UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Útoky využívající Address Resolution Protocol (ARP)

Martin Petráň

Bakalářská práce
2015

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2014/2015**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin Petráň**
Osobní číslo:	**I11147**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Útoky využívající Address Resolution Protocol (ARP)**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je provést analýzu útoků na počítačovou síť využívající ARP. Autor podrobně představí protokol ARP, možnosti jeho využití v počítačové sítí a pro etický hacking. Na základě provedené analýzy autor připraví simulace popsaných útoků v laboratorním prostředí, kde jednotlivé útoky otestuje, zdokumentuje a pokusí se navrhnout řešení ochrany proti těmto útoků. Teoretická část bude použita na rozšíření wiki.upce.cz.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

PUŽMANOVÁ, Rita. TCP/IP v kostce. 2. upr. a rozš. vyd. České Budějovice: Kopp, 2009, 619 s. ISBN 978-80-7232-388-3.
HUCABY, Dave. CCNP SWITCH 642-813 official certification guide. 2. upr. a rozš. vyd. Indianapolis: Cisco Press, c2010, xxvii, 459 s. ISBN 978-1-58720-243-8.
WALKER, Matthew. CEH, Certified Ethical Hacker: exam guide : all-in-one. 2. upr. a rozš. vyd. New York: McGraw-Hill, c2012, xxii, 391 p. ISBN 00-717-7229-4.

Vedoucí bakalářské práce: **Ing. Stanislav Zitta**
Katedra softwarových technologií

Datum zadání bakalářské práce: **20. prosince 2014**
Termín odevzdání bakalářské práce: **11. května 2015**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2015

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 30. 4. 2015 Martin Petráň

Poděkování

Chtěl bych poděkovat svému vedoucímu Ing. Stanislavu Zittovi za odborné vedení, za pomoc a rady při zpracování této práce. Rovněž děkuji Fakultě elektrotechniky a informatiky Univerzity Pardubice za zpřístupnění laboratoře počítačových sítí za účelem provádění praktických experimentů. Děkuji také svým rodičům za podporu při studiu.

Anotace

Tato práce se zabývá problematikou útoků pomocí nedokonale zabezpečeného protokolu linkové vrstvy referenčního modelu ISO/OSI. Klade si za cíl popsat jak postup útoku, následky pro oběť, tak i možnosti obrany.

Klíčová slova

ARP, Man-in.the-Middle, Ettercap, SSLstrip, DAI, DHCP Snooping

Title

Attacks using the Address Resolution Protocol (ARP)

Annotation

This bachelor’s thesis discusses cyberattacks that use improperly secured ISO/OSI data-link layer protocol. It aims to describe how to process the attack, the consequences for the victim, and defense capabilities.

Keywords

ARP, Man-in.the-Middle, Ettercap, SSLstrip, DAI, DHCP Snooping

Obsah

Seznam zkratek

ACL	Access Control List
ARP	Address Resolution Protocol
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
ICMPv6	Internet Control Message Protocol version 6
IP	Internet Protocol
ISO	International Organization for Standardization
MAC	Media Access Control
MitM	Man-in-the-Middle
NAT	Network Address Translation
ND	Neighbor Discovery
OSI	Open Systems Interconnection
PAT	Port Address Translation
RA	Router Advertisment
RARP	Reverse Address Resolution Protocol
SSL	Secure Socket Layer
VLAN	Virtual Local Area Network

Seznam obrázků

Seznam tabulek

Úvod

V moderním světě se počítačové a síťové technologie staly nedílnou součástí našeho života. Nároky na dostupnost a pohodlnost stále stoupají. Moderní zaměstnanec nebo vedoucí firmy není vázán nutností setrvávat v kanceláři, firmy implementují řešení umožňující práci vzdáleně z domova nebo na cestách. Uživatelé těchto technologií by se měli řídit určitými pravidly pro přístup ke zdrojům nejen firemním, ale i osobním. Bohužel v mnoha případech jsou uživatelé buď málo poučeni o možných rizicích, nebo upřednostňují vlastní pohodlí na úkor bezpečnosti. Dnes je možné nejen ve městech narazit na mnoho takzvaných „free wi-fi“ připojení, ať už v restauraci, ve vlaku nebo autobuse. Nebezpečí může představovat i nezabezpečená nebo hůře zabezpečená domácí wi-fi síť, ale také nespokojený zaměstnanec s přístupem do intranetu firmy. Při využívání veřejných a špatně zabezpečených připojení by uživatelé měli přizpůsobit své chování, protože kdokoli z ostatních připojených klientů může využít některou z technik útoku pro získání citlivých dat a přístupových údajů.

Tato práce se zabývá typem útoků, ve kterých se útočník snaží zaujmout pozici uprostřed komunikace a získat tak přístup k citlivým datům oběti. Nejprve budou představeny podmínky, které tento typ útoku umožňují, poté samotný útok, možnosti obrany a nástroje umožňující provedení útoků.

V praktické části bude demonstrováno provedení útoku a implementace obranných mechanizmů na úrovni síťových prvků v laboratorním prostředí.

1 Etický hacking

První kapitola stručně představuje význam termínu etický hacking a penetrační testování. Pro detailnější informace odkazuje na zdroje, které se touto tematikou zabývají. Dále je představen referenční model ISO/OSI, konkrétně jeho druhá neboli linková vrstva.

1.1 Princip etického hackingu

Zabezpečení počítačové sítě je náročný úkol, který nemůže být nikdy splněn na sto procent, protože útočník je vždy ten, kdo je o krok napřed. Tomu se snaží zabránit technika zvaná „Etický hacking“. Etický hacker se snaží pomocí série pokusů nedestruktivních technik prolomit zabezpečení sítě a nalézt tak slabé místo v infrastruktuře. Slabé místo může, ale nemusí mít technický charakter, může se jednat například o zaměstnance, který nedbá bezpečnostních zásad, nebo o veřejně přístupné nijak nebo slabě zabezpečené připojení k síti. Útoky jsou v dnešní době nejen stále častější, ale jsou i mnohem sofistikovanější a konečná cena za špatné zabezpečení může být mnohokrát vyšší než investované peníze do infrastruktury a personálu, který se stará o bezpečnost. Etický hacker pomocí penetračních testů prověří, kde je slabé místo, kterému je potřeba věnovat zvýšenou pozornost.

Penetrační test je prováděn systematicky a věnuje se všem aspektům zabezpečení od síťové infrastruktury až po personál podniku. Úkolem takového testu je včas odhalit pokud možno všechny slabiny, které by potencionální útočník mohl využít ve svůj prospěch. Metodikou provádění penetračního testu se zabývá například organizace ISECOM v dokumentu OSSTMM [1] popisujícím stejnojmennou metodologii. Problematikou penetračního testování se podrobněji zabývá Stanislav Zitta ve své diplomové práci [2], obsahující i praktické ukázky.

1.2 Obecné metody Etického hackingu

Jak už bylo zmíněno výše, penetrační test se skládá z připravené posloupnosti kroků. Po základní fázi jednání s klientem o podobě testu jsou na řadě fáze samotného testování. Nejdříve je nutné shromáždit co největší objem dat o subjektu. Tato činnost zahrnuje například skenování portů veřejně přístupných zařízení, jako jsou web servery (nejprve je nutné zjistit, zda jsou servery majetkem firmy a tudíž také cílem testování), ale také získávání všech dostupných informací o firmě a jejích zaměstnancích ať už ze zdrojů, které poskytuje informační systém samotné firmy nebo ze sociálních sítí. Mezi potencionální slabiny zabezpečení patří také to jakým způsobem, nebo zda vůbec, je řešeno přihlašování pracovníků do informačního systému nebo VPN. Špatně řešené přihlašování může mít za následek úplné prolomení bezpečnosti bez ohledu na kvalitu zařízení jako firewall, IPS apod., mezi špatné řešení lze například uvést náchylnost na SQL injection nebo XSS (*Cross site scripting*). Případnou slabinou by byla situace, kdy útočník získal přihlašovací údaje do systému, následně zjistil, že stejné údaje mohou být použity pro přihlášení do SSL VPN a díky tomuto přístupu získá vše potřebné pro přihlášení do vnitřní sítě pod legitimním uživatelským jménem.

V další fázi by se etický hacker pomocí zjištěných údajů pokusil prolomit zabezpečení sítě všemi možnými technikami, které mu získané informace umožňují provést. Pokud například pomocí útoku využívající protokol ARP získá přihlašovací údaje zaměstnance, jeho činnost v síti může zůstat neodhalena, jelikož přihlášení uživatelé nejsou příliš podezřelí, a s přístupem k firemnímu e-mailu a využitím technik tzv. sociálního inženýrství může získat další možnosti pro přístup do vnitřní sítě. Mezi další možnosti patří například využití slabin v aplikacích nebo operačních systémech.

Pokud je cíl úspěšně infiltrován, je potřeba zjistit, k jakým datům se může potenciální útočník dostat po prolomení zabezpečení. Možnosti takového útočníka jsou závislé na zabezpečení vnitřní sítě podniku. Jestliže je zabezpečení nedostačující, útočník může získat systémová práva v operačních systémech serverů nebo uživatelských stanic a tím nad nimi získat plnou kontrolu, špatně zabezpečená databáze může mít za následek únik citlivých informací nebo možnost měnit údaje v databázi. Bezpečnost počítačových sítí by se proto neměla soustředit pouze na pomyslnou hranici mezi intranetem a internetem, ale mělo by se počítat s prolomením tohoto zabezpečení a tím pádem s implementací ochranných mechanizmů i uvnitř sítě. Vnitřní ochranu by měla také zajišťovat firemní bezpečnostní politika, která by měla vynucovat určité minimální požadavky (jako například kvalita a délka hesla) a definovat způsob přístupu k vnitřním firemním zdrojům.

Etickým hackingem se podrobně zabývá autor Matthew Walker ve své publikaci [3].

2 Linková vrstva modelu ISO/OSI a její protokoly

V této kapitole je pospána linková vrstva modelu ISO/OSI a protokoly ARP (*Address Resolution Protocol*), RARP (*Reverse Address Resolution Protocol*) a ICMPv6 (*Internet Conotrol Message Protocol version 6*). Pochopení funkce těchto protokolů je klíčové pro porozumění problematiky útoků, které využívají slabiny ve zmíněných protokolech.

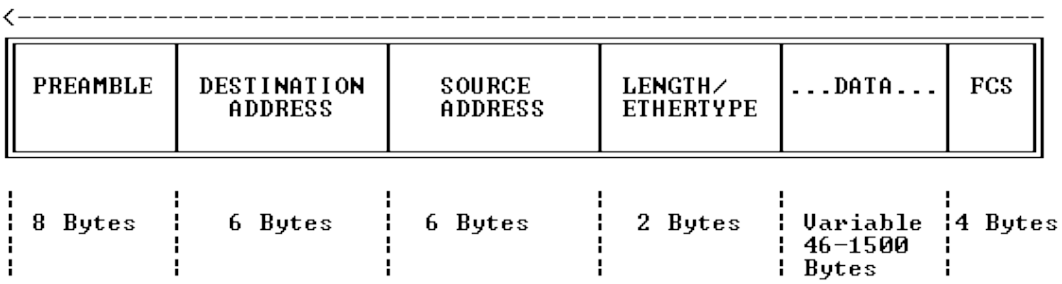
2.1 Linková vrstva a její bezpečnost

Referenční model ISO/OSI, neboli mezinárodní normu ISO 7498, vypracovala standardizační organizace ISO (*International Organization for Standardization*) ve snaze standardizovat počítačové sítě. Model je členěn do sedmi vrstev podle funkcí, kde vyšší vrstva využívá služeb vrstev nižších. Přehledný popis lze nalézt například v knize [4] autorky Rity Pužmanové.

Tabulka 1 - Referenční model ISO/OSI

Aplikační vrstva
Prezentační vrstva
Relační vrstva
Transportní vrstva
Síťová vrstva
Linková vrstva
Fyzická vrstva

Linková vrstva někdy také nazývaná spojová, využívá služby přenosu jednotlivých bitů, kterou jí poskytuje fyzická vrstva. Samotná linková vrstva má pak na starosti přenos tzv. rámců (řádově stovky bytů) vždy mezi dvěma přímo sousedícími systémy. Komunikace je zajištěna pomocí fyzických adres neboli media access control (MAC) adres. MAC adresa má délku 48 bitů, vyjadřuje se v šestnáctkovém tvaru a skládá se ze dvou částí o délce 24 bitů: kód výrobce neboli OUI (*Organization Unique Identifier*) a samotné označení fyzického rozhraní. Adresy se přidělují s cílem naprosté jedinečnosti, kódy výrobců spravuje a přiděluje organizace IEEE, zbývající část adresy pak přiděluje sám výrobce zařízení.[4] Při tvorbě rámce je nutné znát cílovou MAC adresu (obrázek znázorňuje formát rámce technologie Ethernet).



Obrázek 1 - Formát rámce ethernet

Bezpečnostní slabinou nejen linkové vrstvy je fakt, že v počátcích síťových technologií byly vyvíjeny protokoly nutné pro provoz zcela nezabezpečeně, jelikož se nepočítalo s tak plošným nasazením, jakým je dnešní internet. Pokud tedy systém odesílající data vytváří rámec, musí k získání cílové MAC adresy využít nezabezpečeného protokolu ARP (cílovou MAC adresou je myšlená adresa přímého cíle na stejném segmentu sítě nebo adresa směrovače na cestě k cíli). Samotný protokol ARP neobsahuje žádný mechanismus pro ověření, zda obsah zprávy není podvržen útočníkem. Tento nedostatek se začal řešit až v pozdějších letech pomocí zabezpečovacích technologií, které budou popsány níže.

2.2 Address resolution protocol

ARP neboli *Address Resolution Protocol* se používá při znalosti cílové IP adresy stanice pro nalezení příslušné fyzické (*MAC*) adresy. Zdrojová stanice nejprve prohledá paměť pro uchování informací o mapování fyzických a síťových adres (*ARP cache*), pokud se příslušná adresa v paměti nenachází, je nutné využít protokol ARP. Zdrojová stanice sestaví rámec ARP, do kterého vloží svoji fyzickou a IP adresu, IP adresu cíle, se kterým chce komunikovat a rámec odešle na všesměrovou (*broadcast*) fyzickou adresu. Rámec obdrží všechny stanice na stejném segmentu sítě, na kterém se nachází zdroj ARP zprávy. Po obdržení rámce příjemce zkontroluje, zda IP adresa uvedená v ARP zprávě odpovídá adrese přidělené jeho rozhraní, pokud ano odpoví odesláním zprávy obsahující jeho fyzickou adresu. Odpověď protokolu ARP je adresována pouze zdrojové stanici (zdroj ARP dotazu). Jestliže stanice zjistí, že IP adresa v původním dotazu není adresou přidělenou jejímu rozhraní, tak ARP dotaz ignoruje. Pokud se cíl komunikace nachází v jiné síti, ARP dotaz je vyslán pro zjištění fyzické adresy směrovače, který slouží jako výchozí brána pro danou síť.

Protokol ARP má určitá omezení, díky nimž stanice nezahlcuje síť dotazy pro každý rámec, pro který nezná cílovou IP adresu. Prvním z těchto omezení je, že si stanice musí pamatovat, jaké dotazy již vyslala, jestliže je připraven rámec k zapouzdření a jediné co chybí, je cílová fyzická adresa, je možné, že aplikace připravila další data, která vyžadují odeslání na stejnou cílovou IP adresu. Takové rámce je potřeba zařadit do fronty a počkat na odpověď na původní ARP žádost namísto generování žádosti pro každý nově vytvořený rámec. Další omezení zabraňující záplavě dotazů na fyzickou adresu je to, že stanice může vyslat pouze jeden stejný dotaz za sekundu.

Pro větší efektivitu práce tohoto protokolu jsou získané informace dočasně uloženy do tak zvané ARP cache. Tato paměť uchovává informace o mapování fyzických a síťových adres získaných protokolem ARP, typicky po dobu 10 nebo 20 minut. Při dosažení maximální doby platnosti záznamu mapování se údaj vymaže a pro další komunikaci je nutné opět využít protokol ARP. Aktualizace této paměti probíhá nejen aktivně po přijetí odpovědi na dotaz u zdrojové stanice, ale také pasivně díky obsažené zdrojové fyzické i síťové adrese v ARP dotazu. Ve speciálním případě tzv. *gratuitous ARP*, stanice sama vysílá zprávy pro aktualizaci paměti ostatních uzlů sítě.

Rámec ARP nemá záhlaví pevné délky, protože protokol lze využít na různých síťových technologiích, proto je nutné na začátku zprávy uvádět délky následujících polí. Odpověď se od dotazu v zásadě neliší, cílová stanice pouze přidá do zprávy svojí fyzickou adresu a změní kód zprávy z dotazu na odpověď.

Tabulka 2 - Formát zprávy ARP

Typ přenosového média	Typ protokolu	Délka adresy MAC	Délka síťové adresy	Kód zprávy	Zdrojová adresa MAC	Zdrojová síťová adresa	Cílová adresa MAC	Cílová síťová adresa

Protokol ARP a jeho činnost je podrobně popsán organizací IETF v dokumentu RFC 826 [5] (STD 37) a RFC 1027 [6].

2.3 RARP

Protokol RARP (*Reverse Address Resolution Protocol*) se využívá v případě, kdy stanice zná pouze svoji fyzickou adresu a potřebuje zjistit IP adresu. Taková situace vzniká například u stanic, které nemají pevné disky, tudíž postrádají možnost uchovat svoji IP adresu pro natažení operačního systému přes síť. Protokol RARP v tomto případě umožňuje stanici komunikovat po síti výhradně na základě své fyzické adresy.

RARP je odvozen z protokolu ARP a používá i stejný formát zprávy (viz Tabulka 2). RARP není omezen na získání pouze vlastní IP adresy, pomocí tohoto mechanismu lze získat jakoukoliv adresu IP při znalosti fyzické adresy.

V souvislosti s RARP je nutné čtenáři přiblížit také RARP server. Stanice sloužící jako RARP server obsahuje databázi fyzických adres s přiřazenými IP adresami. Server naslouchá RARP dotazům odesílaným všem stanicím v síti, které obsahují zdrojovou fyzickou adresu a na základě záznamů v databázi vyplní pole síťové adresy žadatele a odešle odpověď na adresu stanice, která vygenerovala dotaz.

Jelikož vlastní fyzická adresa není dostatečná informace pro plnou komunikaci v síti, je protokol RARP většinou nahrazen komplexnějšími protokoly jako BOOTP nebo DHCP.

Organizace IETF popisuje protokol RARP v RFC 903 [7] (STD 38).

2.4 ICMPv6

Tato podkapitola čtenáře nejprve velmi stručně seznámí s protokolem IPv6 a poté představí jeho součást a to konkrétně protokol ICMPv6, který je v prostředí IPv6 používán podobně jako protokol ARP popsaný výše. Pro pochopení práce ICMPv6 není nutná detailní znalost kompletního standardu IPv6, k jeho hlubšímu porozumění může posloužit publikace autora Pavla Satrapy [8].

Postupným rozvojem počítačových sítí bylo nutné řešit některé nedostatky protokolu IPv4, zejména nedostatek adresního prostoru. Nová verze protokolu nabízí 128 bitů dlouhé adresy oproti 32 bitům předchozí verze. Již z délky adresy vyplývá, že IPv6 adresace umožňuje začlenit 48 bitů dlouho fyzickou adresu přímo do síťové adresy. Mezi další výhody plynoucí z délky adresy IPv6 patří možnost jejího hierarchického přidělování a tím efektivnější směrování mezi sítěmi. Přechod na nový internetový protokol je proto mezi odborníky vítanou událostí, kterou ale nelze realizovat ze dne na den.

Pro potřeby této práce je nyní vhodné popsat způsob získání a tvorby adresy protokolu IPv6. Tato adresa se typicky dělí na dvě části, prefix a identifikátor rozhraní, zapisuje se v šestnáctkové soustavě, kde se šestnáctibitové skupiny oddělují dvojtečkou. Prefix je stanici přidělován směrovačem, identifikátor rozhraní pak stanice sama odvodí od fyzické adresy rozhraní pomocí mechanizmu EUI-64. Pro názornost bude uveden jednoduchý příklad.

Nechť je globální směrovací prefix přidělený síti například 2001:0008:85A3::/48. K této části adresy se přidá identifikátor podsítě o délce 16 bitů, tím je získán 64 bitů dlouhý prefix například 2001:0008:85A3:4220::/64. Nyní je možné odvodit zbytek adresy podle fyzické adresy přidělené danému rozhraní pomocí mechanismu EUI-64. Pokud je fyzická adresa 00:AC:50:C2:12:23, na je mezi třetí a čtvrtou dvojici hexadecimálních znaků vloženo 16 bitů s hodnotou FFFE a dochází k inverzi druhého bitu v adrese, který rozlišuje globální identifikátory od lokálních. Výsledný identifikátor rozhraní má tak podobu 002AC:50FF:FEC2:1223, spojením s prefixem pak vznikne finální verze IPv6 adresy, jejíž zápis lze podle definovaných pravidel zkrátit na 2001:8:85A3:4220:2AC:50FF:FEC2:1223. Kompletní informace o IPv6 adresaci lze nalézt v RFC 4291 [9] z roku 2006.

Nyní po objasnění několika základních prvků nového protokolu lze přejít k jedné z jeho součástí, ICMPv6. „Protokol řídících hlášení ICMPv6 má stejné funkce a používá stejný formát jako jeho předchůdce pro IPv4 ale číslo protokolu je 58 nikoli 1 jako u IPv4.“ [4]. ICMP (jak verze ICMPv4, tak i ICMPv6) slouží k přenosu specifických chybových a informativních zpráv. V IPv6 nahrazuje protokol ARP mechanismus pro objevování sousedů, neboli *Neighbor Discovery*, dále jen ND. ND využívá pro svoji funkčnost zprávy protokolu ICMPv6 typu 133 – 137.

Tabulka 3 - Typy zpráv ICMPv6

133	*Router Solicitation (Výzva směrovači),* stanice si po startu vyžádá adresy všechny nejbližších směrovačů.
134	*Router Advertisment (Ohlášení směrovače)*, informace od směrovače.
135	*Neighbor Solicitation (Výzva sousedovi)*, zjišťuje fyzické adresy sousedů na základě síťových adres.
136	*Neighbor Advertisment (Ohlášení souseda)*, odpověď na *Neighbor Solicitation.*
137	*Redirect (Přesměrování)*, indikace lepší cesty do cílové sítě.

Zjišťování fyzických adres pomocí ND mechanismu probíhá následovně. Nejprve vysílající stanice sestaví ICMPv6 zprávu typu 135 výzva sousedovi, kterou odešle na adresu vyzývaného uzlu. Adresa vyzývaného uzlu je skupinová adresa sestavená z pevně daného prefixu FF02:0:0:0:0:1:FF00::/104, za který se připojí posledních 24 bitů IPv6 adresy pro niž hledáme fyzickou adresu. Každá IPv6 stanice naslouchá skupinovým zprávám určeným pro její rozhraní. Na přijatou zprávu odpovídá zprávou ohlášení souseda (ICMPv6 typ 136), z níž se tazatel dozví fyzickou adresu souseda. Kompletní specifikace ND je obsažena v RFC 4861.

Jak možná již vyplynulo z výše uvedeného, samotný ND nijak neřeší otázku bezpečnosti, a to konkrétně zda odpověď na výzvu sousedovi přišla z legitimního zdroje. Tento nedostatek se snaží napravit *Secure Neighbor Discovery* (dále jen SEND). SEND k dosažení ověření původce zprávy využívá jiný typ identifikátoru rozhraní než typ EUI-64 popsaný výše. Jako identifikátor rozhraní je v tomto případě použit standart CGA (*Cryptographically Generated Address*), kde jako základ identifikátoru rozhraní slouží veřejný klíč vlastníka stanice spojený s několika dalšími údaji jako například prefix adresy. Z těchto údajů je vygenerován *hash* pomocí algoritmu SHA-1, z jehož výstupu se využívá prvních 64 bitů jako identifikátor rozhraní. Při objevování sousedů je pak připojena doplňující volba s veřejným klíčem odesilatele, která umožňuje snadno ověřit pravost a původ zprávy. Celou zprávu podepisuje soukromý klíč vlastníka, což zaručuje, že v případě odposlechnutí zprávy útočníkem, nemůže být zpráva modifikována, jelikož útočník nezná soukromý klíč odesilatele zprávy. SEND byl definován v roce 2005 v RFC 3971.

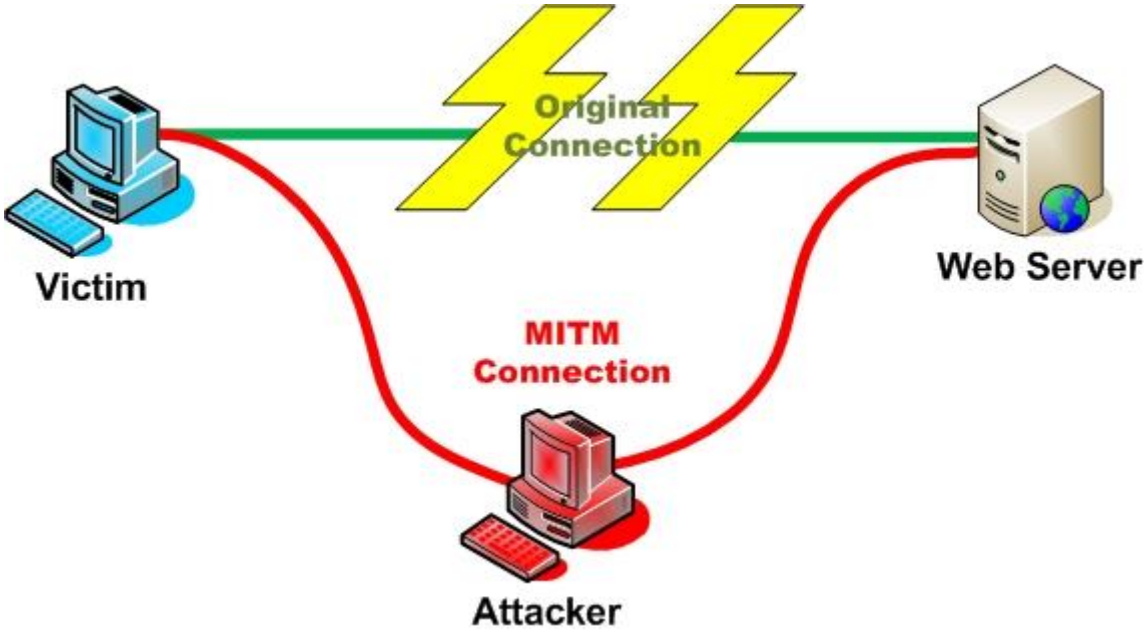
3 Útoky využívající protokoly pro mapování adres

Třetí kapitola seznámí čtenáře s některými útoky, které využívají bezpečnostní slabiny v protokolech používaných pro mapování adres. Nejprve bude přiblížen obecný princip útoku *Man-in-the-Middle* a nebezpečí, která z něj plynou. Poté bude popsán postup útoků v jednotlivých podkapitolách.

3.1 Man-in-the-Middle

Jako první bude představen koncept takzvaných *Man-in-the-Middle* nebo také *MitM* útoků. Tento typ útoku spoléhá na schopnost útočníka dostat se doprostřed komunikace mezi obětí a serverem. Útok tohoto typu je snadno proveditelný za pomoci nástrojů a technik popsaných níže. Organizace OWASP zmiňuje *man-in-the-middle* na svých webových stránkách [10].

Teoreticky lze popsat postup a následky útoku asi takto. Nejprve musí útočník zařídit, aby oběť odesílala veškerou komunikaci určenou pro server právě jemu. Tohoto lze docílit například technikou zvanou *ARP poisoning*. Pokud útočník úspěšně provede tuto část, je nutné, aby stejného efektu docílil i na straně serveru, tudíž aby server odesílal veškerá data patřící oběti na adresu útočníka. Tímto je zajištěno odposlouchávání obousměrné komunikace za předpokladu, že útočník zajistí správné přeposílání dat oběma směry.



Obrázek 2 - Ilustrace útoku MitM [20]

Za předpokladu, že útočník úspěšně provedl útok, má nyní přístup k veškeré komunikaci mezi obětí a serverem (často se jedná spíše o komunikaci mezi obětí a výchozí bránou sítě kde se útočník i oběť nacházejí). V takovém případě se útočník může bez problémů dostat k citlivým údajům, nebo dokonce některé údaje v komunikaci měnit. Čtení a záměně citlivých dat lze zabránit pomocí šifrování například využitím VPN nebo zabezpečené verze protokolu HTTP, neboli HTTPS. Samotné HTTPS nedokáže zaručit bezpečnost komunikace, jak bude popsáno níže, je nutné implementovat další mechanismy pro zaručení bezpečnosti komunikace s webovým serverem.

3.2 Gratuitous ARP

Nevyžádané ARP zprávy (*Gratuitous ARP*) jsou žádosti nebo odpovědi, které nejsou při normálním chování podle standardu ARP nutné. Nevyžádané ARP zprávy jsou popsány například na webu tvůrců programu Wireshark [11]. V případě nevyžádané ARP odpovědi se jedná o zprávu, které nepředcházel žádný ARP dotaz. Nevyžádaný ARP dotaz má vyplněná pole zdrojové a cílové IP adresy na adresu odesilatele dotazu. Nevyžádané ARP mají praktická využití například při změně adresy stanice. Taková stanice vyšle nevyžádanou ARP zprávu, aby informovala ostatní zařízení o změně. Mezi další využití například patří vyslání nevyžádané ARP zprávy při startu stanice, aby ostatní zařízení v síti měla připravený mapovací záznam v jejich ARP tabulkách, nebo vyslání informace o fyzické adrese přepínači. V neposlední řadě může nevyžádaná ARP zpráva pomoci odhalit konflikt IP adres.

V rámci útoků *man-in-the-middle* popsaných výše jsou nevyžádané ARP zprávy využívány jako prostředek pro změnu ARP tabulek oběti a serveru nebo směrovače tak, aby záznamy v těchto tabulkách zaručovaly útočníkovi úlohu prostředníka v komunikaci. Toho lze dosáhnout vysláním nevyžádané ARP odpovědi na adresu oběti, informující o změně fyzické adresy. Taková zpráva pak obsahuje původní IP adresu směrovače nebo serveru, fyzická adresa je ale změněna na adresu útočníka. Výsledkem toho je, že oběť vytvoří IP paket se správnou IP adresou, nicméně jej zapouzdří do rámce linkové vrstvy s cílovou fyzickou adresou útočníka. Tímto způsobem lze protokol ARP využít k provedení *man-in-the-middle* útoku, pokud se útočník nachází na stejné síti jako oběť.

3.3 ARP poisoning

Jak bylo popsáno výše, protokol ARP udržuje záznamy mapování síťových a fyzických adres v ARP tabulce, kterou má uloženou v paměti zvané *ARP cache*. Záznamy v této tabulce jsou udržovány po určitou dobu typicky 10 nebo 20 minut, po vypršení této doby je nutné pomocí ARP dotazu obnovit záznam v tabulce. Mechanismus zvaný *gratuitous ARP* umožňuje stanicím vyslat zprávu, která aktualizuje ARP tabulku jiné stanice.

Chování protokolu ARP využívá technika útoku zvaná *ARP poisoning* nebo také *ARP spoofing*. Za normální situace má stanice uloženou hodnotu fyzické a síťové adresy brány nebo serveru ve své ARP tabulce. Při vytváření standardu tohoto protokolu nebylo bráno

v potaz potencionální zneužití jeho funkcionalit. Z toho vyplývá, že protokol ARP nijak neověřuje původce vyžádaných ani nevyžádaných zpráv.

Samotný útok tohoto typu začíná vytipováním oběti. K takovým účelům lze využít jeden z mnoha nástrojů schopných skenovat rozsah sítě, na které se aktuálně zařízení nachází. Pokud útočník vybral cíl pro útok a stejným způsobem zjistil adresu výchozí brány sítě, může přistoupit k samotnému provedení útoku.

V první řadě je třeba „otrávit“ tabulky mapování adres protokolu ARP, tak aby komunikace mezi nimi probíhala výhradně přes útočníkovo zařízení. Využije se vygenerování nevyžádané ARP zprávy, která zajistí, aby stanice odesílala data na linkové vrstvě právě útočníkovi. Vzhledem ke skutečnosti, že ARP odpovědi jsou vysílány na specifickou adresu, ostatní stanice v síti, které nejsou pro útočníka zajímavé, komunikují naprosto běžným způsobem. Po úspěšném „otrávení“ cílů musí útočník zajistit, aby byla komunikace úspěšně odesílána a nedošlo tak k odhalení útoku. Tuto funkci provádějí níže popsané nástroje automaticky, lze jí ale zajistit i manuálně za pomoci pravidel směrování (v operačním systému Linux se jedná o pravidla iptables).

Jakmile je zajištěn tok dat přes útočníkovo zařízení a jejich správné směrování, může útočník začít odposlouchávat nebo měnit komunikaci oběti. K těmto účelům lze využít například nástroj Wireshark, který přehledným způsobem zobrazuje veškerou síťovou komunikaci, obdobně lze využít například nástroj tcpdump v Linuxu. Oba zmíněné nástroje umožňují efektivní filtrování a ukládání získaných dat do souborů pro pozdější analýzu, takže je pro útočníka snadnější uložit veškerou komunikaci oběti do souboru a později z těchto informací získat maximální možný užitek, ať už se jedná o přístupová jména a hesla nebo o citlivé informace jiného druhu.

3.4 Neighbor discovery attack

Útok podobný tomu, jenž byl popsán v předchozí kapitole, je útok využívající slabiny v *Neighbor Discovery* v rámci IPv6, kde útočník musí zfalšovat zprávy protokolu ICMPv6.

Útok probíhá velmi podobně jako v předchozím případě, rozdílem je typ zprávy využitý k přesměrování toku dat oběti. V předchozím případě byla využita nevyžádaná ARP odpověď jako nástroj pro změnu záznamu mapování fyzických a síťových adres v ARP paměti oběti. Pro provedení stejného útoku v prostředí IPv6 je nutné využít zprávy protokolu ICMPv6, konkrétně se jedná o zprávu *Neighbor advertisment* neboli oznámení souseda (ICMPv6 typ 136). Tato zpráva je za normální situace odpovědí na dotaz a obsahuje síťovou a fyzickou adresu stanice generující odpověď. Stejně jako v předchozím případě lze tuto zprávu odeslat i bez předcházejícího dotazu jako oznámení o změně údajů v adresaci. Této skutečnosti může opět využít útočník ve svůj prospěch a efektivně přesměrovat veškerou komunikaci mezi obětí a například bránou na svojí stanici. Jeremy Stretch tuto problematiku shrnul na webu packetlife.net v článku s názvem *IPv6 Neighbor Spoofing* [12].

V dalších kapitolách bakalářské práce budou popsány možnosti obrany proti tomuto útoku, jeden z mechanismů byl zmíněn již výše, jedná se o bezpečnou implementaci *Neighbor Discovery* neboli *Secure Neighbor Discovery* (SEND).

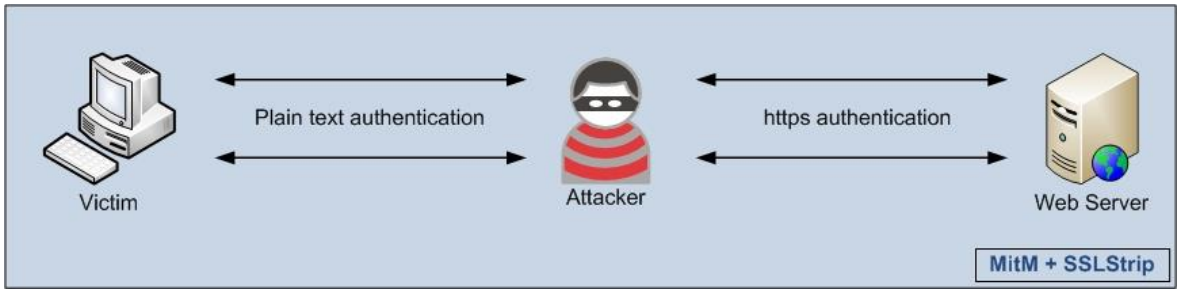
3.5 Útoky využívající pozice man-in-the-middle

Zmíněné techniky útoku umožňují útočníkovi získat výhodnou pozici, ze které je schopen odposlouchávat a měnit komunikaci oběti. Kromě jednoduchého odposlouchávání komunikace lze využít další postupy k získání citlivých dat. Některé z těchto postupů jsou popsány v následujících podkapitolách.

3.5.1 SSL strip

V roce 2009 na konferenci Black Hat DC představil Moxie Marlinspike [13] techniku zvanou jako *SSL Striping*. Tato metoda útoku spočívá ve schopnosti útočníka převést komunikaci zabezpečeného protokolu HTTPS na nezabezpečenou verzi HTTP.

Jak již bylo zmíněno výše, při klasickém *man-in-the-middle* útoku není útočník schopen přečíst komunikaci, která je šifrovaná. *SSL strip* umožňuje útočníkovi rozdělit komunikaci mezi obětí a serverem na dvě oddělené části. Oběť při odeslání dotazu na webový server typicky používá nezabezpečený protokol HTTP, nebo je na zabezpečené stránky přesměrovávána z nezabezpečeného připojení. Pokud tedy úvodní dotaz od klienta a odpověď serveru útočník zachytí, pak nástroj *SSL strip* zajistí rozdělení komunikace na část oběť-útočník a útočník-server. Oběť nevědomky komunikuje s útočníkovou stanicí pomocí nezabezpečeného protokolu, tedy odesílá všechna data bez šifrování. Server je nastaven tak, aby pro komunikaci citlivých dat vyžadoval zabezpečené připojení, proto útočník přeposílá data serveru pomocí zabezpečeného protokolu, ze strany serveru se tak zdá být všechno v pořádku. Situaci ilustruje následující obrázek.



Obrázek 3 - SSL strip [21]

Při provádění útoku může být útočník odhalen pozorným uživatelem, který se stal obětí tohoto útoku. Pokud se totiž uživatel například přihlásí na emailovou službu, kde je samozřejmě očekávána zabezpečená komunikace, v prohlížeči si může povšimnout, že je využíván protokol HTTP namísto HTTPS. Je nutné podotknout, že většina běžných uživatelů toto nekontroluje vůbec, nebo kontrolují pouze ikonu zámku před URL v prohlížeči. Ikona ovšem není spolehlivým indikátorem bezpečného připojení. V pozdějších verzích nástroje *SSL strip* je přidána možnost odeslání ikony zámku do prohlížeče oběti, což může navodit falešný pocit bezpečí.

3.5.2 DNS spoofing

Pro představení tohoto útoku je nutno čtenáře nejdříve stručně seznámit s protokolem DNS a jeho funkcí.

Protokol DNS (*Domain Name System*) zajišťuje v počítačových sítích převod IP adres na doménová jména a naopak. Systém DNS je organizován v hierarchické struktuře takzvaných DNS serverů, které mezi sebou komunikují záznamy mapování doménových jmen na síťové adresy. Pokud uživatel ve svém webovém prohlížeči zadá adresu serveru pomocí doménového jména, například „www.priklad.cz“, tak stanice musí vyslat žádost na překlad zadaného jména na IP adresu DNS serveru, který požadovanou adresu zašle v odpovědi na tento dotaz. Překlad doménových jmen je nutný z toho důvodu, že počítačové sítě nerozumí doménovým jménům a komunikace v nich probíhá výhradně na základě adres.

Samotný *DNS spoofing* využívá možnost pozměňování respektive odpovídání útočníkovou stanicí na odposlechnuté zprávy. Po zachycení dotazu na překlad doménového jména útočník odpoví vygenerovanou odpovědí, která z pravidla překládá požadovanou doménu na IP adresu útočníka nebo zřízeného podvodného serveru. Pro provedení tohoto útoku je k dispozici celá řada nástrojů umožňující reagovat pouze na určité dotazy, jinými slovy, útočník nahlédne do dotazu DNS a pokud se oběť dotazuje na určitý server, odesílá odpověď, jestliže se oběť dotazuje na z útočníkova pohledu nezajímavý server, dotaz přepošle legitimnímu DNS serveru. Stanice oběti po přijetí odpovědi DNS od útočníka komunikuje s podvodným serverem, který považuje za legitimní. Takový server většinou obsahuje věrnou kopii webových stránek, na které se oběť dotazovala. Pokud je takovýto útok dobře naplánován a útočník si dá práci s přípravou zfalšovaných webových stránek, klient se většinou nijak nedozví, že své údaje zadává do podvodné webové aplikace.

3.5.3 Surf jacking

Pokud se útočník nachází uprostřed komunikace, která probíhá přes šifrované spojení má možnost získat platné *session ID* neboli identifikátor relace, který mu umožní „unést“ relaci oběti tak, že server bude považovat příchozí zprávy od útočníka za zprávy od legitimního klienta. Tohoto lze využít například pro získání dalších citlivých údajů nebo pro změnu nastavení účtu oběti, například lze uvézt změnu hesla nebo doručovací adresy v případě internetového obchodu.

Průběh útoku je následující. Útočník získal pozici uprostřed komunikace, ale není schopen číst šifrované zprávy oběti adresované pro *https://zabezpecenastranka.com*. Pokud tedy oběť ve stejnou dobu otevře další záložku v prohlížeči a pokusí se přistoupit na webové stránky pomocí nezabezpečeného připojení například *http://nezabezpecenastranka.com,* útočník je schopen tento dotaz zachytit a vytvořit odpověď, která informuje prohlížeč oběti o přesunutí dotazovaných webových stránek na adresu *http://zabezpecenastranka.com* tedy na nezabezpečenou verzi prvních stránek. Prohlížeč zná identifikátor relace pro spojení s první webovou stránkou a tak ho použije i pro nezabezpečenou komunikaci.

Tímto útočník dosáhl toho, že identifikátor relace, který mu umožní vydávat se za oběť je odeslán bez použití šifrování, není pro něj tedy problém ho zachytit a zneužít. Útok popisuje například publikace OWASP [10].

Obrana proti tomuto útoku může být implementována například přidáním atributu *secure* při odesílání identifikátoru relace v *cookie*. Tím dosáhneme toho, že prohlížeč neodešle *session ID* přes nezabezpečené připojení. Další možností obrany je zamezení útoku *man-in-the-middle*.

4 Návrh ochrany proti útokům využívajícím protokol ARP

V této kapitole bude popsáno několik mechanismů ochrany proti již popsaným metodám útoku.

4.1 DHCP snooping

DHCP snooping je technologie primárně používaná na obranu proti vložení falešného DHCP serveru do sítě. Jestliže je útočník schopen vložit vlastní DHCP server do sítě, může stanicím rozesílat falešné informace, zejména týkající se adresy výchozí brány a adres DNS serverů. Tímto způsobem může provést *man-in-the-middle* útok nebo přeložit doménové jméno na IP adresu jeho vlastního serveru.

DHCP snooping řeší tyto problémy následujícím způsobem. Na přepínači je nastaveno pro každé rozhraní, zda je důvěryhodné nebo není, neboli zda se na tomto rozhraní může nacházet DHCP server nebo ne. Po zapnutí této funkce jsou všechna rozhraní v nedůvěryhodném stavu, postačí tedy definovat důvěryhodná rozhraní. Další z funkcí zmíněné technologie je možnost limitovat počet DHCP požadavků na přidělení adresy pro jednotlivé stanice. Tento limit stanovuje, kolik požadavků může stanice vyslat za vteřinu, pokud je tento limit překročen rozhraní se přepne do stavu *error-disabled* a blokuje veškerou komunikaci, dokud není obnoveno správcem do původního stavu. Schopnost limitovat počet požadavků umožňuje zabránit vyčerpání rozsahu přidělovaných adres. Pokud je rozsah adres vyčerpán útočníkem, další legitimní uživatel, který by se připojil k síti, by neobdržel IP adresu a nebyl by tak schopen komunikovat.

DHCP snooping udržuje tabulku mapování přidělovaných IP adres a fyzických adres stanice, která si výpůjčku vyžádala. Tabulka obsahuje například také dobu, po kterou je vypůjčená adresa platná. Tuto tabulku využívá také technologie popsaná v následující podkapitole.

4.2 Dynamic ARP inspection

Dynamic ARP inspection neboli DAI pracuje podobně jako předchozí technologie. Stejně jako DHCP snooping, i DAI klasifikuje rozhraní jako důvěryhodná nebo nedůvěryhodná. Jakákoliv ARP zpráva, která dorazí na nedůvěryhodné připojení, je tímto mechanismem zkontrolována, zda obsahuje platná data. Kontrola probíhá pomocí tabulky vybudované funkcí DHCP snooping, proti které se kontroluje IP adresa a fyzická adresa obsažená v ARP zprávě. Pokud se jedná o platnou kombinaci, zpráva je odeslána dále, v případě falešné zprávy vytvořené útočníkem za účelem provedení útoku se zpráva zahazuje a generuje se logovací zpráva dle nastavení logování na příslušném přepínači. Zprávy přicházející na důvěryhodné rozhraní nepodléhají kontrole.

Obdobně jako v předešlém případě je základní nastavení po zapnutí funkce takové, že všechna rozhraní jsou považována za nedůvěryhodná. Pro správnou funkci je tedy nutné

přepnout rozhraní propojující síťové prvky, jako je směrovač nebo další přepínač, do důvěryhodného stavu.

Stejně jako v případě technologie DHCP snooping nabízí DAI možnost limitovaní. To v tomto případě specifikuje maximální povolené množství ARP zpráv za vteřinu. V případě překročení daného limitu se rozhraní chová totožně jako v předchozí situaci, tedy přepne na chybový stav a blokuje veškerou komunikaci.

Oba zmíněné mechanismy, DAI i DHCP snooping, tak i doplněk popsaný v následující podkapitole, vysvětluje kniha doporučená pro profesionální síťovou certifikaci společnosti Cisco [15].

4.3 ARP access list

V případě, že se v sítí nachází stanice se staticky přidělenou adresou připojená na nedůvěryhodné rozhraní, je nutné funkci DAI oznámit, že taková stanice existuje.

Toho lze docílit využitím mechanismu *ARP access list*, zkráceně ARP ACL. Konfigurace ARP ACL probíhá upřesněním páru fyzické a IP adresy a následně jeho předáním funkci DAI.

Vytvoření ARP ACL a specifikování páru fyzické a IP adresy lze provést následující sérií příkazů:

```
Switch(config)# arp access-list <Název>
Switch(config-acl)# permit ip host <IP adresa> mac host <Fyzická adresa>
```

Po vytvoření ARP ACL jej předáme funkci DAI tímto příkazem:

```
Switch(config)# ip arp inspection filter <Název ACL> vlan <VLAN>
```

Chování mechanismu DAI pak bude upraveno tím způsobem, že příchozí ARP zpráva je nejdříve zkontrolována na shodu se záznamem v ARP ACL, pokud není shoda nalezena, zpráva je kontrolována proti tabulce mechanismu DHCP snooping. Jestliže je k předchozímu příkazu přidáno klíčové slovo *static,* nebude prověřována dynamicky vytvořená tabulka, pokud tedy nebude nalezena shoda v ARP ACL, zpráva bude zahozena bez další kontroly.

4.4 RA Guard

V prostředí nového standardu internetového protokolu, IPv6, jsou funkce protokolu ARP vykonávány protokolem ICMPv6. Podrobnější popis postupů získání fyzické adresy a typů zpráv využívaných k tomuto účelu je obsažen v kapitole 2.4 ICMPv6.

Na síťových prvcích, především na přepínači, lze implementovat mechanismy, které zabrání šíření nežádoucích zpráv typu *Router Advertisment* (ohlášení směrovače nebo zkratkou RA). Tento typ zprávy, pokud by se mohl volně šířit sítí, umožňuje útočníkovi

předstírat, že jeho stanice je směrovač a tím oklamat oběť tak, aby odesílala veškerou komunikaci na útočníkovu fyzickou adresu.

Tímto mechanismem je *Router Advertisment Guard* neboli RA Guard. Nastavení probíhá pomocí specifikace politik zacházení se zprávami typu *router advertisment*. RA Guard nabízí tři možnosti chování. První z těchto možností je *host,* která zaručuje zahození všech zpráv typu *router advertisment*. Tato politika je vhodná pro rozhraní připojená ke koncovým zařízením. Druhou možností je specifikovat politiku s názvem *router,* ta provádí kontrolu každé ICMPv6 zprávy a zároveň povoluje zprávy *router advertisment*. Při využití této možnosti lze dále specifikovat, který zdroj může tyto zprávy využívat. Posledním typem politiky je *trust*, tento typ neprovádí žádnou kontrolu a povoluje všechny zprávy.

```
Switch(config)# ipv6 nd raguard policy <název>
Switch(config-ra-guard)# device-role host/router/trusted-port
```

Vytvořená politika se pak přiřadí rozhraní nebo VLAN.

```
Switch(config)# interface GigabitEthernet0/0
Switch(config-if)# ipv6 nd raguard attach-policy <název>
```

Na všech rozhraních přepínače, na kterých se nebude nacházet připojení ke směrovači, tudíž nejsou očekávány zprávy typu RA, se přidělí příslušná politika, útočníkovi tak bude zabráněno v provedení útoku.

4.5 Ochrana na úrovni operačního systému

Ochrana proti útokům pomocí ARP protokolu může být implementována i na úrovni operačního systému. Toto řešení není vždy aplikovatelné a od uživatele operačního systému vyžaduje pokročilejší znalosti.

V prostředí operačního systému Microsoft Windows lze použít definování statického záznamu v ARP tabulce [19]. Tento způsob obrany je efektivní ve stabilním prostředí, nejčastěji například ve firemní síti. Méně efektivní bude u přenosných zařízení, která se často přemísťují mezi různými sítěmi. Uživatel by pak v každé síti musel nejdříve zjišťovat fyzickou a IP adresu výchozí brány, vytvořit statický záznam pro nový směrovač, smazat starý záznam a až poté začít připojení využívat. Statické přidání záznamu do ARP tabulky lze provést následujícím příkazem:

```
arp -s <IP adresa> <Fyzická adresa>
```

V prostředí systému Linux má příkaz pro přidání statického záznamu do ARP tabulky stejnou podobu. Linuxové operační systémy navíc v základní konfiguraci ignorují *gratuitous ARP*. Toto nastavení lze změnit změnou hodnoty v souboru určujícím, zda operační systém příjme všechny ARP zprávy (hodnota 1) nebo nepřijme nevyžádané odpovědi (hodnota 0). Změnu lze provést následujícím příkazem:

```
echo 0 > /proc/sys/net/ipv4/conf/all/arp_accept
```

Samotné ignorování nevyžádaných ARP odpovědí ale nezaručuje ochranu proti ARP útokům. Útočník může odeslat zfalšovaný ARP dotaz, podle kterého si příjemce změní záznam v ARP tabulce, tak aby vyhovoval útočníkovi. Tento typ útoku se prakticky neliší od vysílání nevyžádaných odpovědí, k dosažení cíle je pouze použito vyslání zfalšovaného ARP dotazu s vědomím, že cílová stanice využije tento dotaz pro pasivní aktualizaci ARP tabulky. Z těchto důvodů zůstává jedinou spolehlivou metodou obrany definování statického ARP záznamu.

4.6 HTTP strict transport security

Pokud zabezpečení na úrovni lokálních síťových prvků selže nebo není vůbec implementováno, může útočník snadno provést základní fázi útoku a získat pozici uprostřed komunikace. V takovém případě může využít nástroje SSL strip pro efektivní odposlouchávání zabezpečeného připojení.

Technologie HTTP strict transport security neboli HSTS, dává možnost ochrany před tímto typem útoku ze strany serveru. Popisovaný bezpečnostní standard pro internetovou komunikaci spočívá v přinucení klienta komunikovat výhradně pomocí zabezpečeného připojení. Jako nedostatek lze zmínit, že pro efektivní práci tohoto standardu je nutné aby HSTS bylo podporováno prohlížečem, nebo aby klient využíval zabezpečené verze protokolu DNS tzv. DNSsec.

Důvodem těchto nedostatků je, že klient se o nutnosti komunikovat přes zabezpečené připojení nemusí dozvědět, pokud útočník zachytí první zprávu, ve které je klient informován serverem o nutnosti využití HTTPS pro komunikaci.

Řešení pomocí podpory v internetových prohlížečích spočívá v integrovaném seznamu serverů, které implementují technologii HSTS. Přestože zmíněné řešení není ideální je to lepší než se problémem nezabývat, neboť útočník může získat přístup ke stanici oběti a seznamy modifikovat. Jako další nevýhodu podpory v prohlížečích je nutné zmínit poměrně složitou implementaci, neboť tvůrci prohlížeče musí zjišťovat, zda daný server používá tuto technologii či nikoliv, pokud se záznam nenachází v seznamu a na dotyčnou stránku přistupuje uživatel poprvé nebo po uplynutí platnosti dynamického záznamu, útočník si odchycením první zprávy zajistí ideální podmínky k útoku. V neposlední řadě je také nutné uvést, že ne všechny prohlížeče tuto technologii implementují. Jako příklad prohlížeče bez podpory HSTS lze uvést Internet Explorer od společnosti Microsoft.

Řešení pomocí protokolu DNSsec naráží na problém nedostatečného rozšíření využívání tohoto protokolu. Tato skutečnost se v budoucnu nejspíše změní, avšak s širším využitím DNSsec bude také stoupat snaha o jeho prolomení, což může mít za následek vytvoření nového typu útoku, který umožní padělat zprávy protokolu DNSsec.

5 Nástroje používané pro provádění útoků

Kapitola představuje nástroje umožňující provedení útoku typu *man-in-the-middle*. Zmíněné nástroje automatizují vytvoření nežádoucí ARP zprávy a její odeslání na adresu oběti. Navíc poskytují přehledné grafické rozhraní, čímž umožňují útok provést bez jakýchkoliv hlubších znalostí o protokolech.

5.1 Ettercap

Jako první bude představen nástroj Ettercap používaný v operačních systémech typu Linux. Ettercap byl původně vyvíjen pouze pro odposlouchávání komunikace na lokální síti, nicméně během jeho vývoje byly přidávány další a další funkce a výsledný produkt má tedy mnohem více funkcí.

Po zapnutí režimu odposlechu je možné provést útok *man-in-the-middle.* Jakmile je získána pozice uprostřed komunikace, nabízí Ettercap automatické zachytávání citlivých údajů široké škály protokolů, jako příklady lze uvést SSH1, FTP, ICQ, TELNET, SMB, LDAP, HTTP a další. Navíc umožňuje provádět detekování operačního systému, služeb a otevřených portů oběti, bez odesílání paketů, tedy čistě díky odposlouchávání komunikace v síti. Pokud je útok veden proti zabezpečenému připojení HTTPS, Ettercap nabízí možnost zachytit certifikát serveru a dynamicky vytvořit nový, obdobný, který bude následně odeslán oběti. Tento typ útoku nicméně vyžaduje, aby uživatel potvrdil, že certifikátu důvěřuje, jelikož certifikát odeslaný touto metodou není podepsaný certifikační autoritou. To snižuje efektivitu útoku neboť je od oběti vyžadována další akce, která budí podezření, že něco není v pořádku.

Další z funkcí tohoto softwaru je možnost filtrovat komunikaci podle předem definovaných filtrů, nebo měnit její obsah. Všechny akce i části komunikace jsou přehledně logovány a umožňují tak zkušenějšímu útočníkovi provádět i sofistikovanější typy útoků.

Obrázek 4 - Grafické uživatelské rozhraní Ettercap

Grafické rozhraní Ettercapu je intuitivní a pro základní provedení útoku postačí krátký návod, volně dostupný na internetu. Při provádění pokročilejších útoků lze zvolit ovládání pomocí příkazů a vstupních souborů obsahujících útočníkem definované filtry. Pro manipulaci s údaji v rámcích a zprávách ARP je nutné spouštět Ettercap s právy uživatele root.

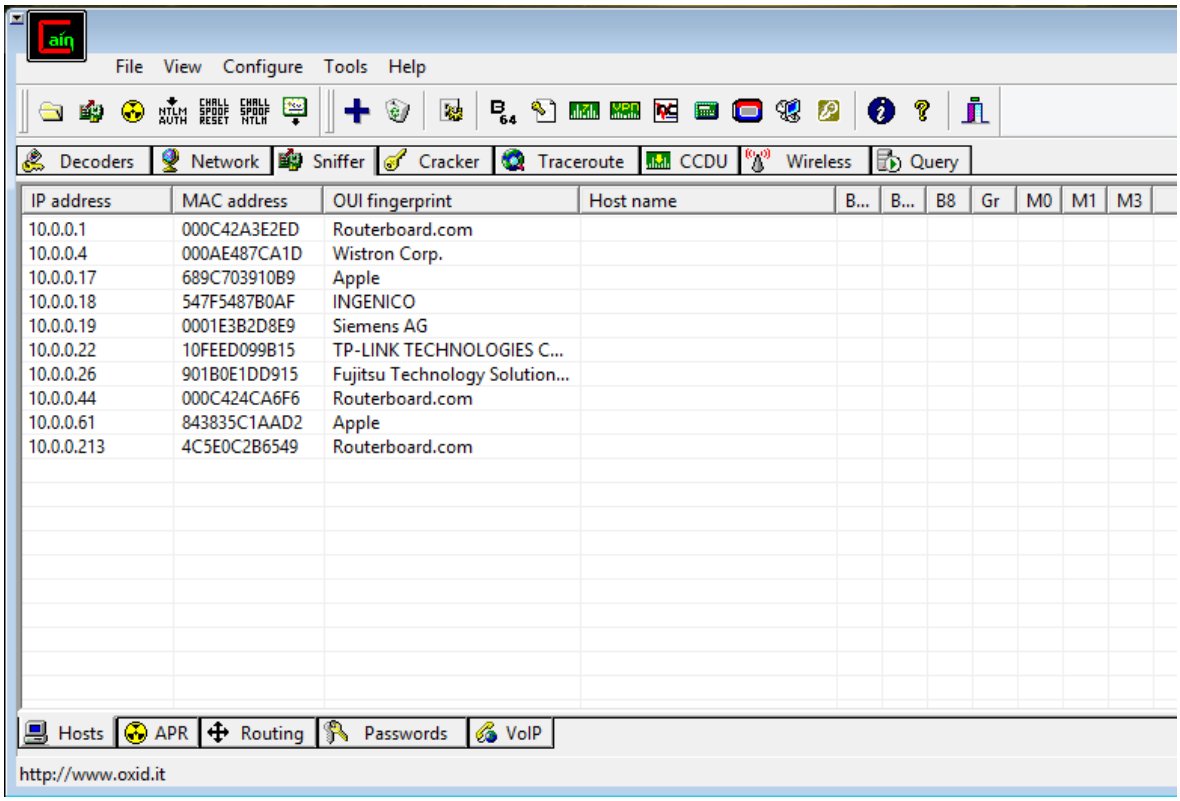
Závěrem lze tedy shrnout, že nástroj Ettercap se velice snadno ovládá pomocí grafického uživatelského rozhraní, což umožní provádět odposlouchávání a útoky uživatelům bez technických dovedností. Pro zkušené uživatele nabízí mnoho rozšíření a funkcí, které mohou útok rozšířit a zefektivnit. Nástroj také umožňuje provádění *man-in-the-middle* útoků i pomocí jiných metod jako je *ICMP redirect* nebo provedení útoku v prostředí IPv6. Další informace lze nalézt na webových stránkách projektu [17] nebo v manuálových stránkách, případně v nápovědě grafického rozhraní.

5.2 Cain & Abel

Cain & Abel je volně dostupný program určený pro obnovu hesel v prostředí operačního systému Microsoft Windows. K tomuto účelu využívá techniky jako například slovníkové nebo *brute force* útoky, kdy je snaha získat heslo pomocí otestování co největšího množství možných kombinací znaků. Jako další lze jmenovat možnost obnovy hesla z různých pamětí *cache* nebo pomocí odposlouchávání sítě. Autor projektu, Massimiliano Montoro, upozorňuje, že program byl vyvíjen s úmyslem usnadnit práci správcům sítí nebo vyšetřovatelům provádějícím forenzní činnost [16].

Nejnovější verze tohoto softwaru umožňuje provádět *ARP poisoning* a tím efektivně umožňuje provést *man-in-the-middle* útok.

Ovládání programu je jednoduché a v uživatelském rozhraní se lze snadno orientovat. Tato skutečnost však může umožnit provádět útok i lidem bez technických znalostí.



Obrázek 5 - Uživatelské rozhraní Cain & Abel

Na obrázku je znázorněno uživatelské prostředí pro provádění útoku pomocí ARP protokolu. Pro provedení útoku je nejprve nutné zapnout *sniffing* neboli odposlouchávání veškeré komunikace na síti. Poté lze provézt prohledání lokální sítě, které zobrazí veškerá nalezená zařízení v síti (viz Obrázek 4). Následně jsou vybrány cíle útoku a spuštěn *ARP poisoning*. Jakmile je získána pozice uprostřed komunikace Cain & Abel automaticky prohledává HTTP dotazy na případné citlivé údaje. Ty jsou pak zobrazeny v záložce *Passwords*.

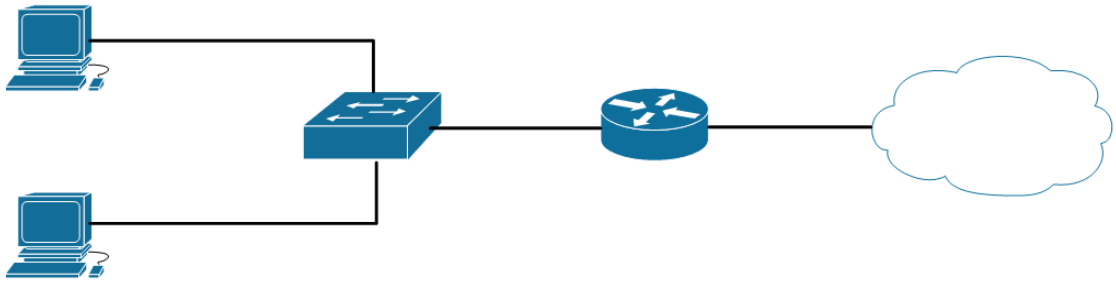
Cain & Abel tak představuje velmi snadno ovladatelný nástroj, který celý proces útoku plně automatizuje a umožňuje tak provádění útoku naprosto každému.

6 Praktická ukázka útoků a ochrany

V následující části bude demonstrováno samotné provedení útoku včetně ukázky útoku typu DNS spoofing a využití nástroje SSL strip pro získání jména a hesla oběti pro přihlášení k emailové službě. V dalším názorném příkladu bude předvedeno využití ochrany proti předvedenému útoku, konkrétně výše popsané mechanismy DHCP snooping a DAI.

6.1 Topologie sítě a konfigurace zařízení

Praktická část byla realizována s pomocí síťových prvků určených pro výuku v univerzitní laboratoři. Zvolena byla co nejjednodušší topologie postačující pro názornou ukázku útoku a obrany proti němu. Útočníkova stanice využívá operační systém Kali Linux. Jedná se o volně dostupný operační systém, který má předinstalované nástroje pro penetrační testování, mezi těmito nástroji také výše zmíněný Ettercap. Operačním systémem na stanici oběti je Windows 7. Síťové prvky směrovač (*router*) a přepínač (*switch*) jsou zařízení firmy Cisco, konkrétně se jedná o modely Catalyst 2960 a směrovač řady 2800. V topologii se jak útočník, tak i oběť nachází ve stejné síti, pro jejich přímou komunikaci se tedy nevyužívá směrovač. Z důvodu demonstrace využití nástroje SSL strip je jedno rozhraní směrovače připojeno do internetu. Díky tomu lze demonstrovat odposlechnutí přihlašovacích údajů nebo jiných citlivých dat.



Obrázek 6 - Topologie sítě

Směrovač byl nakonfigurován tak, aby poskytoval stanicím připojeným do vnitřní sítě IP adresy pomocí protokolu DHCP. Toho bylo docíleno následujícími konfiguračními příkazy:

```
Router(config)# ip dhcp excluded-address 172.16.0.1 172.16.0.10

Router(config)# ip dhcp pool PRIV
Router(dhcp-config)# network 172.16.0.0 255.255.255.0
Router(dhcp-config)# default-router 172.16.0.1
```

První z příkazů zajišťuje vyloučení prvních deseti adres z celkového rozsahu dostupného pro přidělování adres. Je nutné zajistit, aby se služba DHCP nepokusila přidělit například adresu, kterou používá směrovač. Po tomto příkazu následuje nastavení samotného přidělování adres. Jméno rozsahu si lze libovolně zvolit. Příkaz network určuje podsíť, ze

které budou adresy přidělovány. Poslední příkaz nastavuje adresu směrovače, ta bude zaslána stanicím jako adresa výchozí brány.

Následují příkazy pro nastavení rozhraní na směrovači:

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address dhcp
Router(config-if)# ip nat outside

Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 172.16.0.1 255.255.255.0
Router(config-if)# ip nat inside
```

První rozhraní je určeno pro připojení k internetu, adresu směrovač získá pomocí DHCP protokolu. Pro připojení k internetu je také nutné překládat vnitřní adresy na vnější, k tomu slouží technologie NAT. Pro pochopení funkce technologie NAT lze odkázat například na web howstuffworks.com [14]. Aby NAT věděl, kde je vnitřní a kde vnější síť, je nutné na příslušných rozhraních určit jejich polohu. K tomu slouží druhý z příkazů. V rámci konfigurace vnitřního rozhraní je nutné zadat IP adresu. Adresa bude sloužit jako výchozí brána pro stanice ve vnitřní síti. Dále také podle adresy rozhraní směrovač ví, kam bude přidělovat adresy pomocí protokolu DHCP.

Konfigurace zmíněného překladu adres (NAT):

```
Router(config)# access-list 1 permit 172.16.0.0 0.0.0.255

Router(config)# ip nat inside source list 1 interface FastEthernet0/0
overload
```

Nejprve je nutné pomocí příkazu *access list* určit, pro které zdrojové IP adresy se má převádět překlad. V druhém příkazu je pak směrovači řečeno, že zdrojové adresy určené prvním příkazem se budou překládat na adresu rozhraní připojeného do internetu. Jedná se o variantu NAT kde je překlad všech vnitřních IP adres prováděn na jedinou adresu pomocí čísel portů, v tomto případě na adresu rozhraní FastEthernet 0/0. Tento mechanismus se nazývá *Port Address Translation* zkráceně PAT.

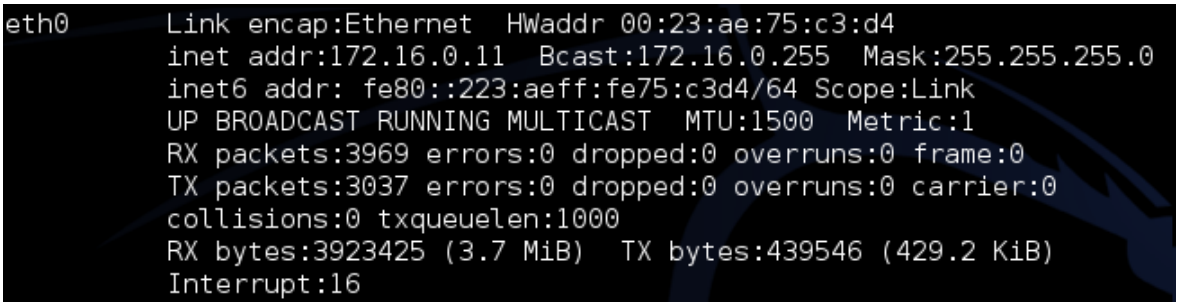
Poslední nutnou částí konfigurace směrovače je určení směrování:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.169.0.1
```

Tímto příkazem určíme, že všechny pakety s cílovou adresou jinou než přímo připojenou směrovači mají být odeslány přes rozhraní připojené k internetu. Zmíněným postupem je zaručeno propojení vnitřní sítě s internetem.

Obě stanice jsou nastaveny tak, aby získávaly IP adresu dynamicky pomocí protokolu DHCP. Pro úplnost následující obrázky znázorňují přidělené IP adresy a fyzické adresy obou stanic.

Obrázek 7 - Konfigurace stanice oběti



Obrázek 8 - Konfigurace stanice útočníka

6.2 Demonstrace útoku na nezabezpečené síti

V této kapitole bude názorně předveden útok pomocí nástroje Ettercap. Útočník úspěšně získá pozici uprostřed komunikace mezi obětí a výchozí bránou, následovat bude ukázka využití nástroje SSL strip a útoku typu DNS spoofing. Alternativně lze pro provedení ARP útoku využít i následující příkaz.

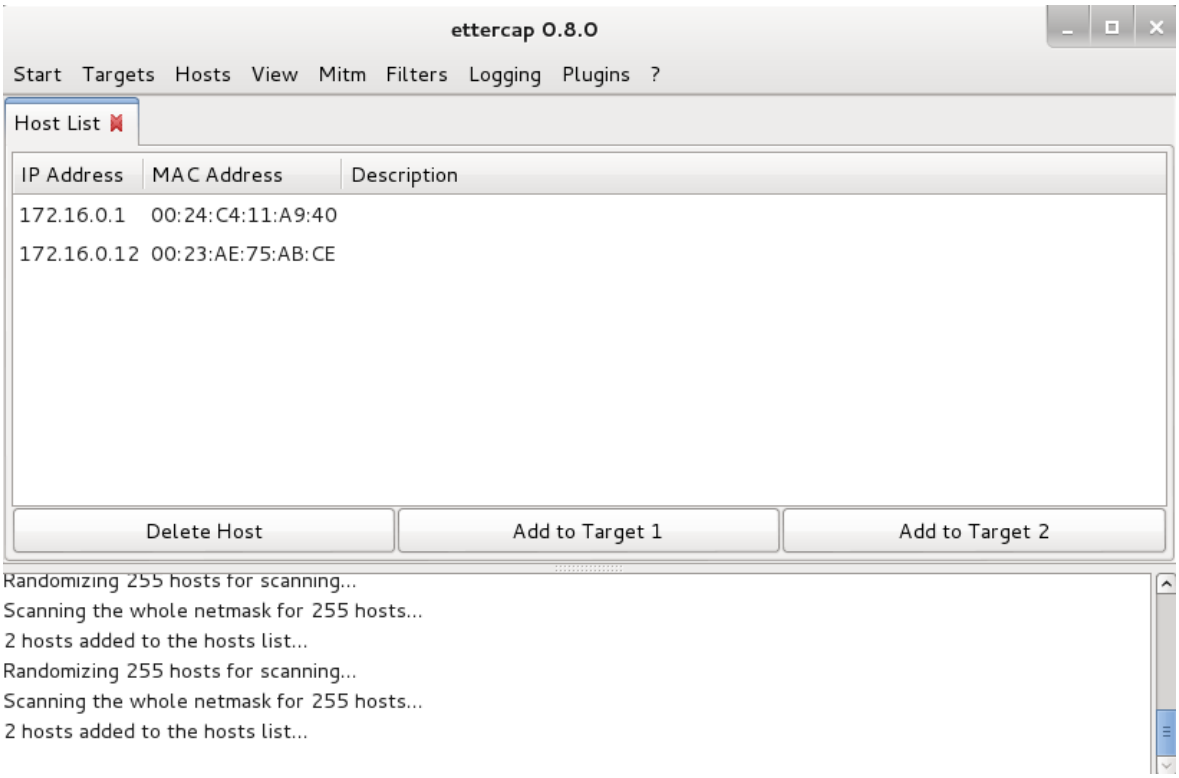
```
arpspoof -i <rozhraní stanice> -t <IP oběti> <IP výchozí brány>
```

Nejprve je zobrazen stav ARP tabulky na straně oběti:

Obrázek 9 - ARP tabulka Windows 7

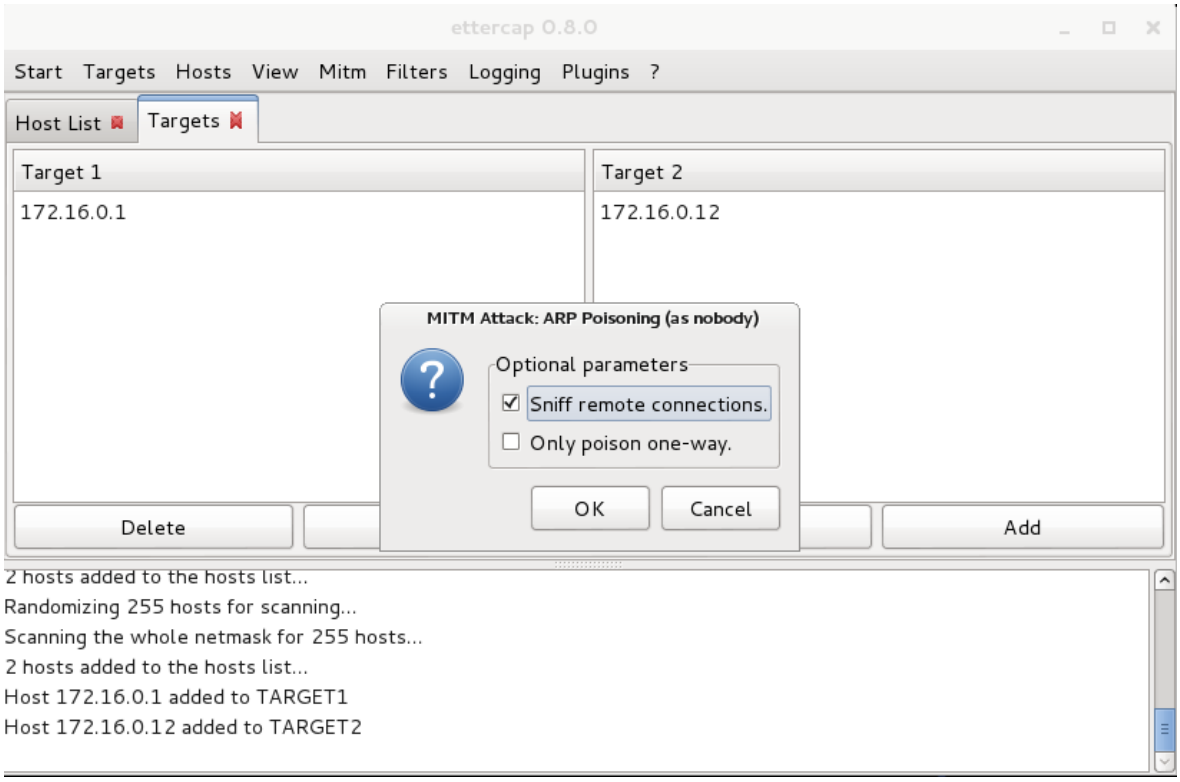
Z tabulky je zřejmé, že stanice oběti nemá doposud žádný záznam odpovídající stanici útočníka.

Na straně útočníka je nyní spuštěn výše popsaný nástroj Ettercap. Útok je zahájen detekováním ostatních zařízení v síti.



Obrázek 10 - Ettercap detekce zařízení

Z obrázku je patrné, že v testované síti se nachází pouze dvě zařízení. První je detekován směrovač, druhé ze zařízení je oběť budoucího útoku. Jak již bylo popsáno, pro úspěšné provedení útoku je nutné, aby byly nežádoucí ARP zprávy zaslány oběma stranám komunikace. Označíme obě zařízení jako první, respektive druhý cíl.



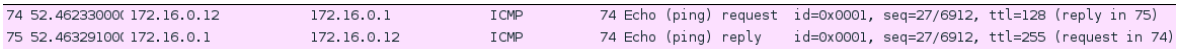
Obrázek 11 - Cíle a typ útoku

Po označení cíle je nutné zvolit typ útoku, pro úspěšné odposlechnutí všech možných citlivých údajů zvolíme první z nabízených alternativ. Ta umožňuje odposlouchávat komunikaci v obou směrech. Po potvrzení dialogu zobrazeného na obrázku Ettercap automaticky provede útok. O úspěchu útoku se můžeme přesvědčit z výpisu ARP tabulky na straně oběti.

```
Rozhraní: 172.16.0.12 --- 0xb
  internetová adresa    fyzická adresa        typ
  172.16.0.1            00-23-ae-75-c3-d4     dynamická
  172.16.0.11           00-23-ae-75-c3-d4     dynamická
  172.16.0.255          ff-ff-ff-ff-ff-ff     statická
  224.0.0.22            01-00-5e-00-00-16     statická
  224.0.0.252           01-00-5e-00-00-fc     statická
  239.255.255.250       01-00-5e-7f-ff-fa     statická
  255.255.255.255       ff-ff-ff-ff-ff-ff     statická
```

Obrázek 12 - ARP tabulka oběti při útoku

Z výpisu tabulky je patrné, že útok proběhl úspěšně. Jako první záznam je zobrazena IP adresa výchozí brány, u které je ale uvedena fyzická adresa útočníkovy stanice. Ta je včetně IP adresy také v dalším záznamu, který je legitimním záznamem o mapování útočníkovy IP adresy na jeho skutečnou fyzickou adresu. K otestování schopnosti odposlouchávat komunikaci lze použít například klasický ping ze stanice oběti na adresu výchozí brány. Útočník pak může například pomocí programu Wireshark zachytit danou komunikaci. Tuto situaci ilustruje následující obrázek.



Obrázek 13 - Ping zachycený programem Wireshark

Nyní lze pozici uprostřed komunikace využít k získání citlivých dat. Přihlašovací údaje se většinou odesílají přes šifrované připojení, což v danou chvíli znemožňuje přímé čtení dat. K překonání tohoto omezení bude v následující části využit nástroj SSL strip.

První z předpokladů využití tohoto nástroje je již splněn, veškerá komunikace oběti je odesílána skrze útočníkovu stanici. Pomocí následujících příkazů bude nakonfigurován a spuštěn nástroj SSL strip.

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

Zmíněným příkazem zajistíme předávání paketů z jednoho rozhraní na druhé v rámci operačního systému Linux.

Následující příkaz zajistí přesměrování příchozích paketů na port, na kterém bude poslouchat SSL strip.

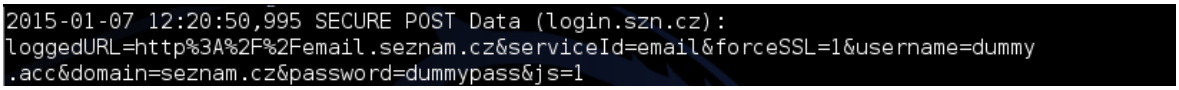
```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --
to-port 54321
```

Port uvedený v poslední části příkazu lze libovolně zvolit, pokud se jedná o neobsazený port. V příkladu zvolen port 54321.

Jako poslední je uveden příkaz pro spuštění samotného nástroje, kde je uveden zvolený port pomocí přepínače „–l“.

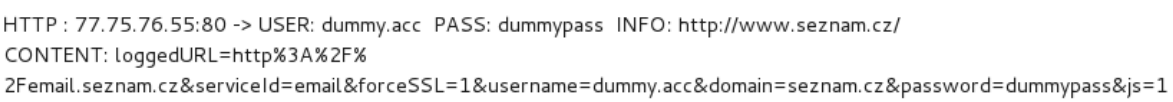
```
sslstrip.py -l 54321
```

Za předpokladu, že se nyní oběť pokusí přihlásit například k emailové službě, bude útočník bez problémů schopen přečíst přihlašovací údaje. Jednou z možností je využití logovacího souboru nástroje SSL strip, kam jsou ukládány všechny zachycené metody POST protokolu HTTP. Příklad zachycených údajů v logovacím souboru je znázorněn na obrázku číslo dvanáct.



Obrázek 14 - SSL strip log

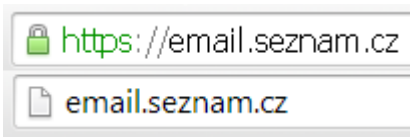
Další možnost nabízí nástroj Ettercap, který rovněž zobrazuje všechny zachycené metody POST.



Obrázek 15 - Ettercap HTTP POST

V neposlední řadě lze zachytávat veškerou komunikaci jedním z dostupných programů určených pro tyto účely. Výhodou předešlých možností je větší přehlednost.

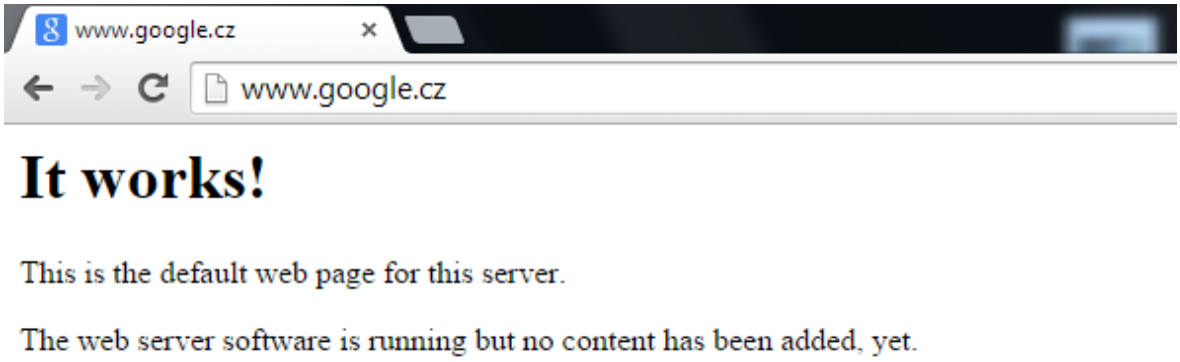
Oběť může pojmout podezření, že se stala cílem útoku, pokud pozorně sleduje, jaký protokol je použit pro komunikaci s cílem. Z principu funkce nástroje SSL strip vyplývá, že oběť s útočníkovou stanicí komunikuje nezabezpečeným protokolem. Možným varovným znamením tak je použitý protokol pro komunikaci. Jestliže si je oběť vědoma toho, že pro přihlášení do emailové služby byl vždy používán zabezpečený protokol, může být útočník odhalen ještě dříve, než bude mít možnost získat jakékoliv informace.



Obrázek 16 - Rozdíl v URL

Při kontrole se nelze spoléhat na ikonu zámku, která může být prohlížeči odeslána pomocí nástroje SSL strip. Nejefektivnější metodou kontroly je sledovat použitý protokol. Tedy zda se komunikuje nezabezpečeným HTTP nebo zabezpečeným HTTPS protokolem.

Další možností pro útočníka je již zmíněné podvrhnutí požadované webové stránky, neboli DNS spoofing. K tomuto účelu lze využít poměrně širokou škálu nástrojů, mezi které patří například DNSspoof nebo DNSchef. Výsledek tohoto útoku je takový, že oběť nevědomky přistupuje k podvržené webové stránce. Na obrázku je zachycen pokus oběti přistoupit na webovou stránku, který byl útočníkem zachycen a přesměrován na lokální webový server útočníka.



Obrázek 17 - DNS spoofing

Po ukončení útoku Ettercap automaticky provede obnovení ARP tabulek oběti a výchozí brány. Situaci dokumentuje následující obrázek.

```
Rozhraní: 172.16.0.12 --- 0xb
  internetová adresa    fyzická adresa        typ
  172.16.0.1            00-24-c4-11-a9-40     dynamická
  172.16.0.11           00-23-ae-75-c3-d4     dynamická
  172.16.0.255          ff-ff-ff-ff-ff-ff     statická
  224.0.0.22            01-00-5e-00-00-16     statická
  224.0.0.252           01-00-5e-00-00-fc     statická
  239.255.255.250       01-00-5e-7f-ff-fa     statická
  255.255.255.255       ff-ff-ff-ff-ff-ff     statická
```

Obrázek 18 - ARP tabulka po útoku

6.3 Útok na zabezpečené síti

V druhém scénáři budou na přepínači implementovány ochranné mechanismy DHCP snooping a DAI. Pro zjednodušení nebude detailně popisován průběh útoku ani nastavení stanic jako v předchozí situaci, v případě nejasností týkajících se průběhu útoku lze čtenáře odkázat na předešlou kapitolu nebo na webové stránky projektu OWASP [10].

V tomto případě byla serverem DHCP oběti přidělena IP adresa 172.16.0.17, útočník zůstává na adrese 172.16.0.11, stejně jako brána má také totožnou adresu s předchozím příkladem, tedy 172.16.0.1. Pro zjištění všech konfiguračních detailů lze opakovat zadání příkazů z předchozí kapitoly. Nastavení směrovače zůstává nezměněno, nastavení přepínače bude v úvodu upraveno tak, aby bylo zabráněno útočníkovi v provedení útoku.

Nejprve je pro úplnost na následujícím obrázku znázorněna tabulka fyzických adres na jednotlivých rozhraních přepínače. Jedná se o adresy stanic oběti a útočníka a vnitřní rozhraní směrovače neboli výchozí brány.

```
1    0023.ae75.abce    DYNAMIC    Fa0/2
1    0023.ae75.c3d4    DYNAMIC    Fa0/3
1    0024.c411.a940    DYNAMIC    Fa0/1
```

Obrázek 19 - Tabulka fyzických adres na přepínači

Nyní budou představeny konfigurační příkazy použité pro implementaci obranných mechanismů na přepínači. V první řadě je nutné zapnout mechanismus DHCP snooping, který na přepínači vytvoří tabulku mapování IP adres na fyzické adresy na základě zachycených DHCP požadavků od stanic na síti. Zapnutí této služby provádí následující příkaz:

```
Switch(config)# ip dhcp snooping
```

Poté je nutné určit VLAN, neboli virtuální lokální síť, na které bude DHCP snooping pracovat.

```
Switch(config)# ip dhcp snooping vlan 1
```

Při nastavování VLAN lze zmínit více než jednu, v takovém případě jsou čísla uváděna oddělená čárkou, pokud je nutné zadat celý rozsah od určitého čísla po další číslo, příkaz je zapsán například v následujícím tvaru:

```
Switch(config)# ip dhcp snooping vlan 1-20
```

Jakmile je služba DHCP snooping zapnutá na globální úrovni, je nutné specifikovat nastavení rolí rozhraní. Rozhraní přímo připojené ke směrovači, nebo obecně, rozhraní připojené směrem k DHCP serveru bude uvedeno jako důvěryhodné. Základní nastavení všech rozhraní je nedůvěryhodné, pro správné přidělování IP adres DHCP serverem je tedy nutné změnit nastavení na rozhraní, na kterém se nachází server DHCP. Pro ostatní nedůvěryhodná rozhraní, lze nastavit limit na počet žádostí o přidělení IP adresy. Tato funkce umožňuje zabránit tomu, aby útočník intenzivním vysíláním požadavků vyčerpal dostupný adresní rozsah pro přidělování. Další možností nastavení je specifikovat místo pro ukládání získaných záznamů, můžeme tím například určit, že záznamy budou ukládány na vzdálený server pomocí protokolu TFTP [18].

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

Nejprve nastavení důvěryhodného rozhraní. Od zadání tohoto příkazu budou povoleny DHCP odpovědi z tohoto směru. Jinými slovy, tímto směrem se nachází DHCP server, tudíž odpovědi přicházející na toto rozhraní jsou legitimní.

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# ip dhcp snooping trust
```

Dále bude nastaven limit pro požadavky na DHCP server, které mohou stanice vyslat po dobu jedné minuty. V tomto konkrétním případě se jedná o dvacet požadavků za vteřinu.

```
Switch(config)# interface FastEthernet0/2
Switch(config-if)# ip dhcp snooping limit rate 20

Switch(config)# interface FastEthernet0/3
Switch(config-if)# ip dhcp snooping limit rate 20
```

Nyní lze pokročit k nastavení služby DAI. Obdobně jako v předchozím případě se mechanismus DAI zapíná pro jednotlivé VLAN. Syntaxe příkazu je velmi podobná, zadávání více VLAN je totožné.

```
Switch(config)# ip arp inspection vlan 1
```

Stejně jako v případě nastavování služby DHCP snooping i v případě DAI jsou všechna dostupná rozhraní v základním nastavení v nedůvěryhodném režimu. Toto nastavení změníme příkazem:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# ip arp inspection trust
```

Jako volitelné možnosti konfigurace následuje nastavení limitů pro odesílání ARP zpráv. V základním nastavení na nedůvěryhodném rozhraní je limit patnáct zpráv za vteřinu. Následující příkazy limit sníží na deset zpráv za vteřinu.

```
Switch(config)# interface FastEthernet0/2
Switch(config-if)# ip arp inspection limit rate 10

Switch(config)# interface FastEthernet0/3
Switch(config-if)# ip arp inspection  limit rate 10
```

Situace v síti je po konfiguraci taková, že přepínač si na základě DHCP zpráv vytvoří tabulku mapování přidělených IP adres na fyzické adresy. Dále pak kontroluje ARP zprávy, zda hodnoty v nich uvedené odpovídají hodnotám ve výše zmíněné tabulce. Pokud hodnota neodpovídá, zprávu přepínač zahodí. Pokud limit ARP zpráv překročí deset zpráv za vteřinu, přepínač přepne rozhraní do stavu *error-disabled*, v tomto stavu není možné přes rozhraní komunikovat až do doby, než je správcem stav obnoven.

Služba DHCP snooping pomocí inspekce komunikace mezi klientem a DHCP serverem zjistí mapování IP adres na fyzické adresy. Konkrétní případ znázorňuje obrázek níže. Lze si povšimnout, že mapování je kompletní pro stanice útočníka i oběti.

```
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  ----------
----------
00:23:AE:75:C3:D4   172.16.0.11     86381       dhcp-snooping  1     FastEther
net0/3
00:23:AE:75:AB:CE   172.16.0.17     86274       dhcp-snooping  1     FastEther
net0/2
Total number of bindings: 2
```

Obrázek 20 - DHCP snooping

Zobrazení statistik DAI lze provést pomocí příkazu:

```
Switch# show ip arp inspection statistics
```

Výstup tohoto příkazu je přehledná tabulka zachycující statistiky odeslaných a zahozených ARP zpráv, včetně stručného přehledu konfigurace služby.

```
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    1     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
    1              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    1                   0                        0                      0
```

Obrázek 21 - DAI statistika

Pokud se nyní útočník pokusí zahájit útok, bude jeho činnost logována (v případě tohoto příkladu pouze na výstup do konzole) a ARP zprávy zahozeny.

```
*Mar  1 00:37:42.214: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/
1, vlan 1.([0024.c411.a940/172.16.0.1/0023.ae75.c3d4/172.16.0.11/00:37:41 UTC Mo
n Mar 1 1993])
*Mar  1 00:37:43.237: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/
1, vlan 1.([0024.c411.a940/172.16.0.1/0023.ae75.c3d4/172.16.0.11/00:37:42 UTC Mo
n Mar 1 1993])
*Mar  1 00:37:44.244: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/
1, vlan 1.([0024.c411.a940/172.16.0.1/0023.ae75.c3d4/172.16.0.11/00:37:43 UTC Mo
n Mar 1 1993])
```

Obrázek 22 - DAI logování

```
Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
----      ---------        -------     ----------      ---------
   1              3              3              3              0

Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
----   ------------    -----------  -------------   -------------------
   1              3              0              0                     0

Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
----   -----------------   ----------------------   ---------------------
   1                   0                        0                       0
```

Obrázek 23 - DAI statistika po útoku

Pokud útočník zvolí agresivnější taktiku a překročí povolený limit počtu ARP zpráv za vteřinu, přepne se rozhraní přepínače, na kterém je útočník připojen, do stavu *error-disabled* a veškerá komunikace bude přerušena.

```
FastEthernet0/3 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0024.f76b.c083 (bia 0024.f76b.c083)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Obrázek 24 - Stav rozhraní po překročení limitu

Závěrem lze tedy situaci shrnout tak, že útočník nebyl schopen útok provést, byl odhalen a byla mu znemožněna jakákoliv další komunikace na daném rozhraní.

6.4 Útok v prostředí s DAI a statickými IP adresami

V posledním případě bude otestováno chování ochranných mechanismů, pokud útočník i oběť budou mít IP adresu nastavenou manuálně, neboli DHCP snooping nebude mít v tabulce mapování příslušných IP adres na fyzické adresy. Adresace zůstává stejná jako v posledním případě.

Účelem tohoto experimentu je otestovat, zda nastavení statických adres umožní obejít bezpečnostní opatření z předešlého příkladu. Oběti i útočníkovi byly nastaveny statické IP adresy, neexistuje tedy záznam o mapování adres a není nastaven ani ARP ACL. V takovém případě je experiment velice krátký, neboť pokud pro příslušný pár fyzické a IP adresy neexistuje mapovací záznam a tento pár není povolen ani v žádném ARP ACL, přepínač zprávu ARP zahazuje.

Platí tedy stejně jako v předešlém případě, že útok není možný, navíc v tomto případě není možná ani běžná komunikace, neboť stanice se nikdy nedozví fyzické adresy svých sousedů. Obdobně jako v předešlém případě, i zde je při překročení nastavených limitů rozhraní přepnuto do neaktivního chybového stavu. Pokud tedy v síti existují prvky se statickou IP adresou, které nejsou připojeny na důvěryhodné rozhraní je pro komunikaci nutné využít ARP ACL.

Závěrem lze tedy dodat, že využití statických adres v prostředí s dynamickým přidělováním pomocí protokolu DHCP, neumožní útočníkovi mechanismus DAI obejít.

Závěr

Cílem práce bylo představení *man-in-the-middle* útoků prováděných pomocí nedokonalosti protokolu ARP, obrany proti nim a možných následků

Teoretická část nejprve uvádí čtenáře do problematiky etického hackingu. Dále je představena linková vrstva modelu ISO/OSI a protokoly zaručující její funkčnost, s důrazem na protokol ARP. Po představení základních pojmů pokračuje teoretická část popisem útoků prováděných pomocí protokolů pro mapování adres včetně těch, jejichž princip je postaven na pozici uprostřed komunikace. Následující kapitola se věnovala obraným metodám použitelným pro znemožnění provedení útoku. V poslední kapitole teoretické části byly představeny nástroje využívané pro provedení útoků. Jeden z těchto nástrojů byl použit i pro provádění útoků v rámci realizace praktické části, konkrétně se jednalo o nástroj Ettercap.

V úvodu praktické části je nejprve popsána topologie sítě, na které byly útoky prováděny. Poté byl předveden názorně útok na nezabezpečené síti včetně následků, které takový útok může mít pro oběť. V další podkapitole praktické části byl stejný útok proveden na zabezpečené síti, kde je demonstrována funkčnost mechanismů zajišťující bezpečnost na linkové vrstvě. Poslední podkapitola praktické části pak popisuje chování DAI v případě, že neexistuje záznam v mapovací tabulce funkce DHCP snooping.

V závěru je nutno zmínit velmi vysoké riziko plynoucí z útoků prováděných na linkové vrstvě a to i navzdory faktu, že útočník se musí nacházet ve stejné síti s obětí, čemuž lze například v podnikové síti zabránit zvýšenou fyzickou bezpečností a správnou konfigurací síťových prvků. V momentě kdy je útočník schopen provést takový útok, jsou následky pro oběť často velmi nepříjemné, proto je nutné nepodceňovat riziko útoků využívajících protokol ARP.

Práci by bylo možné rozšířit o podrobný popis a případové studie obdobných útoků v prostředí IPv6. Možnosti útočníka i ochrany byly v této práci pouze nastíněny, aby byl čtenář obeznámen s možností provádět útoky i v následující verzi protokolu IP.

Literatura

[1] **HERZOG, Pete**. ISECOM. *OSSTMM 3* [online]. 2010 [cit. 2015-01-22]. Dostupné z: http://www.isecom.org/mirror/OSSTMM.3.pdf

[2] **ZITTA, Stanislav**. *Penetrační testování*. Pardubice, 2013. Diplomová práce. Univerzita Pardubice, Fakulta elektrotechniky a informatiky.

[3] **WALKER, Matthew**. *CEH, Certified Ethical Hacker: exam guide : all-in-one*. New York: McGraw-Hill, c2012, xxii, 391 p. ISBN 00-717-7229-4.

[4] **PUŽMANOVÁ, Rita**. *TCP/IP v kostce*. 2. upr. a rozš. vyd. České Budějovice: Kopp, 2009, 619 s. ISBN 978-80-7232-388-3.

[5] RFC 826. *An Ethernet Address Resolution Protocol*. IETF, 1982. Dostupné z: https://www.ietf.org/rfc/rfc826.txt

[6] RFC 1027. *Using ARP to Implement Transparent Subnet Gateways*. IETF, 1987. Dostupné z: https://www.ietf.org/rfc/rfc1027.txt

[7] RFC 903. *A Reverse Address Resolution Protocol*. Stanford University: IETF, 1984. Dostupné z: https://www.ietf.org/rfc/rfc903.txt

[8] **SATRAPA, Pavel**. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011, 407 s. CZ.NIC. ISBN 978-80-904248-4-5.

[9] RFC 4291. *IP Version 6 Addressing Architecture*. IETF, 2006. Dostupné z: https://tools.ietf.org/html/rfc4291

[10] Man-in-the-middle attack. OWASP. *OWASP* [online]. [cit. 2014-12-08]. Dostupné z: https://www.owasp.org/index.php/Man-in-the-middle_attack

[11] Gratuitous_ARP. WIRESHARK. *Wireshark* [online]. [cit. 2014-12-08]. Dostupné z: http://wiki.wireshark.org/Gratuitous_ARP

[12] **STRETCH, Jeremy**. IPv6 neighbor spoofing. In: *PacketLife.net* [online]. 2009 [cit. 2014-12-12]. Dostupné z: http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/

[13] **MARLINSPIKE, Moxie**. SSLstrip. *Thoughtcrime.org* [online]. [cit. 2014-12-13]. Dostupné z: http://www.thoughtcrime.org/software/sslstrip/

[14] **TYSON, Jeff**. How Network Address Translation Works. *HowStuffWorks.com* [online]. 2001 [cit. 2015-01-21]. Dostupné z: http://computer.howstuffworks.com/nat.htm

[15**] HUCABY, Dave**. *CCNP SWITCH 642-813 official certification guide*. Indianapolis: Cisco Press, c2010, xxvii, 459 s. ISBN 978-1-58720-243-8.

[16] **MONTORO, Massimiliano**. *Oxid.it* [online]. 2014 [cit. 2015-01-31]. Dostupné z: http://www.oxid.it/cain.html

[17] **ORNAGHI, Alberto a Marco VALLERI**. *Ettercap* [online]. 2014 [cit. 2015-02-01]. Dostupné z: http://ettercap.github.io/ettercap/index.html

[18] DHCP Snooping. CISCO. *Cisco* [online]. 2015 [cit. 2015-03-21]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html

[19] Přidání položky statické mezipaměti protokolu ARP. MICROSOFT. *Microsoft TechNet* [online]. [cit. 2015-03-07]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc781485%28v=ws.10%29.aspx

[20] Man-in-the-Middle. In: *OWASP* [online]. 2007 [cit. 2015-04-25]. Dostupné z: https://www.owasp.org/images/2/21/Main_the_middle.JPG

[21] SSLStrip. In: *Exploitedsecurity* [online]. 2013 [cit. 2015-04-25]. Dostupné z: http://exploitedsecurity.org/wp-content/uploads/2013/08/SSLStrip.jpg