpis Kerberos politik ve výchozím nastavení



Zdroj: Vlastní zpracování s využitím [8]

User ticketem je zamýšlen již zmíněný TGT ticket.

Porty:

88 TCP, UDP – Kerberos KDC
749 TCP – Kpasswd služba pro změnu klientského hesla
543 TCP – Kerberos Login

Samotný proces z vyšší perspektivy probíhá způsobem získání ticketu od doménového kontroleru na kterém běží služba KDC vydávající tickety. Jakmile je ticket vydán a předán vlastníkovi (uživateli), je tento ticket využíván pro proces autentifikace a autorizace na všech ostatních serverech případně službách kam

daný uživatel přistupuje. Tam pak probíhá ověření platnosti daného ticketu vzhledem k jeho časové omezenosti.

Nyní si rozepišme celý proces více do hloubky.

Autentizace uživatele: [13]

V našem případě popisujeme autentifikaci ve struktuře s doménou, kde testovací počítač s Windows 10 je součástí domény. Nevyužíváme zde NTLM (NT LAN MANAGER) autentizaci, která může nastat v případě, že počítač není součástí domény, nebo například jsou firewallem blokovány porty Kerberosu samotného, které pak znemožňují naslednou komunikaci.
Není zde využívána ani autorizace za pomoci certifikátů, smartcard ani biometrických prvků. V našem případě využíváme v mnohých případech velmi rozšířený způsob za pomoci klasického zadání uživatelského jména a hesla.

Následně se vzhledem k použití protokolu Kerberos vygeneruje Secret Key, který je kombinací uživatelského jména s doménou a zadaným heslem nad kterými je provedena jednosměrná hashovací funkce.

Klient zašle žádost, tzv. KRB-AS-REQ požadavek obsahující KRB-REQ-BODY s informacemi o uživatelském jmému, doméně, SPN službě, adrese klienta a podporovaných šifrách v plain textu. Tento požadavek je doručen na Authentification Server (AS). Vzhledem k tomu, že AS vyžaduje před-autentifikaci, je vygenerována a zaslána zpět chybová hláška KRB-ERROR obsahující kód informující o nutnosti před-autentifikace. Před-autentifikace není brána jako chyba ale je to výchozí nastavení služby KDC.

Je tedy zapotřebí zaslat nový KRB-AS-REQ požadavek obsahující časovou známku zašifrovanou za pomoci Secret Key klienta.

AS si najde daného uživatele zasílající tuto žádost v AD stromu a vytvoří si také jeho Secret key za pomoci kterého je schopen ověřit platnost zasílaného požadavku právě na základě rozširování časové známky a zjištění zda je stálé platná. Rád bych zmínil, že právě čas na jednotlivých zařízeních je velmi důležitým prvkem a musí být mezi sebou synchronizován. Pokud by zaslaná známka byla

[13] Samuraj-cz: Kerberos část 5 – Princip Kerberos Autentizace – [cit.2017.5.1] Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-5-princip-kerberos-autentizace/

posunuta o více než 5 min než je čas na serveru s AS, nebyla by známka označena za platnou. Mimo jiné také dochází ke kontrole, zda AS již neobdržel stejnou nebo novější známku.

V případě, že žádost vyhoví je vygenerován na AS Session Key, který šifruje komunikaci mezi klientem a také TGT ticket.

AS tedy připraví odpověd typu KRB-AS-REP, která obsahuje jmeno uživatele, Session key, zašifrováný za pomoci klientského Secret key a také vygenerovaný TGT ticket zašifrovaný za pomoci KDC Secret key.

Obrázek 5 - Ukázka TGT ticketu za pomoci příkazu klist tgt

```
PS C:\Users\tester.BLUE> klist tgt

Current LogonId is 0:0x4efca1

Cached TGT:

ServiceName           : krbtgt
TargetName (SPN)      : krbtgt
ClientName            : tester
DomainName            : BLUE.HEAVEN
TargetDomainName      : BLUE.HEAVEN
AltTargetDomainName: BLUE.HEAVEN
Ticket Flags          : 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Session Key           : KeyType 0x12 - AES-256-CTS-HMAC-SHA1-96
                      : KeyLength 32 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00
StartTime             : 11/28/2017 10:15:43 (local)
EndTime               : 11/28/2017 20:15:43 (local)
RenewUntil            : 12/5/2017 10:15:43 (local)
TimeSkew              :  + 0:00 minute(s)
EncodedTicket         : (size: 1030)
0000  61 82 04 02 30 82 03 fe:a0 03 02 01 05 a1 0d 1b  a...0...........
0010  0b 42 4c 55 45 2e 48 45:41 56 45 4e a2 20 30 1e  .BLUE.HEAVEN. 0.
0020  a0 03 02 01 02 a1 17 30:15 1b 06 6b 72 62 74 67  .......0...krbtg
0030  74 1b 0b 42 4c 55 45 2e:48 45 41 56 45 4e a3 82  t..BLUE.HEAVEN..
```

Zdroj: Vlastní zpracování

Ticket flags – nám sdělují příznaky, které jsou na ticketu nastaveny, pro nás může být zajímavý flag typu pre_authent, který nám říká, že klient byl již autentifikován KDC před tím než byl tento ticket vydán. A to právě za již dříve zmíněného požadavku KRB-AS-REQ.

Na klientské straně dochází k rozšifrování Session key za pomoci vlastněného Secret key a jeho uložení. TGT ticket rozšifrovat nelze a jeho životnost je výchozím nastavení 10 hodin. Dochází ale k reautentizaci, při každém přihlášení se vytváří nový TGT. Jeho význam je v použití pro komunikaci s KDC, nevyužívá se již Secret Key, ani heslo uživatele ani další údaje zmíněné výše. TGT obsahuje jméno klienta, adresu, dobu platnosti a Session Key. TGT ticket

dokáže rozšifrovat pouze KDC a společně se Session key, který je jeho součastí si KDC nemusí udržovat žádné další informace.

Přihlášení uživatele ke specifické službě v síti.[14]

Je nutné sestavit žádost KBT-TGS-REQ která se odesíla na TGS, obsahuje informační údaje o žádosti samotné, jménu služby, která je vyžadována atp. Její druhou částí je již zmíněný TGT ticket a identifikace klienta šifrovaná za pomoci Session Key, které tak zastupují přístupové údaje uživatele.

Na straně KDC TGS využije TGT ticket, rozšifruje jej a získá Session Key za pomoci, kterého je možné dozvědet se informace o klientovi, a ověří ho.

Pokud je vše v pořadku, odpoví TGS zpět KRB-TGS-REP, které je zasláno zpět klientovi a obsahuje: jméno uživatele, servisní ticket pro požadovanou službu obsahující SPN dané služby a Session Key pro komunikace mezi klientem a službou zašifrovaný za pomoci Session Key z TGT (klient – KDC).
Klient získá Service Ticket, rozšifruje si Session Key potřebný pro komunikaci ze službou a obojí si uloží.

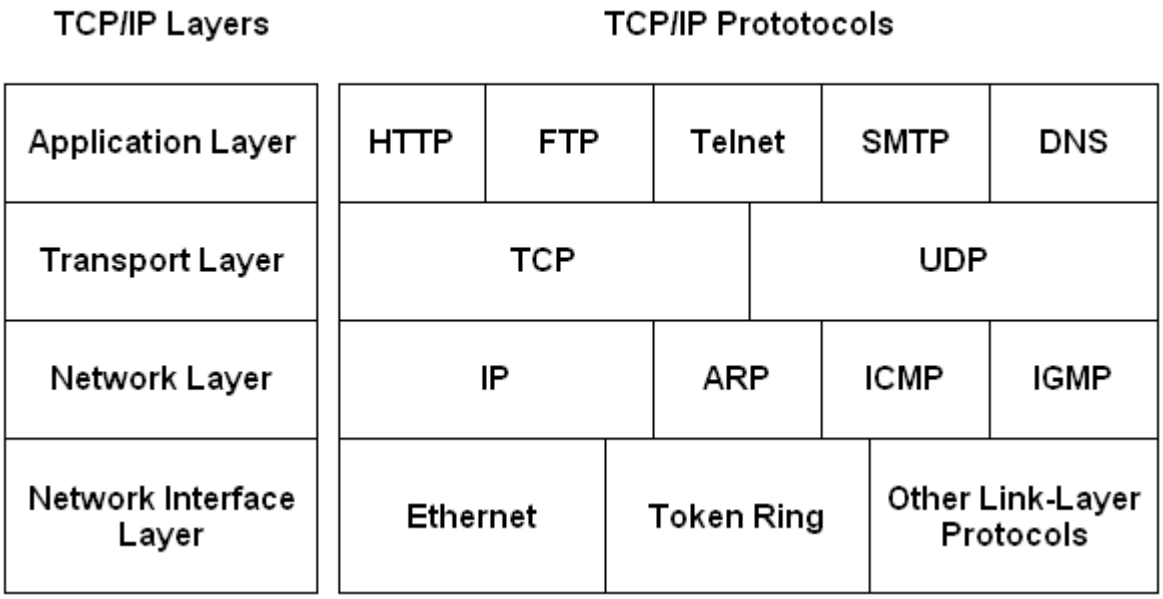
Je zapotřebí Service ticket, obsahujicí údaje o žádosti, jméno požadované služby, a serveru kde je provozována společně s již zmíněným TGT ticketem pro ověření na KDC službou TGS. Díky tomu dostává klient zpět požadovaný Service ticket, který si rozšifruje a získá Session key, nutný pro komunikaci se službou. [15]

[14] Samuraj-cz: Kerberos část 5 – Princip Kerberos Autentizace – [cit.2017.5.1]
Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-5-princip-kerberos-autentizace/
[15] Samuraj-cz: Kerberos část 5 – Princip Kerberos Autentizace – [cit.2017.5.1]
Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-5-princip-kerberos-autentizace/

2.5 Úvod do TCP/IP

TCP/IP je sada protokolů, která zahrnuje protokol TCP a protokol IP [16]. Jedná se ale i o síťovou architekturu, která je definována počtem vrstev a jejich použití s konkretními protokoly. Nejnižší vrstva architektury je vrstva síťového rozhraní umožňující přístup k fyzickému přístupovému médiu[17]. Síťové vrstvy IP (+ ICMP, ARP), transportní vrstvy TCP, UDP a vrstvy aplikační (např. FTP, SSH, HTTP)

Obrázek 6 - Vrstvy protokolu TCP/IP



Zdroj: http://sourcedaddy.com/windows-xp/images/uti1.gif

V naší síti používáme Internetový protokol verze 4 (IPv4), který je 4 tou verzí protokolu IP, který byl definován jako jeden ze standartů pro internetovou komunikaci[18]. Jedná se o protokol nespojovaný a nespolehlivý. Nenavazuje tedy spojení, a odesílá data i přes to, že neví, zda je příjemce ochoten data přijmout.

[16] Earchiv.cz: TCP/IP – Úvod – [cit.2017.5.1]
Dostupné z http://www.earchiv.cz/l225/slide.php3?l=3&me=2
[17] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]*. 2., aktualiz. 2006. ISBN 80-251-1278-0.Str.245
[18] Wikipedia: IPv4 – [cit.2018.3.1]
Dostupné z https://en.wikipedia.org/wiki/IPv4

Síťová vrstva IP v našem případě IPv4 využívá 4bajtový tedy 32 bitový adresní prostor, který nám umožní využívat 2^{32} adres.

Komunikace se skládá právě z IP paketů, které obsahují sekci s hlavičkou (header) a sekci data.

- Sekce header se skládá ze 14 sekcí, 13 z nich je povinných kromě sekce „options“ která je volitelná.[16]

Obrázek 7 - Hlavička protokolu TCP/IP

IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Zdroj: [17]

Z našeho hlediska úvodu do problematiky si popišme některé sekce hlavičky IPv4.

Version: udává verzi paketu, v našem případě verze 4, verze 6 zde není rozebírána.

Time To Live (TTL): určuje životnost daného paketu, je specifikován v sekundách, v případě, že paket projde směrovačem (routerem) je jeho hodnota snížena o jedna. Pokud je hodnota 0, je paket zahozen a odeslána zpráva informující o vypršení platnosti paketu přijemci.

Protokol: definovaný komunikační standard, který zajišťuje pravidla pro komunikaci mezi dvěmi subjekty. Zde je vyjádřen číslem, které zastupuje daný protokol. Více informací lze získat z RFC 790, které toto přiřazení definuje[19]. V našem případě bude nejvíce důležitý protokol ICMP s číslem 1. TCP s číslem 6 a UDP s číslem 17.

Source IP address: zdrojová adresa z které je paket odeslán

[19] IETF – RFC790 specifikace – [cit. 2018.3.1]
Dostupné z: https://tools.ietf.org/html/rfc790

Destination IP address: cílová adresa na kterou by měl být paket doručen

Dle organizace IANA[20] která dohlíží nad rozdělením IP address byli definovány adresní rozsahy pro různé použití. Tyto rozsahy jsou definovány jako standard v dokumentu RFC1918, který je volně k nahlédnutí[21].

Pro adresy soukromých sítí jsou vyčleněna následující síťová čísla:[16]

Třída A – 10.0.0.0
Třida B – 172.16.0.0 až 172.31.0.0
Třída C – 192.168.0.0 až 192.168.255.0

V našem případě využíváme třídu A.

Uveďme si tedy nyní pro nás zajímavé protokoly:

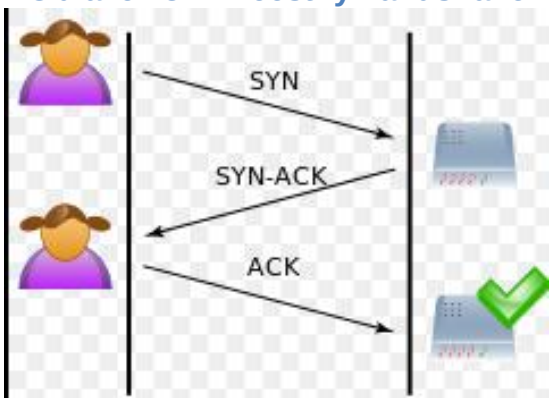
TCP – Transmission Control Protocol – protokol poskytuje garantované doručení (je spolehlivý) ve správném pořadí (je spojový) a je využíván mnoha aplikacemi, kde je této vlastností využiváno.

Při komunikaci mezi aplikacemi je vždy zapotřebí nejprve navázat spojení. K tomu se využívá tzv. trojcestný handshake (three-way handshake) při kterém se obě strany domluví na spojení. Již z názvu vyplývá, že jde o tři kroky.[22] V prvním klient – strana žádající o spojení odešle TCP packet s příznakem SYN – volá vzdálený host zda je k dispozici. Vzdálený host odpovídá, že je k dispozici a odesíla zpět packet s příznakem SYN & ACK a posléze strana žádající spojení zpečetí spojení a odešle paket příznakem ACK.

[20] Wikipedia – IANA – [cit. 2018.3.1]
Dostupné z: https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority
[21] IETF – RFC1918 specifikace – [cit. 2018.3.1]
Dostupné z: https://tools.ietf.org/html/rfc1918

[22] SANDERS, Chris. Analýza sítí a řešení problémů v programu Wireshark. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5. Str. 127

Obrázek 8 - Třicestný handshake



Zdroj: https://cs.wikipedia.org/wiki/SYN_flood

Obrázek 9 - Hlavička protokolu TCP

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Zdroj: https://en.wikipedia.org/wiki/Transmission_Control_Protocol

UDP – User Datagram Protocol - nezaručuje doručení samotné ani ve správném pořadí. Bloky, které jsou přenášeny se označují jako UDP datagramy právě kvůli nespojovanému způsobu fungování, tedy nenavazování spojení. Není proto vhodný tam, kde vyžadujeme, aby informace byla vždy doručena a nemohlo dojit ke ztrátě dat.

ICMP – Internet Control Message Protocol – ve většině případů se využívá pro zasílání chybových oznámení v případě nedostupnosti vzdáleného počítače služby. ICMP zpráva je zapouzdřena v IP datagramu. Mezi nejznámnější případy využití je nástroj ping, který zasílá ICMP zprávy vyjadřující dostupnost nebo nedostupnost daného cíle.

Z předešlé části víme, že protokol IP síťové vrstvy je bezstavový (nespojovaný) a nespolehlivý. Pokud ale chceme změnit způsob fungování přenosových služeb můžeme tak učinit právě za pomoci transportní vrstvy a protokolu TCP.

K rozlišení komunikujících aplikací se využivájí čisla portů, které jsou rozdělené do jednotlivých skupin nacházejících se v rozsahu 1 – 65535 a jsou spravována organizaci IANA.

3. Instalace testovacího prostředí

Než začneme zmíněným testováním bezpečnosti, je zapotřebí nejdříve připravit testovací platformu skládající se ze zmíněných systému a jeho funkcionalit.

Celé prostředí je v rámci naší praktické části je implementováno za pomoci virtualizačního nástroje Hyper-V ale může být využita i například bezplatně dostupná aplikace VirtualBox.

3.1 Microsoft Windows Server 2012R2

Po nainstalování samotného operačního systému je důležité doinstalovat AD DS a DNS. Server tedy bude sloužit jako doménový kontroler.

Hostname : master
Doména : blue.heaven
IP adresa : 10.0.0.1

V první řadě musíme doinstalovat službu AD DS.

Existují dvě možnosti instalace, první je skrz GUI (Graphic User Interface) průvodce, druhá za pomoci Microsoft Powershell commandletů.

V našem případě volíme pro instalaci Microsoft Powershell, který je součástí naší instalace Windows. Jedná se o prostředí příkazového řádku a skriptovací jazyk nové generace od společnosti Microsoft.[23]

1) Instalace AD DS služby s management konzolí

Install-WindowsFeature –Name AD-Domain-Services –IncludeManagementTools

2) Instalace domény ‘blue.heaven’

Install-ADDSForest –DomainName “blue.heaven”

Commandlet samotný nabízí další možnosti instalace se specifikováním cest k databázi služby AD DS, Logovacím souborům atp., ale v našem případě ponecháváme defaulní nastavení. Služba DNS serveru je nainstalována společně s instalací domény.

3.2 Microsoft Windows 10

Klientský operační systém bude připojen pouze do domény.

Hostname : flatron
Doména : blue.heaven
IP adresa : 10.0.0.10
Uživatel : test

Po instalaci, která je reprezentovaná grafickým průvodcem je v systému nakonfigurována síťová karta a stroj připojen do domény.

3.3 Kali Linux

V našem scénáři figuruje distribuce Kali Linux jako samostatný virtuální stroj právě pro otestování obou operačních systému Windows v síti. Vzhledem k dalšímu testování, které je prováděno z klientské stanice např. skenování doménového

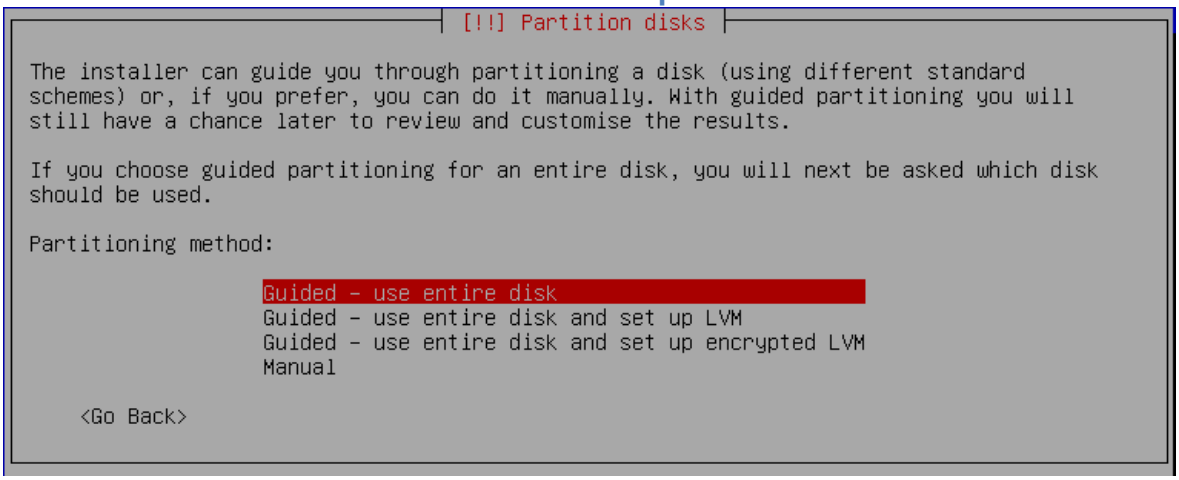
[23] WILSON, Ed. *PowerShell: [průvodce skriptováním: pro verzi 3.0. a vyšší]*. Brno: Computer Press, 2015. ISBN 978-80-251-4386-5. Str. 237

kontroleru, je Kali Linux nainstalovaný jako virtuální stroj na klientském operačním systému, tak abychom dokázali simulovat reálné podmínky.
V současné době, a dle zkušeností autora, je zcela běžné mít nainstalován virtualizační nástroj na svém firemním laptopu nebo stanici. Z tohoto důvodu pro následnou instalaci je možné stáhnout ze stránek výrobce instalační ISO obraz, který je možné následně provozovat ve volbě LIVE, kdy je celá distribuce zavedena z instalačního ISO obrazu bez instalace na pevný disk, tak i instalaci klasickou, kdy dochází k nainstalování systému na pevný disk.[24]

Popíšeme si tedy důležité kroky instalace na pevný disk.

Po úvodním nastavení jazyka, země a rozvržení klávesnice, dojde k zavedení základních komponent pro pokračování samotného instalátoru, pokusu o nastavení sítě z DHCP serveru, jména počítače a možnosti připojení do domény – v našem případě bez nastavení, daný stroj do domény nepřipojujeme. Nastavíme heslo administrátora a vybereme časovou zónu, ve které se nacházíme.

Obrázek 10 - Rozdělení pevného disku



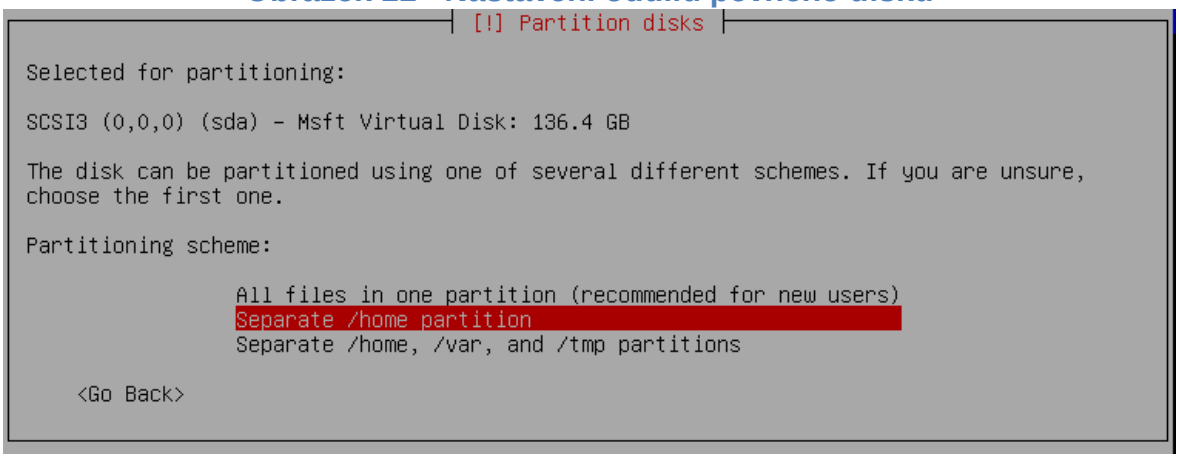
Zdroj: Vlastní zpracování

Zvolíme asistovaného průvodce, který nám s rozdělením disku pomůže. Následně vybereme pevný disk, který chceme rozdělovat. V našem případě máme disk pouze jeden a proto volíme /dev/sda.

[24] Kali Linux – Downloads [2018.4.1]
Dostupné z: https://www.kali.org/downloads/

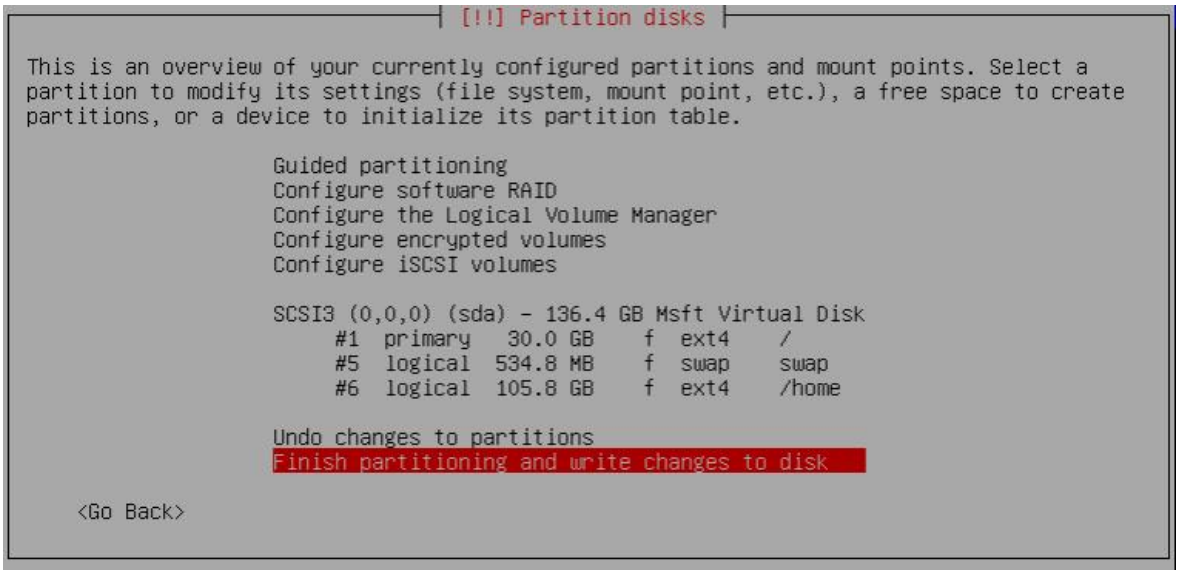
Dle průvodce lze vybrat zapsání všech adresářů do jednoho oddílu. Zde si dovolím vybrat možnost, kdy separujeme alespoň oddíl /home, obsahující domovské adresáře uživatelů, na samostatný oddíl. Toto nastavení je vhodné v případě, kdy bychom chtěli instalovat systém znovu a nechtěli přijít o uživatelská data. Pokud by k této situaci došlo, v předchozím nastavení by bylo nutné zvolit manuální rozdělení disků a označit oddíl s uživatelskými adresáři za /home.

Obrázek 11 - Nastavení oddílů pevného disku



Zdroj: Vlastní zpracování

Obrázek 12 - Rozdělení disku - Závěrečný přehled změn

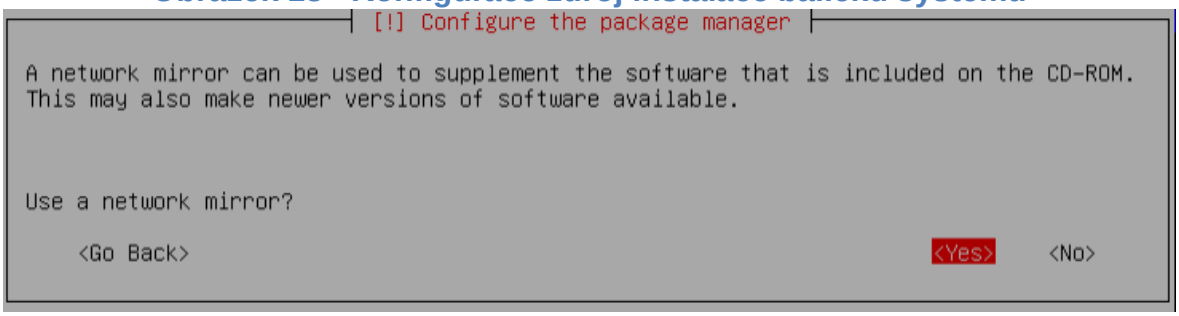


Zdroj: Vlastní zpracování

Závěrečné shrnutí vytvořených oddílu. Filesytém je zde zvolen žurnálovací ext4, který je nastaven jako výchozí. Na primárním disku se náchází náš systém, který ma velikost 30GB a je označen jako „/“ ekvivalent „C:“ v Microsoft Windows. Zmíněný /home pro uživatelská data je zde jako /home s velikostí 105,8GB. Tato velikost je pro naše účely naprosto zbytečná, ale může být nadále využita například pro logování apod.

Následně zapíšeme změny na disk a tím ukončíme nastavení pevného disku. Dojde k rozdělení, vytvoření filesystému a začne instalace operačního systému. V této chvíli můžeme ještě nastavit síť a stáhnout aktualní verze balíků namísto verzí, které jsou součástí instalačního ISO obrazu.

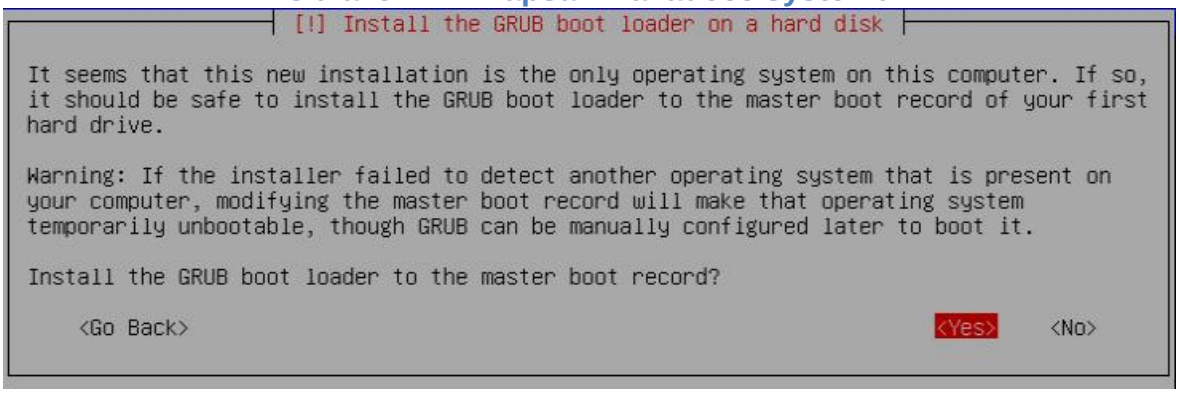
Obrázek 13 - Konfigurace zdroj instalace balíčků systému



Zdroj: Vlastní zpracování

Následuje nastavení proxy, které necháváme prázdné a pokračujeme k zapsání zavaděče GRUB na pevný disk. Zvolíme zapsání na /dev/sda, jelikož máme v systému pouze jeden disk a budeme ho používat i jako hlavní pro následný start systému.

Obrázek 14 - Zapsání zavaděče systému



Zdroj: Vlastní zpracování

Restartujeme, odpojíme USB flash disk, případně změníme pořadí zařízení pro zavedení systému, kdy na prvním místě bude náš pevný disk a počkáme zavedení.

Ve výchozím nastavení se přihlašujeme jako uživatel root s heslem „toor“, který je tzv. superuživatel, obdoba role „administrátor“ v systému Windows.[25]

Hostname : kali
Doména : stroj není zapojen do domény
IP adresa : 10.0.0.9

4. Testování prostředí

Z pohledu každého útočníka je velmi důležité zjistit co nejvíce informací o jeho potenciálních cílích, identifikovat jejich jednotlivé slabiny a poté proniknout do požadovaného systému. Nejlépe nepozorovaně, bez vyvolání podezření ze strany systémových administrátorů cílového systému nebo jednotlivých prvků v síti jako například IDS.

Z toho důvodu přichází ke slovu nejprve skenování vzdáleného systému. Distribuce Kali Linux nabízí sadu nástrojů přímo určených pro skenování jednotlivých cílů, nejznámějších z nich je nástroj NMAP.

Nástroj slouží k oskenování jednotlivých portů vzdáleného systému a zjištění zda jsou otevřené či uzavřené. V případě, že je toto možné, identifikujeme vzdálený systém a jednotlivé služby, které jsou k dispozici.

Vzhledem k tématu práce bude využíván i nástroj Metasploit, který slouží jak k vyhledávání zranitelností na vzdáleném systému, tak i k jejich využití a proniknutí do cílových systémů za pomocí exploitů, které jsou jeho součástí. Díky možnostem přizpůsobení samotného programu, lze snadno doinstalovat další případné moduly a vždy vlastnit poslední aktualizované nástroje a exploity.

[25] SOBELL, Mark G. Linux: praktický průvodce. Praha: Computer Press, 1999. Operační systémy. ISBN 80-7226-190-8. Str.20

Nejdříve se pokusíme získat kontrolu nad klientskou stanicí Windows 10 a to v různých scénářích, poté se pokusíme zjistit slabiny systému Windows 2012R2.

Snahou je zůstat při skenování prostředí co nejvíce skryt, aby se komunikace nestala podezřelou, i přestože v našem scénaři nepočítame s prvky typu IDS/IPS.

Ve většině případů penetračního testování se využívá nejdříve tzv. pasivní odposlech a poté odposlech aktivní ke shromaždování informací o vzdáleném systému. Výhodou prvně zmíněného je právě ona pasivita, kdy je možné sesbírat důležité informace na internetu, vhodně položenými dotazy do vyhledávače Googlu, které nám pomohou při odhalování a rozkrývaní např. domén a k nim přidruženým službám, poskytujícím obrázek o prvcích v celém rozsahu námi uvedené domény.

Vzhledem k tomu, že v našem případě jsou cíle pevně specifikovány, a práce se nezabývá útoky z Internetu, nebudeme se zabývat výše zmíněným.

Následující praktická část se bude skládat z jednotlivých scénářů, které budou poukazovat na možnosti získání různých druhů informací, jak z klientské stanice tak i doménového řadiče v závislosti na jeho konfiguraci a případný útok na něj.

4.1 Klientská stanice Windows 10 - Útočník s fyzickým přístupem k PC

Tato sekce se zabývá eskalací uživatelských práv a shromažďování informací o síťovém prostředí, kdy útočník využivá klientskou stanici a má k ní fyzický přístup. Lze ji dále rozdělit na možnosti, kdy útočník vlastní přístupové údaje na přihlášení do domény jako řadový zaměstnanec (v našem případě s právy domain user) a možnost, kdy tyto údaje nemá.

4.1.1 Bez přihlašovacích údajů:

Útočník má možnost fyzického přístupu k počítači, ale nevlastní přihlašovací údaje.

Pokud je počítač uzamčený nebo očekává přihlašovací údaje, které jsou pro útočníka neznámé, je možné aplikovat následující postup.

Restart samotného počítače a vstup do BIOSU. Pokud je BIOS chráněn heslem a to je pro nás neznámé nebo není nastaveno jako výchozí vzhledem k výrobci samotnému, lze vyzkoušet možnost fyzického otevření samotného počítače a za pomoci konkrétní propojky na základové desce (bývá označena jako CLEAR CMOS), můžeme vyresetovat nastavení BIOSU do defaultních parametrů – bez zadaného hesla. Lze vyzkoušet i chvilkové vyjmutí baterie základní desky, která ji pomáhá udržovat informace v případě např. výpadku elektrické energie a docílit tím stejného účinku. Je zapotřebí zmínit, že výše uvedené možnosti lze provést u většiny desktopových typů PC, nikoliv notebooku, kde tento postup nelze aplikovat tak jednoduše a vyžadoval by důkladné rozebrání.

V Biosu lze poté nastavit pořadí BOOT ORDERU (posloupnost zařízení z kterých se snaží počítač zavést operační system), kdy v případě odsunutí pevného disku na druhé místo a předřazení USB portu nebo CD-ROMU na místo první, se můžeme pokusit zavést námi dodaný operační systém.

V některých případech není nutné vstupovat do samotného BIOSU, ale po spuštení PC a zmačknutí funkční klávesy, většinou ESC, lze vstoupit rovnou do nastavení BOOT ORDERU a vybrat zařízení, ze kterého bude systém zaveden. Může nastat situace, kdy je USB médium již zapojeno, ale není k dispozici. V současné době již valná většina klasických PC nabízí využití USB konektoru pro zavedení systému, a proto neexistence této volby může být způsobena dodatečným zakázáním právě v BIOSU počítače. Výše uvedený postup lze použít, v nastavení BIOSU nalézt sekci pojednávající o zaváděných zařízeních a upravit

ji. Není možné přesně určit, kde se daný prvek nachází, vzhledem k různým výrobcům, upravujícím si nastavení na míru. Dle zkušenosti a současně vzhledem k relativně intuitivnímu menu se můžeme k nastavení dopátrat.

Po úspěšném uložení konfigurace BIOSU, restartu počitače a vložení daného média do USB nebo CD-ROM mechaniky, můžeme zavést například software HIRENS BOOT.[26]

Jedná se o sadu nástrojů, kterou je možné použít pro analýzu stavu daného počítače, ať už v případě jeho nefunkčnosti nebo právě v tomto případě pro zajištení přístupu do systému Windows 10, který je na daném počítači nainstalován.

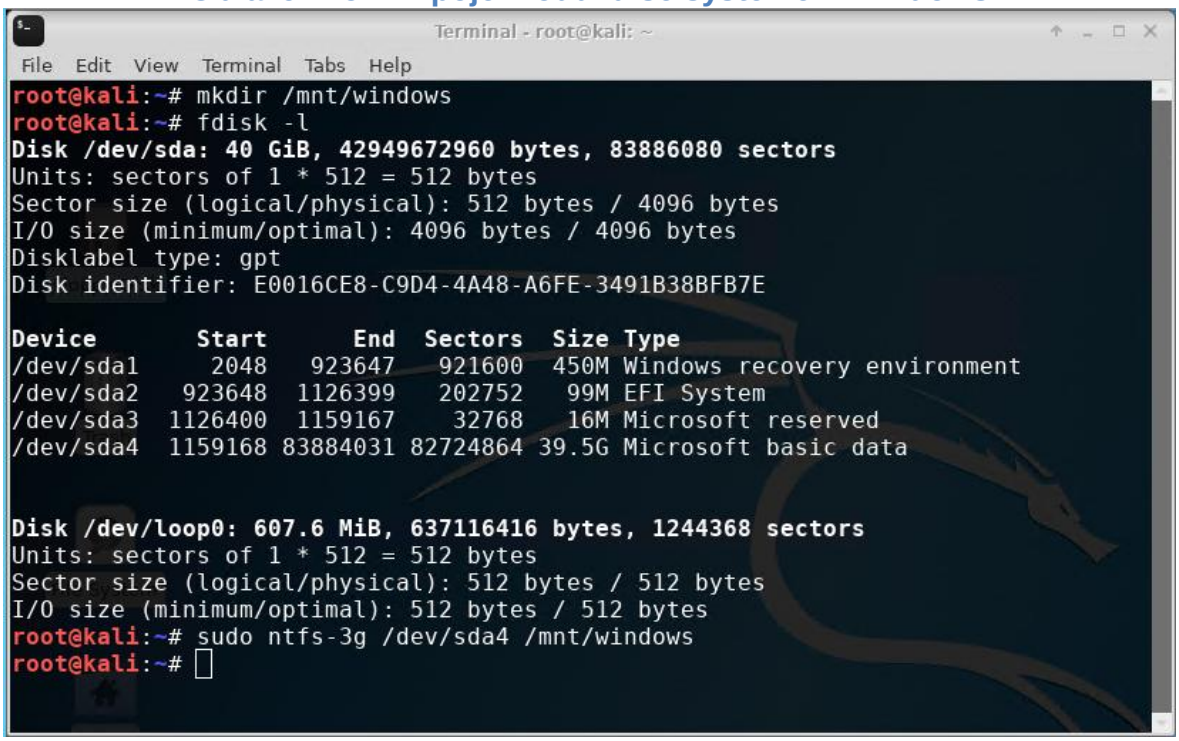
Využijeme možnosti vytvoření nového lokálního uživatelského účtu, který nám zajistí následné přihlášení do prostředí. V případě, že by systém samotný obsahoval nějaký přednastavený lokální účet – například lokálního administrátora, je možné vyresetovat heslo i tohoto účtu a díky tomu se přihlásit k dané stanici. Ať už za pomoci této nebo předchozí možnosti jsme schopni v případě, že klientský disk není zašifrovaný, zajistit si privilegia lokálního administrátora na daném systému. V případě, že bude disk se systémem Windows šifrování využivat, nelze tuto možnost použít. Jelikož součástí našeho testovacího prostředí je i KALI Linux, Ukažme si tuto situaci na příkladu.

Po úspěšném startu distribuce je zapotřebí se dostat k datům systému Windows. Konkrétně k SAM (Security Account Manager) databázi, která je přístupná jak z registrů systému Windows a to HKEY_LOCAL_MACHINE\SAM\SAM tak ve výchozím nastavení ve složce WINDOWS\SYSTEM32\Config\. V rámci zabezpečení smí k databázi přistupovat pouze procesy systému a nelze ho za běhu číst či kopírovat. Jedna z možností, jak si zajistit přístup do počítače je následující.

Vytvoříme adresář v /mnt/windows do kterého připojíme zařízení sda4 na kterém se nachází již zmíněný systém Windows.

[26] Hirensboot – Download [2018.4.1]
Dostupné z: http://www.hirensbootcd.org/

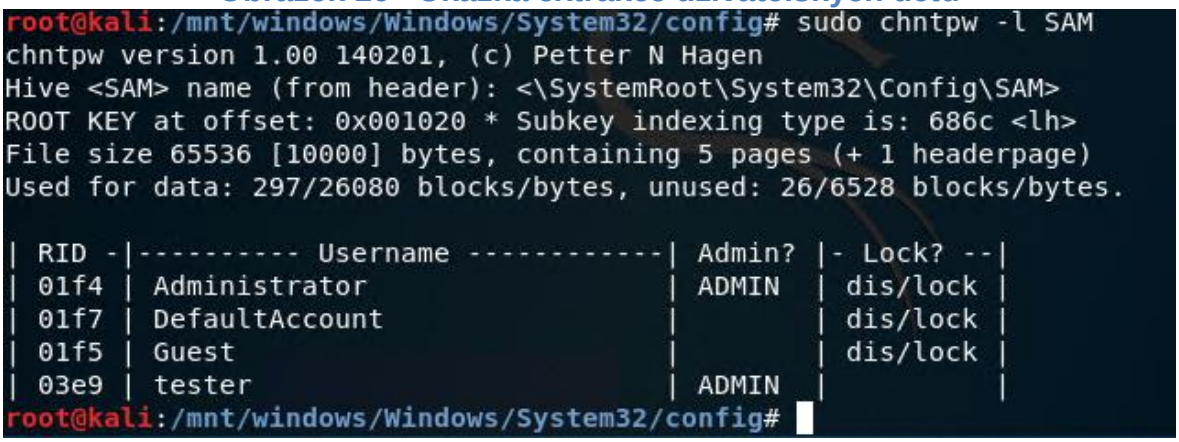
Obrázek 15 - Připojení oddílu se systémem Windows



Zdroj: Vlastní zpracování

Po spuštění aplikace chntpw[27] lze vyextrahovat seznam uživatelů ze souboru SAM obsahující databázi uživatelských účtů.

Obrázek 16 - Ukázka extrakce uživatelských účtů

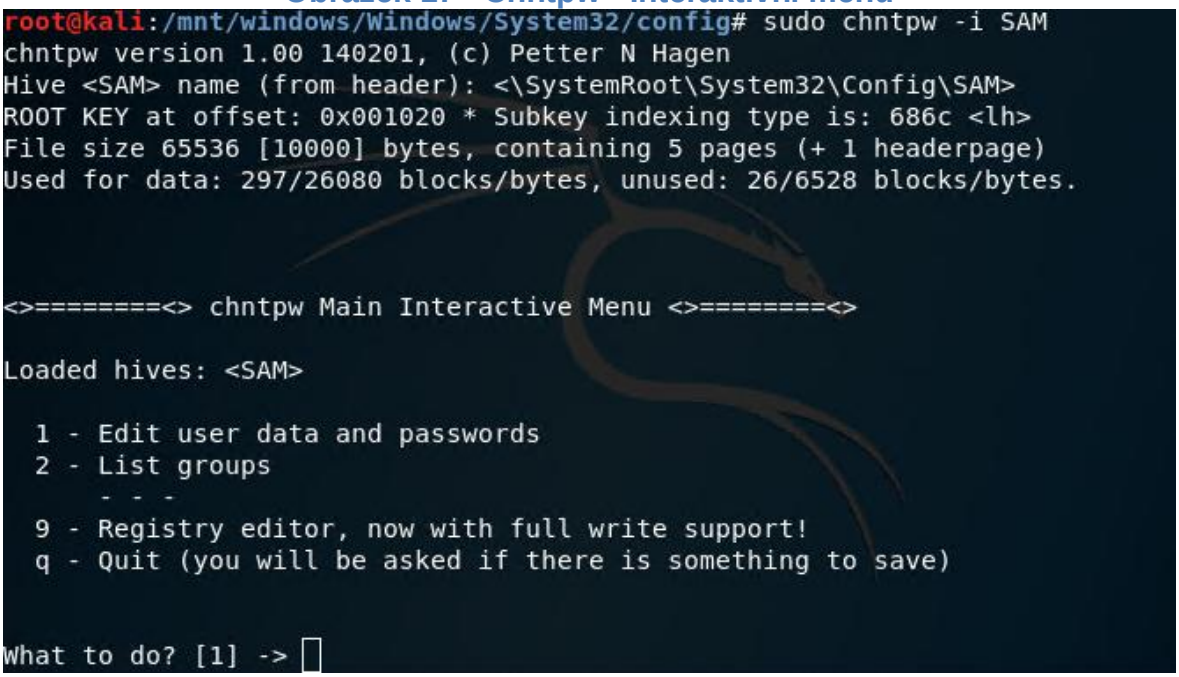


Zdroj: Vlastní zpracování

[27] Chntpw – Extrakce databáze SAM – Download [2018.4.1]
Dostupné z: http://www.chntpw.com/download/

Následně po spuštení v interaktivním režimu za pomoci přepínače -i a specifikování souboru s databází, máme možnost vybrat z nabídky.

Obrázek 17 - Chntpw - Interaktivní menu



Zdroj: Vlastní zpracování

Zvolíme první možnost a jsme vyzváni o zadání user number (RID) uživatele, kterého chceme upravovat.

Následně je možné zvolit jednu z možností a tím například vymazat definované heslo uživatele.

Obrázek 18 - Modifikace uživatelského účtu

Zdroj: Vlastní zpracování

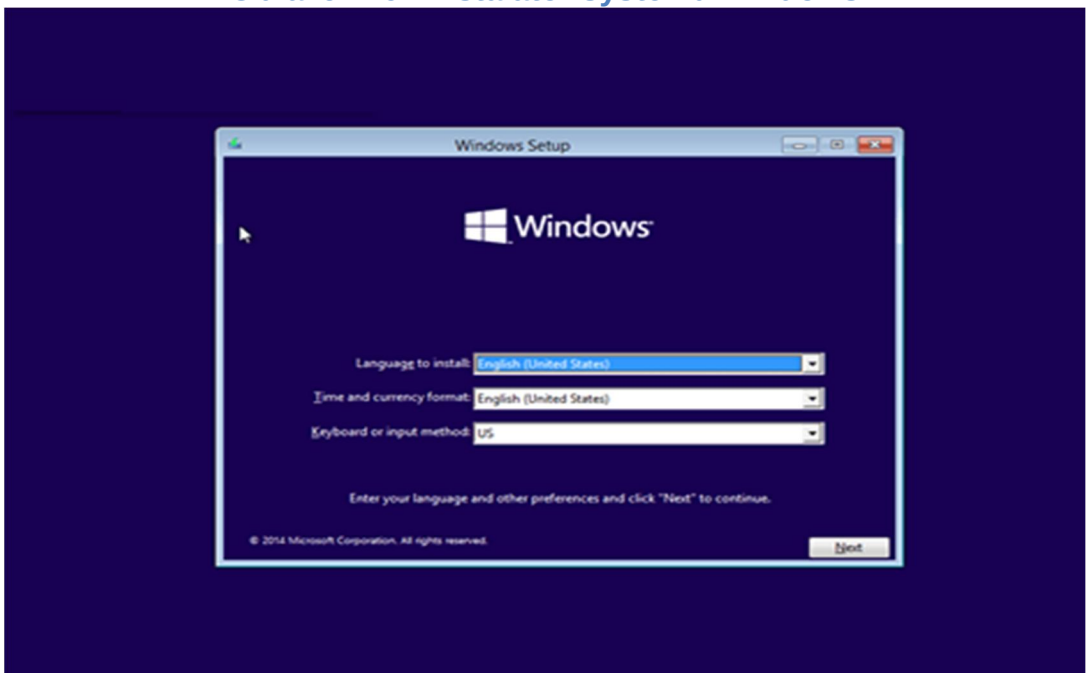
Po změně a opuštění editoru stačí pouze uložit změny a spustit systém Windows.

Další možností na restart hesla uživatele je následující:

Využíváme zde předešlého načtení systému z připojeného USB disku. V tomto případě využijeme disk s instalačním systémem, který musí odpovídat systému, na který se chceme přihlásit. V našem případě instalační disk systému Windows 10.[28]

[28] 4Sysops.com – Reset hesla Windows 10 – [cit. 2018.4.1]
Dostupné z: https://4sysops.com/archives/reset-a-windows-10-password/

Obrázek 19 - Instalátor systému Windows



Zdroj: Vlastní zpracování

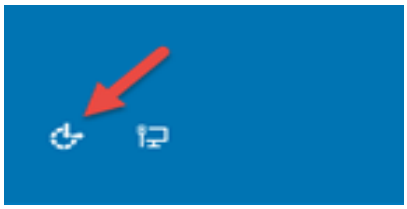
Po zmáčknutí kláves SHIFT + F10 se zobrází příkazový řádek.

Za pomoci následujícího příkazů vytvoříme kopii souboru utilman.exe a následně přepíšeme originální soubor za pomoci souboru cmd.exe, který zastupuje příkazovou řádku.

move d:\windows\system32\utilman.exe d:\windows\system32\utilman.exe.bak
copy d:\windows\system32\cmd.exe d:\windows\system32\utilman.exe

Vzhledem k tomu, že utilman se spoustí v případě kdy na úvodním přihlašovacím okně klikneme na ikonu Usnadnění přístupu (Ease of Access) nebo využijeme klávesy Windows + U, která nám otevře přikazovou řádku s administrátorskými právy pod uživatelem SYSTEM.

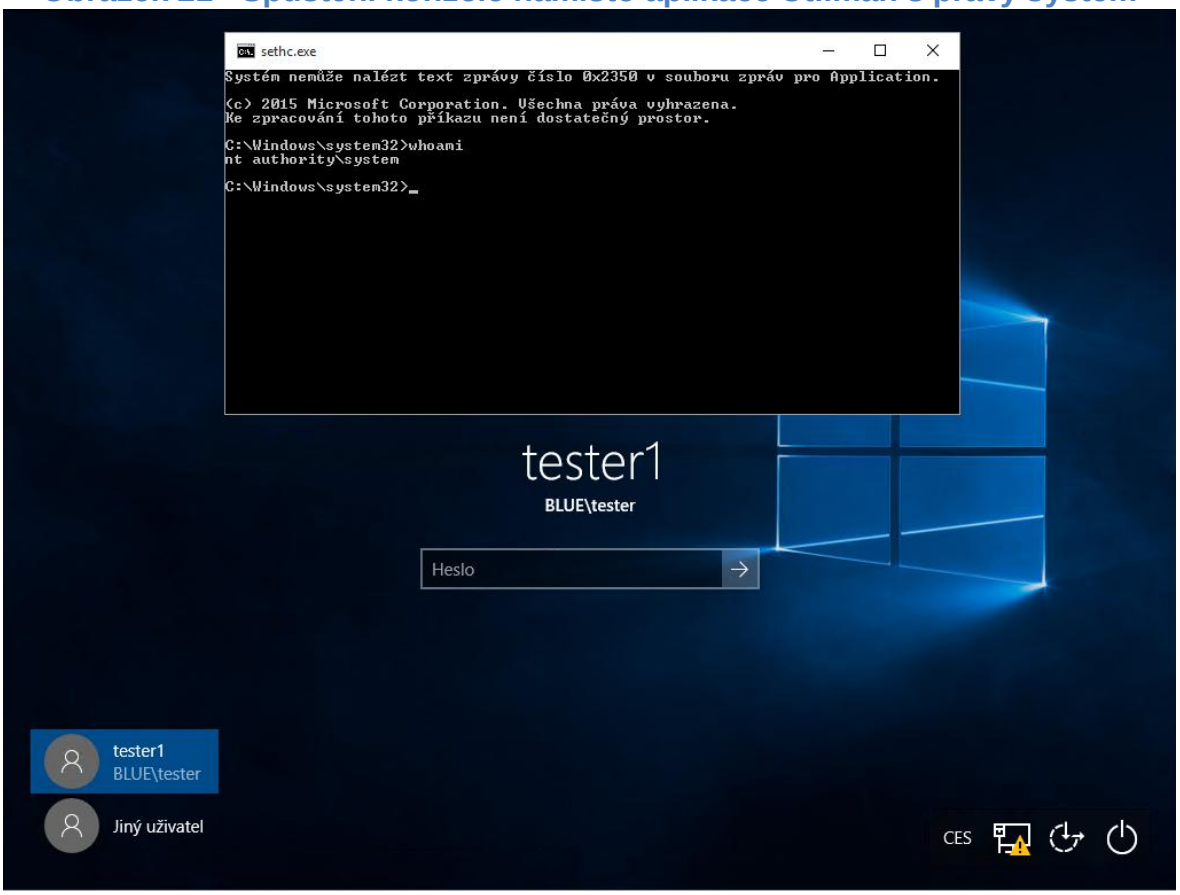
Obrázek 20 - Aplikace Utilman



Zdroj: Vlastní zprcování

Stejný mechanismus lze použít při přepsání souboru sethc.exe namísto utilman.exe souborem CMD. Kdy sethc.exe zajišťuje přístup ke „Sticky Keys“ umožnující usnadnění. Po restartu a výzvě na login lze vyvolat „Sticky Keys“ za pomoci zmáčknutí klávesy SHIFT 5x za sebou. Tím vyvoláme stejnou příkazovou řádku jako výše.

Obrázek 21 - Spuštění konzole namísto aplikace Utilman s právy system



Zdroj: Vlastní zpracování

V eskalovaném přikazovém řádku si můžeme založit lokální uživatelský účet, případně změnit heslo ke stávajícímu administrátorskému.

Založení nového lokálního účtu za pomoci příkazů:
net user tester /add
net localgroup administrators tester /add

V tomto případě nemá uživatel nastaveno heslo.

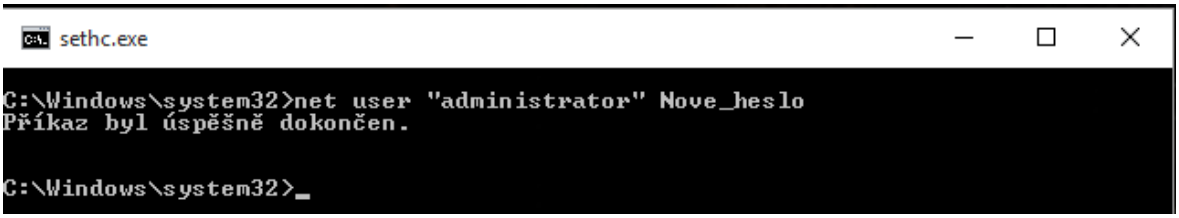
Stejného chování lze docílit přes GUI za pomoci příkazu:
control userpasswords2

Otevře se klasický dialog na přidání nového uživatelského účtu. Je důležité zmínit, že GUI ukazuje pouze účty, které nejsou skryté.

Proto je vhodné využívat příkazový řádek a pro další nastavení si vypsat všechy účty patřící do skupiny administrators na daném počítači:
net localgroup administrators

Následně pak můžeme změnit heslo danému uživateli ve skupině administrators:
net user “administrator” Nove_heslo

Obrázek 22 - Změna administrátorského hesla



Zdroj: Vlastní zpracování

V některých případech se nám může stát, že účet je z nějakého důvodu zakázán a neumožňuje přihlášení. Tento účet nebude zobrazen v GUI “User Accounts”, které bylo popisováno výše.

Z tohoho důvodu lze tento účet učinit aktivním za pomoci:
net user “administrator” /active:yes

Od aktualizace Windows 10 Anniversary edition, nelze spoustit Windows 10 do recovery modu a následně příkazové řádky bez znalosti administrátorského hesla systému. Je proto výhodnější použít změnu hesla za pomoci HIRENS BOOT popisováného výše.

Samozřejmě existují I další produkty, jako například Ophcrack Live CD.[29] Jedná se o systém na bázi Linuxu, kde je možné za pomoci přiložených programů připojit systém WINDOWS 10 podobně jako v případě Kali Linuxu.

4.1.2 S přihlašovacími údaji:

Pokud jsme zaměstnancem dané společnosti a vlastníme účet do domény, máme přístup usnadněn a jsme schopni se přihlásit do daného systému. V případě, že naše práva na systém jsou omezená, což většinou býva standartní přístup v korporátním prostředí, je potřeba pro privilegované akce využit lokálního administrátora. Pro tento účel je možné využít postup zmíněný výše. Vzhledem k implementaci UAC, která bývá standartně zapnuta je účet s administrátorskými právy nutný pro další akce.

UAC – User Access Control – neboli Řízení uživatelských účtů bylo zavedeno od verze Windows Vista a snaží se zvýšit bezpečnost za pomoci omezení oprávnění.

Při přihlášení standartního uživatele do systému je vygenerován přístupový token (access token), který obsahuje informace o právech, které uživatel vlastní. Přihlášený uživatel tak pracuje v kontextu neprivilegovaného standartního uživatele a v případě, že aplikace vyžaduje práva administrátora, je uživatel dotázán na jeho uživatelské jméno a heslo. Koncept samotný si klade za cíl právě ono zmíněné zvýšení bezpečnosti, které od sebe odděluje neprivilegovaný a privilegovaný přistup. Dialog upozorňující uživatele, že daná aplikace, případně úloha vyžaduje zvýšení práv, by mělo mimo jiné i dovést k zamyšlení, zda je toto opravdu potřebné.

V případě administrátora systému jsou v konceptu UAC vygenerovány tokeny dva. Standartní uživatelský token bez vyšších oprávnění a administrátorský, který daná práva obsahuje. Standartní token je používán pro spuštění všech aplikací v systému. V případě, že aplikace požaduje vyšší oprávnění je i administrátor upozorněn a požádán o schválení elevace práv na vyšší úroveň. Vzhledem k tomu, že byl vygenerován i administrátorský token, není zapotřebí vyžadovat znovu jeho uživatelské jméno a heslo. Proces UAC a jeho

[29] Ophracrack – Distribuce Live CD – [2018.4.1]
Dostupné z: http://ophcrack.sourceforge.net/

chování lze ovlivnit za pomoci jednotlivých stupňů v bezpečnostních politikách (Local Security Policy) nebo politikách GPO.[30]

4.2 Klientská stanice Windows 10 - Útočník bez fyzického přístupu k PC

Předešlé scénáře využívaly známých možností průniku, kdy útočník vlastní nebo nevlastní přihlašovácí údaje do systému a dále se poté zaměřily na eskalaci práv na úroveň lokálního administrátora.

Nyní se podívejme na způsob otestování systému Windows 10 z vnějšího prostředí. V našem případě z distribuce Kali Linux nainstalované na samostatném virtuálním stroji.

Po spuštením konzole:
Nejprve zjišťujeme otevřené naslouchající porty na vzdáleném stroji a pokusíme se je identifikovat.

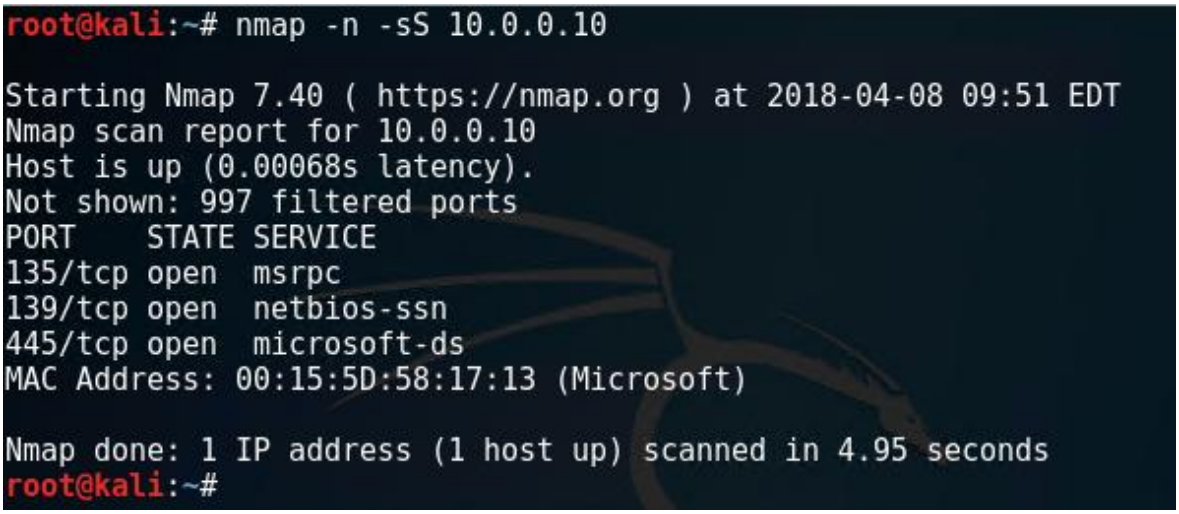
Pro tento účel využijeme TCP skenu. Samotný sken funguje na základě třícestného navázání spojení (three-way handshake) a následné odezvy vzdáleného serveru při testování plného rozsahu vzdálených portů.

Odesíláme TCP paket s příznakem SYN a čekáme na odpověd vzdáleného serveru. Pokud vzdálený server odpoví paketem s příznakem SYN/ACK víme, že daný port je otevřený a čeká na spojení. V případě příznaku RST značící RESET je port považován za zavřený. Pokud nedojde zpět žádná odezva, nebo dojde paket ICMP o nedostupnosti je port označen jako FILTERED a je předpokládán firewall který danou komunikaci zakázal.[31]

[30] Microsoft Docs – UAC – [cit. 2018.4.1]
Dostupné z: https://en.wikipedia.org/wiki/Rainbow_table
[31] NMAP – Port Scanning Techniques – [cit.2018.4.1]
Dostupné z: https://nmap.org/book/man-port-scanning-techniques.html

Samotný TCP scan se spouští za pomoci parametrů -sS. V našem případě využíváme parametr -n, zajišťující nepřekládání IP adres na doménová jména. Toto je pro nás výhodné ze dvou důvodů. První z nich nám zajistí rychlejší sken, kdy neproběhne dotaz na překlad, který by nás mohl v případě skenování větších rozsahů IP adres zpomalovat. Druhým důvodem je zvýšená aktivita na síti, která by na nás mohla upozorňovat. Každý požadavek na DNS překlad generuje další provoz, a to nemusí být žádoucí. Práce samotná si neklade za úkol poskytnout řešení skenu, které by bylo nejlepší z hlediska obejití IDS/IPS zařízení, ale i tak chce poskytnout příklady na základě autorovi zkušenosti.

Obrázek 23 - NMAP - TCP Scan



Zdroj: Vlastní zpracování

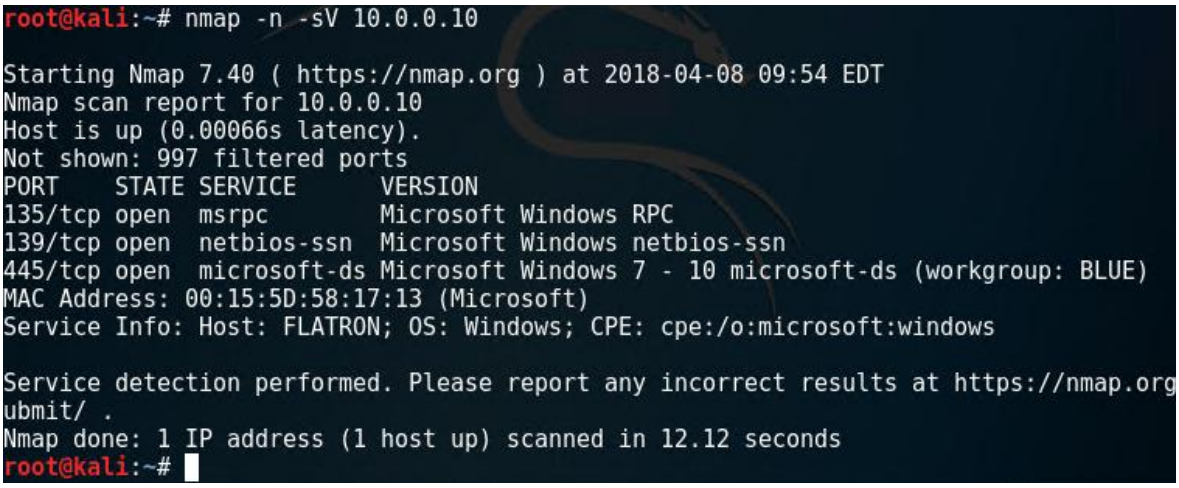
Ze skenu je možno vidět otevřené naslouchající porty vzdáleného systému.

Další krokem je detailní zjištění běžících služeb na jednotlivých portech. NMAP na základě vlastní databáze přiřadí jména služeb příslušným portům. Toto přiřazení nemusí být ale správné, vzhledem k tomu, že služba může běžet na jakémkoliv portu, který administrátor zvolí.

Z tohoto důvodu využijeme přepínač -sV, který využívá vlastní systém pro identifikaci služeb[32] běžích na otevřených portech.

[32] Nmap – Version Detection – [cit.2018.4.2]
Dostupné z: https://nmap.org/book/man-version-detection.html

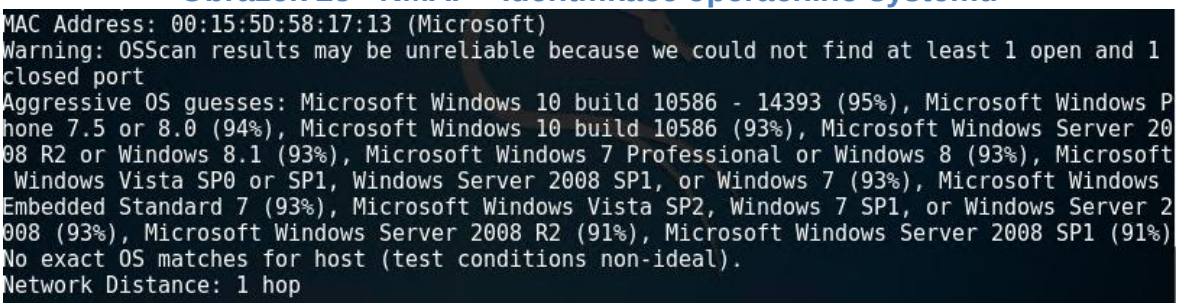
Obrázek 24 - NMAP - Identifikace služeb Windows 10



Zdroj: Vlastní zpracování

Z následujícího skenu si již můžeme udělat bližší obrázek o vzdáleném systému a pokračovat dotazem na detekci operačního systému. Volíme přepínač -O.

Obrázek 25 - NMAP - Identifikace operačního systému



Zdroj: Vlastní zpracování

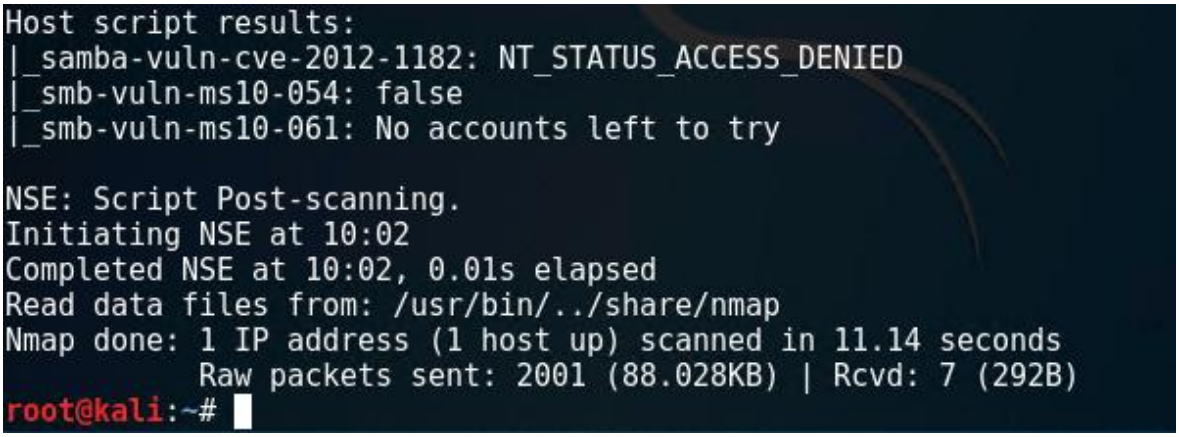
Z výpisu vyplývá, že s největší pravděpodobností se jedná o klientský systém Windows 10 v sestavení 10586 – jedná se ale o odhad a díky relativně vysokým hodnotám dalších možností, které jsou si velmi blízko, si nemůžeme být stoprocentně jisti.

Nmap sám o sobě poskytuje sadu skriptů na identifikaci zranitelných míst, které nám mohou odhalit problémy se zabezpečením.

nmap -v –script vuln 10.0.0.1[33]

Parametr -v nám umožní tzv. „upovídaný“ režim, kdy můžeme vidět průběh všech kroků, které se právě zpracovávají

Obrázek 26 - NMAP - test zranitelností



Zdroj: Vlastní zpracování

Vidíme, že systém neobsahuje žadnou testovanou zranitelnost.

Mezi další nástroje pro zjištění aktuálního stavu systému vzhledem k možnosti napadení je Nessus od společnosti Tenable.

Pro jeho instalaci jsou zapotřebí následující kroky:
Stáhnutí aktuální verze ze stránek společnosti[34]. Vybereme správný balíček vzhledem k naší verzi Kali Linux, a stáhneme. V našem případě 64-bitová verze balíku Debian.

Provedeme instalaci:
Dpkg -i jméno_balíčku – nainstalujeme balíček
/etc/init.d/nessusd start – nastartujeme službu Nessus.

Následně lze za pomoci prohlížeče otevřít přihlašovací stránku.

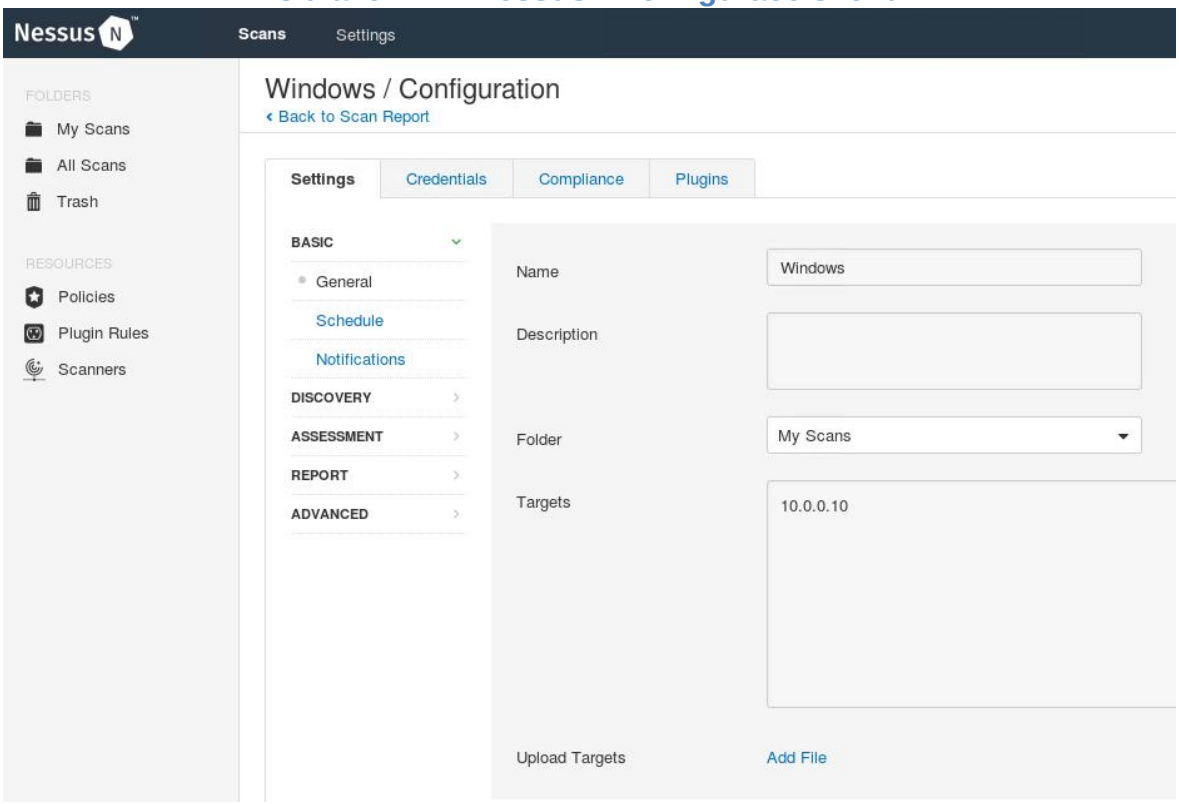
[33] LinuxHint – Nmap Auditory – [cit.2018.4.2]
Dostupné z: https://linuxhint.com/nmap-port-scanning-security/
[34] Nessus – Software Download – [cit.2018.4.2]
Dostupné z: https://www.tenable.com/downloads/nessus

https://localhost:8834

Po zaregistrování na stránkach výrobce můžeme využít volně přístupnou edici, která dostačuje pro naše testování. Následně jsme vyzváni pro konfiguraci hesla uživatele admin.

Založíme nový sken a nakonfigurujeme „Advanced Scan“, v našem případě pouze položku „target“, která značí náš cílový stroj.

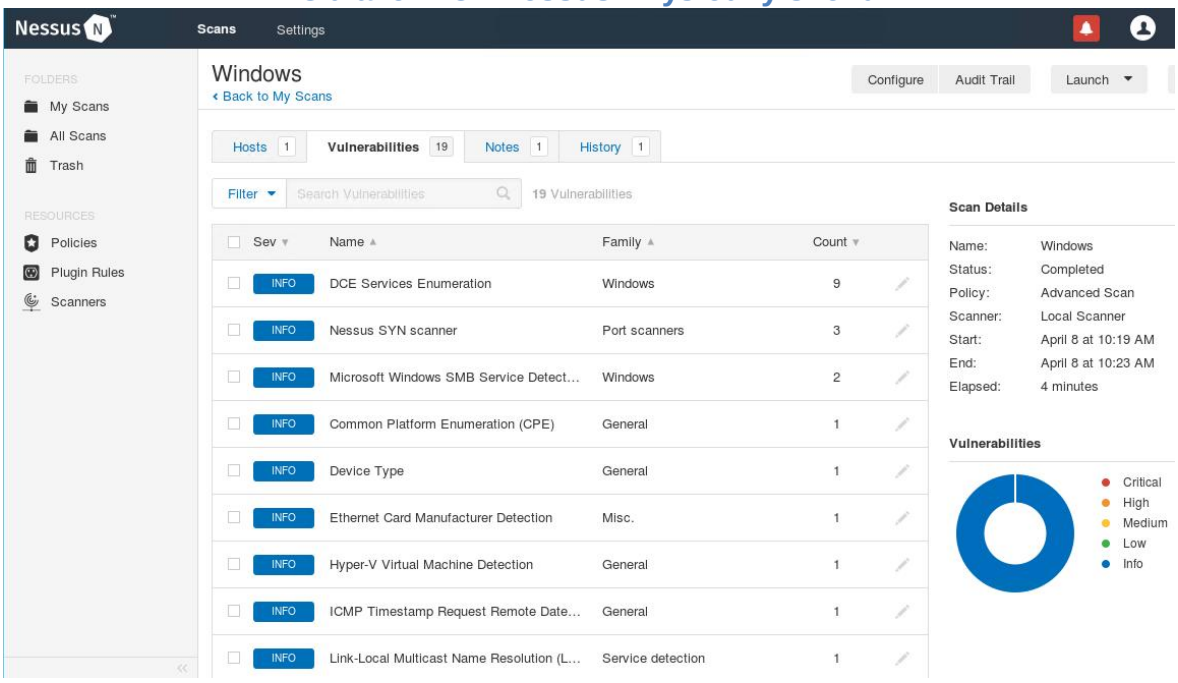
Obrázek 27 - Nessus - Konfigurace skenu



Zdroj: Vlastní zpracování

Výsledkem je seznam všech nazelených chyb na cílovém systému. V našem případě jsme nalezli pouze chyby klasifikované jako „info“ tudíž pouze určitá doporučení, která je vhodná vzít na zřetel.

Obrázek 28 - Nessus - Výsledky skenu



Zdroj: Vlastní zpracování

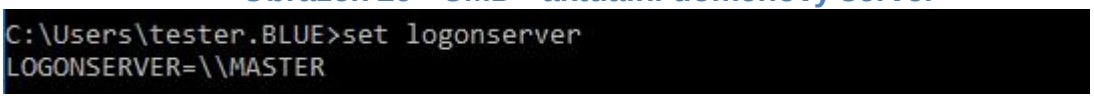
4.3 Klientská stanice Windows 10 - Odhalení doménového serveru

Scénář ukazuje možnost enumerace prostředí v případě, kdy útočník je uživatelem daného počítače a je připojen do domény. V našem teoretickém scénáři víme, jakou má přidělenou IP adresu cíl našeho útoku – doménový server. Pro uvedení příkladu do praxe, kdy nemáme o vzdáleném cíli informace ukažme způsob, jak se k dané adrese případně DNS jménu dostat.

Nejjednodušší cestou na klientském počítači je vypsání systémových proměných přes příkazovou řádku.

Příkaz **SET LOGONSERVER** nebo **SET L** nám ukáže proměnou LOGONSERVER s hodnotou \\MASTER – jménem našeho cíle ke kterému jsme v rámci domény právě přihlášeni.

Obrázek 29 - CMD - aktuální doménový server



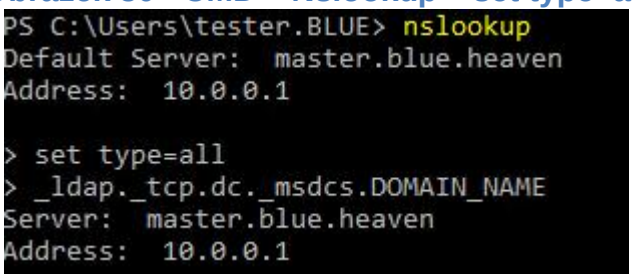
Zdroj: Vlastní zpracování

Další možností může být přikaz NSLOOKUP v interaktivním režimu.

Za pomoci příkazu níže lze získat záznam o umístění služby (SRV) v našem případě doménového kontroleru za pomoci služby DNS.

V uváděném příkladě náš kontroler hostuje i službu DNS, a proto se dozvídáme stejnou IP adresu, která zajišťuje překlad jako adresu služby doménového kontroleru. Pokud by server samotný nehostoval společně i službu DNS, je zapotřebí za pomoci dotazu zjistit daný doménový server viz. níže.

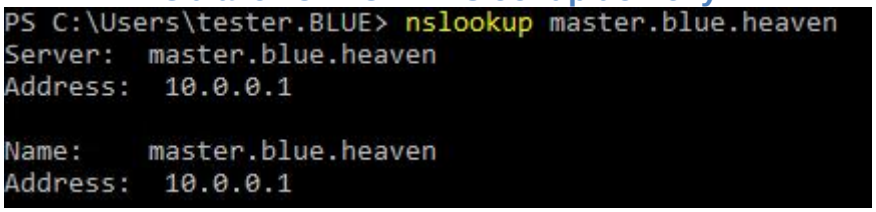
Obrázek 30 - CMD – Nslookup – set type=all



Zdroj: Vlastní zpracování

Jinou možností na získání IP adresy může být dotaz na DNS server, který nám zajistí překlad. Hodnota server je DNS server zajištující námi dotazovaný překlad společně s jeho IP adresou a následuje odpověd.

Obrázek 31 - CMD Nslookup domény



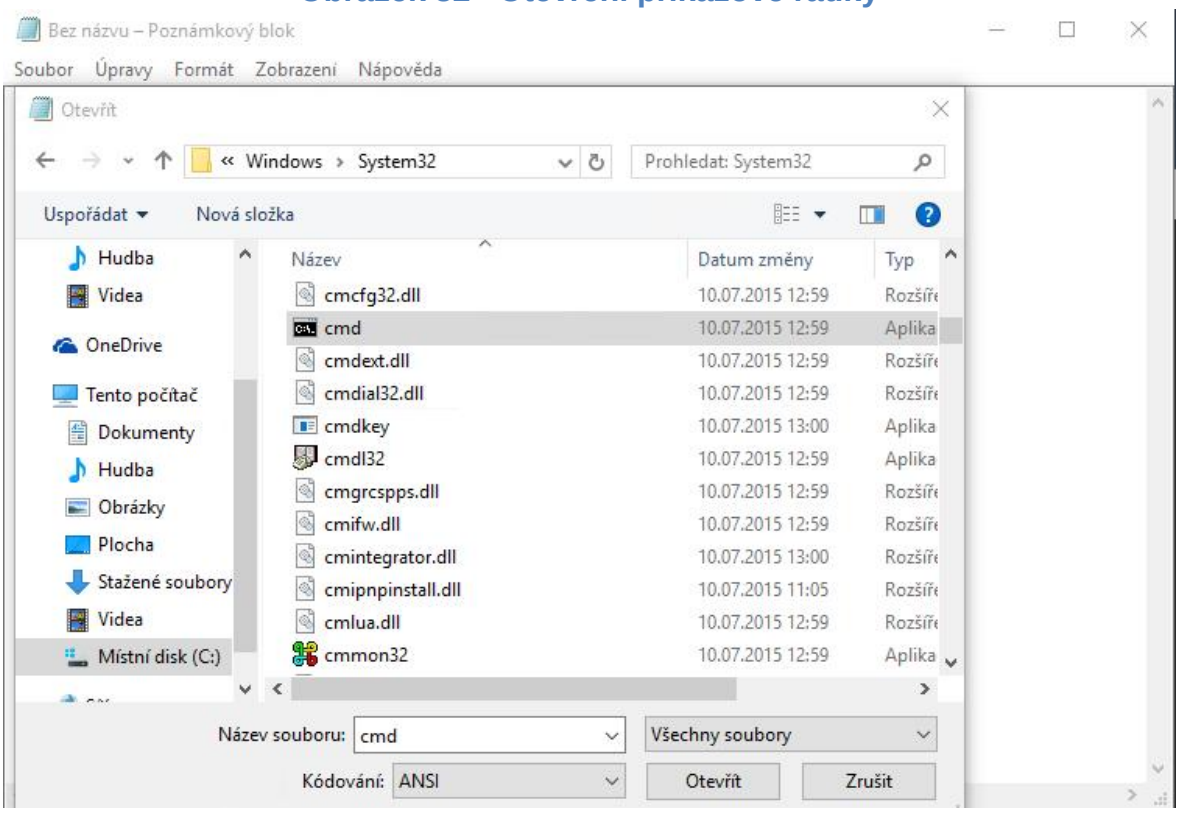
Zdroj: Vlastní zpracování

Samozřejmě je možné spustit dotaz se jménem master zjištěným za pomoci SET a dostat obdobný výsledek.

Příkazová řadka může být na počítači skryta a nebude jí možné standartním způsobem sputit – přes nabídku START nebo prostým zapsáním příkazu cmd po zmáčknutí tlačítka WINDOWS.

Je možné vyzkoušet trik, kdy otevřeme například poznámkový blok – notepad, zvolíme Soubor, Otevřít, vpravo dole vybereme namísto textových souboru všechny soubory. V kořenovém adresáři s instalací systému vybereme složku Windows\System32, kde najedeme cmd.exe.

Obrázek 32 - Otevření příkazové řádky



Zdroj: Vlastní zpracování

Tento postup lze využít v případech, kdy není využito sofistikovanějšího mechanism jako například App lockeru, který zabrání spuštění definovanému spektru uživatelů.

Po zjištění doménového serveru můžeme cílit naše další útoky konkrétním způsobem.

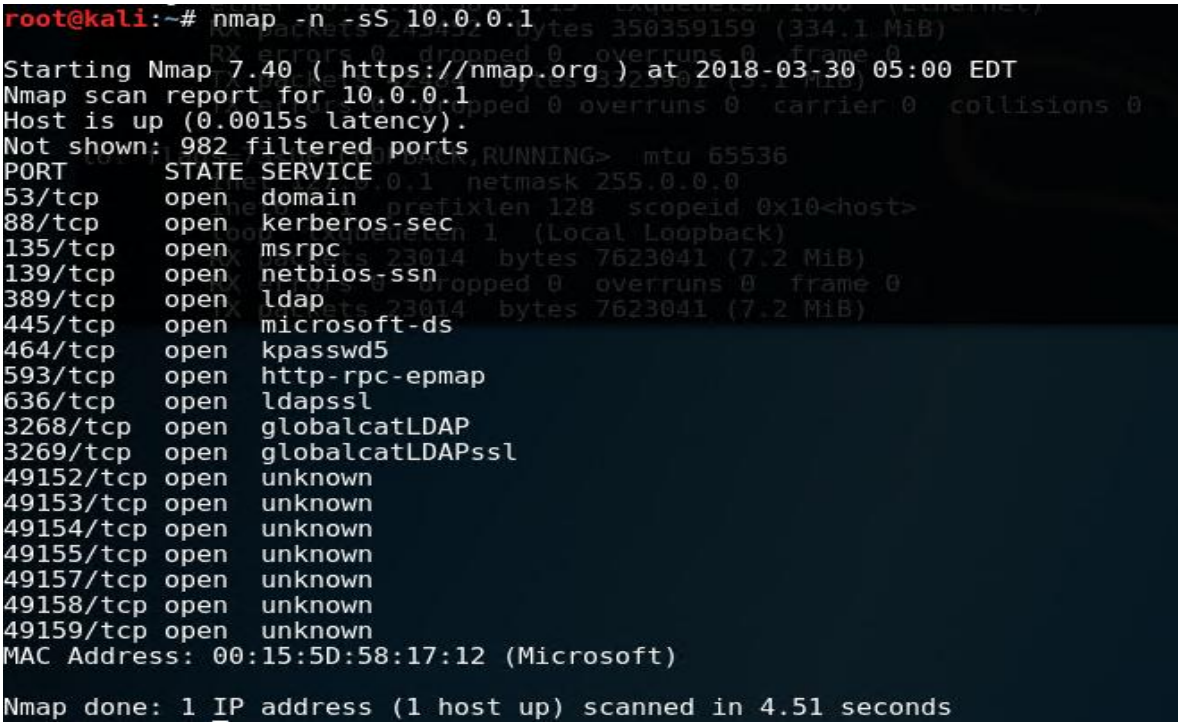
4.4 Windows 2012R2 – enumerace systému

Postup pro enumeraci systému bude v prvním krocích stejný jako při testování Windows 10. Zahájíme TCP skenem vzdáleného systému a zjistíme otevřené naslouchající porty. Dále pak zjistíme konkrétněji běžící služby na jednotlivých portech a pokusíme se zjistit verzi daného systému.

V našem případě probíhá testování z virtuálního stroje umístěného na klientském stroji s Windows 10. Můžeme zde využít již popsané instalace Kali Linuxu v prostředí Virtual Box tak i využití funkcionality Windows Subsystem for Linux pro doinstalování Kali Linuxu přímo do prostředí Windows[35]. Námi uvedený postup zohledňuje první variantu.

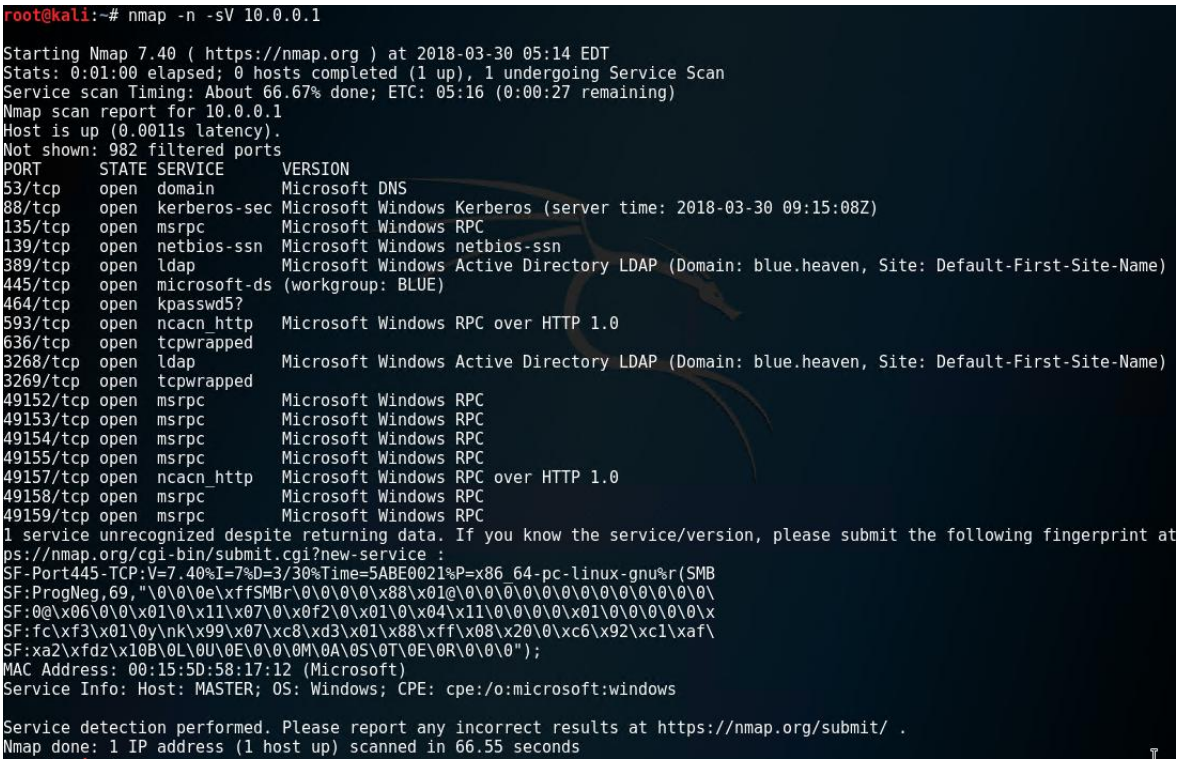
[35] Superuser – How to install Linux Sybsystem for Windows – [cit.2018.04.02] Dostupné z: https://superuser.com/questions/1217167/cant-find-windows-subsystem-for-linux-feature-to-install-bash-for-windows

Obrázek 33 - NMAP - TCP sken



Zdroj: Vlastní zpracování

Obrázek 34 - NMAP – Identifikace služeb Windows Server 2012R2



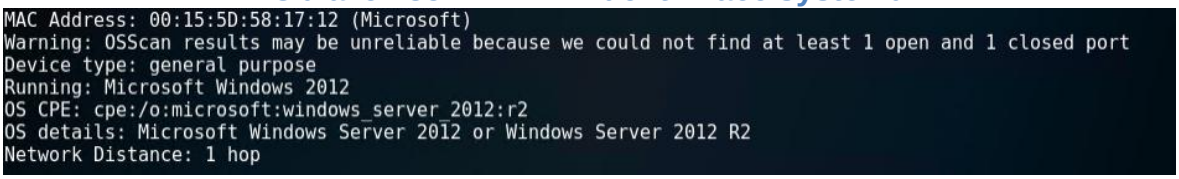
Zdroj: Vlastní zpracování

Po úvodním TCP skenu [Obrázek 33], který odhalil běžící služby na jednotlivých portech, přistoupíme k zevrubnějšímu odhalení služeb.

Parametr -sV nám poskytne detailnější výpis jednotlivých služeb [Obrázek 34]. Můžeme se tedy dozvědět nastavený čas na serveru a z toho případně usoudit v jakém časovém pásmu se nachází.

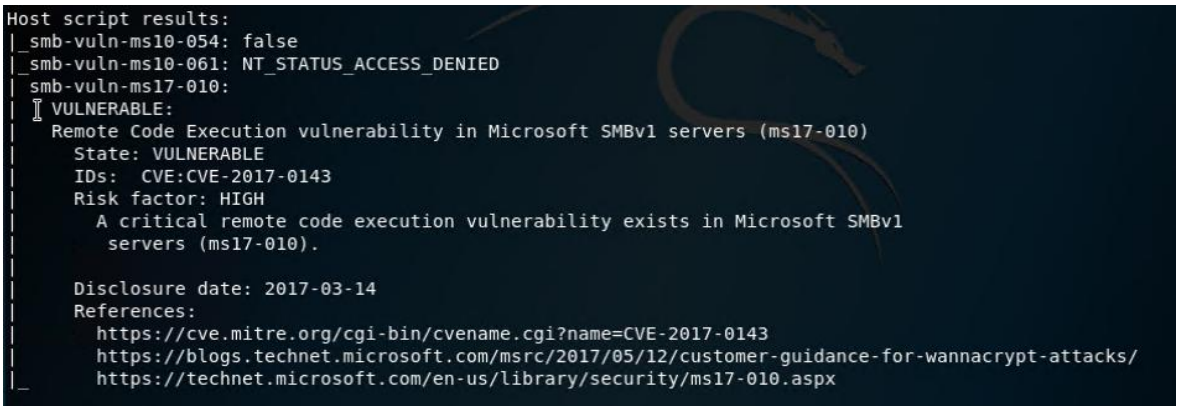
Následuje identifikace systému, kde je systém identifikován jako Windows Server 2012.

Obrázek 35 - NMAP - Identifikace systému



Zdroj: Vlastní zpracování

Obrázek 36 - NMAP - Identifikace zranitelností



Zdroj: Vlastní zpracování

nmap -v –script vuln 10.0.0.1[36] - výstup je zde zkrácený z důvodu vetší přehlednosti.

V našem případě je systém identifikován jako zranitelný vůči chybě ms17-010. Na výstupu vidíme krátky popis chyby a odkazy na stránky zabývající se danou chybou.

[36] LinuxHint – Nmap port scanning security – [cit.2018.4.2]
Dostupné z: https://linuxhint.com/nmap-port-scanning-security/

MS 17-010

Využívá otevřeného portu 445 a zneužití chyby v Microsoft Windows SMB Serveru, který nevhodně nakládá s příchozími požadavky a díky tomu lze za pomoci speciálně upravené zprávy spustit nebezpečný kód, který zajistí přístup do systému.[37]

Této chyby využíval nechvalně známý ransomware WannaCry[38], který poté zašifroval data na počítači a požadoval dále výkupné pro obnovení předchozího stavu. Pro využití dané chyby je možné použít nástroj Metasploit distribuce Kali Linux.

4.5 Kali Linux - Metasploit

V prostředí Kali Linux je zapotřebí před spuštěním provést následující kroky.
Sputit SQL server pro Metasploit, vytvořit a inicializovat databázi.

service postgresql start
msfdb init

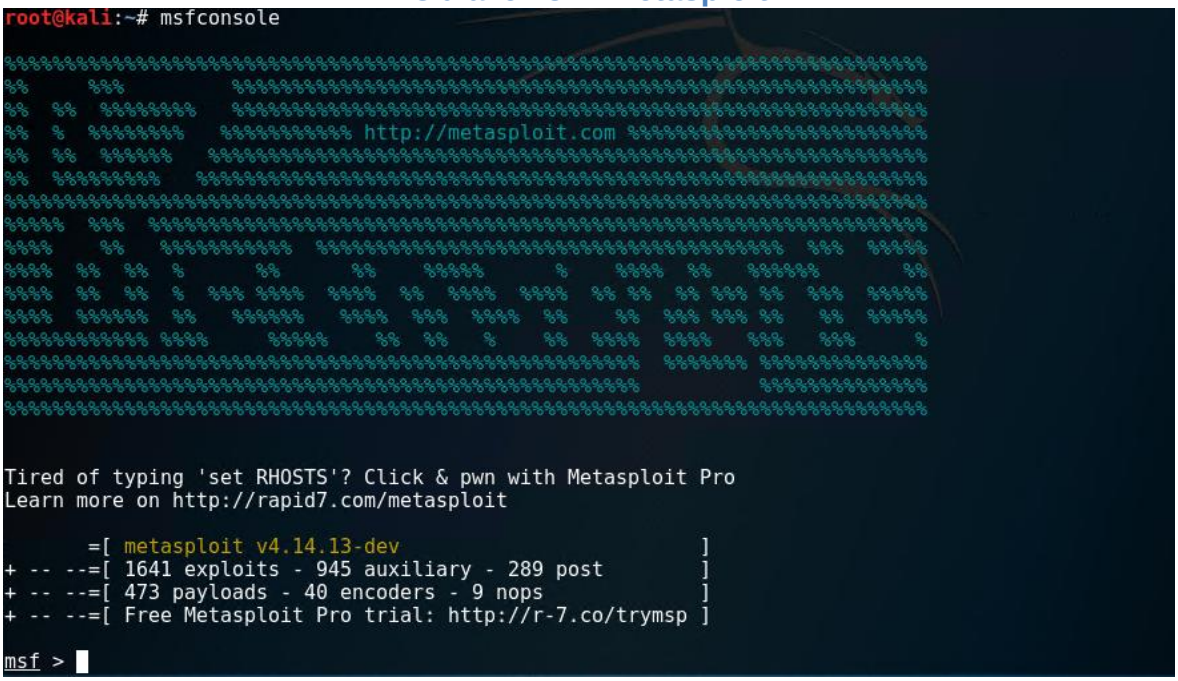
Pro další kroky je zapotřebí vymezit základní pojmy, které se společně s Metasploitem využívají.

Exploit: Program, který má za úkol využít chybu nalezenou ve vzdáleném systému, připadně programu.
Payload: Kód, který udržuje přístup v systému po úspěšném provedení exploitu.

Nejedná se samozřejmě o plný výčet pojmů, které Metasploit obsahuje. Nástroj samotný nabízí širokou škalu dalších možností, které umožňují např. pokročilé techniky skrývání před bezpečnostními zařízení typu IDS/IPS, které ale nejsou součastí práce.

[37] Microsoft – Security Bulletin MS17-010 – [cit.2018.4.2]
Dostupné z: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
[38] Paul-sec – WannaCry – [cit.2018.4.2]
Dostupné z: http://www.paul-sec.com/wannycry-wannadecrypt0r-ms17-010.html

Obrázek 37 - Metasploit

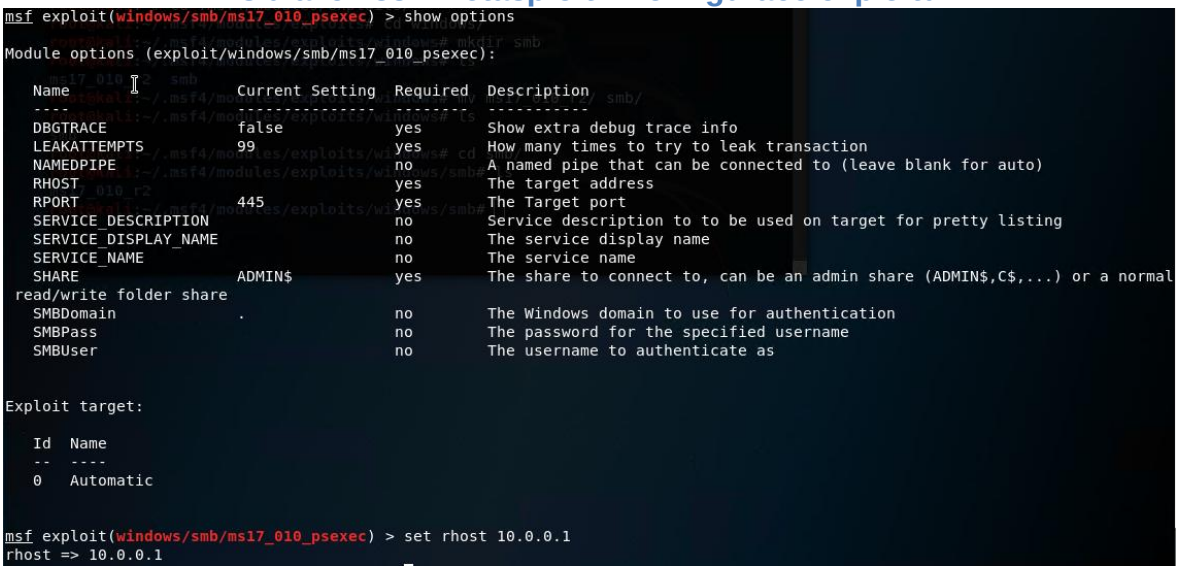


Zdroj: Vlastní zpracování

V předešlé kapitole byla identifikována zranitelnost ms17-010. Po zadání příkazu search ms17-010 zjistíme, že Metasploit obsahuje exploit na danou zranitelnost. V případě, že by danou zranitelnost neobsahovatl, bylo by nutné stáhnout daný exploit z webových stránek a naimportovat.

Vídíme, že máme k dispozici dva exploity vzhledem k zadané zranitelností. Ta lze vybrat přikazem use a cestou ke zranitelnosti. Po výběru a zadání příkazu show targets vidíme systémy pro které je daný exploit funkční. Zranitelnost neobsahuje námi detekovaný operační systém, a proto tento exploit nevyužijeme. Druhý exploit nazvaný ms17_010_psexec není již omezen verzí operačního systému, a proto můžeme přistoupit k jeho nastavení.

Obrázek 38 - Metasploit - Konfigurace exploitu



Zdroj: Vlastní zpracování

Příkazem show payloads[39] je možné nastavit jaký typ payloadu budeme využívat po úspěšné exploitaci systému. Metasploit nabízí široké spektrum payloadů, které lze využít. Ať už se jedná o nástroj VNC zprostředkující přístup na vzdálenou plochu daného systému, příkazovou řádku systému Windows nebo například Meterpreter, který bude využíván i pro naši ukázku.

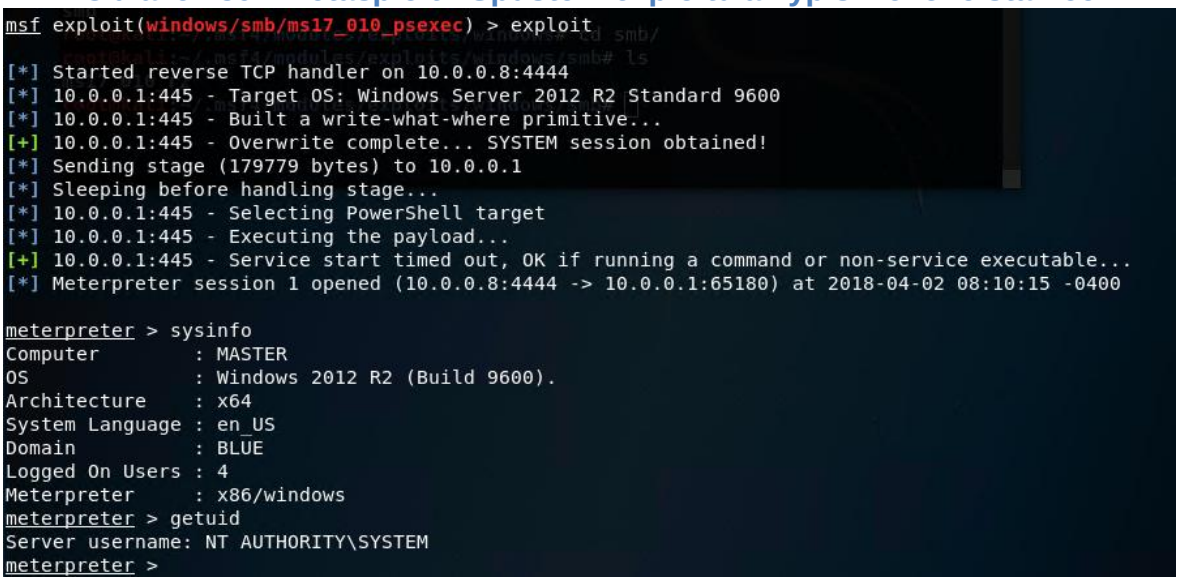
Při exploitaci systému Windows nabízí Metasploit payload typu Meterpreter, ten nám poskytne příkazový shell podobný klasickému Windows shellu, ale nabídne nám i nadstavbové příkazy, které nám umožní lehčeji získat potenciálně zajímavé informace. Příklady jednotlivých příkazů pro Meterpreter jsou k dispozici zde. [40]

Nyní můžeme přistoupit k jeho spuštění a ověřit si, zda se opravdu nacházíme na dáném vzdáleném serveru.

[39] BURNS, Bryan. *Security power tools*. Sebastopol, CA: O'Reilly, c2007. ISBN 978-0596009632.str. 208

[40] Offensive-Security – Meterpreter basics – [cit.2018.4.2]
Dostupné z: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

Obrázek 39 - Metasploit - Spuštění exploitu a výpis z cílové stanice



Zdroj: Vlastní zpracování

Po úspěšné exploitaci a zadání příkazu sysinfo a getuid vidíme, že se opravdu nacházíme na cílovém systému s právy SYSTEM, které nám umožní neomezený přístup k vzdálenému systému.

4.6 Zranitelnosti

Předchozí příklad ukazoval jednu z možností jak využít chybu, která byla nalezena na vzdáleném systému a poté využil již připraveného modulu v aplikaci Metasploit.

Velmi dobrým pomocníkem při hledání zranitelností je portál https://www.cvedetails.com/ , který nám poskytne přehled všech nalezených chyb vzhledem k vybranému operačnímu systému.

Jako příklad může sloužit přehled zranitelností Windows Serveru 2012. Je zde možné vidět a dále procházet jednotlivé nalezené chyby v operačním systému. Konkrétní informace ke každé nalezené chybě s popisem její závažnosti a odkazy na případné exploity chyby.

Obrázek 40 - CVE Details - Zranitelnosti Windows Server 2012

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2012	5		2	2						1		2			
2013	51	12	17	17	3			1		2	2	21			4
2014	38	9	11	5	3					6	5	12			4
2015	155	16	46	11	9			1		31	26	60			1
2016	156	8	42	19	7					16	28	76			
2017	235	24	51	18	4		1			6	107	15			
2018	45	3	3	2							23				
Total	685	72	172	74	26		1	2		62	191	186			9
% Of All		10.5	25.1	10.8	3.8	0.0	0.1	0.3	0.0	9.1	27.9	27.2	0.0	0.0	

Zdroj: [41]

Námi nalezená chyba je vedena pod identifikátorem CVE-2017-0143. Po jejím vyhledání lze nalézt její základní popis společně s dalšími odkazy, které obsahují například modul pro zneužití dané chyby v aplikaci Metasploit.

Jinou možností je využití stránek https://www.exploit-db.com, které nám umožňují stahnutí přímo exploitů daných chyb a dále je využít.

V našem případě by se jednalo o https://www.exploit-db.com/exploits/41891/.

[41] CVE Details – Windows 2012 Vulnerabilitiy overview – [cit. 2018.4.4] Dostupné z : https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

5 Nejlepší praktiky k ochraně zvoleného prostředí

Každý operační systém v této době se snaží aplikovat prvky bezpečnosti již ve svém základním nastavení. V současnosti operační systém Windows obsahuje řadu nastavení pro zvýšení bezpečnosti. Jedná o systém aktualizací, který jej udržuje v nejnovějším sestavení a snaží se tím zabránit neaktuálnosti či případné zranitelnosti systému vůči nalezeným chybám. V systému jsou již ve většině případů v základním nastavení přítomna pravidla pro zvýšení bezpečnosti. Nelze ale každý operační systém nastavit vždy optimálním způsobem již v základním nastavení, právě z důvodu individualizace daného systému a vyžadovaných služeb, které jsou využívány, tak i vzhledem k síťovému prostředí ve kterém se nachází.

Z tohoto důvodu je vhodné vždy zvážit možnost dalšího nastavení pro zvýšení bezpečnosti daného operačního systému.

5.1 BIOS / UEFI

BIOS představuje nízkoúrovňový software, který zajišťuje start celého počítače. Jde o komunikaci mezi firmwarem jednotlivých komponent a operačním systémem. Ve většině moderních PC v současné době je využíváno UEFI namísto předchozího BIOSU, které nabízí mnohem propracovanější uživatelské rozhraní a další vylepšení jako například možnost ovládání za pomoci myši nebo dotykové obrazovky, které nebylo u BIOSU možné. BIOS samotný je uložen v paměti typu ROM nebo EEPROM přimo na základové desce, UEFI je uloženo v paměťovém modulu (NVRAM) nebo na pevném disku kde má samostatný oddíl.[42] Princip ale zůstává naprosto stejný a ve většině případů se stále využívá ustálený název BIOS.

Protože BIOS řídí následné zavedení dalších komponent, jako i následné spuštění operačního systému, je velmi vhodné ho zabezpečit.

[42] CHIP – Secure Boot – [cit.2018.4.4]
Dostupné z: https://www.chip.cz/casopis-chip/earchiv/vydani/rocnik-2013/chip-08-2013/uefi-secure-boot-prilis-bezpecny-start-pc/

BIOS samotný poskytuje zabezpečení přístupu administrátorským heslem, bez kterého není možné se přihlásit.

Jako další vhodné nastavení se jeví možnost přistupu pouze k jednomu zařízení, ze kterého se bude snažit BIOS systém zavést, a to tedy pevného disku. Další zařízení, která jsou ve výchozím nastavení přiřazena do boot orderu by měla být odebrána případně explicitně zakázana. Příkladem může být právě možnost zavedení z USB karty, sítě nebo jiných periferií.

Dále je velmi vhodné zajištění daného hardwaru proti neoprávněnému průniku a vymazání právě již zmíněného nastavení BIOSU. Je proto vhodné při výběru hardwaru počítat i s touto variantou a zvolit vhodnou počítačovou skříň, která bude poskytovat možnost uzamčení.

5.2 Přístup na pevný disk

,.

Naše předchozí scénaře využily možnost, kdy nebyl zaveden primární operační systém z pevného disku, ale načten podvržený systém na disku USB. Z tohoto důvodu nebyl primární operační systém chráněn jeho vlastními obranými mechanismy a došlo k zneužití jeho částí. Je proto velmi vhodné pevný disk šifrovat. Operační systém Windows 10 i 2012R2 nabízí nástroj BITLOCKER, který zašifruje celý pevný disk a pro jeho přístup k němu je nutné vlastnit číselný kód. Nedostane se tím tedy do situace popsané v oddílu 4.1, kdy si útočník připojil disk za pomoci distribuce KALI LINUX.

SECURE Boot – Volba dostupná s UEFI BIOSEM dovolí spouštět pouze operační systémy, které obsahují svůj podpis v tzv. KEK (Key Enrollment Keys)[36]. Jedná se o klíče, které pocházejí od vývojářů daného operačního systému a obsahují jak klíče, tak i hashe částí hodnot operačního systému. Ve většině případů jsou ale s novým počítačem obsahujícím operační systém Windows 8[36] a novější importovány pouze klíče společnosti Microsoft, které tím ale znemožní využívání Secure Bootu jinými operačními systémy.

V současnosti se již objevují klíče pro operační systém Linux, ale není pravidlem, že by každá distribuce toto umožňovala.

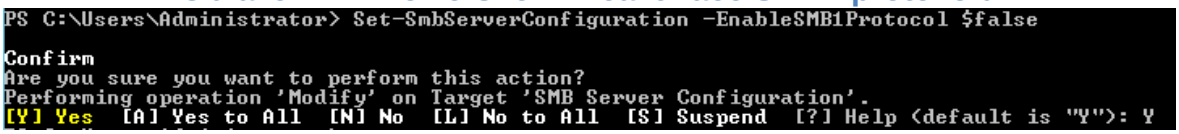
Výhodou tohoto konceptu je, že UEFI dovolí zavést pouze podepsaný systém a tím se vyhýbáme možnosti zavedení ROOTKITU, který by poté mohl působit v operační paměti. UEFI tedy umožňuje provozovat pouze operační systémy, ke kterým vlastní jejich podpis.

5.3 Chyba MS 17-010

Samotná chyba je už opravena v rámci bezpečnostního updatu společnosti Microsoft – lze najít pod označením KB4012212 u katalogu služby Microsoft Update. Nebo přímo na stránkách společnosti.[43]

Manuální cesta pro zabránění zneužití této zranitelnosti znamená zakázání SMBv1 na cílovém stroji. Popíšeme si dvě varianty dostupné ze stránek Microsoft, první za pomoci konfigurace samotné služby a druhé úpravou registru.[44]

Obrázek 41 - Powershell - Deaktivace SMB1 protokolu



Zdroj: Vlastní zpracování

[43] Microsoft – MS17-011 Security Update – [cit.2018.4.4]
Dostupné z: https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

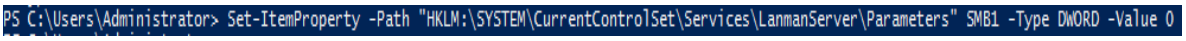
[44] Microsoft – How to detect, enable and disable SMBv1, SMBv2, SMBv3 in Windows and Windows Server – [cit.2018.4.4]
Dostupné z: https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

Druhou variantou může být úprava klíče který se nachází:

HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Zde upravíme hodnotu klíče DWORD s názvem SMB1 na hodnotu 0. Lze toho docílit jak manuální úpravou přes registry systému, tak příkazem Powershellu.

Obrázek 42 - Powershell - Úprava hodnot registru



Zdroj: Vlastní zpracování

5.4 Group Policy Management

V našem testovacím scénáři je Windows 10 součástí domény, a proto jsou jeho jednotlivá nastavení spravována za pomoci GPO. Není vhodné provádět individuální zásady zabezpečení na jednotlivých počítačích za pomoci Local Security Policy nebo například registru, ale ponechat toto nastavení v rámci globálního GPO, které zajistí centrální management politik pro jednotlivé stanice.

V rámci zabepečení představíme nejdříve vhodný způsob nastavení GPO politik pro operační systém Windows 10 a poté i pro variantu serveru.

5.4.1 Group Policy Management - Windows 10

Kapitola 4 pojednávající o útočníkovi bez přihlašovacích údajů, umožnila přístup do počítače za pomoci přistupu do BIOSU počítače. Řešením této situace je již zmíněné šifrování pevného disku a zamezení přístupu do BIOSU jak administrátorským heslem, tak i fyzickým zabezpečením počítače. Může nastat například možnost, kdy je zapnut Secure Boot a útočník využije instalační CD systému Windows společně s metodou popsanou v kapitole 4. Z tohoho důvodu, pokud se už nejedná o Windows 10 s Anniversary aktualizací, která vyžaduje zadání hesla administrátora, je zapotřebí tuto skutečnost zohlednit a zakomponovat ji do nastavení bezpečnostních politik.

Ukažme si tedy ukázku vhodných nastavení, které by mohli být v rámci domény nakonfigurovány a aplikovány. Námi představované politiky jsou nastavovány pro klienta se systémem Windows 10, je možné i vhodné, část těchto politik aplikovat i v rámci doménového kontroleru. Práce samotná si nebere za úmysl obsáhnout veškeré nastavení, ale ukázat možnosti a aplikovat část z nich. V rámci hierarchie AD se nyní tedy bavíme o OU Testing_Machines, které tato nastavení obsahuje.

Ohledně vytváření politik samotných existuje mnoho různých přístupů. V některých případech správci upřednostňují založení nové politiky pro konfiguraci jednotlivé funkčnosti a vyhrazují jim vždy individuální politiku, je tedy vždy zřejmé, co politika konkrétně obsahuje.

V druhém, naprosto odlišném případě, administrátor vytvoří jednu politiku, ve které konfiguruje naprosto vše. V našem případě využíváme střed mezi těmito dvěma přístupy a dělíme politiky, které se zabývají nastavením počítače a nastavením uživatele. Máme tedy dvě politiky a v každé máme nakonfigurovanou pouze specifickou větev. Výše uvedené přístupy mohou být vždy odlišně aplikovány v závislosti na rozsahu a složitosti daných systémů nebo preferencích daného administrátora. V našem případě volíme zlatý střed.

Příklad z kapitoly 4, kdy útočník po vložení instalačního média má k dispozici konzoli s administrátorskými právy, lze omezit zde.

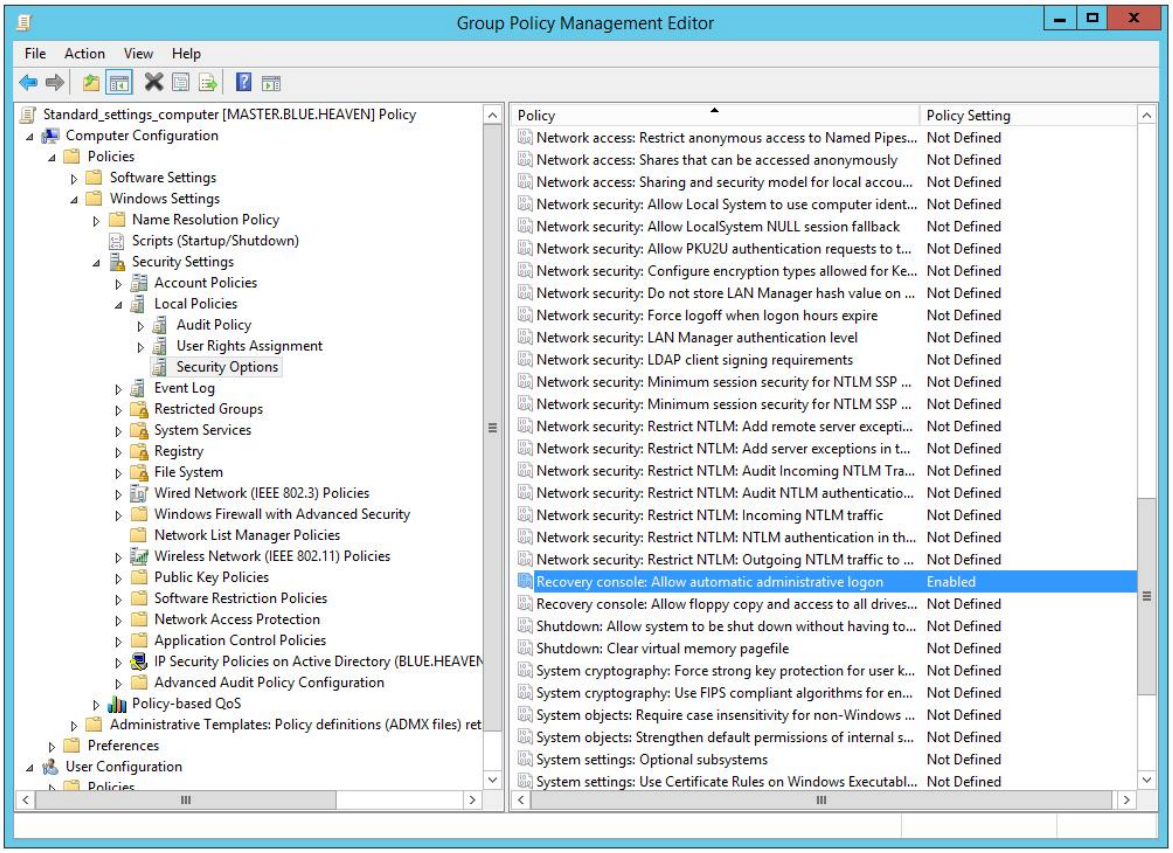
- **Recovery console – Allow automatic administrative logon**

Cesta: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

  - Nastavením volby **Recovery Console: Allow automatic administrative logon** na **Disabled.**

Nyní je nutné při spuštení Recovery console vždy zadat přihlašovací údaje administrátora.

Obrázek 43 - GPO - Editace politik - Recovery console

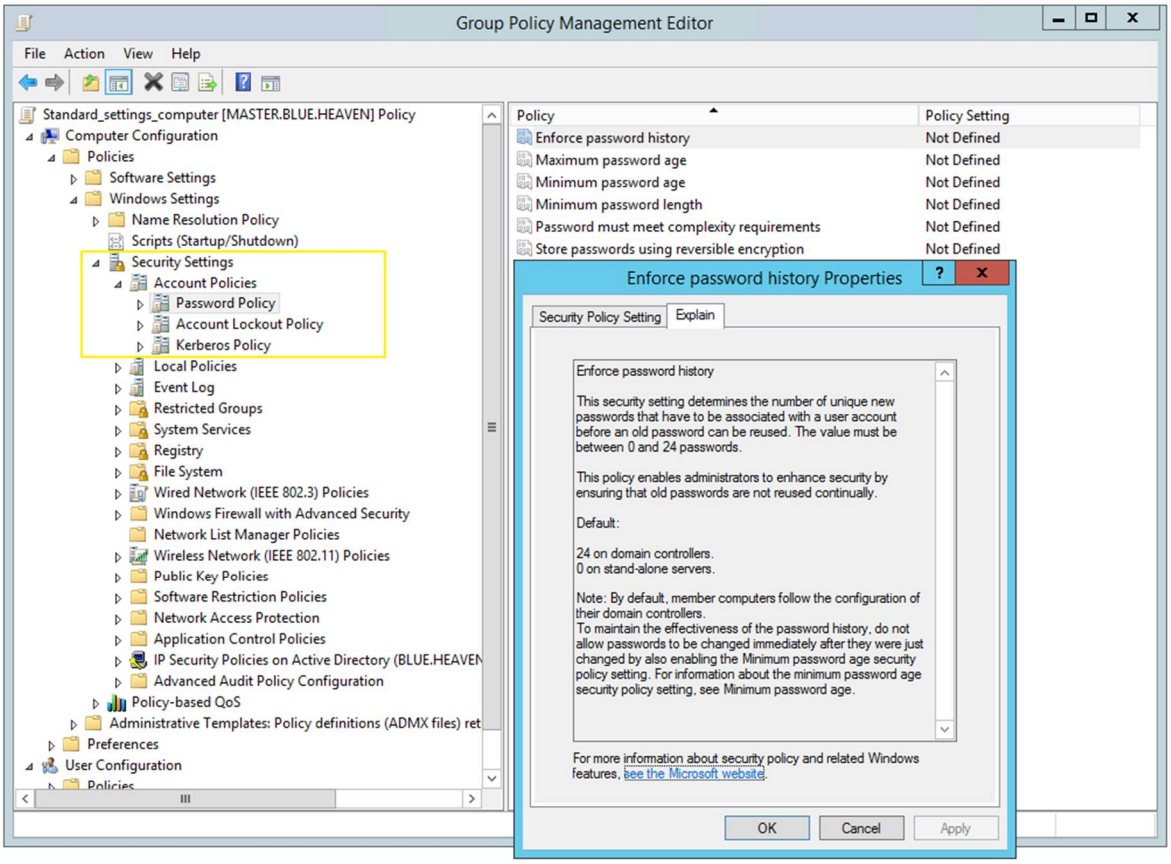


Zdroj: Vlastní zpracování

Představme si ukázku dalších nastavení, která jsou vhodná z pohledu bezpečnosti.

Account Policies – řeší nastavení účtů samotných. Obsahuje tři jednotlivé podskupiny a definice nastavení. Velkou výhodu může být, že u každého jednotlivého nastavení v sekci Explain je vysvětlení dané politiky a nastavení, které je využito jako výchozí v případě, pokud není politika definována.

Obrázek 44 - GPO - Account Policies



Zdroj: Vlastní zpracování

Je velmi vhodné zapřemýšlet o nastavení hesel samotných, a to například u možnosti ukládání jejich historie – tzv. „Enforce Password History“, pro zajištění nastavení rozdílných hesel ze strany uživatele při jejich expiraci.

- **Enforce password history**

Cesta: Computer Configuration\Policies\Windows Settings\Security Settings\Account policies\Password Policy

  - Nastavením volby **Enforce password history** na hodnotu dle uvážení, například **5.**

Další velmi vhodná hodnota ohledně podmínek na složitost zadaného hesla je již nastavena. Jak bylo zmíněno výše, každá politika obsahuje záložku „Explain“, která nám danou politiku popíše. Velmi důležitá je informace o výchozím nastavení, které je u každé politiky uvedeno. Říká nám, zda bude politika aktivní ve výchozím nastavení, tedy „Not Define“. V našem případě je ve výchozím nastavení zapnutá na doménových kontrolerech, ale vypnutá v případě klasického počítače, který není doménovým kontrolerem. Vzhledem k tomu, že se uživatelé v korporátním prostředí přihlašují vůči doméně, která je ověřuje, zajistí nám toto výchozí nastavení právě samotnou nutnost zadání komplexních hesel ze strany uživatele.

- **Account lockout policy**

Cesta: Computer Configuration\Policies\Windows Settings\Security Settings\Account policies\Account Lockout Policy

  - Zde se nachází tři volby, řídící chování v případě špatného zadání kombinace uživatelského jména a hesla.

Ze zkušenosti se volba “Account lockout threshold” nastavuje na 3 neplatná přihlášení, po kterých se účet zamkne na 15 minut za pomoci volby Account lockout duration. Volba je spojena s “Reset account lockout counter after”, který vynuluje čítač špatných přihlášení, volby jsou navzájem propojené.

- **Accounts: Rename administrator account**

Cesta: Computer Configuration\Policies\Windows Settings\Security Settings\Local policies\Security Options

  - Volba **Accounts: Rename administrator account** na **dle uvážení**

Z důvodu povědomí o existenci účtu lokálního administrátora na každém počítači je běžnou praxí právě jeho přejmenování, už například z důvodu, aby nebyl uživateli zbytečně uzamykán apod.

Microsoft Windows nabízí velké množství těchto nastavení a pojednává o nich ve své dokumentační databázi.[45] Je vždy na administrátorovi daného prostředí, aby zvážil, které nastavení je vhodné a které nikoliv vzhledem k aktualní situaci a potřebám společnosti. Kompletní možnosti v nastavení bezpečnosti týkajících se Security Options jsou k nalezeni na stránkách společnosti Microsoft.[46]

5.4.2 Konfigurace Windows 2012 R2

V serverové edici je obecně doporučováno společnosti Microsoft využívat vestavěný nástroj **Security Configuration Wizard**[47] umožňující kontrolu stávajího nastavení systému a vytvoření GPO politik pro bezpečnější konfiguraci systému.

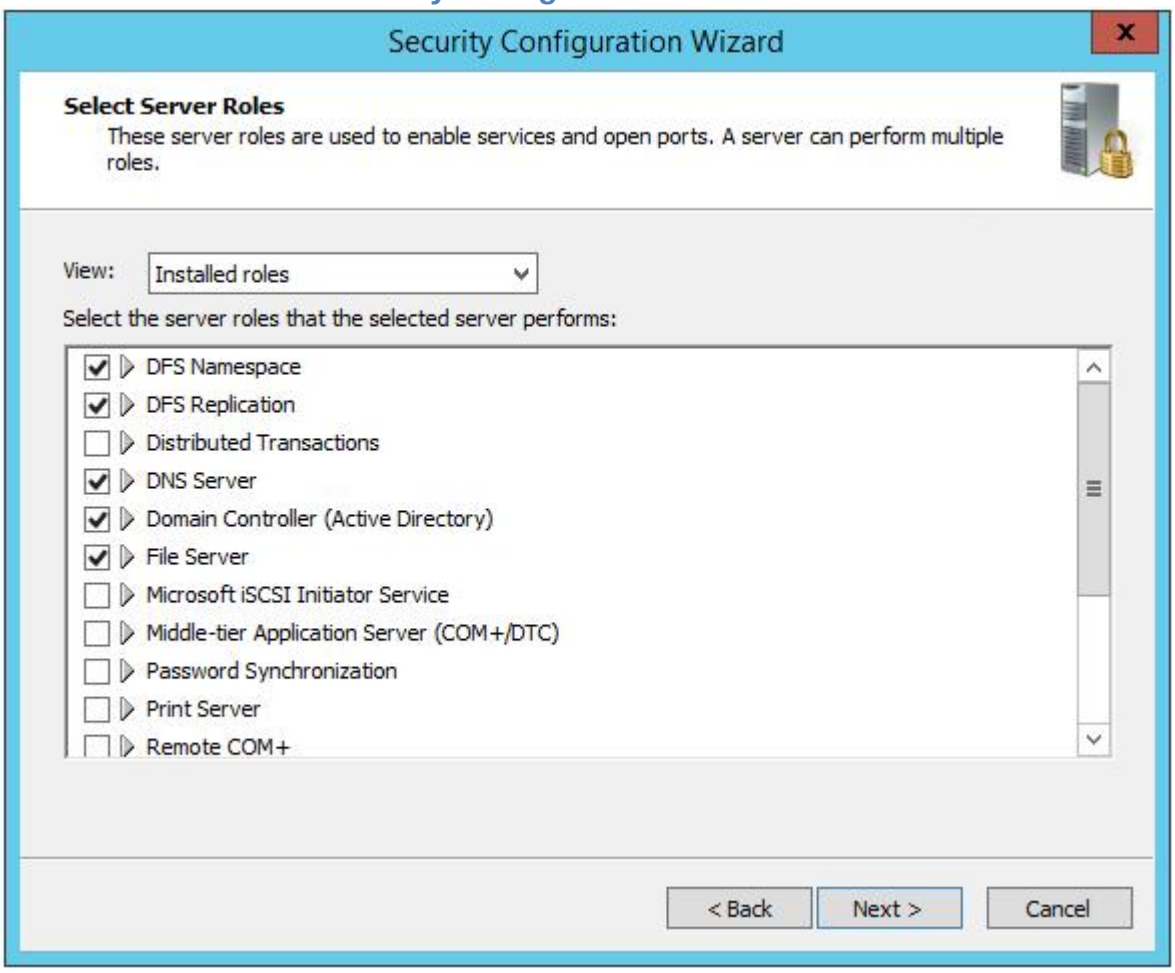
U každého serveru je zapotřebí správně porozumět jeho roli z hlediska celé síťové infrastruktury. Mezi otázky, které by měly být kladeny patří:[48]

6 Jaká je role daného serveru v infrastruktuře?
7 Kdo bude k serveru přistupovat?
8 Máme předpřipravenou šablonu pro tento typ role?
9 Jaké služby musí server nabízet?
10 Jaké protokoly služby by měly být zpřístupněny na firewallu?

Průvodce po zodpovězení všech těchto otázek dokáže administrátorovi vygenerovat nastavení, které může být nadále implementováno.

[45]Microsoft: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-policy-settings
[46] Microsoft : Security Options – [cit.2018.4.4]
Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-options
[47] Microsoft : Server Hardening: Windows Server 2012 – [cit.2018.4.4]
Dostupné z: https://technet.microsoft.com/en-us/security/jj720323.aspx
[48] Windows Server 2012 Security from End to Edge and Beyond: Architecting, Designing, Planning, and Deploying Windows Server 2012 Security Solutions, 2013, 542 s. ISBN: 9781597499804, str. 21

Obrázek 45 - Security Configuration Wizard – nastavení - role

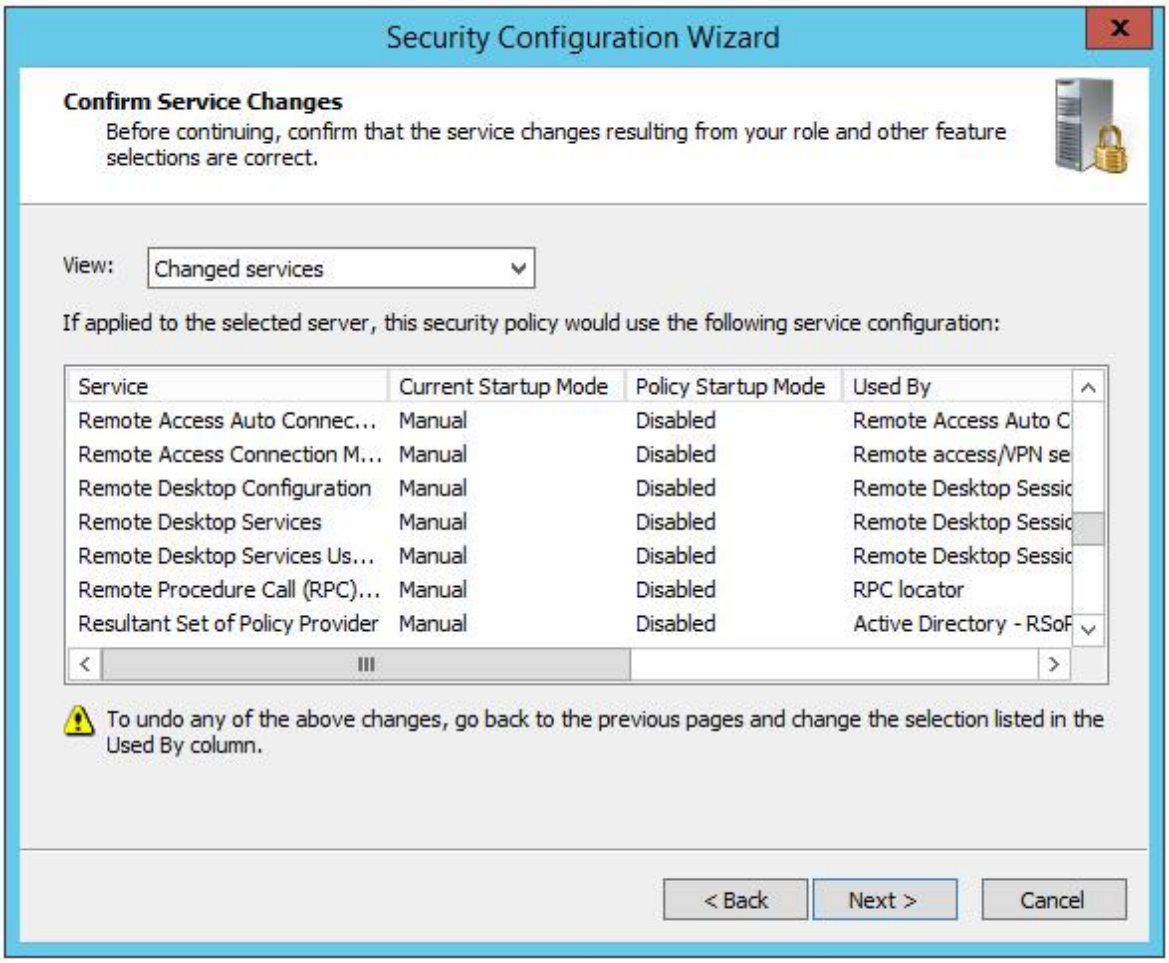


Zdroj: Vlastní zpracování

Nejdříve je zapotřebí specifikovat dané role serveru, a dále upravit start jednotlivých služeb při startu počítače. Je proto zapotřebí již v počátku rozvážně vyhodnotit celou situaci a nezakázat si například vzdálený přístup k počítači.

Další sekce obsahují nastavení brány Windows Firewall vzhledem k běžícím službám, dále pak úpravy registrů, které upravují jednotlivé protokoly, které jsou využívány v komunikaci mezi jednotlivými počítači. Bohůžel vyšší kompatibilita se staršími systémy s sebou přináší větší množství potenciálních hrozeb.

Obrázek 46 - Security Configuration Wizard – nastavení - služby



Zdroj: Vlastní zpracování

V závěru se nachází sekce auditační, která je velmi důležitá pro zajištění informací o jednotlivých akcích, probíhajících na serveru. Je velmi vhodné aktivovat nejen úspěšné pokusy o změnu či přihlášení do systému, ale právě i ty neúspěšné, které nám mohou pomoci odhalit podezřelou aktivitu.

Obrázek 47 - Security Configuration Wizard - nastavení - auditace

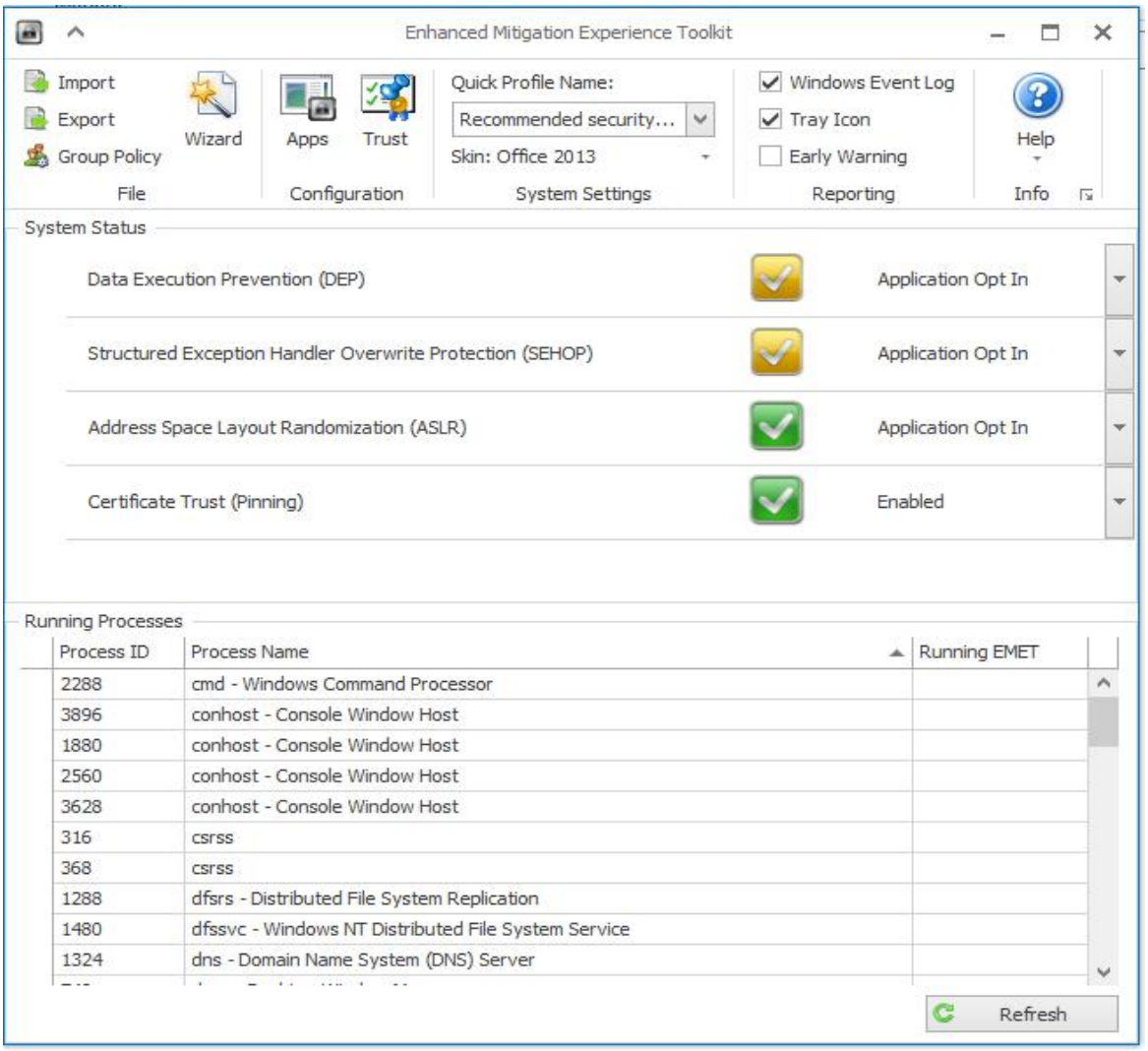
Zdroj: Vlastní zpracování

V dialogu samotném je vždy zapotřebí vyvážit množství logovaných dat a výkon samotný. Následující nastavení proto dovoluje vybrat druh událostí, které mají být zaznamenány. Příkladem jednoho z užitečných nastavení může být volba Logon Events, která zaznamenává jednotlivé pokusy o přihlášení. Je ale nadále vhodné ji omezit pouze na neúspěšné pokusy, a tím si zajistit vyšší výkonnost systému, který nebude zaznamenávat všechny události, ale zajistí nám i informace o neúspěšných přístupech. Toto nastavení nelze aplikovat v rámci samotného nástroje, ale je zapotřebí upravit politiky GPO zabývající se bezpečnostním auditováním „security auditing“.

Vygenerovaný XML soubor s nastavením lze přímo aplikovat na daný server nebo uložit pro pozdější nastavení.

Dalším velmi vhodným přístupem je nástroj **EMET** (Enhanced Mitigation Experience Toolkit), který se snaží zabránit zneužití chyb v softwaru[49]. Mimo jiné například proti chybám typu code execution – útočník využije chyby v softwaru, přetečení zasobníku, které mu umožní vložit škodlivý kód a následně ho vykonat.

Obrázek 48 - EMET - hlavní okno



Zdroj: Vlastní zpracování

[49] Microsoft: EMET – [cit. 2018.4.4]
Dostupné z: https://support.microsoft.com/cs-cz/help/2458544/the-enhanced-mitigation-experience-toolkit

Bezpečnostní auditování

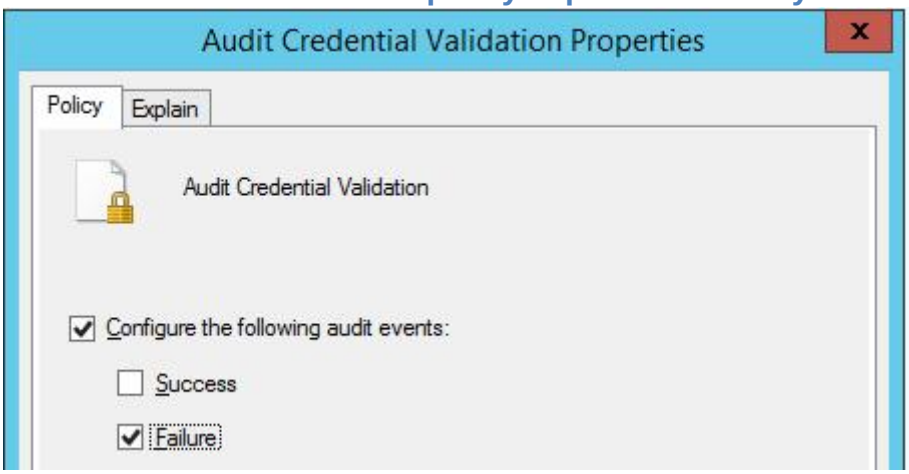
Auditováním se rozumí proces, kdy shromažďujeme informace o uskutečněných akcích a následně je analyzujeme.[50]

Pro nastavení již zmíněného auditování neúspěšných pokusů o příhlášení, je nutné nakonfigurovat politiku „Audit Credential Validation“ v kategorii „Account Logon“.

Cesta: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon

Ve výchozím nastavení u serverové edice systému se editují pouze úspěšné pokusy o přihlášení. Pokud tedy chceme auditovat neúspěšná přihlášení do systému je nutné toto nastavit v rámci politiky.

Obrázek 49 - Auditace neúspěšných přihlášení do systému



Kategorie bezpečnostních politik „Audit Policies“, je velmi rozsáhlá a je zde velká možnost konfigurace na základě jednotlivých potřeb. Jednotlivé politiky jsou detailně popsány na stránkách společnosti Microsoft.[51]

[50] *Security strategies in Windows platforms and applications*. Second edition. Sudbury, MA: Jones & Bartlett Learning, 2014. 396 str. ISBN 9781284031652. str. 58
[51] Microsoft: Security Audit Policy Settings – [cit. 4.4.2018]

Mezi další praktiky na doménových kontrolerech se může jevit například přeposílání systémových událostí na jiný server. Toto nastavení může být vhodné právě v případě, že daný server je kompromitován a útočník za sebou chce zahladit stopy. Pokud budou důležité události přeposílány na jiný server, je zde vysoká možnost, že budou odhaleny první kroky útočníka před tím, než začne dané události upravovat pro svůj prospěch.

Pro toto nastavení se využívá funkcionality „**Windows Event Forwarding – (WEF),** která zasílá tyto informace na „Windows Event Collector – WEC“ server[52], shromažďující tyto informace a může nám tak zajistit další prostředek ochrany.

Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings

[52] Microsoft: Windows Event Forwarding – [cit.2018.4.4]
Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Závěr

Každý software, případně hardware může být teoreticky napadnutelný. Dříve či později lze nalézt způsob, jak získat neoprávněným způsobem přístup k informacím nebo schopnostem daného systému. V současné době je bezpečnost samotná velmi diskutovaná, ale čím dál tím více implementována do operačních systémů. V současnosti už pomalu přicházíme o možnost vypnout například aktualizace operačního systému jako v dřívějších dobách. Ve většině případů je tato nutnost opodstatněná, a to díky rozrůstajícím se hrozbám, které mohou počítačové systémy napadnout. Tato situace nastala právě u demonstrace penetračního testovaní u serverové verze operačního systému Windows. Je nutné zmínit, že právě tato chyba byla opravena přes aktualizační kanály společnosti Microsoft.

U každého operačního systému je třeba počítat s jeho přednastavenými hodnotami a umět systém nakonfigurovat vzhledem k jeho využití. Není vhodné zanedbávat bezpečnost, byť pouze jednoho stroje v síti. Řetěz celé infrastruktury je tak silný, jako jeho nejslabší člen. Útočník by mohl využít této slabiny a postupně získávat vyšší oprávnění při využívání slabin jednotlivých strojů.

V základním nastavení je operační systém již nakonfigurován proti hrozbám, které byly objeveny v dřívějších letech a předpokládá se tak jejich možné zneužití. Současně jsou povoleny aktualizace systému, které zajišťují aktuálnost daného produktu. Práce se snažila upozornit jak na možnost zneužití operačního systému za pomoci hardwaru samotného a neprivilegovaného přístupu k němu, tak i poukázat na nutnost pravidelných aktualizací, právě z důvodu nových hrozeb, které se kontinuálně objevují. V závěru bylo poukázáno na další dodatečné nastavení systému pro zajištění vyšší bezpečnosti za pomoci konfigurace politik GPO.

Celkově si myslím, že ačkoliv statistiky hovoří o vzrůstajícím trendu nových hrozeb na operační systémy, lze současně pozorovat i vzestupný trend bezpečnosti samotné, kdy jsou vyvíjeny nové aplikace na podporu bezpečnosti

operačních systému a na společnosti samotné je kladen stále vyšší tlak v oblasti zabezpečení.

Seznam použitých zdrojů

1. **SMITH, Ben. a Brian KOMAR**. Zabezpečení systému a sítě Microsoft Windows. Přeložil David KRÁSENSKÝ, přeložil Anna RYCHETSKÁ. 2006. ISBN 80-251-1260-8.
2. **CVE DETAILS**: Vulnerability statistics [online].2016 [cit.2016.26.12] Dostupné z: http://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26.
3. **CVE DETAILS**: Vulnerability statistics [online].2016 [cit.2016.26.12] Dostupné z:http://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26.
4. **Microsoft**: Windows 10 Compare Table document - [cit.2017.5.1] Dostupné z:http://wincom.blob.core.windows.net/documents/ Win10CompareTable_FY17.pdf
5. **Microsoft**: Windows Server 2012 R2 Products and Editions Comparison[cit.2017.5.1] Dostupné z: https://blogs.msdn.microsoft.com/robmar/2014/02/10/windows-server-2012-r2-products-and-editions-comparison/
6. **NEMETH, Evi, Garth SNYDER a Trent R. HEIN.** Linux: kompletní příručka administrátora: 2. aktulizované vydání. Brno: Computer Press, 2008. Administrace (Computer Press). ISBN 978-80-251-2410-9.
7. **Dráb, Martin**: Jádro systému Windows,2011,472 s. ISBN: 978-80-251-2731-5.
8. **William, R.Stanek**: Mistrovství v Microsoft Windows Server 2008 – Kompletní informační zdroj pro profesionály,2009,1364 s. ISBN: 978-80-251-2158-0.
9. **Samuraj-cz**: Kerberos část 1 - Active Directory komponenty – [cit.2017.5.1] Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-1-active-directory-komponenty/
10. **Samuraj-cz**: Kerberos část 3 – Single Sing-On a protokol Kerberos – [cit.2017.5.1] Dostupné z http://www.samuraj-cz.com/clanek/kerberos-cast-3-single-sign-on-a-protokol-kerberos/
11. **Microsoft**: Basic Concepts for the Kerberos Protocol – [cit.2017.11.27] Dostupné z: https://technet.microsoft.com/en-us/library/cc961976.aspx

12. **Samuraj-cz**: Kerberos část 3 – Single Sing-On a protokol Kerberos – [cit.2017.5.1]
Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-cast-3-single-sign-on-a-protokol-kerberos/

13. **Samuraj-cz**: Kerberos část 4 – Hlavní termíny Kerberos protokolu – [cit.2017.5.1]
Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-cast-4-hlavni-terminy-kerberos-protokolu/

14. **Wikipedia**: Kerberos Version 5
Dostupné z:
https://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service

15. **Samuraj-cz**: Kerberos část 4 – Hlavní termíny Kerberos protokolu – [cit.2017.5.1]
Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-cast-4-hlavni-terminy-kerberos-protokolu/

16. **Samuraj-cz**: Kerberos část 5 – Princip Kerberos Autentizace – [cit.2017.5.1] Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-cast-5-princip-kerberos-autentizace/

17. **PUŽMANOVÁ, Rita.** Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1278-0.

18. **Earchiv.cz**: TCP/IP – Úvod – [cit.2017.5.1]
Dostupné z http://www.earchiv.cz/l225/slide.php3?l=3&me=2

19. **Wikipedia**: IPv4 – [cit.2018.3.1]
Dostupné z: https://en.wikipedia.org/wiki/IPv4

20. **IETF** – RFC790 specifikace – [cit. 2018.3.1]
Dostupné z: https://tools.ietf.org/html/rfc790

21. **Wikipedia** – IANA – [cit. 2018.3.1]
Dostupné z:
https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

22. **SANDERS, Chris.** Analýza sítí a řešení problémů v programu Wireshark. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

23. **IETF**: RFC1918 specifikace – [cit. 2018.3.1]
Dostupné z: https://tools.ietf.org/html/rfc1918

24. **WILSON, Ed.** PowerShell: [průvodce skriptováním: pro verzi 3.0. a vyšší]. Brno: Computer Press, 2015. ISBN 978-80-251-4386-5.

25. **SOBELL, Mark G.** Linux: praktický průvodce. Praha: Computer Press, 1999. Operační systémy. ISBN 80-7226-190-8.
26. **Kali Linux**: Downloads [2018.4.1]
Dostupné z: https://www.kali.org/downloads/
27. **Hirensboot**: Download [2018.4.1]
Dostupné z: http://www.hirensbootcd.org/
28. **Chntpw**: Extrakce databáze SAM – Download [2018.4.1]
Dostupné z: http://www.chntpw.com/download/
29. **4Sysops.com**: Reset hesla Windows 10 – [cit. 2018.4.1]
Dostupné z: https://4sysops.com/archives/reset-a-windows-10-password/
30. **Ophracrack**: Distribuce Live CD – [2018.4.1]
Dostupné z: http://ophcrack.sourceforge.net/
31. **Microsoft Docs**: UAC – [cit. 2018.4.1]
Dostupné z: https://en.wikipedia.org/wiki/Rainbow_table
32. **NMAP**: Port Scanning Techniques – [cit.2018.4.1]
Dostupné z: https://nmap.org/book/man-port-scanning-techniques.html
33. **Nmap**: Version Detection – [cit.2018.4.2]
Dostupné z: https://nmap.org/book/man-version-detection.html
34. **LinuxHint**: Nmap Auditory – [cit.2018.4.2]
Dostupné z: https://linuxhint.com/nmap-port-scanning-security/
35. **Nessus**: Software Download – [cit.2018.4.2]
Dostupné z: https://www.tenable.com/downloads/nessus
36. **Superuser**: How to install Linux Sybsystem for Windows – [cit.2018.04.02]
Dostupné z: https://superuser.com/questions/1217167/cant-find-windows-subsystem-for-linux-feature-to-install-bash-for-windows
37. **LinuxHint**: Nmap port scanning security – [cit.2018.4.2]
Dostupné z: https://linuxhint.com/nmap-port-scanning-security/
38. **Microsoft**: Security Bulletin MS17-010 – [cit.2018.4.2]
Dostupné z: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
39. **Paul-sec**: WannaCry – [cit.2018.4.2]
Dostupné z: http://www.paul-sec.com/wannycry-wannadecrypt0r-ms17-010.html
40. **BURNS, Bryan:** Security power tools. Sebastopol, CA: O'Reilly, c2007. ISBN 978-0596009632

41. **Offensive-Security**: Meterpreter basics – [cit.2018.4.2] Dostupné z: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

42. **CVE Details**: Windows 2012 Vulnerabilitiy overview – [cit. 2018.4.4] Dostupné z : https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

43. **CHIP:** Secure Boot - [cit.2018.4.4] Dostupné z: https://www.chip.cz/casopis-chip/earchiv/vydani/rocnik-2013/chip-08-2013/uefi-secure-boot-prilis-bezpecny-start-pc/

44. **Microsoft**: MS17-011 Security Update – [cit.2018.4.4] Dostupné z: https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

45. **Microsoft**: Security policy settings – [cit.2018.4.4] Dostupné z:https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-policy-settings

46. **Microsoft**: How to detect, enable and disable SMBv1, SMBv2, SMBv3 in Windows and Windows Server – [cit.2018.4.4] Dostupné z: https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

47. **Microsoft**: Security Options – [cit.2018.4.4] Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-options

48. **Thomas W Shinder Yuri Diogenes**: Windows Server 2012 Security from End to Edge and Beyond: Architecting, Designing, Planning, and Deploying Windows Server 2012 Security Solutions, 2013, 542 s. ISBN: 9781597499804

49. **SOLOMON, Michael**: *Security strategies in Windows platforms and applications*. Second edition. Sudbury, MA: Jones & Bartlett Learning, 2014. ISBN 9781284031652.

50. **Microsoft**: Server Hardening: Windows Server 2012 – [cit.2018.4.4] Dostupné z: https://technet.microsoft.com/en-us/security/jj720323.aspx

51. **Microsoft:** Security Audit Policy Settings – [cit. 4.4.2018] Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings

52. **Microsoft**: EMET – [cit. 2018.4.4]
Dostupné z: https://support.microsoft.com/cs-cz/help/2458544/the-enhanced-mitigation-experience-toolkit

53. **Microsoft**: Windows Event Forwarding – [cit.2018.4.4]
Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam použitých zkratek a vysvětlení pojmů

AD DS – Active Directory Domain Services

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

GPO – Group Policy Objects

LDAP – Lightweight Directory Access Protocol

IDS/IPS – Intrusion Detection systém

Commandlet – příkaz využívaný v prostředí Windows Powershell

BIOS – Basic Input-Ouput system, firmware osobního PC

UEFI – novější verze BIOS

SAM – Security Account Manager

GUI – Graphic User Interface

Rootkit – sada softwaru maskující přítomnost škodlivého kódu

Hyper-V – Microsoft hypervizor – Zajištuje virtualizaci

VirtualBox – Software třetí strany zajišťující virtualizaci

Hirens BOOT – sada nástrojů pro opravu a diagnostiku PC

Ransomware – škodlivý software, zašifruje data a vydírá uživatele

VNC – vzdálený přístup k počítači