UNIVERZITA PARDUBICE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2020/2021 Michal Ředina

Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Využití penetračního testování pro zvýšení bezpečnosti počítačových zařízení

Bakalářská práce

2021

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Michal Ředina**
Osobní číslo:	**I17134**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Téma práce:	**Využití penetračního testování pro zvýšení bezpečnosti počítačových zařízení**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Cílem této práce je návrh metodiky a opatření pro zvýšení bezpečnosti z hlediska standardního používání PC s operačním systémem Windows nebo Linux.

Teoretická část bude zaměřena na oblast, která se zabývá nástroji sloužícími pro penetrační testování, zejména OS Kali linux a Parrot Linux.

V praktické části autor provede reálné penetrační testy s cílem prověřit a zhodnotit úroveň zabezpečení. Pro penetrační testy budou použity nástroje OS Kali Linux nebo Parrot Linux. Výstupem bude vytvoření metodiky a sady opatření za účelem zvýšení bezpečnosti vybraných systémů.

Rozsah pracovní zprávy: **30**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná**

Seznam doporučené literatury:

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

HERTZOG, Raphael, Jim O'GORMAN a Mati AHARONI. Kali Linux Revealed: Mastering the Penetration Testing Distribution. Cornelius NC: Offsec Press, 2017. ISBN 9780997615609.

Georgia, WEIDMAN. Penetration Testing. Publishing house: No Starch Press, US. Release Date: June 14 2014, 495 pages. ISBN: 1593275641.

David KENNEDY, Jim O'GORMAN, Devon KEARNS, Mati AHORONI. Publishing house: No Starch Press, US. Metasploit. Release date: July 15 2011. 328 pages. ISBN: 159327288X.

Vedoucí bakalářské práce: **Ing. Miloslav Macháček, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **15. listopadu 2019**
Termín odevzdání bakalářské práce: **7. května 2020**

Univerzita Pardubice Česká republika
L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Ing. Lukáš Čegan, Ph.D.
pověřený vedením katedry

V Pardubicích dne 17. prosince 2019

Prohlašuji:

Prohlašuji, že tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne: 13. 8. 2021 .....

Ředina Michal

PODĚKOVÁNÍ

Tímto bych velmi rád poděkoval Ing. Miloslavu Macháčkovi, Ph.D., za jeho odbornou pomoc, všechny rady a připomínky při zpracování bakalářské práce a stejně tak i za výborné vedení a dohlížení na tvorbu práce.

ANOTACE

Bakalářská práce se zaměřuje na návrh metodiky a opatření pro zvýšení bezpečnosti z hlediska standardního používání počítače s operačním systémem Windows nebo Linux. V hlavní části budou představeny nástroje sloužící pro penetrační testování zejména v operačních systémech Kali Linux a Parrot Linux a typy útoků prováděné těmito nástroji. Součástí práce budou provedené co nejreálnější penetrační testy s cílem prověřit a zhodnotit úroveň zabezpečení. Výstupem práce bude vytvoření metodiky a sady opatření za účelem zvýšení bezpečnosti vybraných systémů.

KLÍČOVÁ SLOVA

Penetrační testování, bezpečnost, Linux,

TITLE

Use of penetration testing to increase the security of computer devices

ANNOTATION

The bachelor's thesis focuses on the design of methodology and measures to increase security in terms of standard use of computers running Windows or Linux. The main part will introduce the tools used for penetration testing, especially in the operating systems Kali Linux and Parrot Linux and the types of attacks performing the tools. The work will include the most realistic penetration tests tested in order to perform and evaluate the level of security. The output of the work will be the creation of a methodology and a set of measures to increase the security of selected systems.

KEYWORDS

Penetration testing, security, Linux,

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

ARM	Advanced RISC Machine
ARP	Address Resolution Protocol
BIOS	Basic Input/Output System
CD	Compact disc
DDOS	Distributed denial of service
DOS	Denial of service
GNU	GNU is not Unix
ICMP	Internet Control Message Protocol
IP	Ingress Protection
ISO	International Organization for Standardization
MAC	Media Access Control
MINIX	Svobodný otevřený operační systém
MSF	Metasploit Framework
PC	Personal computer
RAM	Random Access Memory
SAM	Security Account Manager
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WPA-PSK	Wi-Fi Protected Access
XML	Extensible Markup Language

Úvod

Informatika je od samého začátku velmi rychle se rozvíjející obor, z čehož vyplývá, že ne vždy bylo důsledně dbáno i na bezpečností hrozby s ním spojené. S růstem používání informačních technologií docházelo ke stále většímu růstu útoků.

Škody, které může útočník způsobit, mohou vést ke katastrofálním následkům, které lze přirovnat k živelním katastrofám. Aktuální požadavky na zvyšování bezpečnosti a vyšší nároky na zabezpečenou infrastrukturu mě vedly k napsání této bakalářské práce.

Penetrační testy jsou vhodným způsobem, jak předcházet incidentům, které by mohly mít negativní následky. Jejich hlavním úkolem je zvýšit zabezpečení systémů nebo eliminovat případné hrozby.

Bakalářská práce je zaměřena na metodiky a opatření pro zvýšení bezpečnosti z hlediska standardního používání počítače s operačním systémem Windows. V rámci teoretické části budou představeny nástroje, které je možné využívat pro penetrační testování.

1 LINUX A LINUXOVÉ DISTRIBUCE

První kapitola je zaměřena na Linux a linuxové distribuce. Distribuce Linuxu představuje operační systém, který je založený na linuxovém jádře. Tento operační systém má otevřený zdrojový kód, který můžeme libovolně používat, sdílet, kopírovat a také upravovat podle svých vlastních potřeb. Rozdíl oproti ostatním operačním systémům, které nejsou svobodné, je nutnost striktně dodržovat veškeré licenční podmínky. [26]

Historie Linuxu se datuje od roku 1983, kdy Richard Matthew Stallman začal vytvářet nový operační systém, který by využíval svobodný a otevřený software. Výsledkem projektu byl operační systém GNU. Následně roku 1990 probíhal vývoj jádra Hurd, který měl zajistit chod operačního systému GNU a zároveň také jeho komunikaci s hardwarem. [26]

1. 1 HISTORIE

V roce 1991 začal Linus Torvalds na univerzitě ve finských Helsinkách tvořit vlastní jádro. Vývoj byl podstatně rychlejší v porovnání s vývojem jádra Hurd a výsledkem celého projektu bylo sloučení jádra Linuxu a operačního systému GNU. Linus Torvalds se inspiroval komerčním projektem MINIX, jehož autorem byl Andrew Tanenbaum. Projekt se stával stále populárnějším a začal získávat větší pozornost okolí. Současné logo Linuxu představuje tučňák Tux, které bylo vytvořeno v roce 1996 na základě obrázku od autora Lettry Ewinga. [26]

1. 2 LINUXOVÉ DISTRIBUCE

Linuxovou distribucí se označuje spojení linuxového jádra, dalších programů a nástrojů. Tím vznikne komplexní operační systém. Díky možnosti volného šíření najdeme v současnosti více než 450 distribucí, které se od sebe mohou lišit balíčkovacím systémem určeným k instalaci programů nebo například náročností požadavků na hardware, proto je možné i na méně výkonném hardwaru nebo speciálním zařízení spustit linuxovou distribuci. [11]

Linuxové distribuce, které jsou vhodné pro penetrační testování, jsou Kali Linux, Parrot OS a také další alternativní distribuce. Tyto distribuce patří k nejpoužívanějším a nejvhodnějším, neboť už mají v sobě řadu přeinstalovaných aplikací a nástrojů. [11]

1. 2. 1 KALI LINUX

Jednou ze specializovaných distribucí Linuxu je Kali Linux, který je vyvíjen společností Offensive Security už od roku 2013. Aktuální verze je 2020.4. Kali Linux je projekt s otevřeným zdrojovým kódem. Tato linuxová distribuce je založena na projektu Debian a je zaměřena zejména na penetrační testování. [31][10]

Jednou z hlavních výhod je podrobná a přehledná dokumentace a také možnost volného šíření a bezplatného užití. Kali Linux nabízí možnost instalace sytému na vývojových jednodeskových počítačích jako například Raspberry Pi. [31]

1. 2. 2 PARROT OS

Projekt byl zahájen v roce 2013. Aktuální verze je 4.10. Parrot OS je založen na projektu Debian. Je navržen tak, aby jeho silnou stránkou bylo bezpečné soukromé používání. Aplikace a nástroje, které tento operační systém zahrnuje, se zabývají kybernetickou bezpečností, forenzní analýzou, reverzním inženýrstvím, a nástroje určené k běžnému užití a vývoji softwaru.

Parrot OS disponuje lehkým grafickým prostředním, které umožňuje rychlou a plynulou práci i na starším zařízení. Výhodou je, že je možnost vybrat si mezi dvěma verzemi, kdy jedna je zaměřena na bezpečnost a penetrační testování. Druhá verze těmito nástroji nedisponuje, a proto je určena na běžné domácí použití, ale je možné nástroje dodatečně instalovat.

1. 2. 3 ALTERNATIVNÍ DISTRIBUCE

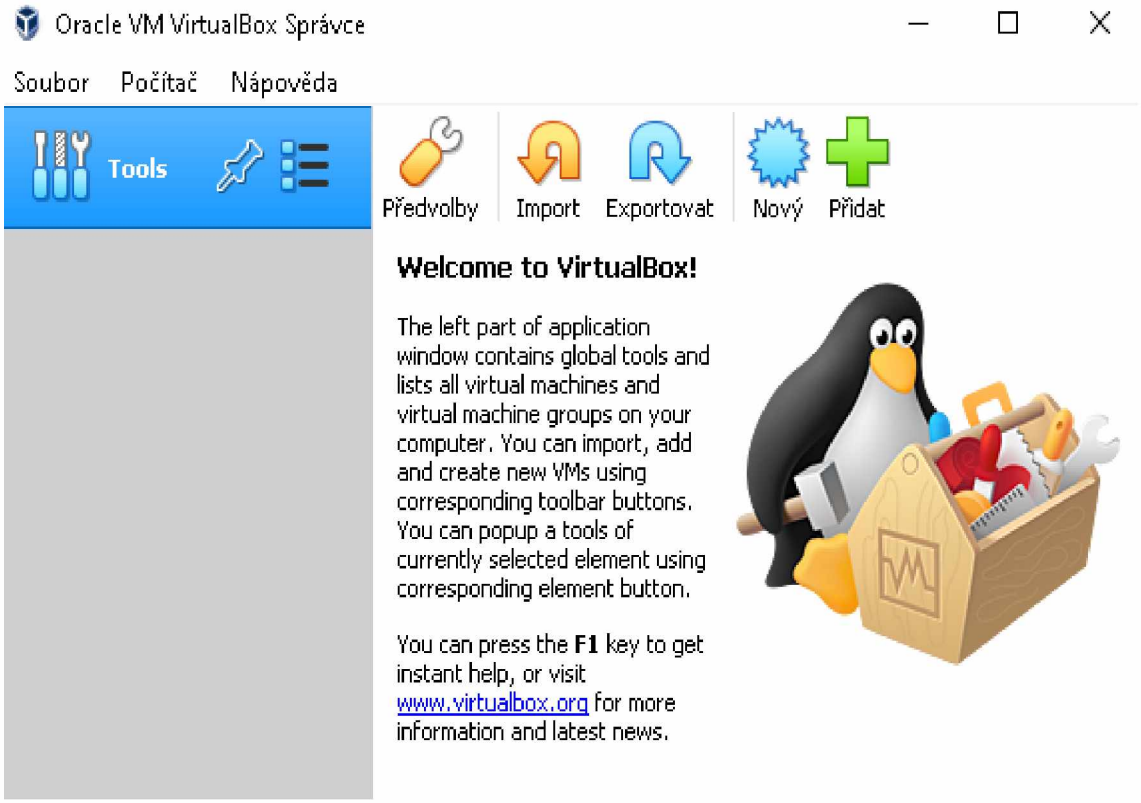
Tyto distribuce nejsou tak obvyklé, ale jsou určené také k penetračnímu testování.

Mezi alternativní distribuce patří:

- BlackBox;
- BlackArch;
- Bugtraq;
- Pentoo Linux;
- Fedora Security Lab.

1. 3 PŘÍPRAVA A INSTALACE LINUXOVÝCH DISTRIBUCÍ

Nejprve bylo nutné stáhnout software VirtualBox, který je dostupný pro operační systémy typu Windows, Linux, MacOS X a Solaris. U operačního systému Windows bylo nutné potvrdit dialogová okna, protože je nutné instalovat dodatečné periferie, které slouží pro síťové rozhraní, tisk a další funkce, které mohou usnadnit práci. Po úspěšné instalaci byl software spuštěn (Obrázek 1: VirtualBox).



Obrázek 1: VirtualBox

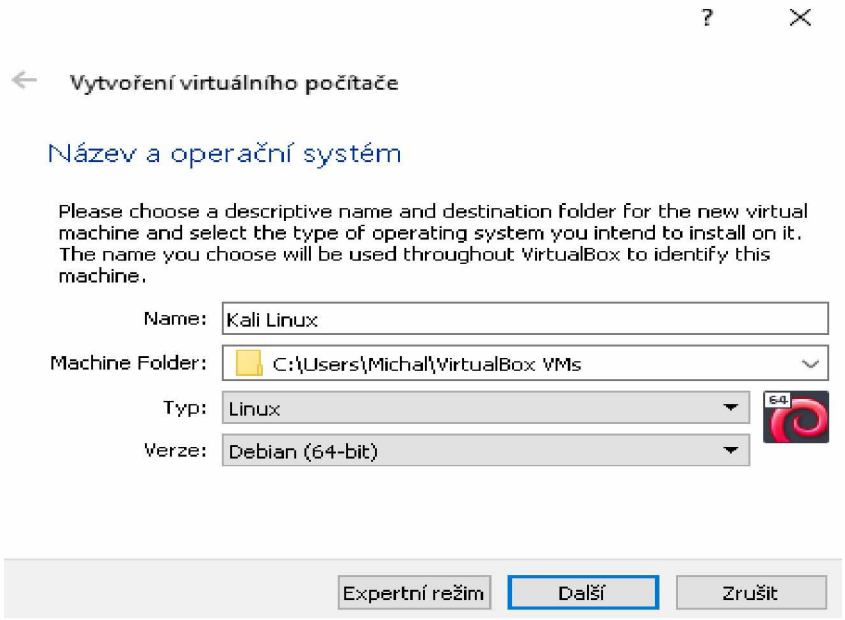
Zdroj: Vlastní zpracování

Kali Linux i Parrot OS je možné stáhnout jako ISO soubor. Po stažení je vhodné zkontrolovat kontrolní součet pomocí sha1, zda nebylo se souborem manipulováno. Dále je možné stáhnout už připravený virtuální stroj, který lze importovat do virtualizačního softwaru.

Jinou možností je využít obraz určený pro ARM zařízení, například na Raspberry Pi. Pro instalaci Kali Linux bude využit ISO souboru pro ukázku. Při instalaci Parrot OS bude použit připravený virtuální stroj.

1. 3. 1 INSTALACE VIRTUÁLNÍHO STROJE KALI LINUX

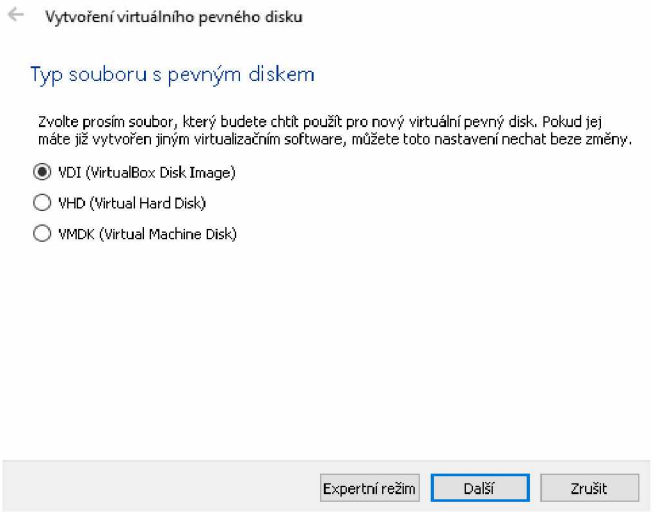
Pro vytvoření virtuálního počítače je zapotřebí zadat jeho jméno, typ a verzi (viz Obrázek 2: Název a zvolení operačního systému).



Obrázek 2: Název a zvolení operačního systému

Zdroj: Vlastní zpracování

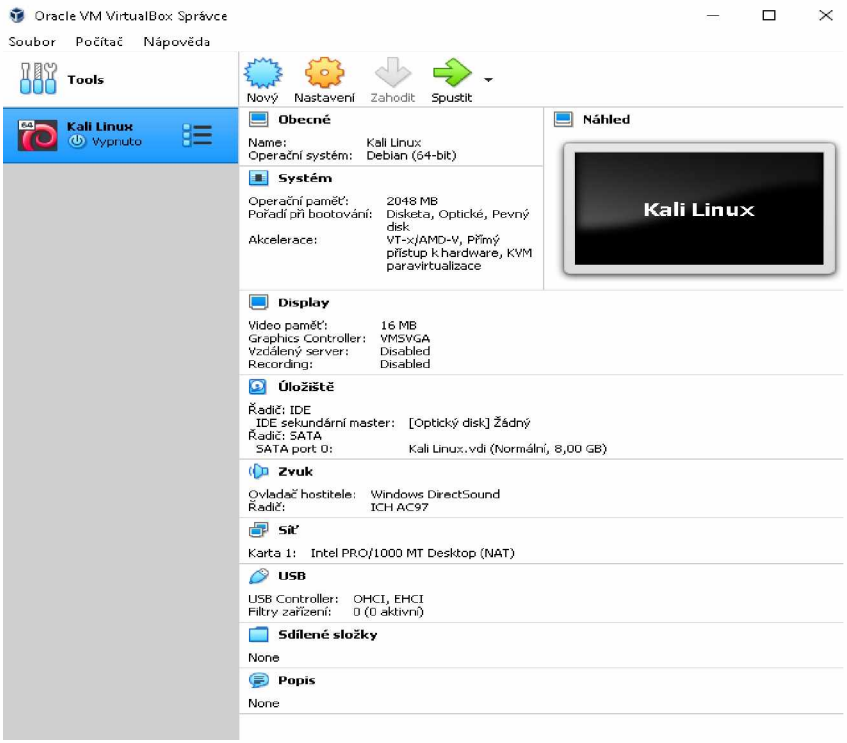
Po vyplnění názvu je přidána nejvyšší hodnota RAM paměti, kterou si může virtuální stroj alokovat. Následuje dialogové okno pro vytvoření virtuálního disku, jenž bude sloužit k instalaci systému. Z různých typů disku byl zvolen výchozí (viz Obrázek 3: Typ souboru s pevným diskem).



Obrázek 3: Typ souboru s pevným diskem

Zdroj: Vlastní zpracování

Bylo zvoleno pevné úložiště pro zajištění rychlejší odezvy systému, neboť dynamický typ postupně alokuje disk až do maximální hodnoty. Posledním krokem k vytvoření šablony je volba umístění diskového souboru a tím je úspěšně vytvořen virtuální stroj (viz Obrázek 4: Virtuální stroj Kali Linux).

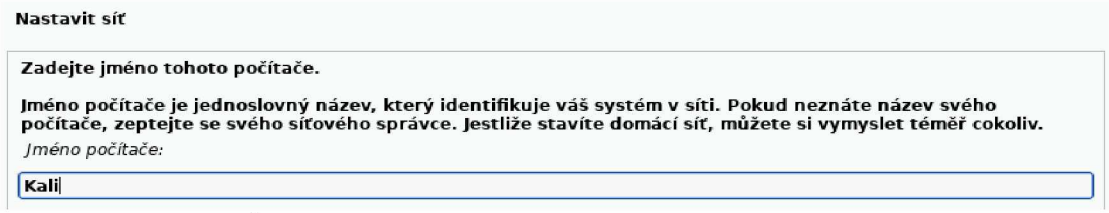


Obrázek 4: Virtuální stroj Kali Linux

Zdroj: Vlastní zpracování

Při spuštění šablony Kali Linux se zobrazí nabídka pro vložení ISO disku, kde je nutné zadat správnou cestu k danému souboru. Po úspěšném zavedení systému se zobrazí průvodce instalace. V prvním kroku se nastaví jazyk (čeština), umístění (Česká republika) a rozložení klávesnice.

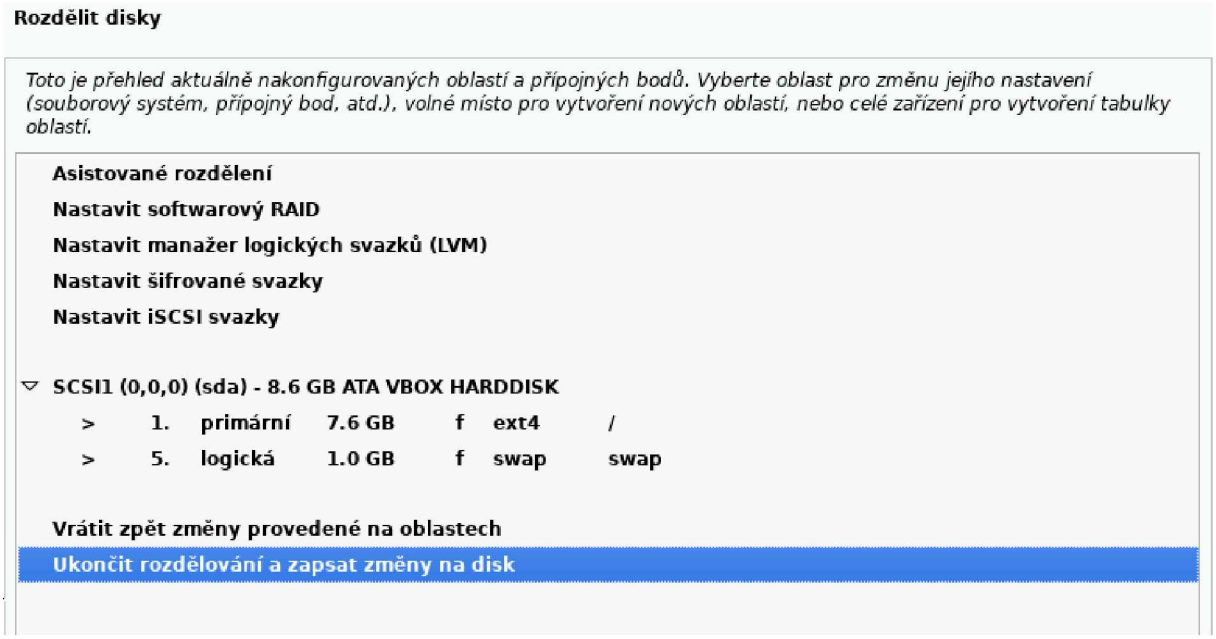
Pro identifikaci počítače v síti je nutné ho pojmenovat *(viz* Obrázek 5: Jméno v síti*)*. Následuje vyplnění domény, která zůstane prázdná, protože k účelu bakalářské práce není potřeba přidat počítač k doméně.



Obrázek 5: Jméno v síti

Zdroj: Vlastní zpracování

Vyplníme jméno uživatele, účtu a heslo, které slouží k přihlašování do systému. V závěru se volí jednotka, na niž se systém instaluje. Pro zjednodušení bude použito asistované rozdělení. Zvolíme disk a nastavení, že všechny soubory budou v jedné oblasti. Ukončíme rozdělení disku a potvrdí se všechny potřebné změny *(viz* Obrázek 6: Rozdělení disku*)*.

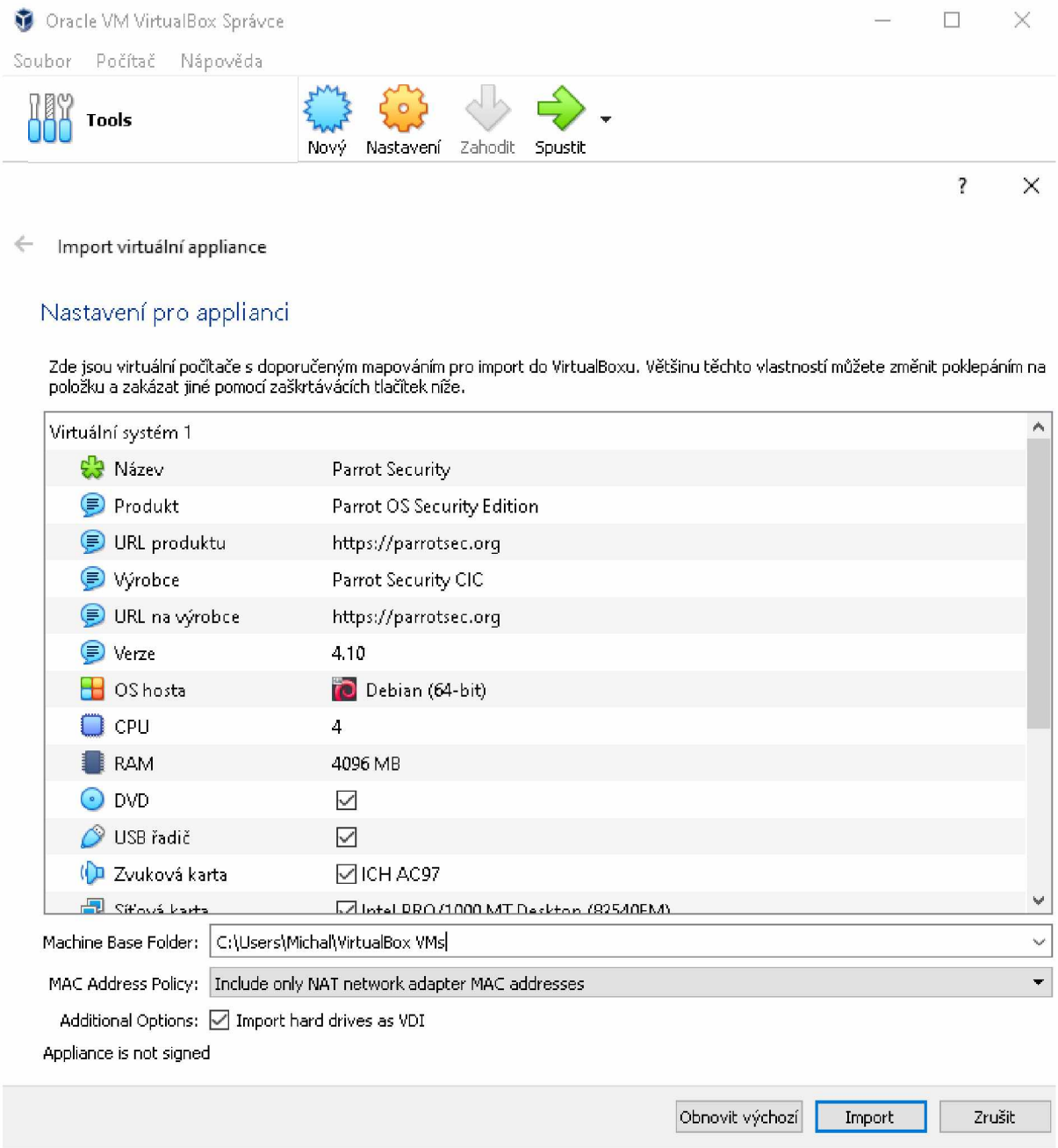


Obrázek 6: Rozdělení disku

Zdroj: Vlastní zpracování

1. 3. 2 INSTALACE VIRTUÁLNÍHO STROJE PARROT OS

Pro instalaci Parrot OS do VirtualBoxu byl použit předpřipravený soubor s celým operačním systémem. Tento soubor je připraven přímo od výrobce k importování do virtualizačního nástroje (viz Obrázek 7: Importování Parrot OS).

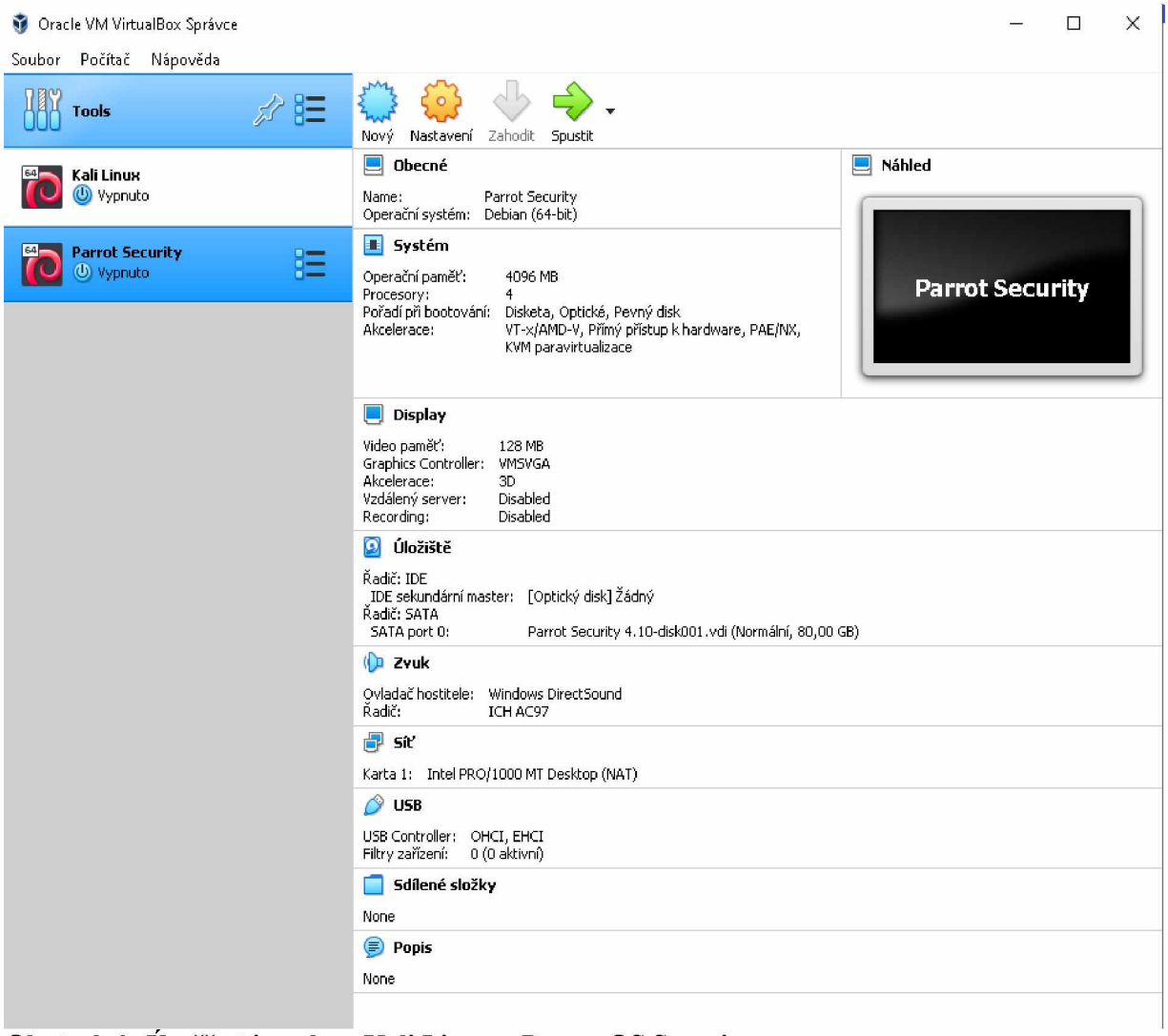


Obrázek 7: Importování Parrot OS

Zdroj: Vlastní zpracování

Po úspěšném importu je možné virtuální stroj spustit. Tímto krokem se vyhneme ruční instalaci, jako to bylo v případě instalace Kali Linux (viz Obrázek 4: Virtuální stroj Kali Linux).

V porovnání s první variantou instalace je import předem vytvořeného obrazu od výrobce rychlejší a méně náročný. Obrázek znázorňuje oba operační systémy úspěšně nainstalované (viz Obrázek 8: Úspěšná instalace Kali Linux a Parrot OS Security).



Obrázek 8: Úspěšná instalace Kali Linux a Parrot OS Security

Zdroj: Vlastní zpracování

1. 4 DÍLČÍ SHRNUTÍ

Pro zpracování bakalářské práce jsem se zaměřil na operační systém Linux, protože s tímto prostředím mám osobní zkušenost, tím pádem i představu o principu jeho fungování. Linuxové distribuce dokážou být úzce specializované. Díky tomu si dokážeme pro každou naši potřebu najít vhodně zvolenou distribuci. Proto je Linux nejpoužívanější v serverovém provedení, kde představuje důležitou součást internetu.

Pro penetrační testování jsou linuxové distribuce Parrot OS a Kali Linux nejlepší volbou, protože mají v sobě skryté nástroje, které se nemusí v ostatních operačních systémech vyskytovat, anebo se musí složitě instalovat.

Pro testování je vhodné použít virtualizaci, díky níž nemusí zasahovat do skutečného systému a tím nemusíme mít strach o ztrátu dat a systém.

2 PENETRAČNÍ TESTOVÁNÍ

Jedním z mnoha důvodů, proč využívat možnosti penetračního testování, je například zvýšení bezpečnosti. Penetrační testování nám pomáhá nalézt slabiny a eliminovat hrozby, které nejsou na první pohled vidět. Může se jednat například o zastaralé služby, chyby v nastavení nebo chyby uživatelů.

Bakalářská práce je zaměřena na penetrační testování v oblasti zvýšení bezpečnosti počítačových zařízení. Každý uživatel se může setkat s penetračním testem vědomě, nebo nevědomě. Mezi časté útoky patří podvržené e-mailové zprávy, webové služby a různé způsoby malwaru, které sbírají o uživatelích citlivé informace, nebo znepříjemňují jejich práci.

Cílem této práce je navrhnout metodiky a opatření pro zvýšení bezpečnosti z hlediska standardního používání PC s operačním systémem Windows nebo Linux.

2. 1 KDO JE ÚTOČNÍK

V případě, že je na útočníka pohlíženo jako na počítačového záškodníka, je označován pod pojmem hacker. Velmi důležité je odlišovat útočníky, kteří mají dobrý úmysl, od útočníků se zlým úmyslem. V případě, že má útočník dobré úmysly, je označován jako White Hat. V případě, že má zlé úmysly, je označován jako Black Hat. Existuje i kombinace mezi Black Hat a White Hat – takzvaný Grey Hat neboli šedý klobouk. [32] [30]

Black Hat

Black Hat je označení typické pro „zlého útočníka“, který chce úmyslně poškodit počítačový systém. Záškodník se snaží s využitím různých druhů útoků nalézt nedostatky v zabezpečení počítačového systému. Pokud je Black Hat nalezen, pokouší se dané trhliny zneužít. Jeho cílem je zneužití slabin ve svůj vlastní prospěch. [4]

White Hat

White Hat je označení typické pro „dobrého útočníka“. Tato osoba se zaměřuje v rámci testování na zabezpečení určitého systému. Hlavním cílem dobrého útočníka je nalézt slabá místa v zabezpečení určitého systému a tím i poskytnout zpětnou vazbu testovanému subjektu, aby bylo možné nedostatky napravit. Od Black Hat se liší především tím, že nevyužívá zjištěné slabiny ve svůj vlastní prospěch, je tedy jeho protikladem. [4]

Grey Hat

Grey hat je kombinací Black Hat a White Hat. Cracker si může prohlížet internetové stránky a tím proniknout do určitého počítačového systému, aby poskytl informace administrátorovi o tom, že jeho systém byl napaden. Nastává i situace, kdy může za určitý peněžní poplatek nabídnout opravu chyb, které by mohl pro daný útok využít. [13]

2. 2 TYPY PENETRAČNÍCH TESTŮ

Jednotlivé typy penetračních testů se liší v závislosti na tom, z jakého místa je útok veden, nebo jestli se jedná o interní nebo externí test, a také podle toho, jaké informace má útočník k dispozici. Proto se testy dělí podle pozice útočníka, podle míry znalosti systému nebo aplikace. [20]

Podle pozice útočníka [20]:

- **Externí test**

Jedná se o typ testu, jenž je prováděn především z vnější sítě, tedy z internetu. To znamená, že útočníkem může být kdokoli, kdo má přístup k internetu.

- **Interní test**

Simuluje útok z vnitřní sítě. Je velmi důležité si uvědomit, že do vnitřní sítě se může útočník dostat prolomením ochrany například firewall nebo sociálním inženýrstvím.

Podle míry znalosti systému nebo aplikace [20]:

- **Black box**

Na počátku útočník nemá žádné informace o aplikaci, systému nebo infrastruktuře, proto se první fáze útočníka zabývá sběrem veškerých informací o cílovém subjektu. Údaje, které může útočník před sběrem informací znát, jsou informace z veřejných zdrojů, např. domény, veřejná IP adresa nebo údaje zjištěné pomocí internetových vyhledávačů.

- **White box**

Útočník má veškerou znalost o fungování systému, aplikaci a infrastruktuře. Jedná se o bezpečnostní analytiky, kteří pracují pro danou společnost.

- **Grey box**

Představuje kombinaci Black box a White box. Tester částečně zná systémy a potřebnou dokumentaci. Například se může jednat o bývalého zaměstnance firmy, který byl seznámen s infrastrukturou, nebo o současného zaměstnance nebo testera, který má snadný přístup k části dokumentace infrastruktury.

2. 3 PRŮBĚH TESTU

Jednotlivými průběhy testů se zabývají různé metodiky. Existují i popisy průběhu testů, které je možné použít bez metodiky.

Naplánování testu

V rámci první fáze je zapotřebí dořešit určité organizační záležitosti. V rámci této části jsou vytyčeny a vyobrazeny hlavní cíle testování. Existuje možnost, že tester bude mít k dispozici zdrojové kódy aplikace. [25]

Za předpokladu automatizovaných testů je nutné vybrat nástroje, které poté budou použity. Značný význam má efektivita nástroje, na niž je kladen velký důraz, protože čím je nástroj efektivnější, tím větší je pravděpodobnost, že pokryje potenciální hrozby. [25]

Sběr informací

Součástí této fáze je potřebné získání dostatečného množství materiálu o objektu, který bude testovaný. Množství informací se liší podle typu testu. Jednotlivé typy testu jsou zmíněny výše, jedná se o White-box, Grey-box a Black-box. [25]

Jednotlivé informace je možné získat z veřejných zdrojů, kde jsou volně dostupné, nebo je také možné obstarat je přímou interakcí s objektem, který bude testovaný. [25]

Testování

V průběhu testů se každý tester zaměřuje na jednotlivé cíle. Každý cíl je potřeba detailně prozkoumat pomocí zvolených nástrojů. [25]

V případě, že dochází k nalezení potenciální hrozby, následuje další série testů k detailnějšímu prozkoumání. Podstatné je, aby nedošlo k narušení stability aplikace a také aby uživatelská hesla nebyla vystavená riziku. V případě, že testerovi úspěšně odhalí citlivé údaje, neměly by být zanášené a zmíněné v rámci závěrečného reportu. [25]

Výsledky testování

Poslední fází je celkové posouzení a shrnutí jednotlivých výsledků testování. V této části se sepisuje report. Tato fáze je určena k prezentování jednotlivých výstupů zadavateli. V rámci této části jsou navrženy takové kroky a postupy, aby vedly ke zvýšení bezpečnosti objektu, který byl předmětem testování. [25]

2. 4 DÍLČÍ SHRNUTÍ

Cílem této kapitoly bylo seznámit se s problematikou penetračního testování a také s typy útočníků, kteří za útoky stojí. Útočník není člověk, který dělá jen ilegální činnost, ale i osoba, která zdokonaluje veškeré bezpečnostní systémy ve společnostech a tím chrání jak naše data, tak i data společnosti.

Cílem penetračních testů je vyhledat slabiny v systému a potenciální hrozby, a to za účelem zvýšení bezpečnosti a zabránění záškodníkovi systém napadnout a převzít kontrolu.

Bakalářská práce se zaměřuje na interní testy, protože budeme znát infrastruktury jednotlivých sítí i systémů. Mohlo by se jednat o útočníka, který by měl fyzický přístup k počítači.

3 NÁSTROJE URČENÉ PRO PENETRAČNÍ TESTOVÁNÍ

Tato část bakalářské práce bude zaměřena na nástroje, které jsou používané pro penetrační testování a jejichž cílem je usnadnit rutinní činnosti. Všechny nástroje, které budou použity, jsou volně dostupné a šiřitelné. Blíže představené prostředky jsou jedny z nejznámějších, a proto lze najít podrobné vysvětlení, jak s nimi pracovat.

3. 1 MALTEGO

První zmínka o tomto nástroji je z knihy, která byla vydána roku 2007. Vydání se zabývá nástroji open-source, které jsou určené k penetračnímu testování. V této knize autor popisuje, že je možné využít Maltego jako desktopovou aplikaci, která disponuje grafickým uživatelským rozhraním, nebo je možné ho využít na webové stránce organizace Paterva, která za celým projektem Maltego stojí. Od webové verze bylo poté upuštěno a v současnosti poskytuje program pouze desktopové rozhraní. [17]

Jedná se o nástroj, který je představován z kategorie Open – source inteligence. Maltego popisuje sadu určitých technik, nástrojů a postupů, kdy z běžně veřejně dostupné informace získá konkrétní a určitou zprávu. Dané informace se vztahují k určité entitě, jako je například e-mailová adresa nebo IP adresa a také k modelování relací mezi těmito informacemi. [17]

Velkou výhodou těchto nástrojů je, že ušetří velké množství času a úsilí, protože námaha, kterou by musel penetrační tester vyvinout v případě, že by takový typ informací chtěl získat ručně, je vyšší v porovnání s použitím nástroje, který pochází z kategorie Open – source inteligence. [17]

Jedna z publikací autora Danny Bradburyho zmiňuje praktický příklad, kdy je možné Maltego využít. Při ukázce jeho schopností byla objevena fotka modelky, která obsahovala i její jméno. Nad jejím jménem poté byly spuštěny transformy, které Maltego poskytuje. Později Maltego prezentovalo informace, jako jsou adresy, fotky nebo telefonní čísla. [17]

Jelikož je Maltego nástroj s grafickým uživatelským rozhraním, je práce s ním snazší v porovnání s nástroji, které jsou orientovány na příkazový řádek. Maltego má dva základní stavební kameny. Prvním z nich je entita a druhým je transforms. [17]

Entitou jsou chápány informace, které uživatel zadává a očekává, že budou zjištěna určitá dodatečná data k těm, která zadal, a zároveň i informace, které jsou zjištěné nástrojem Maltego pomocí transforms. [17]

Maltego umožňuje veškeré zprávy, které zjistil, vyobrazit v přehledném grafu entit. V grafické interpretaci je možnost snadného pohybu a pro lepší orientaci je možné v pravém horním okně zobrazit graf v menší podobě.

3. 2 SHODAN

První zmínka o Shodanu byla na konferenci o bezpečnosti ve světě a informačních technologiích z roku 2010. Použití nástroje Shodan na praktických příkladech popsal Michael Schearer, kdy hlavní myšlenky jeho prezentace byly shrnuty do zprávy. [27]

Nástroj Shodan funguje podobně jako internetové prohlížeče, které postupně procházejí jednotlivé webové stránky. Tento nástroj ale nesbírá jednotlivé informace z webových stránek, ale z periférií, jako jsou kamery tiskárny nebo servery, které komunikují po síti. Shodan je schopen objevit i systémy, které jsou zabezpečené a využívají se například k řízení světelné signalizace na křižovatkách. Výsledky vyhledávání poté tento nástroj uchovává v databázi, ve které je mohou poté uživatelé vyhledávat. [27]

3. 3 NMAP

Tento název vznikl spojením dvou slov network a mapper. První zmínka o Nmap se objevila v druhé polovině devadesátých let minulého století. Byl to nástroj, který sloužil ke scanování portů. V dnešní době se z malého nástroje stal velmi komplexní nástroj, který má v sobě zabudován spoustu doplňků, jako je skriptování. [18]

Součástí tohoto nástroje může být i grafické rozhraní, které je přehlednější než výpis v příkazovém řádku. Jedná se o jediný ze síťových scannerů, který má jasnou a přehlednou vizi pro vývoj v budoucnosti. Autor tohoto nástroje je Gordon Lyon, který také napsal nejobsáhlejší a zároveň i nejpodrobnější příručku určenou přímo k tomuto nástroji. [18]

Autoři Engbertson a Broad ve své publikaci zastávají názor, že v případě, že by si měli vybrat pouze jeden nástroj ze všech možných síťových scannerů, byl by to právě Nmap. Je to z toho důvodu, že Nmap disponuje obrovským množstvím možností a také způsobů využití. [6]

Na oficiální stránce nástroje Nmap je uveden detailní popis schopností, které Nmap umožňuje.

Jednou z funkcí jsou způsoby pro zjištění dostupnosti zařízení hosta [24]:

- TCP SYN/ACK,
- UDP,
- SCTP,
- ICMP echo,
- ICMP timestamp,
- ICMP netmask,
- protocol ping,
- arp ping.

Další funkcí jsou způsoby vyhledávání služeb, které host používá a k nimž je připojen [24]:

- TCP SYN,
- TCP,
- ACK,
- Maimon,
- UDP.

Dále je možné zjistit operační systém hosta, protože Nmap umožňuje detekci operačního systému. Výhodou je, že nástroj poskytuje výstupní formát do XML dokumentu. Nmap umožňuje používat skripty, které usnadní práci, a také skenuje, zda daný host trpí zranitelností a umí oklamat Firewall a IDS systémy.

V neposlední řadě lze nástroj možné použít pro benchmark sítě a porovnání těchto výsledků.

3. 4 ETTERCAP

Nástroj slouží k manipulaci síťového provozu a k odposlechu na návazná spojení. Disponuje velkým množstvím různých zásuvných modulů a je vybaven grafickým rozhraním, které je pro uživatele ve srovnání s příkazovým řádkem vhodnější.

Publikace Hacking exposed definuje tento nástroj jako prostředek, s jehož pomocí je možné počítačovou síť, která je založena na více přepínačích, přinutit ke změně chování. Hlavní změna chování je taková, že síť z pohledu útočníka vypadá, jako by jejím centrálním prvkem nebyl switch, ale hub. Tento cíl plní tím, že je schopen ovlivnit chování individuálních klientských stanic, nikoli jednotlivých aktivních prvků switche. Tento druh techniky se nazývá ARP spoofing. [17]

ARP spoofing je založena na rozesílání podvržených dat a nevyžádaných rámců ARP protokolu, které příjemce zahltí podvrženými kombinacemi IP adres a také MAC adres vzhledem k těmto IP adresám. [17]

Jednou ze schopností Ettercap je možnost použití zásuvných modulů a poskytnutí tak rozšíření funkcionality. Je možné přijít do styku s moduly, které provádí útoky na transportní vrstvě ISO/OSI modelu, jako je například SYN flood attack. Dostupné jsou i moduly určené k prohledávání sítě a spojeních, která na této síti existují. Nápovědu k nástroji je možné získat v příkazové řádce pomocí příkazu man8 ettercap.

3. 5 METASPLOIT

Jedná se o bezplatný software. Tento software dnes obsahuje velké množství nastavení, nástrojů a různých kombinací mezi nimi. Existuje komunitní verze, která je zcela zdarma, ale také i placená verze. Nejedná se pouze o jeden prostředek, ale o framework, tudíž umožňuje širokou škálu úpravy exploitů. Ty je poté možné použít pro penetrační testování, lze říct, že Metasploit je databáze zranitelností, kterou lze použít proti oběti.

Historie

Síťový nástroj Metasploit vytvořil v roce 2003, programátor H. D. Moore v průběhu své práce ve společnosti zaměřené na bezpečnost v oblasti počítačů. Ve chvíli, kdy si H. D. Moore uvědomil, jak moc času tráví kontrolou a úpravou exploitů, učinil rozhodnutí, že vytvoří flexibilní framework. Ten byl naprogramovaný v jazyce PERL, který slouží k tvorbě a úpravě exploitů. [14]

První verze Metasploit se datuje od roku 2003. V dubnu 2004 vyšla nová verze Metasploit 2.0, která v sobě zahrnovala celkem 19 exploitů a více než 27 Payload. Po určité době se projektu začal účastnit Matt Miller. Od této chvíle byl Metasploit framework oceňován komunitou, která se zabývá bezpečností informačních technologií. Od této chvíle se stával nezbytným nástrojem potřebným k penetračnímu testování. [14]

V roce 2007 vyšla verze Metasploit 3.0, která byla přepsána do jazyka Ruby. Celkový přechod z jazyka Perl do jazyka Ruby trval okolo osmnácti měsíců. Od té chvíle byl tento prostředek podporován jak ze strany komunity, tak i ze strany počítačové bezpečnosti a zároveň i od jiných uživatelů. [14]

V roce 2009 byl Metasploit nedílnou součástí Rapid7. Společnost, které se zabývá bezpečností informačních technologií, umožnila H. D. Mooreovi utvořit skupinu odborníků, kteří by se zaměřovali jen na vývoj Metasploit frameworku. Po tomto spojení byly vytvořeny placené produkty, jako jsou Metasploit Express a Metasploit Pro. První představuje jednodušší verzi Metasploit frameworku s GUI provedením, zahrnující reporting. Metasploit druhý představuje rozšířenou verzi Expressu Metasploit. [14]

Exploit

Jedná se o skript, který využívá zranitelnost za účelem získání prospěchu. Ve většině případů se jedná o převzetí kontroly jiného zařízení anebo například zahájení nežádoucí instalace softwaru. Jedním ze způsobů, jak ochránit svůj osobní počítač, je pravidelná aktualizace počítačového systému. [19]

Ve většině případů slouží k získání práv pro administrátora, jako je (uživatel root, administrátor). V ojedinělých případech se nejdříve záškodník snaží získat nižší práva a s využitím dalších exploitů se propracuje až k administrátorským právům. [19]

Payload

Kód určený ke spuštění jiného zranitelného systému. S využitím frameworku je možné kód vybrat a odeslat na zranitelný stroj. Například Payload reverse Shell umožňuje vytvořit spojení se zranitelným strojem. Útočník toto spojení vidí formou příkazového řádku na Windows nebo formou terminálu na Linuxu. [29]

Dalším typem Payload je například Meterpreter, kde host očekává zpětnou vazbu v podobě komunikace od vybraného systému. [14]

Shellcode

Jedná se o množinu příkazů, které jsou používány v Payload. Ve většině případů je shell zahájen až po úspěšném Payload. Jako jeden z příkladů je také Meterpreter.

Moduly

Představují části, jež dělají Metasploit výkonným. Modulem se myslí část kódu, která je používána tímto frameworkem. Například jím může být Exploit modul nebo pomocný modul, jenž slouží pro zajištění skenování. [14]

Posluchač

Součástí Metasploit, jenž čeká na zahájení komunikace, která přichází ze zranitelného hosta po úspěšném provedení. [14]

3. 5. 1 SOUČÁSTI METASPLOIT

Tento nástroj poskytuje větší množství rozhraní než jen konzole, příkazový řádek a grafické rozhraní.

MSF konzole

Jedná se o interaktivní konzoli, která je přátelštější k uživateli než MSFcli. Aby bylo možné konzoli spustit, je potřeba zadat do příkazového řádku daný příkaz msfconsole.

Po spuštění se vyobrazí text, který nabízí veškeré informace o verzi, počtu exploitů a Payload, které je možné využívat. Touto částí se budeme zabývat v praktické části, kde si popíšeme i další možnosti.

MSFcli

Používá se na skriptování a kooperaci s ostatními nástroji. Prostředek se přímo spouští z příkazového řádku a díky tomu byla snadnější interakce s ostatními prostředky, jelikož jsou schopny převést výstup do příkazu MSFcli a poté i opačně. Výhodou bylo, že umožňoval přímé spuštění exploitů a Payload. [21]

Bylo ho vhodné používat zejména v situacích, kdy jsme přesně věděli, jaký exploit a které jeho nastavení bychom měli použít. Umožňoval i zobrazit možnosti pomocí parametru O. Nástroj se přestal využívat od roku 2015. [21]

Armitage

Jedná se o kompletně interaktivní a grafickou součást Metasploitu. Tvůrcem je Raphael Mudge. Armitage je volně dostupný nástroj, který nabízí vizualizaci cílů útoku. Další možností, kterou nabízí, je snadnější práce v týmu, kdy přes jednu instanci umožňuje, aby skupina viděla stejné spojení, zachycení dat, sdílení hostingů a spojení přes sdílený log událostí. [2]

3. 6 OSTATNÍ NÁSTROJE

V rámci bakalářské práce budou zmíněny i další nástroje jako například CHNTPW, SQLMap a Aircrack-ng, protože jsou základním pilířem, patří mezi často používané a základní, které by měl tester znát. V rámci penetračního testování existuje celá řada dalších nástrojů.

CHNTPW

Jedná se o softwarový nástroj určený pro resetování nebo vymazání místních hesel, který je používaný systémy Windows NT, 2000, XP, Vista, 7 ,8 ,8.1 a 10. [12]

Nástroj upravuje databázi SAM, kde Windows ukládá hesla. Program je možné použít dvěma způsoby. První z nich – pomocí samostatného nástroje chntpw nainstalovaného jako balíčku dostupného ve většině moderních linuxových distribucích. Druhý způsob – pomocí zaváděcího obrazu CD / USB. U příležitosti desátého výročí softwaru autor změnil licenci na verzi GNU General Public License (GPL) verze 2. [12]

SQLMap

Nástroj sloužící pro automatické zjišťování a využívání nedostatků SQL Injection. SQLMap přebírá kontrolu nad databázovými servery. Software se dodává s výkonnými moduly. Podporované jsou veškeré populární databázové servery Oracle, MySQL, PostgreSQL, Microsoft SQL server a mnoho dalších. [24] [15]

AIRCRACK-NG

Představuje kompletní sadu nástrojů, které slouží pro posouzení zabezpečení Wi-Fi.

Zaměřuje se na mnoho oblastí řešení [1]:

- Monitorování paketů a exportování dat do textového souborů pro další zpracování.
- Útočení pomocí metod přehrání útoku, odmítnutí služby, falešný přístupový bod a další prostřednictvím injekce paketů.
- Testování Wi-Fi karet a ovladačů.
- Prolomení WEP a WPA-PSK.

Všechny příkazy jsou dostupné z příkazového řádku a jedná se primárně o linuxovou sadu nástrojů.

4 MOŽNOSTI REALIZACE ÚTOKŮ

Každé počítačové zařízení je zranitelné a může být vystaveno velkému počtu hrozeb, které jsou spjaté s několika typy útoků. Dělí se na fyzické, vzdálené a kombinované. Mezi fyzické je možné zařadit Linux Live CD, Rainbow tables. Kategorie vzdálených útoků zahrnuje sociální inženýrství, malware, spam, hoax, phishing, pharming, hacking a Dos/DDos. Poslední skupinou jsou kombinované, kde řadíme keylogging. [20]

K jednotlivým útokům na počítačové zařízení potřebuje útočník program, vir, který mu umožní dostat se do počítače. Cílem je získat data, citlivé informace a využít vhodný okamžik k provedení útoku, na který je potřeba větší výpočetní výkon.

Cílem penetračního testování je zhodnotit a prověřit úroveň zabezpečení počítačů, systémů a aplikací prostřednictvím penetračních testů a navrhnout, jak jednotlivé bezpečnostní nedostatky odstranit nebo potlačit.

4. 1 FYZICKÉ

První kategorií, kterou se budeme zabývat, jsou útoky fyzické. Existuje velké množství programů, které je možné využívat pouze v případě, když je osoba u počítače fyzicky. Fyzický kontakt je nutností, protože se jedná o programy, které jsou umístěné na USB Flash disk nebo třeba CD.

Proces útoku začíná tím, že se úložiště vloží do počítačového zařízení a tím pádem je možné zahájit proces zjišťování hesel nebo i jejich mazání. Jednou z hlavních nevýhod je, že útočník musí být u počítače, ale hlavně musí jednat rychle. Metod pro odcizení hesla existuje celá řada, může se jednat například o Linux Live CD nebo Rainbow tables.

4. 1. 1 LINUX LIVE CD

Live CD je takzvané živé médium jako například CD, DVD nebo USB. Jedná se o samostatný disk. Operační systém na živém médiu funguje zcela odděleně od operačního systému počítače, proto je možné ho používat k mazání hesel nebo na obnovu souboru. Existuje celá řada programů, které pracují na tomto principu. [28]

4. 1. 2 RAINBOW TABLES

Programů, které využívají danou metodu, existuje několik. V překladu to znamená „duhové tabulky“. Jedná se o určité tabulky, které obsahují velké sady představených hodnot hash pro jednotlivé hesla. Všechna hesla jsou transformována do jedinečné číselné formy neboli hashe. Tato metoda porovnává jednotlivé hashe a při nalezení shody dokáže rozklíčovat původní heslo. Čím více písmen, číslic a znaků heslo obsahuje, tím jeho dešifrování trvá déle. [23] [9]

Programy, které využívají tuto metodu, jsou například: Ophrack a Cain & Abel. Jsou to nejznámější a nejpoužívanější programy v operačním systému Windows. Jeho nevýhodou je, že jej není možné použít ve Windows 10. Druhý program je vhodný pro starší operační systémy, proto už dnes není tolik používaný.

4. 2 VZDÁLENÉ

Jedná se o typ útoků prováděných na dálku. Vzdálené útoky slouží k tomu, že mohou poškodit nebo změnit jednotlivá data v daném počítačovém zařízení. Dále mohou sloužit ke zjištění přihlašovacích údajů například do bankovnictví, e-mailové schránky nebo sociálních sítí. Typy útoků ovlivňující data obsažená v počítači jsou například sociální inženýrství, malware a hacking.

Sociální inženýrství

Hlavním představitelem je Kevin Mitnick. Jedná se o způsob, jak manipulovat s lidmi s cílem provést určitou akci nebo získat dané informace. Lidé jsou totiž nejslabší článek bezpečnosti. Útočník se může například vydávat za zaměstnance firmy, aby získal určitá data o společnosti. Může vzbudit v oběti pocit, že mají společné zájmy a koníčky, aby mu oběť poskytla data. [22]

Metody útoku – sociotechnika [20]:

- **Přímý přístup** – situace, kdy útočník přímo poprosí oběť o její přihlašovací údaje.
- **Důležitý uživatel** – útočník působí jako autoritativní a nadřízená osoba, jež požádá o informace podřízeného. Jedná se například o hesla a citlivé informace. Pokud má podřízený dojem, že jedná s nadřízeným, údaje mu poskytne.
- **Bezmocný uživatel** – Útočník si vybere nového a nezkušeného zaměstnance a předstírá, že má neplatné údaje, ale potřebuje úkol ihned udělat a poprosí oběť o jeho přihlašovací údaje.

- **Pracovník technické podpory** – záškodník hraje roli zaměstnance v oddělení informatiky a tím se snaží získat údaje od běžných uživatelů. Může se jednat o e-mail, který se jeví jako od administrátora a požaduje potvrzení hesla kliknutím na odkaz. Neproškolení zaměstnanci nemají tušení, že hlavička v e-mailu odesílatele nemusí být pravdivá.

Malware

Je to druh škodlivého počítačového programu. Umožňuje poškodit počítačové systémy. Do této skupiny patří kódy jako například ransomware, počítačové viry a trojské koně. Jeho cílem je získat a poškodit data a vyvolat co největší škodu v napadeném počítači. Ransomware slouží k šifrování dat počítače a slíbí jeho dešifrování za určitou peněžní částku. Spyware je určen k získávání a také odesílání dat z napadeného počítače, ve kterém je nainstalován. Adware znepříjemní práci uživatele na počítači nepřetržitým vyskakováním reklam na internetu. [16]

Spam

Spamming znepříjemňuje práci uživatele nevyžádaným rozesíláním elektronické pošty. Uživatel poté musí rozlišovat, které e-maily jsou důležité a které nevyžádané. Může to vést k zahlcení elektronické pošty. Uživatel tak může kvůli spamu přehlédnout důležitou e-mailovou zprávu. Nejvíce se vyskytuje v e-mailových schránkách, ale může napadnout internetové fórum nebo blogy. V řadě případů obsahuje i malware, jehož cílem je od uživatele získat data, která jsou následně odesílaná útočníkovi. [16]

Hoax

Je takzvaná falešná zpráva, jejímž cílem je zastrašit, pobavit nebo poškodit osoby rozesíláním falešných informací. Velmi často se označuje jako řetězový e-mail, protože ve zprávě klade důraz na přeposílání dalším osobám. [16]

Phishing

Jeho hlavním úkolem je oklamat uživatele za účelem získání dat a také přihlašovacích údajů do e-mailu, sociálních sítí, internetového bankovnictví. Využívá imitaci oficiální internetové stránky. Když uživateli přijde do e-mailu nebo jiné sociální stránky odkaz na falešný web, aby zadal své přihlašovací údaje. Oběť se ale nepřihlásí na skutečné stránky, ale na podvržené útočníkem. Poznat, že se jedná o podvrh internetové stránky, je možné pouze z webové adresy, která se liší od oficiálních webových stránek. [16]

Pharming

Jedná se o formu phishingu, která je ale nebezpečnější a sofistikovaná. Jedná se o útoky zaměřené na DNS serverů, kde přepíše jejich IP adresu. Výsledkem je podvržená stránka nerozeznatelná od skutečné webové stránky, ve které je IP adresa zaměněna za útočníkovu. Princip spočívá v tom, že uživatel zadá skutečnou internetovou stránku, ale bude načtena podvržená stránka záškodníka. Tím pádem na stránce není možné poznat, že je falešná. [16] [22]

V rámci operačního systému Windows může záškodník využít i jinou formu útoku. OS Windows obsahuje soubor „Hosts“, jenž v sobě zahrnuje IP adresy různých navštívených webových stránek. Útočník přepíše IP adresu v souboru Hosts. Tato forma je pro útočníka mnohem snadnější, jelikož zabezpečení DNS serverů je dobré.

Hacking

Záškodník využívá slabiny operačního systému, které překonává. Hacking je možné provádět i bez použití škodlivých programů. Útočník chce poškodit systém nebo se zabavit. [8]

Denial of Service

Je označen také pod zkratkou DoS. Hlavním úkolem je vyřadit službu z provozu. Princip spočívá v tom, že službu zahltí zasíláním požadavků, nebo může využít chybu k restartování nebo vypnutí služby. Jednou z forem útoků DoS je Distributed Denial of Service neboli DDoS. DDoS k útoku používá síť robotů, jejichž úkolem je zasílat příkazy s cílem přehltit danou službu. [5] [7]

4. 3 KOMBINOVANÉ

Jedná se o způsob, který je kombinací předchozích dvou. Jde o spojení použití programu na dálku, ale zároveň vyžaduje fyzický přístup k počítačovému zařízení. Touto technikou je možné použít kterýkoli keylogger.

Výhodou je, že útočník si musí vytipovat oběť. Aby záškodník mohl z počítače ukrást data, potřebuje se k němu přímo dostat, což je nevýhoda. Příkladem je Keylogging.

Keylogging

Je druh programu, který umožňuje zachytit stisknutelné znaky na klávesnici. Umožňuje zaznamenávat snímky ze sledovaného počítačového zařízení. Umí rozeznat, jestli byl k počítačovému zařízení připojen USB flash disk nebo jestli do něj bylo vloženo CD nebo DVD. V případě, že je počítač vybaven mikrofonem nebo webkamerou, je schopen tyto věci využít k pořízení záznamu. Keyloggery existují jak softwarové, tak i hardwarové. [3]

Prvním krokem je instalace do počítačového zařízení zasláním e-mailové zprávy. E-mail obsahuje přílohu se skrytým programem, jehož stažením se nainstaluje i program. Velké množství keyloggerů je určeno k instalaci na počítač. [3]

Hardwarové keyloggery jsou finančně náročné v porovnání se softwarovými. Existuje více typů jako mezičlánek mezi klávesnicí a počítačem, a to přímo zabudované v USB rozhraní. Tento druh keyloggeru útočníci využívají zřídka z finančních důvodů a vizualizace. [3]

V případě, že má antivirus k dispozici určité nástroje, je schopen objevit softwarový keylogger. Hardwarové keyloggery není schopen odhalit, ale může ho odhalit uživatel. Hlavními znaky, díky kterým ho oběť rozpozná, je pomalé načítání internetových stránek, zpomalené zobrazování znaků a písmen při psaní do editoru. Uživatel ho může odstranit 2 způsoby, a to ručně, což je velmi neefektivní a pomalé, nebo pomocí antiviru. [3]

4. 4 DÍLČÍ SHRNUTÍ

Nebezpečí a hrozby existují od začátku, kdy se připojíme k internetu. Každou minutu můžeme být napadeni tisíce hrozbami, proto je důležité umět je identifikovat a eliminovat.

Existují různé způsoby, jak je možné zařízení napadnout. Z pohledu útočníka je nejnáročnějším způsobem fyzický přístup, protože musí jednat velmi rychle a nesmí být přistižen při činu, což je přesný opak útoku přes síť, kdy útočník není limitovaný časem. V případě, že záškodník bude odhalen, nejedná se z jeho pohledu o velkou komplikaci, protože se dokáže skrýt po celé síti internetu a může provádět činnost z jiné části světa.

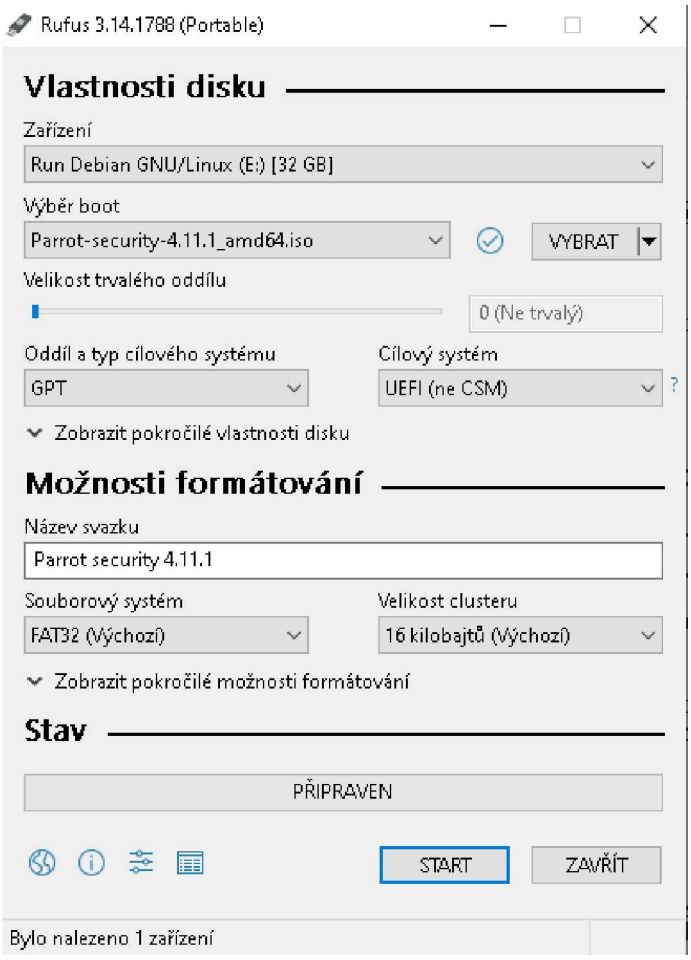
Cílem penetračního testování je zhodnotit a prověřit úroveň zabezpečení počítačů, systémů a aplikací prostřednictvím penetračních testů a navrhnout, jak jednotlivé bezpečnostní nedostatky odstranit nebo potlačit.

5 PRAKTICKÁ ČÁST

V praktické části budou představeny dva typy útoků. První útok se bude zabývat fyzickým penetračním testováním a další test bude prováděn přes síť. Tyto typy jsou zvolené z toho důvodu, že se s nimi můžeme setkat dnes a denně. Fyzický test může být proveden kdekoliv, když necháme své zařízení chvíli bez dozoru. Útoky přes síť je možné provádět z jakéhokoliv místa na kohokoli, kdo je připojen k internetu.

5. 1 FYZICKÉ PENETRAČNÍ TESTOVÁNÍ

V rámci této části využiji svůj vlastní notebook, kde je instalován operační systém Windows 10 Pro. V rámci práce se vycházelo z předpokladu, že počítač byl určitou dobu bez dozoru. Tím získává útočník prostor k tomu, aby odcizil data. Pro přípravu byla vytvořena živá distribuce Parrot OS na USB klíčenku. Instalační médium lze jednoduše vytvořit pomocí nástroje Rufus a také ISO souboru živé distribuce Parrot OS (Obrázek 9: Vytvoření bootovacího USB disku).



Obrázek 9: Vytvoření bootovacího USB disku

Zdroj: Vlastní zpracování

Po úspěšném vytvoření se vloží USB klíčenka do počítače před jeho spuštěním. Při spuštění musíme zvolit jiné pořadí zavedení systému. Tím docílíme, že se zavede místo standardního operačního systému námi zvolený operační systém Parrot OS. Dále je potřeba připojit disk s původním operačním systémem pomocí správce souborů.

5. 1. 1 FYZICKÉ ODSTRANĚNÍ HESLA WINDOWS

V rámci bakalářské práce bude představena metoda, která smaže heslo k uživatelskému účtu a také umožní přidat, nebo odebrat uživatele do skupin. To umožní útočníkovi být v roli administrátora. Postupuje se tak, že se otevře terminál pomocí nabídky aplikací. První příkaz, který je potřeba zadat, je cd a ten slouží ke změně umístění na disku. Tímto příkazem se dostaneme k složce, v níž jsou umístění uživatelé systému Windows (Obrázek 10: Cesta do složky s uživatelskými údaji).

```
┌─[user@parrot]─[~]
└──╼ $cd /media/user/94D06461D0644C14/Windows/System32/config/
┌─[user@parrot]─[/media/user/94D06461D0644C14/Windows/System32/config]
└──╼ $
```

Obrázek 10: Cesta do složky s uživatelskými údaji

Zdroj: Vlastní zpracování

Následuje vypsání veškerých uživatelských účtů pomocí nástroje CHNTPW. Do terminálu zadáme CHNTPW a parametry. První z nich bude parametr l a druhý SAM (Security account manager), díky tomu se nám vypíšou veškeré uživatelské účty. Položky v seznamu pod názvy Michal, Terezka byly vytvořeny pouze pro účel bakalářské práce. Ostatní pojmenování v listu jsou výchozí účty Microsoft Windows, které jsou v našem případě uzamčeny a nejsou v tomto případě ani používány v operačním systému Windows.

```
┌─[user@parrot]─[/media/user/94D06461D0644C14/Windows/System32/config]
└──╼ $chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 131072 [20000] bytes, containing 12 pages (+ 1 headerpage)
Used for data: 295/62696 blocks/bytes, unused: 27/31128 blocks/bytes.

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 01f7 | DefaultAccount                 |        | dis/lock |
| 01f5 | Guest                          |        | dis/lock |
| 03ea | Michal                         |        |          |
| 03e9 | Terezka                        | ADMIN  |          |
| 01f8 | WDAGUtilityAccount             |        | dis/lock |
┌─[user@parrot]─[/media/user/94D06461D0644C14/Windows/System32/config]
└──╼ $
```

Obrázek 11: Seznam uživatelských účtů systému Windows

Zdroj: Vlastní zpracování

Dalším krokem je zadat uživatele, u kterého chceme provádět změnu. V tomto případě se jedná o vlastníka, který je pojmenován Michal.

Z (Obrázek 11: Seznam uživatelských účtů systému Windows) lze vyčíst, že nemá oprávnění administrátora. Roli administrátora účtu přidáme a tím docílíme plné kontroly nad počítačem i v tom případě, že by vlastník neměl plné oprávnění v roli administrátora.

Aby bylo možné dostat se do nabídky (Obrázek 13: Hlavní nabídka programu chntpw) je potřeba korektně zapsat příkaz. První parametr v pořadí symbolizuje uživatele a jeho ID.

Před identifikátor uživatele musí být vloženo 0x, aby byl uveden správný formát zápisu v šestnáctkové soustavě (Obrázek 12: Korektní zápis pro úpravu uživatele a zobrazení menu).

```
┌─[user@parrot]─[/media/user/94D06461D0644C14/Windows/System32/config]
└──╼ $chntpw -u 0x03ea SAM
```

Obrázek 12: Korektní zápis pro úpravu uživatele a zobrazení menu

Zdroj: Vlastní zpracování

Prvním krokem bylo odstranění hesla uživatele. V menu se musela zadat volba jedna, která provede smazání hesla.

```
fullname:
comment :
homedir :

00000221 = Users (which has 3 members)

Account bits: 0x0214 =
[ ] Disabled        | [ ] Homedir req.    | [X] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 2

- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] >
```

Obrázek 13: Hlavní nabídka programu chntpw

Zdroj: Vlastní zpracování

Dále je možné přidělit danému uživateli skupinu, která existuje v systému. Zvolíme volbu číslo čtyři. Zobrazí se nám seznam skupin. V našem případě jsme uživateli přidali skupinu administrátora vedenou pod číslem 220 (viz Obrázek 14: Přidání uživatele do skupin).

```
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > 4

 == ADD USER TO A GROUP
=== Group # 220 : Administrators
=== Group # 221 : Users
=== Group # 222 : Guests
=== Group # 22e : Performance Monitor Users
=== Group # 22f : Performance Log Users
=== Group # 232 : Distributed COM Users
=== Group # 238 : IIS_IUSRS
=== Group # 23d : Event Log Readers
=== Group # 242 : Spr?vci technologie Hyper-V
=== Group # 244 : Remote Management Users
=== Group # 245 : System Managed Accounts Group
=== Group # 247 : Vlastn?ci zaY?zen?

Please enter group number (for example 220), or 0 to go back
Group number? :
```

Obrázek 14: Přidání uživatele do skupin

Zdroj: Vlastní zpracování

Dále nebylo potřeba nic upravovat. Pro ukončení nástroje slouží příkaz q, který zobrazí potvrzovací dialog pro skončení a uložení výstupu změn do systému (viz Obrázek 15: Ukončení programu chntpw).

```
[ ] Disabled        | [ ] Homedir req.    | [X] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 2
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > q

Hives that have changed:
 #  Name
 0  <SAM>
Write hive files? (y/n) [n] :
```

Obrázek 15: Ukončení programu chntpw

Zdroj: Vlastní zpracování

Pro kontrolu byl vypsán list uživatelů, kde pod vlastníkem Michal se zobrazilo oprávnění administrátora a také hodnota tzv. blank, která označuje, že daný uživatel nemá heslo do systému (viz Obrázek 16: Upravený výpis uživatelů se změnami hodnot).

```
┌─[user@parrot]─[/media/user/94D06461D0644C14/Windows/System32/config]
└──╼ $chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 131072 [20000] bytes, containing 12 pages (+ 1 headerpage)
Used for data: 296/62712 blocks/bytes, unused: 27/31112 blocks/bytes.

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 01f7 | DefaultAccount                 |        | dis/lock |
| 01f5 | Guest                          |        | dis/lock |
| 03ea | Michal                         | ADMIN  | *BLANK*  |
| 03e9 | Terezka                        | ADMIN  |          |
| 01f8 | WDAGUtilityAccount             |        | dis/lock |
┌─[user@parrot]─[/media/user/94D06461D0644C14/Windows/System32/config]
└──╼ $
```

Obrázek 16: Upravený výpis uživatelů se změnami hodnot

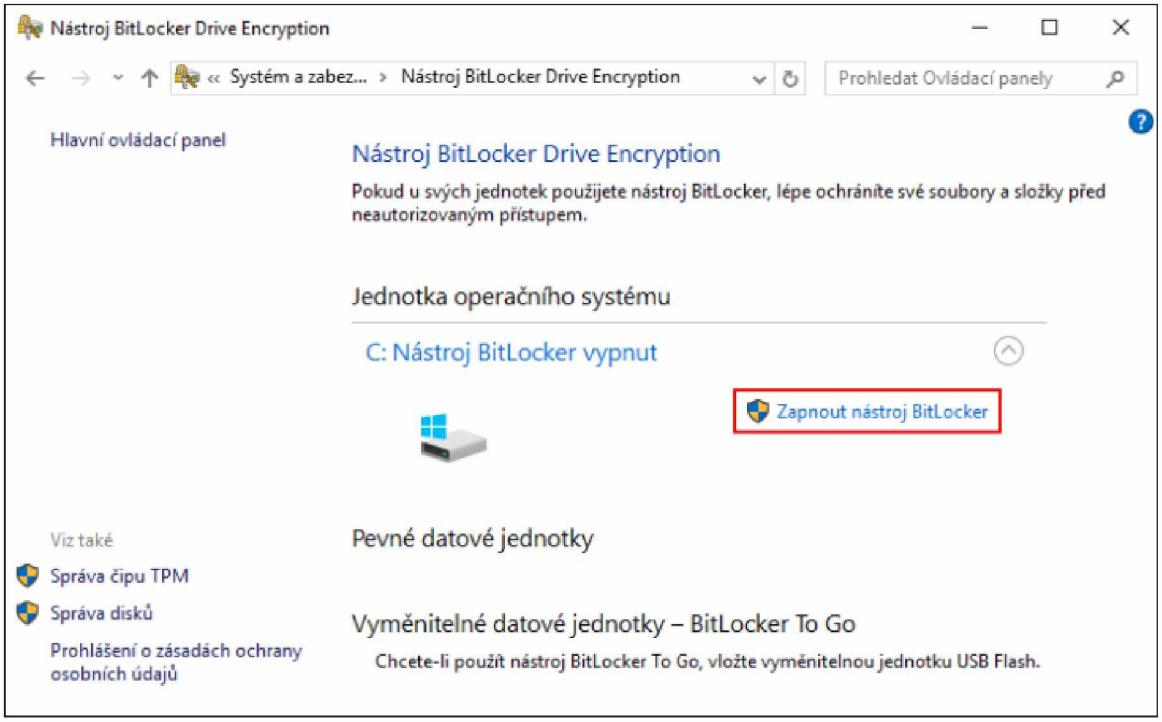
Zdroj: Vlastní zpracování

5. 1. 2 ZÁVĚREM FYZICKÉHO ÚTOKU

Závěrem tohoto útoku bylo, že počítač, který je chvíli bez dozoru a je zabezpečený pouze heslem do operačního systému umožní útočníkovi heslo prolomit a do systému proniknout.

Prvním mechanismem, který umožní zabránit, nebo alespoň zpomalit záškodníka v provádění útoku, je zamknutí pořadí zavádění disků. Tímto docílíme, že by se vždy zavedl pouze náš daný operační systém, nikoli cizí. Následně je nutné zamknout UEFI/BIOS a povolit Secure Boot, který nedokáže zavést jiný operační systém. Ani nadále není toto řešení odolné natolik, aby ho útočník nemohl obejít, neboť při vložení disku do jiného počítače by se útočníkovi podařilo dostat do našeho systému, kde bychom mohli mít citlivé údaje.

Proto bych nadále doporučil použít všechny předchozí varianty a také si zašifrovat náš systémový disk i pomocí integrovaného nástroje v systému Windows 10 Pro a tím je nástroj Bitlocker (viz Obrázek 17: Integrovaný nástroj pro šifrování disku). Tento nástroj je k dispozici pouze ve verzi Windows 10 Pro a vyšších. Pro nižší verze operačního systému doporučuji použít nástroj VeraCrypt.



Obrázek 17: Integrovaný nástroj pro šifrování disku

Zdroj: Vlastní zpracování

5. 2 ÚTOK PŘES SÍŤ

Při demonstraci penetračního útoku prováděného přes síť, bude použit virtuální stroj linuxové distribuce Kali Linux a také operační systémy Windows 7 a Windows 10. U Windows 7 se očekává, že útok bude zdárně proveden, zatímco v rámci systému Windows 10 je předpoklad, že je tento typ zranitelnosti ošetřen. Tento útok slouží pro ukázku v rámci bakalářské práce a neměl by být zneužit pro nelegální činnost.

Po spuštění operačního systému Kali Linux bylo zapotřebí aktualizovat veškeré nástroje a instalovat jeden užitečný program jménem Armitage, který seskupí ostatní nástroje a umožní některé funkce graficky zobrazit. Pro aktualizaci repozitářů a nástrojů použijeme příkaz (viz Obrázek 18: Aktualizace repozitářů a balíčků).

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt upgrade -y
```

Obrázek 18: Aktualizace repozitářů a balíčků

Zdroj: Vlastní zpracování

Nástroj Armitage lze instalovat z repozitáře linuxové distribuce pomocí příkazu (viz Obrázek 19: Instalace Armitage).

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install armitage
```

Obrázek 19: Instalace Armitage

Zdroj: Vlastní zpracování

Před spuštěním Armitage je nezbytné provést kroky, bez kterých by nebylo možné tento program spustit. Musíme zapnout Postgresql databázi a inicializovat Metaspoit databázi pomocí těchto příkazů (viz Obrázek 20: Inicializace databází).

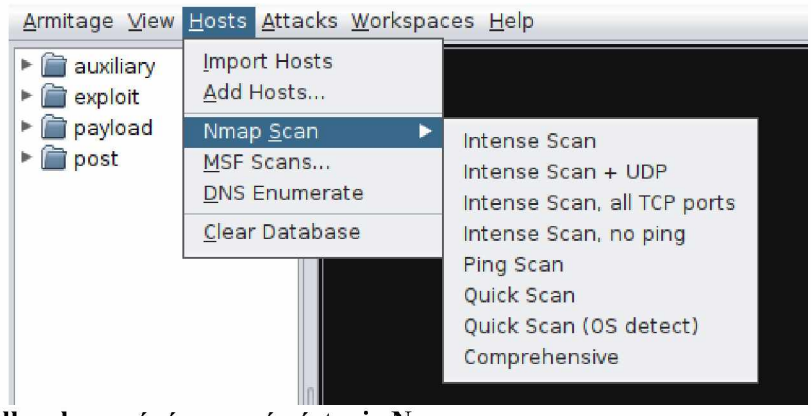
```
┌──(kali㉿kali)-[~]
└─$ /etc/init.d/postgresql start
Starting postgresql (via systemctl): postgresql.service.

┌──(kali㉿kali)-[~]
└─$ sudo msfd init
```

Obrázek 20: Inicializace databází

Zdroj: Vlastní zpracování

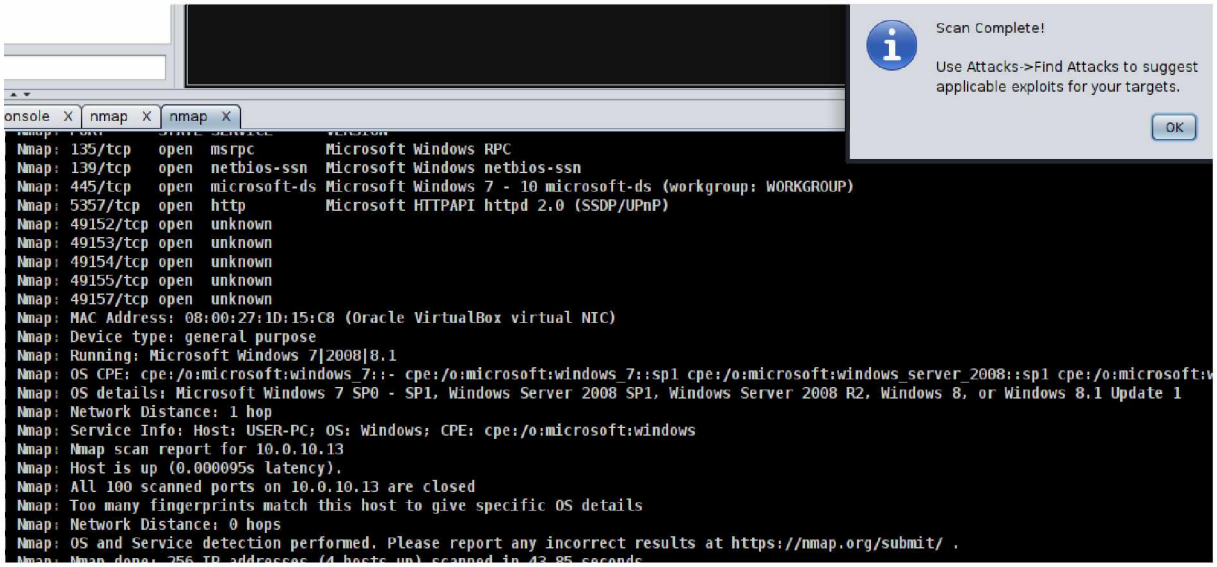
Po spuštění Armitage je zapotřebí najít naše síťová zařízení, na která budeme útočit. Pomocí nabídky vybereme Hosts, který s využitím nástroje Nmap skenuje síť a tím i veškeré zařízení připojené v rámci jedné sítě. V menu je z více možností skenování vybrána metoda Quick scan os detect z toho důvodu, protože zatím stačí znát verzi systému (viz Obrázek 21: Volba skenování pomocí nástroje Nmap). Následně se můžeme rozhodnout, zda na toto zařízení provedeme útok, či nikoli.



Obrázek 21: Volba skenování pomocí nástroje Nmap

Zdroj: Vlastní zpracování

V síti bylo nalezeno zařízení, které má operační systém Windows 7, proto se na něj zaměříme. Pro podrobnější informace provedeme plný sken, který umožňuje zjistit, jaké služby operační systém používá a jaké porty má vystaveny (viz Obrázek 22: Výsledek skenování).

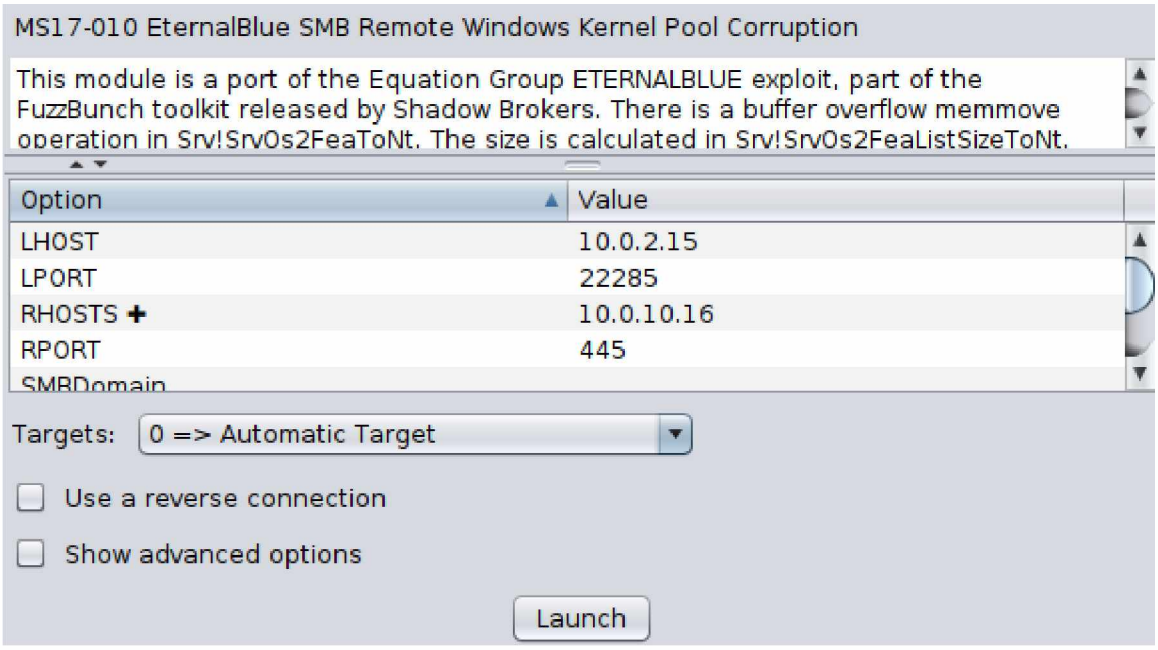


Obrázek 22: Výsledek skenování

Zdroj: Vlastní zpracování

Z výpisu je zřejmé, že port 445, který souvisí se sdílením souboru v systému Windows, je otevřen. Tím můžeme přejít k útoku. Z nabídky vybereme exploit, který je určen na Windows a na službu SMB. Z dostupných informací je znatelné, že se jedná o Windows 7, a proto použijeme známou zranitelnost CVE-2017-0144.

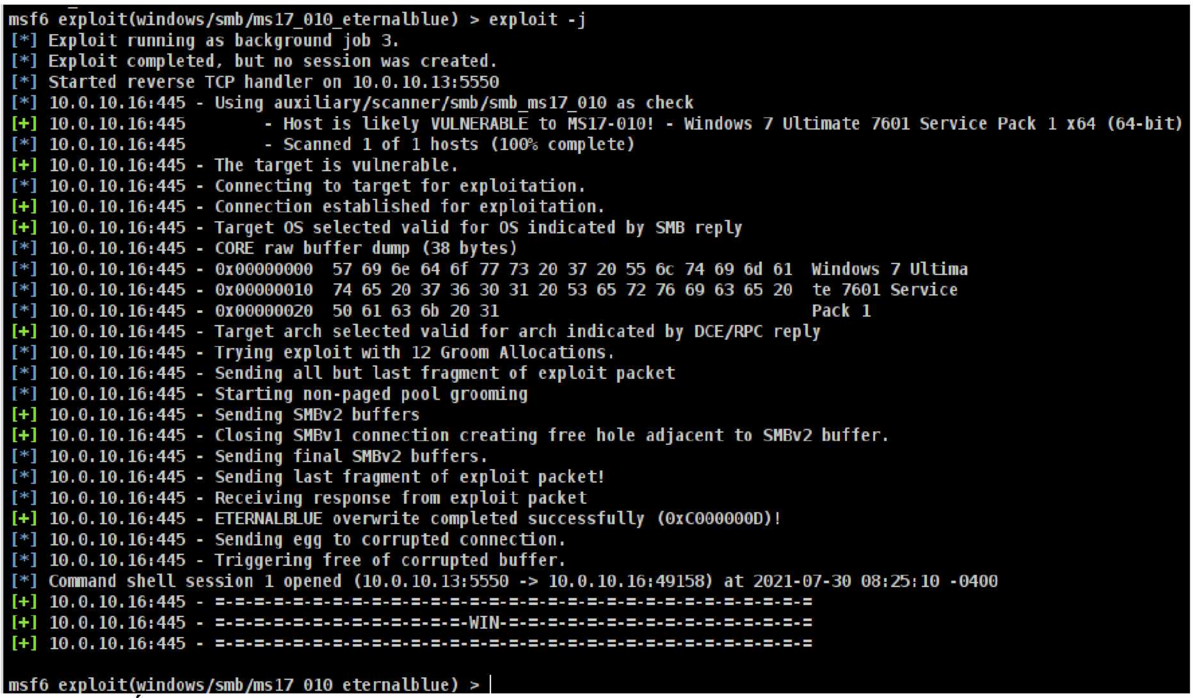
Tato slabina je spjata se známým ransomwarem WannaCry. Útok provedeme tak, že v nabídce vybereme exploit a přetažením na cílové zařízení se objeví dialogové okno s parametry, které jsou automaticky doplněny (viz Obrázek 23: Dialogové okno parametrů).



Obrázek 23: Dialogové okno parametrů

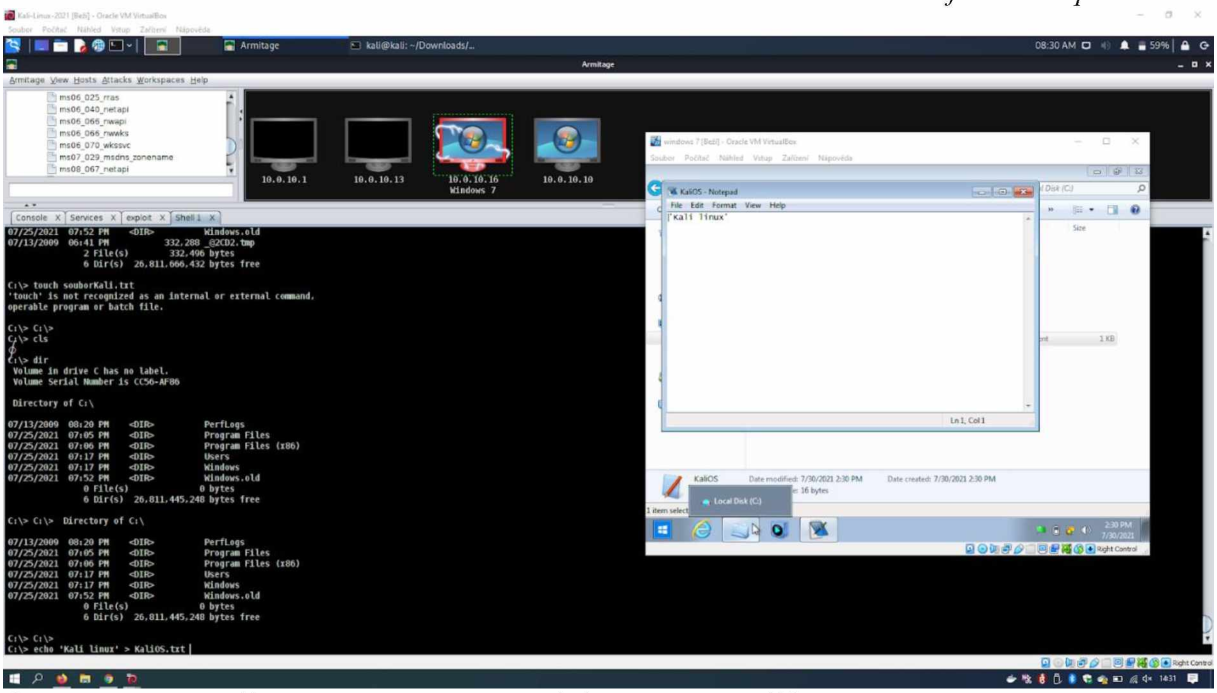
Zdroj: Vlastní zpracování

Na základě výpisu o útoku je zřejmé, že operační systém Windows 7 byl prolomen (viz Obrázek 24: Úspěšný útok na Windows 7).



Obrázek 24: Úspěšný útok na Windows 7

Zdroj: Vlastní zpracování



Obrázek 25: Vytvoření souboru správy administrátora na oběti

Zdroj: Vlastní zpracování

Pro ukázku byl vytvořen v kořenovém adresáři soubor bez vědomí uživatele, protože jsem měl plné právo administrátora na cílovém počítači (viz Obrázek 25: Vytvoření souboru správy administrátora na oběti).

Na systém Windows 10 s číslem sestavení 10240 byl aplikován stejný postup, ale útok nebyl úspěšný, i když toto sestavení má tuto zranitelnost (viz Obrázek 26: Útok na Windows 10). Nepodařilo se navázat korektní spojení s tímto operačním systémem. Tato chyba může být důsledkem programu Metasploit, protože při starší verzi se tato chyba při stejném útoku neobjevila. Další příčinou může být chyba systému Windows 10, která dokázala toto spojení zablokovat.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit -j
[*] Exploit running as background job 5.
[*] Exploit completed, but no session was created.
[*] 10.0.10.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.10.10:445        - Host is likely VULNERABLE to MS17-010! - Windows 10 Enterprise 10240 x64 (64-bit)
[-] 10.0.10.10:445        - Errno::ECONNRESET: Connection reset by peer
[*] 10.0.10.10:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.10.10:445 - The target is vulnerable.
[*] 10.0.10.10:445 - shellcode size: 1277
[*] 10.0.10.10:445 - numGroomConn: 12
[*] 10.0.10.10:445 - Target OS: Windows 10 Enterprise 10240
[*] 10.0.10.10:445 - CommunicationError encountered. Have you set SMBUser/SMBPass?
[-] 10.0.10.10:445 - Exploit failed with the following error: Read timeout expired when reading from the Socket (timeout=30)
[*] Started bind TCP handler against 10.0.10.10:17199
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Obrázek 26: Útok na Windows 10

Zdroj: Vlastní zpracování

Posledním pokusem byl útok na primární počítač, který má veškeré aktualizace a je plně chráněn. Tento útok byl neúspěšný. V konzoli šlo vyčíst, že danou slabinu nelze zneužít a je plně ošetřena.

5. 2. 1 ZÁVĚREM ÚTOK PŘES SÍŤ

Závěrem této ukázky je, že pokud se připojíme k nedůvěryhodnému připojení, jedná-li se třeba o síť, která není chráněna heslem, můžeme se stát jednoduše obětí útočníka.

Mezi radami a doporučeními, které by útočníka mohly zpomalit, nebo přímo zastavit před touto slabinou systému a nově vytvořenou zranitelností, je mít aktualizovaný systém. V aktuálních verzích Windows 10 je tento typ nebezpečné chyby opraven a tím je systém zabezpečen.

Dalším doporučením je vypnutí služeb typu sdílení souborů a tiskáren. Tím zabráníme dalším možnostem útoku, které by mohly být zneužity i v budoucnu. Dalším prvkem, jak se proti útokům přes síť chránit, je použít antivirový program, který dokáže zaznamenávat skenování portů od útočníka. Poslední radou a typem ochrany je, že pokud člověk bude připojen na nezabezpečené síti, lze použít VPN, která slouží pro šifrovanou komunikaci s internetem.

ZÁVĚR

S růstem používání počítačových zařízení roste i náročnost na zajištění bezpečnosti systémů. Pro zlepšení ochrany jednotlivých systémů je důležité využívat penetrační testování. Tato metoda vyhodnocuje slabiny systémů a tím může být uživatel nebo bezpečnostní technik o krok napřed před útočníky, kteří mohou přijít na danou slabinu dříve a zneužít ji.

Metodiky, které jsou v této práci představené, jsou ilustrační a neměly by být aplikovány k ilegální činnosti, která by mohla poškodit firmy nebo uživatele.

Celkové zpracování bakalářské práce bylo následující:

V první části bakalářské práce bylo seznámení se s linuxovými distribucemi a jejich historií. Dále jsme se zaměřili na penetrační testování, zejména na typy testů a také jejich průběh. S touto problematikou úzce souvisí i typy útočníků a testerů.

Druhým krokem bylo seznámení se s nástroji určenými k penetračnímu testování. Mezi hlavní programy patří Maltego, Shodan, Nmap, Ettercap a Metaspolit. Každý nástroj se specializuje na jiné odvětví. Nmap se využívá pro skenování dostupných síťových zařízení. Ettercap se slouží pro útoky typu man-in-the-middle.

Dalším krokem této práce byly způsoby, jimiž může útočník zaútočit na dané zařízení. Rozlišujeme tři kategorie útoků. Při fyzickém útoku je potřeba mít dané zařízení fyzicky k dispozici. Další kategorií je vzdálené napadení, při kterém využíváme síť internet. Poslední možností je kombinovaný útok, při kterém se využívají obě předchozí metody.

V poslední části byly provedeny demonstrativní útoky, které mají upozornit na nedostatky operačního systému Windows a jeho verzí. V rámci bakalářské práce byly provedeny dva útoky – první z nich byl uskutečněn fyzicky k prolomení hesla uživatele. Druhým způsobem bylo napadení počítače přes síť za účelem získání plného oprávnění, neboť při plné kontrole nad zařízením může útočník provádět kteroukoli činnost bez vědomí uživatele.

V rámci praktické části bakalářské práce byla popsána doporučení. Při jejich dodržení může uživatel zastavit nebo eliminovat dopad na počítačové zařízení.

Je důležité říct, že útoků za poslední léta přibývá, a proto je nezbytné být obezřetný. Je potřeba sledovat aktuální trendy útočníků, aby bylo možné se proti novým typům útoků bránit.

SEZNAM POUŽITÉ LITERATURY

[1] Aircrack-ng. Aircrack-ng [online]. Copyright © 2012 [cit. 10.05.2021]. Dostupné z: https://www.aircrack-ng.org/

[2] Armitage [online]. Kali tools, 2014 [cit. 2021-05-05]. Dostupné z: https: //tools.kali.org/exploitation-tools/Armitage

[3] AVAST. Keylogger [online]. AVAST Software, 2016 [cit. 2021-03-28]. Dostupné z: https://www.avast.com/cs-cz/c-keylogger

[4] DEFINO, Steven a Larry GREENBLATT. *Official certified ethical hacker review guide: for version 7.1*. Boston: Course Technology, 2012, xxi, 329 s. ISBN 978-1–133-28291-4

[5] DURAČINSKÁ, Zuzana a Pavel BAŠTA. *DDoS – sofistikovaný útok nebo služba na objednávku?* IT Systems [online]. 2015, [cit. 2021-03-28]. Dostupné z: https://www.nic.cz/files/nic/doc/IT_Security_DDoS_042015.pdf

[6] ENGEBRETSON, Pat a James BROAD. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Waltham, MA: Syngress, c2011, xvii, 159 p. ISBN 15-974-9655-3.

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

[8] Hacking [online]. CZECH NEWS CENTER, ©2019 [cit. 2021-03-28]. Dostupné z: https://www.zive.cz/hacking/sc-381/default.aspx

[9] Hash. Počet-znaků.cz [online]. ©2010–2019 [cit. 2021-03-25]. Dostupné z: http://www.pocet-znaku.cz/hash

[10] HERTZOG, Raphael, Jim O'GORMAN a Mati AHARONI. *Kali Linux Revealed: Mastering the Penetration Testing Distribution.* Cornelius NC: Offsec Press, 2017. ISBN 9780997615609.

[11] Historie operačního systému GNU/Linux. Root.cz: informace nejen ze světa Linuxu [online]. [cit. 2021-05-05]. Dostupné z: https://www.root.cz/texty/historie-operacniho-systemu-gnulinux/

[12] chntpw | Remove, bypass, unlock and reset forgotten Windows password. chntpw | Remove, bypass, unlock and reset forgotten Windows password [online]. Copyright © 2006 [cit. 10.05.2021]. Dostupné z: http://www.chntpw.com/

[13] Kdo je to Hacker? | Security-Portal.cz | Bezpečnost Hacking Komunita. Security-Portal.cz | Bezpečnost Hacking Komunita [online]. Dostupné z: https://www.security-portal.cz/clanky/kdo-je-hacker?fbclid=IwAR3xlcfE4s2BBQ87bl9IR8f1maNX3dxG47bnJ4b03Cl_OGMZTYoSf-YFsVU

[14] KENNEDY, David et al. *Metasploit: The penetration Tester's Guide. San Francisco*: No Starch Press, 2011. ISBN 1-59327-288-X.

[15] KIM, Peter. *The hacker playbook 2: practical guide to penetration testing*. North Charleston (SC): Secure Planet, 2015. ISBN 978-1512214567.

[16] KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

[17] LONG, Johny a W. Aaron BAYLES. *Penetration tester's: open source toolkit*. Canada: Syngress, 2006. ISBN 978-1-59749-021-4.

[18] LYON, Gordon Fyodor. *Nmap network scanning: official Nmap project guide to network discovery and security scanning*. 1st ed. Sunnyvale, CA: Insecure.Com, LLC, c2008, xxix, 434 p. ISBN 09-799-5871-7.

[19] Metasploit For Beginners – The Basics – Modules, Exploits and Payloads [online]. Hsploit, 2017 [cit. 2021-05-05]. Dostupné z: https: / / hsploit.com/metasploit-beginners-1basics-modules-exploitspayloads/.

[20] Metody a typy testů | Integra Czech Republic. [online]. Copyright © 2018 [cit. 13.03.2021]. Dostupné z: https://www.integra.cz/cs/metody-a-typy-testu

[21] Msfcli is no longer available in Metasploit [online]. Rapid7, 2015 [cit. 2021-05-05]. Dostupné z: https://blog.rapid7.com/2015/07/ 10/msfcli-is-no-longer-available-in-metasploit/.

[22] NCKB. Sociální inženýrství. Národní centrum kybernetické bezpečnosti [online]. ©2019 [cit. 2021-03-06]. Dostupné z: https://www.govcert.cz/cs/informacniservis/doporuceni/2486-socialni-inzenyrstvi/

[23] O'DONNELL, Andy. *Rainbow Tables: Your Password's Worst Nightmare* [online]. Lifewire, 2018 [cit. 2021-05-06]. Dostupné z: https://www.lifewire.com/rainbowtables-your-passwords-worst-nightmare-2487288

[24] OREBAUGH, Angela a Becky PINKARD. *Nmap in the enterprise: your guide to network scanning*. Burlington, MA: Syngress Publishing, c2008. ISBN 9781597492416.

[25] Penetrační testy | Etický hacking | Sociální inženýrství. COMGUARD [online]. 2018 [cit. 2021-04-7]. Dostupné z: https://www.comguard.cz/sluzby/sluzby-voblasti-informacni-ict-bezpecnosti/penetracni-testy-eticky-hacking-socialniinzenyrstvi/

[26] POLANKA, Jan. *Historie Linuxu*. Západočeská univerzita v Plzni [online]. Plzeň [cit. 2021-04-07]. Dostupné z: http://home.zcu.cz/ jpolanka/SemprZPS/web/historie.html

[27] Shodan for penetration testers. Las Vegas, 2010. Dostupné z: https://www.defcon.org/images/defcon-18/dc-18-presentations/Schearer/DEFCON-18-Schearer-SHODAN.pdf

[28] UBUNTU ČESKÁ REPUBLIKA. LiveCD [online]. Ubuntu Česká republika, 2019 [cit. 2021-03-06]. Dostupné z: https://wiki.ubuntu.cz/livecd

[29] WEIDMAN, Georgia. *Penetration testing: A Hands-On Introduction to Hacking*. San Francisco: No Starch Press, 2014. ISBN 1-59327-564-8.

[30] WEIDMAN, *Georgia Penetration Testing*. Publishing house: No Starch Press, US. Release Date: June 14 2014, 495 pages. ISBN: 1593275641.

[31] *What is Kali Linux*. Kali Linux official documentation [online]. [cit. 2021-03-05]. Dostupné z: http://docs.kali.org/introduction/what-is-kali-linux

[32] ZITTA, Stanislav. *Penetrační testování*. Pardubice, 2013. Dostupné z: https://portal.upce.cz/StagPortletsJSR168/KvalifPraceDownloadServlet?typ=1&adipidno=20090. Diplomová práce. Univerzita Pardubice, Fakulta elektrotechniky a informatiky, Katedra softwarových technologií.