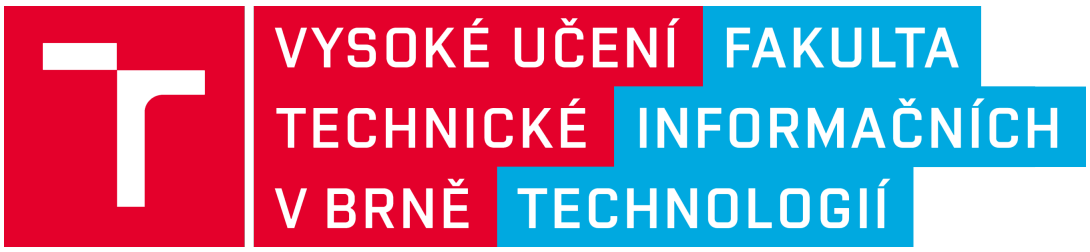
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



DHCP útoky

Projekt do předmětu Přenos dat, počítačové sítě a protokoly (PDS)

Klára Nečasová (xnecas24)

29. dubna 2018

Obsah

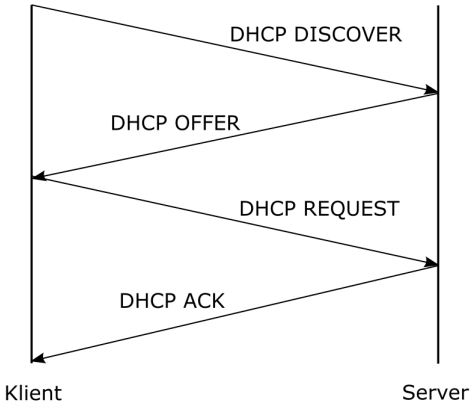
1 Úvod

Cílem projektu bylo nastudovat problematiku DHCP útoků, implementovat aplikace, které realizují DHCP útoky, konkrétně DHCP Starvation a Rogue DHCP Server, a poté demonstrovat činnost aplikací v podmínkách vlastní testovací sítě.

2 DHCP protokol

DHCP (Dynamic Host Configuration Protocol) je síťový protokol, který je využíván DHCP servery. Slouží pro dynamické přidělování různých konfiguračních údajů sítě, jako například uživatelské IP adresy, masky podstíě, IP adresy výchozí brány a IP adresy DNS serveru DHCP klientům. DHCP server nepřiděluje IP adresu klientovi natrvalo. Místo toho nastavuje dobu propůjčení, během níž může klient přidělenou IP adresu používat. Pokud chce klient využívat přidělenou IP adresu i po vypršení doby propůjčení, tak by měl pořádat DHCP server o prodloužení doby propůjčení. V případě, že tak neučiní, je IP adresa uvolněna a může být přidělena jiným klientům [7].

DHCP protokol pracuje na principu klient-server. DHCP klient (UDP, port 68) je počítač, který se připojuje do sítě a požaduje IP adresu a další konfigurační parametry. DHCP server (UDP, port 67) je program, který udržuje databázi, která například obsahuje platné IP adresy, které mohou být přiděleny klientům, nebo dobu propůjčení IP adresy [13]. Dále DHCP server reaguje na požadavky klientů a zasílá jim požadovaná data. Komunikace mezi klientem a serverem sestává z DHCP zpráv. Příklad komunikace klienta se serverem je na obrázku 1 [5].



Obrázek 1: Příklad komunikace DHCP

- **`DHCP DISCOVER`**: Nejdříve klient posílá pomocí broadcastu `DHCP DISCOVER` zprávu, pomocí které žádá server o přidělení IP adresy. Odpověď od serveru je možné rozpoznat na základě identifikátoru zprávy (hodnota pole ID obou zpráv se musí shodovat) [5].
- **`DHCP OFFER`**: Na zprávu `DHCP DISCOVER` odpovídá server broadcastem zprávy `DHCP OFFER`. Ve zprávě je uvedena nabízená IP adresa, síťová maska, doba zapůjčení adresy a další parametry. Pokud již server například nemá žádné volné IP adresy, žádost zamítne a posílá zprávu `DHCP NAK` [5].
- **`DHCP REQUEST`**: Klient na zprávu `DHCP OFFER` reaguje zprávou `DHCP REQUEST`, čímž přijme nabízenou IP adresu. V případě příjmu více zpráv `DHCP OFFER` si klient vybere server, který chce použít. Klient odesílá zprávu `DHCP REQUEST` broadcastem, aby byly všechny servery informovány, který server si klient vybral. Zpráva `DHCP REQUEST` se také používá v případě, kdy klient požaduje prodloužení doby zapůjčení IP adresy. V případě, že server žádost příjme, odešle klientovi zprávu `DHCP ACK`, čímž mu přidělí stejnou IP adresu na další časový interval [5], [4].
- **`DHCP ACK`**: Server, který odeslal zprávu `DHCP OFFER`, si označí IP adresu jako pronajatou. IP adresy, které nabízely servery, jež nebyly vybrány, jsou vráceny do jejich dostupné oblasti. Server potvrzuje volbu IP adresy pomocí zprávy `DHCP ACK`, která obsahuje další údaje týkající se konfigurace. Klient může IP adresu používat po dobu zapůjčení [5], [4].

Pokud klient zjistí, že mu server přidělil IP adresu, která se již používá, tak mu musí poslat zprávu `DHCP DECLINE` a konfigurační proces se musí opakovat. V případě, že se chce klient vzdát přidělené IP adresy, posílá serveru zprávu `DHCP RELEASE` [12].

3 Problematika DHCP útoků

Níže jsou popsány vybrané dva typy DHCP útoků, DHCP Starvation, jehož záměrem je vyčerpat rozsah IP adres legitimního serveru, a Rogue DHCP Server, kdy falešný DHCP server poskytuje klientům vlastní základní síťové parametry.

3.1 DHCP Starvation

Při útoku DHCP Starvation se útočník snaží vyčerpat všechny dostupné adresy DHCP serveru. Toho docílí tak, že odesílá velké množství DHCP zpráv, které obsahují náhodně vygenerované MAC adresy. Jedná se o útok typu *Denial of Service (DoS)*. Útok DHCP Starvation může být proveden dvěma způsoby [3], [1].

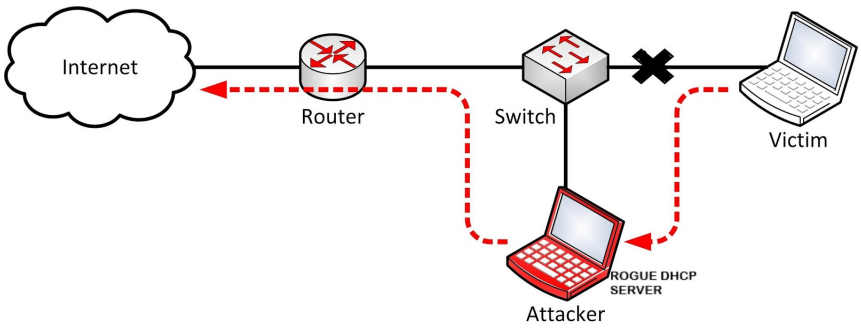
1. **`DHCP DISCOVER` attack**: Útočník odesílá velmi rychle velké množství zpráv `DHCP DISCOVER`. DHCP server není schopen rozlišit, zda se jedná o legitimní nebo falešné žádosti, a proto se snaží každé žádosti vyhovět a odesílá zprávu `DHCP OFFER`. Všechny dostupné IP adresy jsou tedy po určitou dobu zabrány útočníkem a nemohou být přiřazeny žadnému novému klientovi [3], [1].

2. **`DHCP REQUEST` attack**: Útok je důmyslnější než předchozí útok. Útočník odesílá `DHCP DISCOVER` zprávy pomaleji, takže DHCP server je schopný je zpracovat. Na zprávy `DHCP DISCOVER` reaguje server zprávou `DHCP OFFER`. Útočník poté posílá zprávu `DHCP REQUEST`, kterou potvrdí dobu zapůjčení IP adresy. Výsledkem je opět zabrání všech IP adres útočníkem, ale na delší časový interval[1].

3.2 Rogue DHCP Server

Rogue DHCP Server je sever, který je spravován útočníkem namísto síťovým administrátorem. Útočník se snaží znemožnit komunikaci mezi klientem a legitimním DHCP serverem. Posílá klientovi zprávu s falešnými informacemi (`DHCP OFFER` nebo `DHCP ACK`), která musí být klientem přijata dříve, než zpráva odeslaná legitmním serverem. Toho může docílit využitím útoku DHCP Starvation (viz kapitola 3.1). Příklad útoku Rogue DHCP Server je na obrázku 2 [1].

Útočník může zfalšovat IP adresu výchozí brány tak, že ji přiřadí svoji IP adresu. Ve výsledku tedy bude veškerý provoz klienta kontrolován útočníkem, který bude potom data přeposílat na skutečnou výchozí bránu sítě. Jedná se o typ útoku *Man in the middle*. Útočník může také zfalšovat adresu DNS serveru, čímž se dostane mezi klienta a legitimní DNS server. Díky tomu může kontrolovat obsah odpovědí DNS serveru směřujících ke klientovi. Útočník tak může přesně vybrat, kterou část komunikace podvrhne a která zůstane nezfalšovaná [1].



Obrázek 2: Útok Rogue DHCP Server

4 Obrana proti DHCP útokům

Port Security slouží k obraně proti útoku DHCP Starvation. Specifikuje maximální počet MAC adres, který je přiřazen k rozhraní přepínače. Existuje více možností, jak se může přepínač při útoku zachovat. Při překročení maximálního počtu MAC adres jsou rámce s neznámou zdrojovou MAC adresou zahazovány nebo je rozhraní vypnuto [11].

DHCP Snooping poskytuje obranu vůči útoku Rogue DHCP Server. Monitoruje DHCP zprávy, které jsou posílány klientům nebo přijímány klienty připojenými do sítě. Pokud klient přijme `DHCP ACK` zprávu od serveru, tak DHCP Snooping vytvoří záznam v databázovém souboru Binding table. Záznam obsahuje IP adresu, MAC adresu klienta, dobu zapůjčení, VLAN a rozhraní. Administrátoři tak mohou identifikovat porty, ze kterých mohou být přijímány DHCP zprávy od serveru. Odchozí linky od DHCP serveru jsou důvěryhodné, zatímco všechny ostatní přístupové porty jsou nedůvěryhodné. Pokud přepínač přijme zprávu `DHCP OFFER` nebo `DHCP ACK` na nedůvěryhodném portu, zahodí ji a zapíše do logu [2].

5 Popis implementace

Projekt sestává ze dvou aplikací, `pds-dhcpstarve` a `pds-dhcprogue`, které implementují odpovídající typ DHCP útoku, přičemž každá může být použita nezávisle na druhé. Pro implementaci programů byl využit jazyk C++ a knihovna `pcap` [9], která slouží k zachytávání síťového provozu. V projektu byla využita jak pro odesílání DHCP zpráv, tak pro postupné čtení odchycených paketů. Ukončení aplikací je možné pomocí signálu `SIGINT`. Níže jsou popsané zajímavé pasáže implementace aplikací.

5.1 DHCP Starvation

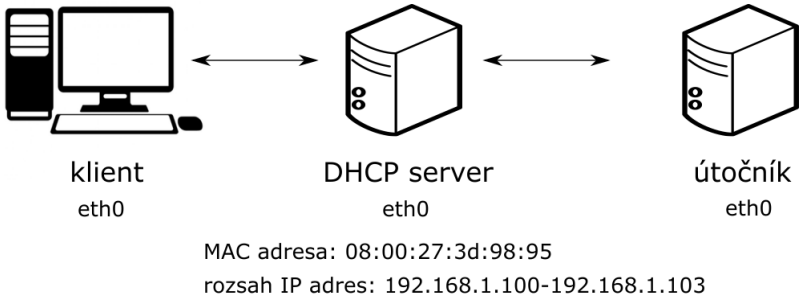
V rámci projektu byla implementována důmyslnější varianta útoku, `DHCP REQUEST` attack, která byla popsána v sekci 3.1. Nejdříve je nastaven pcap filtr, pomocí kterého je možné odchytávat komunikaci na UDP portu číslo 68. Následně je nutné zjistit MAC adresu DHCP serveru, aby bylo možné server zahltit DHCP zprávami. Zprávy `DHCP DISCOVER` a `DHCP REQUEST` obsahují zfalšovanou MAC adresu klienta a jedna komunikace pomocí čtyř DHCP zpráv je určena stejným pseudonáhodným identifikátorem. Náhodné MAC adresy sestávají ze zvoleného unikátního identifikátoru organizace [8] a pseudonáhodného identifikátoru síťové karty. Zprávy `DHCP DISCOVER` jsou generovány v určitých časových intervalech, nejpozději však po uplynutí 2000 ms, což odpovídá maximální době čekání na přidělení IP adresy. Po příjmu zprávy `DHCP OFFER` dojde k odeslání `DHCP REQUEST` zprávy. V případě příjmu zprávy `DHCP ACK` je komunikace se serverem ukončena.

5.2 Rogue DHCP Server

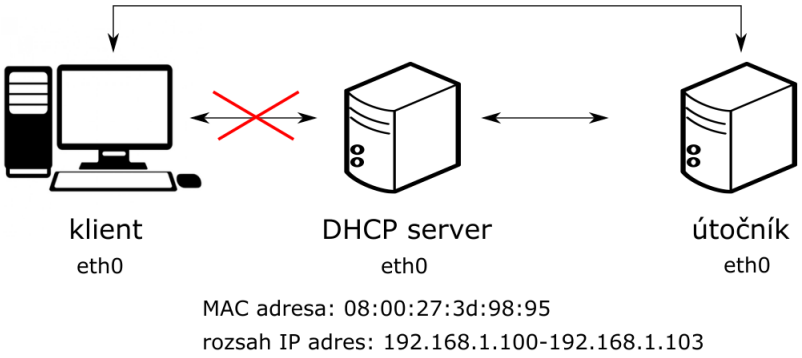
Útok Rogue DHCP Server nastává po útoku DHCP Starvation. Nejdříve je totiž potřeba vyčerpat všechny IP adresy z přiděleného rozsahu legitimního DHCP serveru. Poté může nastoupit Rogue DHCP Server, který klientům nabízí IP adresy ze svého rozsahu IP adres. Pro odesílání zpráv je využita knihovna `pcap`, příjem dat je implementován pomocí `RAW SOCKET`. Falešný server čeká na přijetí zprávy `DHCP DISCOVER` nebo `DHCP REQUEST`, a to po dobu maximálně 10 sekund. V případě, že žádná zpráva nedorazí, čekání se opakuje. Před zpracováním jakékoli DHCP zprávy je nutné ověřit, zda již nevypršela doba vypůjčení IP adresy. Na zprávu `DHCP DISCOVER` server reaguje tak, že klientovi přidělí IP adresu po dobu danou časem výpůjčky. Jelikož je potřeba po vypršení časového intervalu přidělenou IP adresu uvolnit, aby mohla být přidělena jinému klientovi, je přidělená IP adresa spolu s dobou výpůjčky uložena. Po příjmu `DHCP REQUEST` zprávy odesílá server zprávu `DHCP ACK` s podvrženými daty.

6 Demonstrace činnosti

Topologie sítě (viz obrázek 3 a 4), na které byla provedena demonstrace činnosti DHCP Starvation a Rogue DHCP Server útoku, zahrnuje počítač reprezentující legitimního klienta, legitimní DHCP server a útočníka. V rámci DHCP Starvation útoku je útočníkem klient, který po vyčerpání rozsahu IP adres legitimního DHCP serveru spustí falešný server, jež je dále využíván v Rogue DHCP Server útoku.



Obrázek 3: Topologie pro demonstraci DHCP Starvation útoku



Obrázek 4: Topologie pro demonstraci DHCP Rogue Server útoku

Nejdříve provedeme DHCP Starvation útok, jehož cílem je vyčerpat všechny IP adresy nabízené legitimním DHCP serverem. Útočník (klient) získá postupně všechny IP adresy z rozsahu DHCP serveru, poté server na přijaté `DHCP DISCOVER` zprávy přestane odpovídat, což znamená, že došlo k vyčerpání jeho rozsahu IP adres. Na obrázku 5 můžeme vidět čtyři úspěšná přidělení IP adresy útočníkovi, následované dalším odesíláním `DHCP DISCOVER` zpráv, na které však nepřišla žádná odpověď (rozsah IP adres obsahoval jen čtyři IP adresy).

70	100.375036	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0xe20dc252
73	101.376944	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP Offer - Transaction ID 0xe20dc252
74	102.357355	00	0.0.0.0	255.255.255.255	DHCP	313 DHCP Request - Transaction ID 0xe20dc252
75	102.361129	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP ACK - Transaction ID 0xe20dc252
77	103.407549	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0xeaeb2e68
80	104.408958	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP Offer - Transaction ID 0xeaeb2e68
81	105.356691	00	0.0.0.0	255.255.255.255	DHCP	313 DHCP Request - Transaction ID 0xeaeb2e68
82	105.359054	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP ACK - Transaction ID 0xeaeb2e68
84	106.405802	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0x1c3d8f15
87	107.407522	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP Offer - Transaction ID 0x1c3d8f15
88	108.358246	00	0.0.0.0	255.255.255.255	DHCP	313 DHCP Request - Transaction ID 0x1c3d8f15
89	108.361128	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP ACK - Transaction ID 0x1c3d8f15
91	109.403958	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0x179c32b
94	110.405477	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP Offer - Transaction ID 0x179c32b
96	111.352362	00	0.0.0.0	255.255.255.255	DHCP	313 DHCP Request - Transaction ID 0x179c32b
97	111.355089	00	192.168.1.10	255.255.255.255	DHCP	342 DHCP ACK - Transaction ID 0x179c32b
100	112.403709	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0x8729f316
101	115.401625	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0x1085cd40
102	118.400157	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0xab5c1f37
103	121.398963	00	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0x925c8824

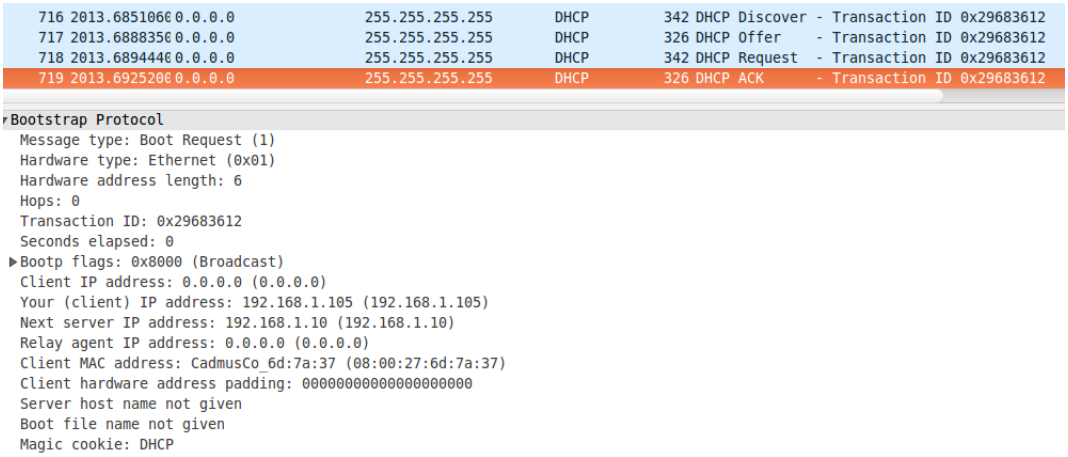
Obrázek 5: Výstup z nástroje Wireshark: přidělení čtyř IP adres útočníkovi

Poté útočník spustí Rogue DHCP Server následujícím příkazem (parametry argumentů se liší v závislosti na konfiguraci sítě):

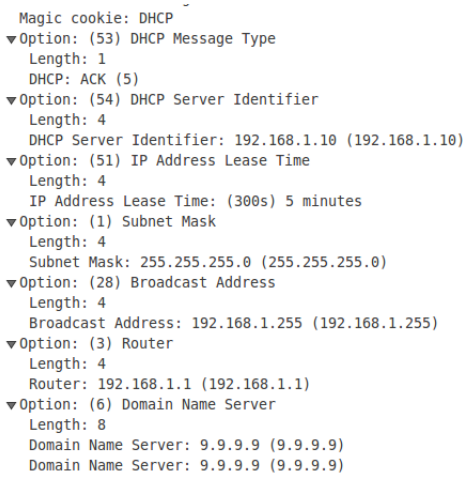
```
sudo ./pds-dhcrogue -i eth0 -p 192.168.1.100-192.168.1.105 -g 192.168.1.1 -n 9.9.9.9
-d test.example -l 300
```

Rogue DHCP Server může představovat výchozí bránu i DNS server, z čehož plyne, že může monitorovat a do jisté míry řídit komunikaci klienta (útok typu *Man in the middle* [6] nebo *Phishing* [10]).

Když klient žádá o IP adresu, je mu nabídnuta IP adresa poskytovaná Rogue DHCP Serverem. Na obrázku 6 a 7, které zobrazují výstup z nástroje Wireshark (zachycena komunikace na serveru), můžeme vidět úspěšné přidělení IP adresy klientovi (proběhla výměna všech čtyř DHCP zpráv). Dalším důkazem zdařilého přidělení je výpis dynamicky přidělené adresy rozhraní `eth0` (viz obrázek 8), kde se nastavená IP adresa shoduje s tou, kterou můžeme vidět ve výstupu z nástroje Wireshark.



Obrázek 6: Výstup z nástroje Wireshark: přidělení IP adresy klientovi, 1. část



Obrázek 7: Výstup z nástroje Wireshark: přidělení IP adresy klientovi, 2. část

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:6d:7a:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.105/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe6d:7a37/64 scope link
       valid_lft forever preferred_lft forever
```

Obrázek 8: Přidělená IP adresa rozhraní `eth0`

Výše popsaná demonstrace činnosti DHCP Starvation a DHCP Rogue Server útoku dokazuje, že útoky byly implementovány korektně. Po provedení DHCP Starvation útoku není schopen nově příchozí klient získat od legitimního DHCP severu IP adresu. V Rogue DHCP Server útoku se Rogue server vydává za legitimní DHCP server, který může sledovat, případně částečně řídit, komunikaci s klienty.

7 Závěr

V kapitole 2 je popsán princip fungování DHCP protokolu, včetně ukázky komunikace mezi DHCP klientem a DHCP serverem. Kapitola 3 objasňuje DHCP Starvation a Rogue DHCP Server útok. Způsoby, jakými je možné předcházet DHCP útokům, jsou shrnuty v kapitole 4. Kapitola 5 obsahuje zajímavé části implementace obou DHCP útoků. Činnost implementovaných aplikací je demonstrována v kapitole 6. Demonstrace probíhala ve vlastní síti tvořené virtuálními stanicemi. Pro sledování komunikace byl použit nástroj Wireshark. Byla prokázána funkčnost obou útoků, protože pomocí nich lze napadnout reálnou nechráněnou síť.

Literatura

[1] *DHCP Exploitation Guide*. https://www.whitewinterwolf.com/posts/2017/10/30/dhcp-exploitation-guide/. [Online; navštíveno 10.4.2018].

[2] *Layer 2 security – DHCP Details, DHCP Snooping*. https://orhanergun.net/2017/03/layer-2-security-dhcp-details-dhcp-snooping/. [Online; navštíveno 12.4.2018].

[3] Peter Halaška. *Generátor kybernetických útoků*, 2016. http://hdl.handle.net/11012/59938. [Online; navštíveno 10.4.2018].

[4] *Vzájemné působení klienta a serveru DHCP*. https://www.ibm.com/support/knowledgecenter/cs/ssw_ibm_i_71/rzakg/rzakgconceptinteract.htm. [Online; navštíveno 5.4.2018].

[5] *Architektura sítí, adresování, konfigurace TCP/IP*. Studijní opora předmětu ISA. [Online; navštíveno 5.4.2018].

[6] *RFC 3552: Guidelines for Writing RFC Text on Security Considerations*. https://www.ietf.org/rfc/rfc3552.txt. [Online; navštíveno 14.4.2018].

[7] *Understanding the basic operations of DHCP*. https://www.netmanias.com/en/post/techdocs/5998/dhcp-network-protocol/understanding-the-basic-operations-of-dhcp. [Online; navštíveno 5.4.2018].

[8] *OUI Lookup Tool*. https://ip.rst.im/oui/Shenzhen%20ViewAt%20Technology%20Co.,Ltd. [Online; navštíveno 12.4.2018].

[9] *Programming with pcap*. https://www.tcpdump.org/pcap.html. [Online; navštíveno 12.4.2018].

[10] *Report on Phishing*. https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf. [Online; navštíveno 14.4.2018].

[11] *How to prevent MAC flooding attacks by configuring switchport port-security*. http://www.omnisecu.com/ccna-security/how-to-prevent-mac-flooding-attacks-by-configuring-switchport-port-security.php. [Online; navštíveno 10.4.2018].

[12] *RFC 2131: DHCP*. https://tools.ietf.org/html/rfc2131. [Online; navštíveno 5.4.2018].

[13] *Technologie počítačových sítí*. http://www.cad.upol.cz/TPS_2018/prednasky/p%C5%99ed%2011.pdf. [Online; navštíveno 5.4.2018].