UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Využití Cain & Abel password recovery tools pro etický hacking na L2 vrstvě

Jiří Auerswald

Bakalářská práce
2016

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří Auerswald**
Osobní číslo:	**I12095**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Využití Cain & Abel password recovery tools pro etický hacking na L2 vrstvě**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je zmapovat možnosti nástroje Cain & Abel pro využití k etickému hackingu na úrovni L2 modelu ISO/OSI. Autor provede analýzu možností tohoto nástroje pro mapování síťového provozu na druhé vrstvě modelu ISO/OSI s důrazem na bezpečnostní rizika této vrstvy. V praktické části autor navrhne a podrobně vyřeší 5 laboratorních úloh.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

ERICKSON, Jon. Hacking: the art of exploitation. 2nd ed. San Francisco, CA: No Starch Press, c2008, x, 472 stran ISBN 15-932-7144-1.
ENGEBRETSON, Pat. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Second Edition. San Francisco, CA: No Starch Press, c2008, xviii, 204 stran. ISBN 978-012-4116-443.

Vedoucí bakalářské práce: **Mgr. Josef Horálek, Ph.D.**
Katedra softwarových technologií

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

prof. Ing. Simeon Karamazov, Dr.
děkan

L.S.

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 09. 05. 2016 Jiří Auerswald

Poděkování

V první řádě bych chtěl poděkovat vedoucímu práce, Mgr Josefu Janu Horálkovi, Ph.D za náměty a podporu při tvorbě této práce. Dále děkuji všem vyučujícím, kteří mi předali cenné znalosti problematiky počítačových síti. V neposlední řadě děkuji svým rodičům za veškerou podporu při studiu.

Anotace

Tato bakalářská práce analyzuje možnosti programu Cain&Abel na linkové vrstvě modelu síťové komunikace ISO/OSI. V teoretické časti je čtenář zasvěcen do problematiky počítačových síti a jejich bezpečnosti se zaměřením na linkovou vrstvu, která je podrobně rozebrána. Dále jsou představeny útoky, které mohou být na linkové vrstvě realizovány a obrana proti nim. Závěrečná kapitola teoretické části pak představuje vybrané partie programu Cain&Abel se zaměřením na linkovou vrstvu. V části praktické jsou představeny tři scénáře útoků provedených prostřednictvím programu Cain&Abel a obrana proti nim.

Klíčová slova

etický hacking, linková vrstva, odposlech, Cain&Abel, sniffer, heslo, ARP cache poisoning

Title

Use of Cain&Abel password recovery tools for ethical hacking on L2 layer.

Annotation

This bachelor’s thesis analyzes abilities of software called Cain&Abel on link layer of network communication model ISO/OSI. Theoretical chapters discuss computer networks and their security focusing on link layer. Further, link layer security treats and mitigation is revealed. Last theoretical chapter describes chosen parts of Cain&Abel. In practice part three scenarios of attack via Cain&Abel and mitigation are demonstrated.

Keywords

Ehthical hacking, link layer, sniffing, Cain&Abel, sniffer, password, ARP cache poisoning

Obsah

Seznam zkratek

ISO/OSI	International Organization for Standardization/Open System Interconnection
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
ARP	Address Resolution Protocol
LAN	Local Area Network
WAN	Wide Area Network
STP	Spanning Tree Protocol
RSTP	Rapid Spanning Tree Protocol
BPDU	Bridge Protocol Data Unit
APR	ARP Poison Routing
HTTP	Hypertext Transfer Protocol
DHCP	Dynamic Host Configuration Protocol
DAI	Dynamic ARP Inspection
SSH	Secure Shell

Seznam obrázků

Úvod

Tato bakalářská práce se detailně věnuje bezpečnostním slabinám linkové vrstvy a etickému použití funkcí programu Cain&Abel, které umí těchto slabin využít. Čtenář je postupně zasvěcen do problematiky etického hackingu a principu síťové komunikace tak, jak ji popisuje model ISO/OSI a z něj vycházející rodina protokolů TCP/IP. Další kapitoly jsou věnovány podrobnému rozboru linkové vrstvy a technologií, které do ní spadají. Rovněž jsou představeny její známé bezpečnostní slabiny a nastíněn způsob, jak tyto slabiny odstranit.

Hlavním cílem této práce je představení programu Cain&Abel password recovery tools a jeho schopností souvisejících s linkovou vrstvou. Tato práce není kompletním manuálem pro všechny funkce programu, kterých je celá řada, ale věnuje se zejména odposlechu na přepínaných sítích a analýze získaných dat včetně prolamování zašifrovaných hesel. Je důležité rozlišovat etické a neetické použití daných funkcí, program byl jeho autorem vyvinut čistě pro etické účely obnovy ztracených hesel a podobně. Principy útoků se však nemění, ať jsou využity eticky či neeticky. Proto je obrana sítě proti těmto útokům kriticky důležitá a tato práce se jí důkladně věnuje.

Cílem praktické části je, na základě funkcí představených v části teoretické, předvést konkrétní příklady práce s programem Cain&Abel. K praktickým úlohám bude poskytnuto step-by-step řešení včetně vysvětlení. Stejně jako provedení útoků bude rovněž podrobně rozebrán a předveden způsob, jak se proti nim bránit.

1 Úvod do problematiky etického hackingu

V novém tisíciletí raketově stoupá využití služeb sítě internet a dá se přepokládat, že se tento trend v blízké budoucnosti nebude měnit. Kromě zjevných výhod, jako jsou sdílení dat, e-mail, internetové obchodování, sociální sítě a mnoho dalších, s sebou využívání internetu přináší nemalé riziko. Tímto rizikem je možnost napadení sítě, odcizení citlivých informací a jejich případnému zneužití. Řešením takové situace může být právě etický hacking.

Ve spojitosti s etickým hackingem často narážíme na pojem penetrační testování. Tyto pojmy si jsou velmi blízké a v některých oblastech se prolínají. Penetrační test lze chápat jako konkrétní aplikaci etického hackingu. Samotné slovo hacking může působit negativně, většinou si pod ním představíme právě ono nabourání se do systému za účelem škodit. Úkolem etických hackerů je ale nalezení bezpečnostních slabin, díky čemuž se dá útoku neetických hackerů zabránit nebo jim alespoň výrazně omezit pole působnosti.

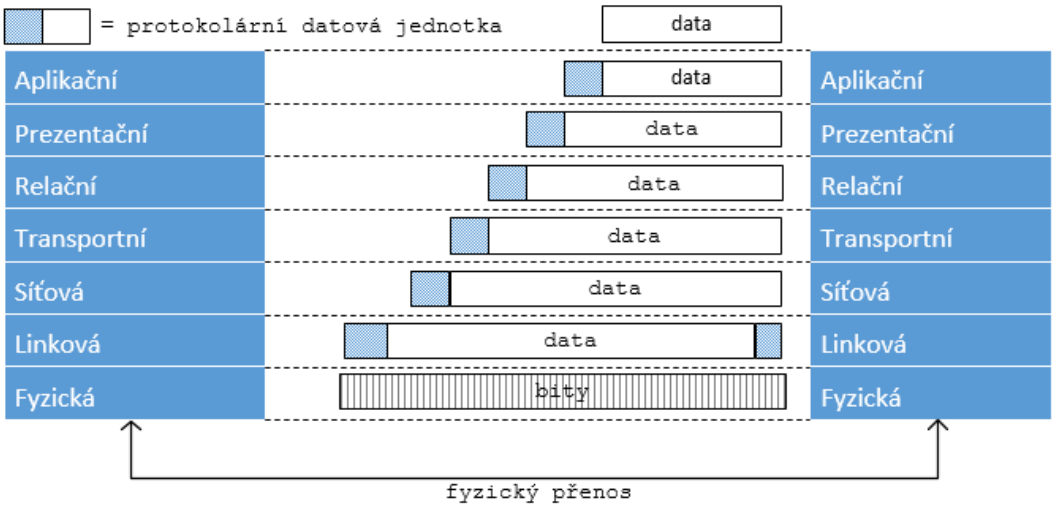
Etický hacking je jedinou možností simulace napadení sítě, provádějí ji počítačový experti s cílem najít bezpečnostní trhliny v síti nebo v operačním systému a posoudit zda je zabezpečení v souladu s politikou organizace požadující testování. Následně dochází k vyhodnocení výsledků a zjištěných nedostatků. Hotový report je předán kompetentním osobám, které jej posoudí a navrhnou řešení nalezených hrozeb vedoucí k jejich odstranění. Etický hacker jedná vždy v souladu s pravidly nastavenými zadavatelem a nemá v úmyslu firmu poškodit. Společnosti, jež na své sítě nechali aplikovat etický hacking běžně neposkytují výsledky analýz z důvodu utajení bezpečnostních slabin. Zveřejnění takových informací by se společnost vystavila vysokému riziku jejich zneužití. (PALMAR, 2001)

2 Model síťové komunikace

Většina datové komunikace dnes probíhá po síti, data jsou přenášena pomocí datových paketů, které procházejí jednou nebo mnoha počítačovými sítěmi od odesilatele k příjemci. Aby takové sítě mohli spolupracovat, musí používat společné protokoly nebo sadu pravidel pro vysílání a příjem datových paketů. Za dobu, po kterou jsou počítačové sítě používány, bylo již vytvořeno mnoho protokolů. Nejvíce používanou je sada protokolů TCP/IP. Pro obecné znázornění, jak by měla síťová komunikace probíhat, byl organizací ISO navržen referenční model ISO/OSI.

2.1 Referenční model ISO/OSI

Jak uvádí (PETERKA, 1999), model ISO/OSI poskytuje obecné paradigma popisující komunikaci mezi uzly sítě. Vzhledem k celkové složitosti a náročnosti je tato komunikace rozdělena do sedmi vrstev, kde každá vrstva zajišťuje provedení specifické části komunikace. Její průběh můžeme popsat takto, komunikující uzel předá data, která chce odeslat aplikační vrstvě, ta je zpracuje a předá další vrstvě, takto data putují modelem dolů, až na fyzické médium, které je přenese k cíli, zde je postup opačný, data jsou předávána po vrstvách vzhůru, každá vrstva provede svou činnost, až jsou data nakonec zpracována aplikací, pro kterou byla určena, například dojde k zobrazení webové stránky. Pro lepší představu situaci ilustruje obrázek (Obrázek 1).



Obrázek 1 – průchod přenášených dat vrstvami ISO/OSI modelu.

V průběhu zpracování přidává každá vrstva k datům svou hlavičku, do které zapisuje data pro identifikaci a směrování dat. Tento proces se nazývá enkapsulace (anglicky encapsulation). Data a hlavička dohromady tvoří datovou část pro bezprostředně následující vrstvu v průběhu zpracování, ta tyto data opatří vlastní hlavičkou a předá dál, takto proces pokračuje, až dojede k přenesení dat k příjemci. Ten provádí opačný proces, tedy de-kapsulaci, jednotlivé vrstvy postupně odeberou své hlavičky a příjemce obdrží příslušná data.

Všechny potřebné operace jsou seskupeny do logických sekvencí na každé vrstvě modelu.

- **aplikační** – poskytuje aplikacím rozhraní pro komunikaci v síti,
- **prezentační** – zajišťuje kompatibilitu formátů dat, komprimace a šifrování,
- **relační** – navazuje, udržuje a ukončuje relaci, rovněž obsahuje funkce pro autentizaci a autorizaci,
- **transportní** – zaručuje integritu a konzistentnost dat, a opravuje případné chyby,
- **síťová** – stará se o směrování paketů a logickou adresaci,
- **linková** – zapouzdřuje pakety do rámců a řídí přístup k fyzickému médiu (podrobně rozebrána v 3. kapitole),
- **fyzická** – definuje vlastnosti fyzického média, vytváří proud bitů jednotlivých rámců.

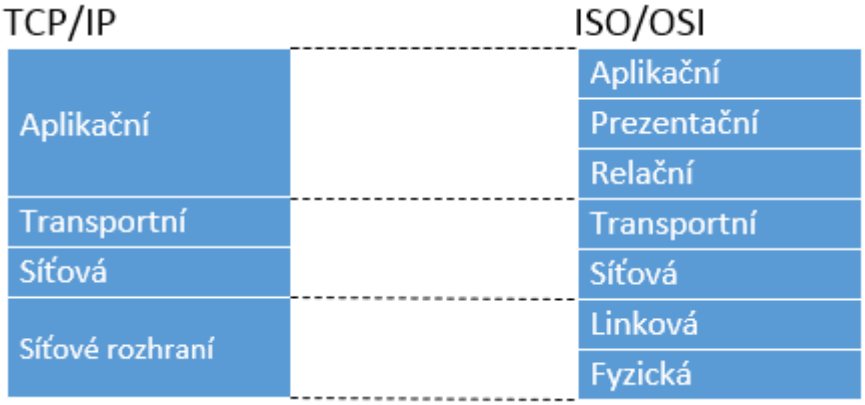
Nutno podotknout, že OSI model, je pouhým modelem. Není deklarována nutnost jeho použití pro realizaci síťové komunikace, ačkoli většina protokolů a systémů se ho drží. Je dobrý zvláště pro popis a pochopení fungování sítě.

2.2 Síťový model TCP/IP

Síťový model TCP/IP byl vyvinut v průběhu 60. při tvorbě sítě ARPANET[1] v Americe. Z počátku byl používán na Unixových počítačích univerzit a vládních zařízeních. Dnes je široce používán v celé síti Internet a implementován na většině komunikačních platforem.

[1] Experimentální síť agentury ARPA ministerstva obrany USA, později posloužila jako základ sítě Internet.

TCP/IP je rovněž vrstevnatým modelem, avšak nevyužívá všechny vrstvy ISO/OSI modelu. Oba modely jsou ale ekvivalentní, co se týká služeb a funkcí, viz Obrázek 2. Vrstva síťového rozhraní slučuje fyzickou a linkovou vrstvu, na síťové vrstvě je implementován protokol IP, poskytuje stejně služby jako síťová vrstva modelu ISO/OSI, na transportní vrstvě pracují protokoly TCP[2] respektive UDP[3], aplikační vrstva slučuje funkce zbylých vrstev modelu ISO/OSI. (PETERKA, 1999)



Obrázek 2 – srovnání TCP/IP a ISO/OSI.

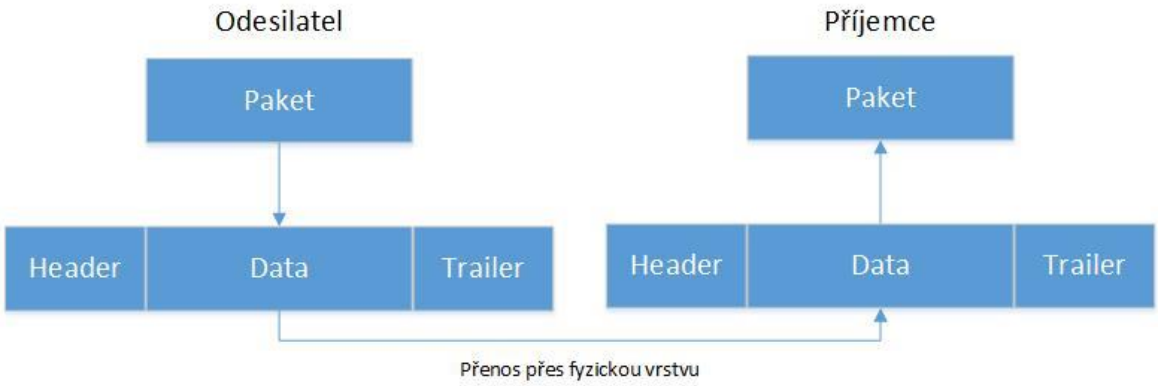
[2] Umožňuje spolehlivý a spojovaný přenos dat.
[3] Poskytuje nespolehlivý a nespojovaný přenos.

3 Rozbor linkové vrstvy

Linková vrstva využívá služeb vrstvy fyzické pro přenos bitů skrze komunikační médium. Jejími hlavními úkoly jsou:

- Poskytnout přesně definované služby vrstvě síťové.
- Ošetřit chyby vzniklé při přenosu.
- Regulovat tok dat tak, aby spolu mohla komunikovat různě rychlá zařízení.

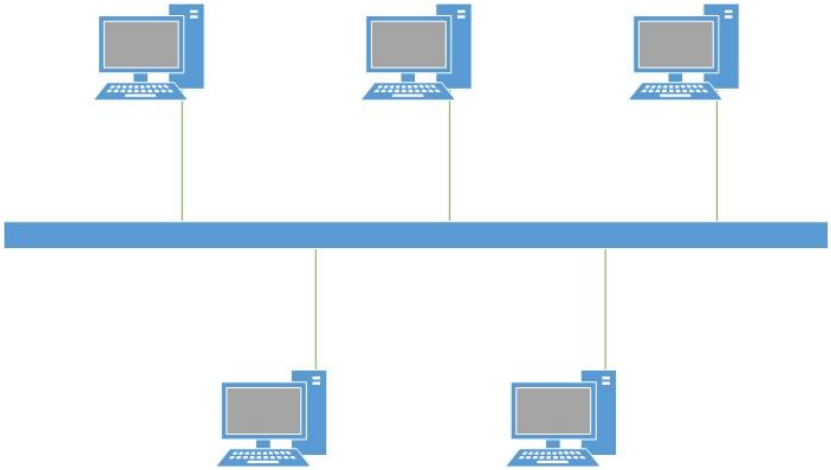
Pro splnění těchto úkolů linková vrstva přijímá pakety tvořené síťovou vrstvou a zapouzdřuje je do rámců, které následně prostřednictvím fyzické vrstvy přenese. Každý takový rámec se skládá ze tří částí. Jedná se o hlavičku rámce (anglicky header), která, mimo jiné, obsahuje fyzickou adresu odesilatele a příjemce, datovou část, do které je zapouzdřen celý paket a takzvaný trailer, neboli kontrolní část rámce, která slouží k detekci chyb vzniklých při přenosu. Správa rámců tvoří jádro fungování linkové vrstvy. (TANENBAUM, 2003)



Obrázek 3 – schéma přenášení dat

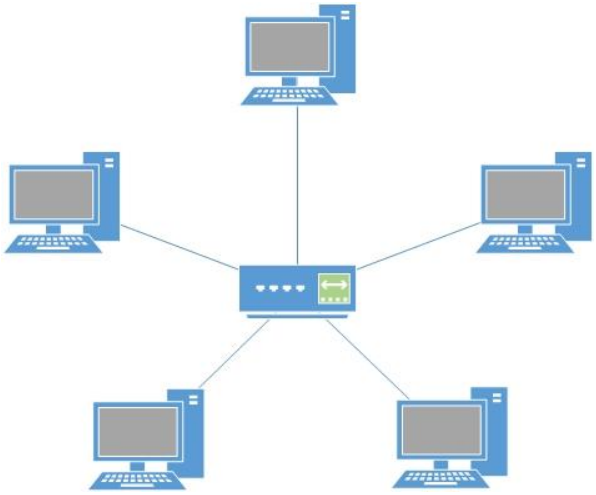
3.1 Ethernet

Dnes nejrozšířenější síťovou technologií v drátových sítích je bezesporu Ethernet. Ten byl vyvinut v letech 1972 – 1975 v laboratořích firmy Xerox pod názvem DIX Ethernet a později, v roce 1983 s drobnými změnami standardizován organizací IEEE jako norma IEEE 802.3. Ethernet realizuje fyzickou a linkovou vrstvu modelu ISO/OSI. Jako médium byly dříve používány koaxiální kabely, v současnosti jsou nahrazeny kroucenou dvoulinkou (anglicky twisted pair) nebo optickou kabeláží. Při použití koaxiálních kabelů se pracovní stanice zapojovali zpravidla do topologie sběrnice (Obrázek 4), při tomto zapojení vzniká velká kolizní doména zahrnující celý segment sítě. Pokud dojde k situaci, kdy se dva nebo více uzlů rozhodne vysílat po médiu data současně, dojde ke kolizi a tím pádem k jejich znehodnocení. Tomu zabraňuje metoda CSMA/CD. Zjednodušeně, každá stanice naslouchá provozu na médiu, pokud neprobíhá žádná komunikace, začne vysílat, pokud ano, čeká. Podrobnosti o fungování této metody naleznete v (TANENBAUM, 2003).



Obrázek 4 – sběrnicová topologie

Je-li médiem pro přenos kroucená dvoulinka, zapojují se počítače do topologie hvězda (Obrázek 5). Kroucená dvoulinka umožňuje pouze spojení point-to-point, pokud tedy chceme propojit více než dvě zařízení, je nutné nasadit centrální rozbočující prvek. Prvotním řešením bylo použití rozbočovače (anglicky hub), ten funguje na jednoduchém principu. Data přijatá na libovolném portu překopíruje na všechny ostatní porty, bez ohledu na to, kterému uzlu mají být doručena. Toto řešení není vhodné nejen proto, že nezmenšuje kolizní doménu, ale hlavně kvůli tomu, že odeslaná data jsou přenesena ke všem dalším uzlům v síti, které je mohou jednoduše přečíst, což je nezanedbatelné bezpečnostní riziko. Druhým a mnohem sofistikovanějším řešením je použití přepínače (anglicky switch), jenž je podrobně rozebrán v kapitole 3.4. (TANENBAUM, 2003)

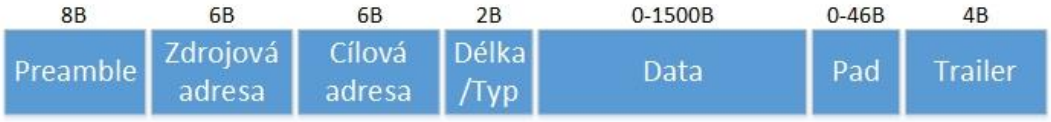


Obrázek 5 – topologie hvězda

3.1.1 Ethernetový rámec

Protokolární datovou jednotkou na linkové vrstvě je rámec, v případě užití technologie Ethernet je přidán přívlastek Ethernetový. Rámec zapouzdřuje paket vytvořený síťovou vrstvou, tento paket tvoří datovou část rámce. Ethernetový rámec začíná takzvanou preambulí, jedná se o úvodní sekvenci bitů, jenž značí začátek rámce. Bity

sekvence jsou nastaveny na 101010 s výjimkou posledního bytu, jehož poslední dva bity mají hodnotu 11. Poslední byt v této podobě je definován standardem IEEE 802.3 a nazývá se Start of Frame delimiter. Poté následuje zdrojová a cílová fyzická adresa zařízení, mezi kterými je rámec posílán. Pole délka (802.3)/typ (DIX) určuje délku datové části případně typ přenášeného protokolu síťové vrstvy. Do pole data je pak vložen kompletní paket předaný síťovou vrstvou. Stejně jako je určena maximální délka datové části, která je 1500 bytů, existuje i délka minimální, ta je stanovena na 46 bytů. Pokud jí datová část rámce nedosahuje, je použit takzvaný pad, tedy část rámce sloužící pro případné dosažení minimální délky. Na konci rámce je ještě 4 bytový trailer, který slouží ke kontrole integrity přenesených dat. Struktura rámce Ethernet je graficky znázorněna na obrázku (Obrázek 6). (TANENBAUM, 2003)



Obrázek 6 – struktura rámce Ethernet

3.2 MAC adresa

Každé zařízení v síti vlastní globálně unikátní identifikátor – Media Access Control adresu. Tato adresa má délku 48 bitů a obvykle je vyjadřována hexadecimálně ve formátu xx-xx-xx-xx-xx-xx, kde x symbolizuje libovolnou číslici hexadecimální soustavy. Adresa je uložena v interní paměti síťového hardware a je koncipována jako neměnná, existují však určité způsoby, jak ji změnit. První tři byty MAC adresy jsou tvořeny tzv. OUI, jedná se o identifikátor výrobce, ten je přidělován správcem adresního prostoru, druhá polovina adresy jedinečně identifikuje konkrétní zařízení a je určována výrobcem. Existuje i několik speciálních MAC adres, jednou z nich je adresa ff-ff-ff-ff-ff-ff, ta slouží k všesměrovému vysíláni (broadcast), rámec s touto adresou v poli příjemce je určen pro všechna zařízení v síti. (PUŽMANOVÁ, 2006)

3.3 Přepínač

Přepínač nazývaný také switch, je aktivní síťový prvek pracující na linkové vrstvě, svou funkcí nahrazuje méně sofistikovaný rozbočovač a výrazně zefektivňuje provoz v lokální síti. Zefektivnění tkví v tom, že přepínač ve většině případů nekopíruje přijatý rámec na všechny porty, ale zasílá ho pouze na port, za kterým se nachází příjemce. Přeposílání probíhá v jednom ze dvou základních módů. Prvním z nich je mód store and forward, ten funguje tak, že přepínač uloží celý rámec do vyrovnávací paměti, zkontroluje hlavičku a kontrolní součet a až poté je poslán dál. Druhou možností je mód cut-trough, kdy přepínač odesílá rámce hned, jakmile načte adresu příjemce, což výrazně snižuje latenci. Existuje ještě třetí mód zvaný adaptive switching, ten přepíná mezi výše zmíněnými módy dle aktuální potřeby. Pokud je komunikace bezchybná přepínač používá mód cut-trough, jakmile se začne objevovat větší množství chyb, přepne do módu store and forward, aby síť nebyla zbytečně zahlcována chybnými rámci. Přeposílání rámců

přímo jejich příjemci namísto rozesílání do celé sítě krom zefektivnění přináší také významné zlepšení bezpečnosti, protože se tím pádem data nedostanou k zařízením, kterým nenáleží a která by je mohla eventuálně odposlechnout a zneužít.

Protože na linkové vrstvě jsou identifikátory zařízení MAC adresy, přepínač se právě podle nich rozhoduje, na který port data odešle. Pro mapování MAC adres na porty si přepínač ve své interní paměti vytváří dynamickou datovou strukturu zvanou Content addressable memory table, takzvanou CAM tabulku. Ta je po zapnutí přepínače prázdná, jakmile spolu začnou zařízení komunikovat, přepínač začne tabulku plnit. Přijme-li rámec, jehož zdrojovou adresu v tabulce nemá, uloží ji spolu s portem, na kterém byl rámec přijat, do tabulky a pokud v ní nenalezne cílovou adresu spolu s cílovým portem, odešle rámec na všechny porty kromě portu, ze kterého rámec přijal. Pokud je stanice z portu odpojena, údaje s ní spojené jsou z tabulky okamžitě vymazány. Jak lze předpokládat, kapacita CAM tabulky není neomezená, pokud dojde k naplnění tabulky, přepínač obvykle přejde do módu, kdy se chová jako hub, tedy přeposílá rámce na všechny porty. Pokud na portu neprobíhá žádná komunikace, jsou po nějaké době (obvykle 5 minut) údaje z tabulky odstraňovány, čímž se uvolňuje kapacita pro nové záznamy. (PUŽMANOVÁ, 2006)

3.4 ARP protokol

Pokud v síti ethernet při použití protokolů TCP/IP chce jedno zařízení komunikovat s druhým, musí znát jeho MAC a IP adresu. Své adresy má zařízení uloženy v paměti a snadno si je načte, cílové adresy je nutno zjistit. Cílová stanice bývá obvykle označena doménovým jménem, to je DNS[4] serverem přeloženo na IP adresu. Pokud je známa IP adresa, je třeba zjistit i cílovou MAC adresu, k tomuto účelu slouží address resolution protocol (ARP). Princip jeho fungování je následující, stanice hledající MAC adresu k dané IP adrese pošle do sítě ARP žádost (anglicky request) jako broadcast (cílová MAC adresa ARP žádosti je ff-ff-ff-ff-ff-ff), tu přijmou všechny stanice v síti, odpovídá ale pouze stanice s hledanou IP adresou, která zasílá ARP odpověď (anglicky reply) jako unicast stanici, která iniciovala žádost. Aby zjišťování nemuselo probíhat stále dokola, existuje ARP cache, kde jsou uchovány (po omezenou dobu v řádu minut) spárované IP a MAC adresy. (TANENBAUM, 2003)

[4] Domain name system, hierarchický systém doménových jmen používaný pro překlad jmen na IP adresy a naopak.

bits	0 – 7	8 – 15	16 – 31
0	Hardware type (2B)		Protocol type (2B)
32	Hardware size (1B)	Protocol size (1B)	Operation code (1B)
64	Sender MAC address (6B)		
96	Sender MAC address (cont.)		Sender IP address (4B)
128	Sender IP address (cont.)		Target MAC address (**6B**)
160	Target MAC address (cont.)		
192	Target IP address (4B)		

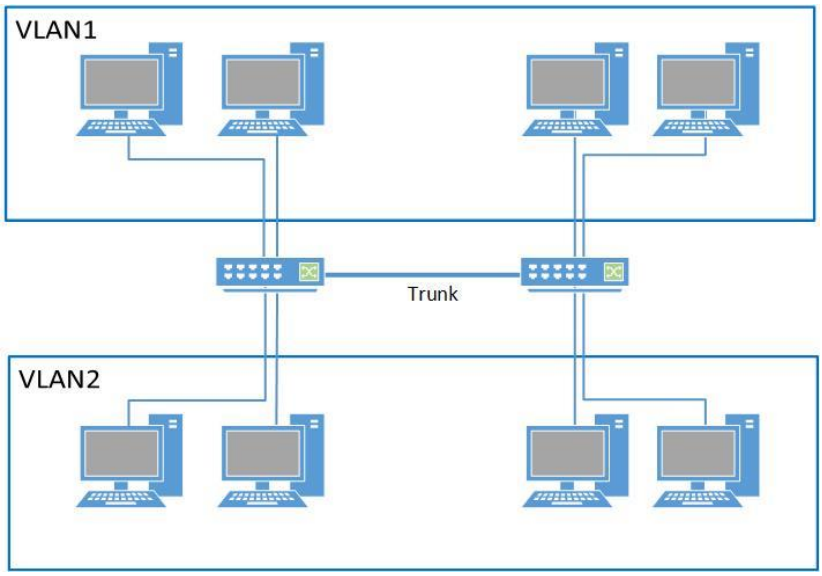
Obrázek 7 – struktura ARP paketu

3.5 VLAN

Virtual LAN (VLAN) je technologie, která dokáže fyzickou přepínanou síť rozdělit na více logických, vzájemně se neovlivňujících sítí. Jednotlivé VLANy jsou od sebe úplně odděleny a zařízený v různých VLAN spolu nemohou přímo komunikovat. Pokud je komunikace vyžadována, musí být použito zařízení, které umí směrovat pakety, obvykle to bývá router[5] nebo L3 switch[6]. V oblasti VLAN jsou definovány dva základní typy portů. Jedná se o typ access a trunk. Pokud je port typu access, slouží k připojení koncové stanice a je třeba ho zařadit do VLAN, ve které se má stanice nacházet. Trunk je port, přes který mohou proudit rámce z různých VLAN. Aby bylo možné příslušnost rámce k VLAN identifikovat, byl vytvořen standart IEEE 802.1q neboli trunking protokol. Funguje tak, že na trunk portu je hlavička každého rámce rozšířena o 4B informaci obsahující číslo VLAN. Trunky jsou využity zejména pro propojení více přepínačů, na kterých jsou nakonfigurovány stejné VLANy. Pomocí trunků pak mohou komunikovat zařízení fyzicky připojená k různým přepínačům, ale logicky patřící do jedné VLAN. Pro lepší pochopení je situace zachycena na obrázku (Obrázek 8). (PUŽMANOVÁ, 2006)

[5] Zařízení pracující na síťové vrstvě směrující pakety mezi různými sítěmi, česky se nazývá směrovač.

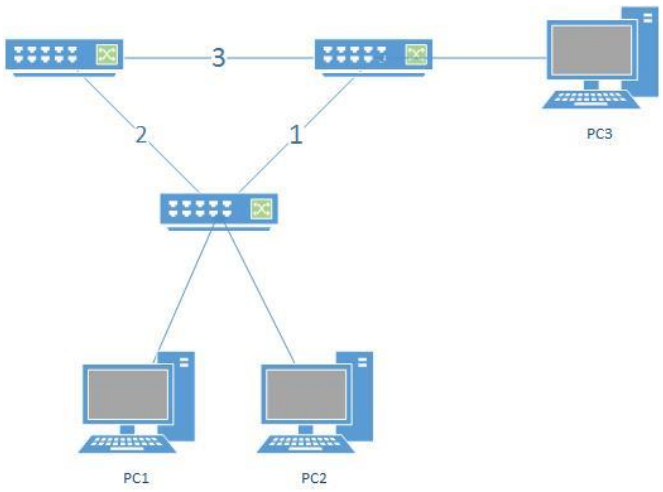
[6] Zařízení fungující zároveň jako router i switch.



Obrázek 8 – VLAN.

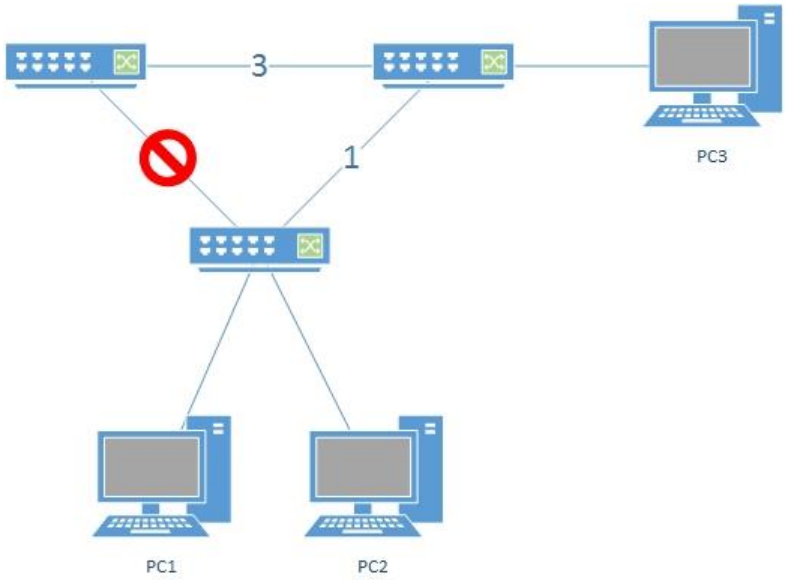
3.6 Spanning Tree Protokol

Redundance zvyšuje spolehlivost sítě a odstraňuje místa náchylná k selhání. Kupříkladu, pokud dojde v topologii na obrázku (Obrázek 9) k výpadku linky 1, stanice PC1 a PC2 mohou stále komunikovat s PC3 díky linkám 2 a 3. Redundantní fyzická topologie ovšem přináší problémy v podobě vzniku smyček. Pokud je v síti smyčka, dochází k vzniku broadcastových bouří. Je-li do takové sítě vyslán broadcast, každý přepínač ho odešle na všechny porty, kromě toho, ze kterého jej obdržel. Protože na linkové vrstvě chybí mechanizmus, který by omezoval životnost rámců, broadcastové rámce donekonečna kolují v síti a jejich počet se neustále zvyšuje, čímž je sít poměrně rychle zahlcena až dojde k jejímu výpadku. Pro řešení těchto problémů byl navržen protokol STP.



Obrázek 9 – redundatní topologie

STP zaručuje logickou bezsmyčkovost topologie. Blokováním portů, které by mohli vytvořit smyčku, dosahuje toho, že všechny uzly v síti spojuje vždy jen jedna logická cesta. Blokovaný port neodesílá ani nepřijímá žádné rámce kromě BPDU rámců, které slouží k určení blokovaných portů a jejich případnému odblokování, pokud dojde ke změně v topologii.



Obrázek 10 –logická topologie po nasazení STP

Nejkratší cesta je vypočítána tak, že v síti je nejprve zvolen tzv. root bridge, tedy výchozí přepínač. Každý další přepínač v síti pak pomocí STP algoritmu vypočte ideální cestu a na základě tohoto výpočtu pak určí, které porty budou blokovány a které ne.

Tento výpočet musí proběhnout při každé změně topologie a může u STP trvat až 50 sekund, což je při dnešních požadavcích na výkon sítě velice dlouhá doba. Z tohoto důvodu byl v roce 2001 představen protokol RSTP, který díky upravenému algoritmu dosahuje konvergence za maximálně 6 sekund obvykle však za méně než 1 sekundu. (PUŽMANOVÁ, 2006)

4 Bezpečnostní hrozby na linkové vrstvě

Každá vrstva modelu TCP/IP má své bezpečnostní hrozby a zranitelná místa. V této kapitole budou shrnuty hrozby na linkové vrstvě. Přestože je linková vrstva jednou z nejnižších v modelu, porušení bezpečnosti zde má za následek kompromitování služeb všech vyšších vrstev. Útoky lze rozdělit podle toho, na které komponenty linkové vrstvy se zaměřují, jsou to útoky na MAC adresy, na ARP protokol nebo na VLANy.

4.1 CAM table overflow

Tento útok je znám rovněž pod názvem MAC address flooding. Tabulka CAM je datová struktura v paměti přepínače, která mapuje adresy MAC zařízení připojených k

jednotlivým portům, a podle které se pak přepínač rozhoduje, na který port má příchozí rámec přeposlat. Tato technika spočívá v přetečení kapacity tabulky CAM přepínače, což má ve většině případů za následek, že se přepínač začne chovat jako rozbočovač a dojde tedy k rozesílání rámců do celé sítě, čímž je umožněno odposlouchávání provozu. Mimoto dochází také k výraznému navýšení síťového provozu, čímž může dojít k odepření některých služeb. Hlavní nevýhodou této techniky je, že ne každý přepínač reaguje na přetečení tabulky CAM stejně, což výrazně ovlivňuje efektivitu útoku. (SPANGLER, 2003) Samotný útok lze provést například pomocí nástroje macof, který je součástí balíku Dsniff[7]. Syntaxe příkazu pro přeplnění tabulky CAM je následující:

```
macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times].
```

Obrana

Účinnou, avšak nepříliš praktickou metodou obrany je vytvoření statických záznamů CAM tabulky. Takové záznamy jsou vždy nadřazeny záznamům dynamickým a není možné je měnit bez přístupu ke konfiguračnímu rozhraní přepínače. Dnes však většina renomovaných výrobců přepínačů v jejich operačních systémech implementuje zabezpečení portů. To spočívá především v omezení množství MAC adres, které smí být k portu připojeny. Na překročení tohoto limitu pak přepínač reaguje dle konfigurace zabezpečení. Konkrétně, firma Cisco používá pro zabezpečení portů tzv. Port security, v překladu tedy ochranu portů. Ta umožňuje nastavit zmiňovaný počet MAC adres, které smí být k portu v tabulce přiřazeny, na překročení tohoto limitu reaguje podle toho, který ze tří režimů je zvolen. Jedná se o režimy Protect, Restrict a Shutdown. (HARPER, a další, 2008)

- **Protect** – po překročení povoleného počtu adres zahazuje všechny příchozí rámce z neznámého zdroje, dokud počet opět neklesne pod limit.
- **Restrict** – funguje stejně jako režim Protect s tím rozdíle, že navíc navyšuje SecurityViolation counter.
- **Shutdown** – okamžitě přepíná port do stavu err-disabled.

4.2 Port stealing

Dalším útokem zaměřujícím se CAM tabulku přepínače je útok jménem Port stealing. Jak název napovídá, cílem útoku je, zjednodušeně řečeno, odcizení portu oběti a unesení komunikace. Princip útoku popisuje (SPANGLER, 2003). Přepínač plní svou CAM tabulku tím způsobem, že čte zdrojové adresy rámců přicházejících na jednotlivé porty a podle nich pak plní, případně aktualizuje záznamy v CAM tabulce. Útočník v tomto případě vytvoří rámec, jehož zdrojová MAC adresa je stejná jako adresa oběti a cílová adresa se rovná adrese útočníka. Přepínač si po přijetí takového rámce aktualizuje záznam v CAM tabulce a rámce, které jsou adresovány oběti nyní přeposílá na port, na který je připojen útočník. V tuto chvíli narážíme na zásadní úskalí tohoto útoku. Stanice

[7] Sada nástrojů pro bezpečnostní audit a penetrační testování.

oběti bude s vysokou pravděpodobností vysílat další rámce, kterými si oběť opět přivlastní svůj port. Útočník tedy musí přepínač stále zaplavovat dalšími a dalšími rámci s podvrženými adresami, aby se mu podařilo odposlechnout co největší část komunikace. Pokud chce útočník uvést CAM tabulku do původního stavu a poslat oběti unesená dat tak, aby si pokud možno ničeho nevšimla, přestane posílat podvržené rámce, pošle oběti ARP-request a počká na odpověď ARP-reply. Výměnou těchto rámců dojde k obnovení původního stavu CAM tabulky.

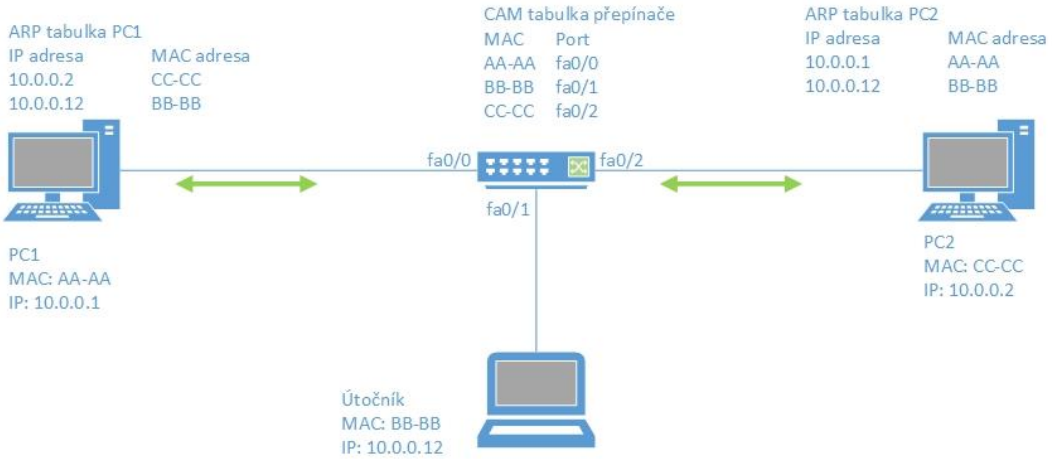
Obrana

Obrana proti tomuto útoku se shoduje s obranou proti útoku CAM table overflow (kapitola 4.1). Je zapotřebí zabezpečit porty přepínače tak, aby nebylo možné libovolně měnit mapování MAC adres na porty v CAM tabulce. (SPANGLER, 2003)

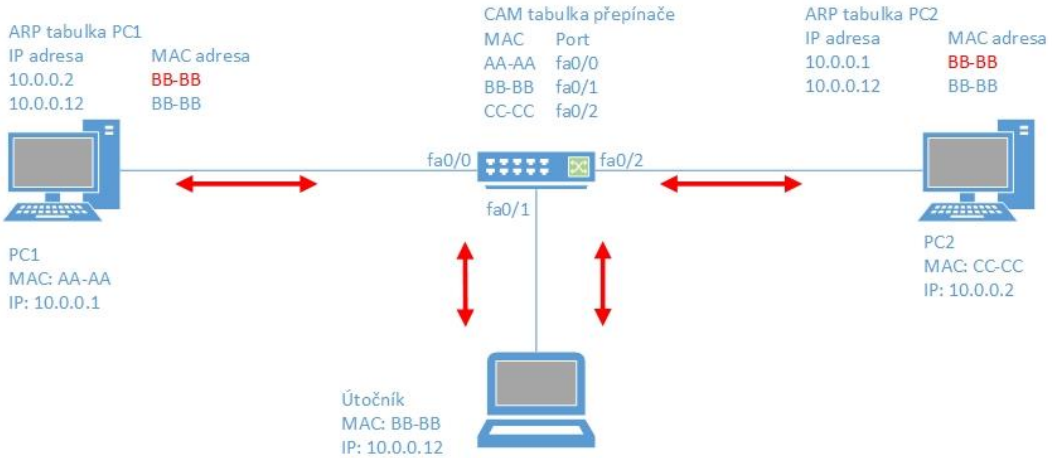
4.3 ARP cache poisoning

Útok jménem ARP cache poisoning spoléhá na slabiny protokolu ARP. Protokol ARP slouží k nalezení adresy MAC zařízení, pokud známe pouze jeho adresu IP, zjištěné dvojice IP – MAC jsou pak uloženy v tabulce ARP. Každý host na síti dynamicky aktualizuje svoji ARP tabulku pomocí protokolu ARP a jeho rámců ARP-request, ARP-reply. Slabina spočívá v tom, že host je schopen zapsat do své tabulky ARP změny bez předchozího vyslání příslušného ARP-request rámce. Tuto situaci nazýváme gratuitous (bezdůvodné) ARP. Těmito nevyžádanými zprávami s podvrženými adresami je pak otrávena ARP cache zařízení účastnících se komunikace, čímž dochází k přesměrování provozu, který nyní proudí k útočníkovi. Ten může rámce dále přeposílat uzlu, se kterým stanice komunikuje a naopak. Čímž dojde ke kompletnímu přesměrování komunikace a oběť nepozná, že je odposlouchávána, jedná se tedy o útok typu man-in-the-middle. Pohodlné provedení tohoto útoku umožňuje pro operační systémy Windows program Cain & Abel, pro Linux pak například program Ettercap, oba s grafickým uživatelským rozhraním.

Pro názornost je uveden konkrétní příklad. Na obrázku (Obrázek 11) lze vidět malou přepínanou síť, kde jsou ARP cache stanic již naplněny. Pokud bude chtít útočník přesměrovat síťový provoz mezi stanicemi PC1 a PC2, bude muset otrávit jejich ARP cache tak, že pomocí bezdůvodných ARP zpráv změní v ARP tabulce počítače PC1 MAC adresu počítače PC2 na svou MAC adresu a obdobně v tabulce PC2 MAC adresu PC1 rovněž na svou MAC adresu. Situaci po provedení ARP cache poisoningu znázorňuje Obrázek 12, šipky na obrázcích znázorňují, kudy proudí data. V tuto chvíli již veškerý provoz mezi PC1 a PC2 proudí přes počítač útočníka, který může dle libosti analyzovat nebo pozměňovat proudící data. Aby nedošlo k přerušení komunikace a tím pádem ke zjištění, že něco v síti není v pořádku, je třeba nastavit počítač útočníka tak, aby přeposílal přijaté pakety. Programy jako je Cain&Abel toto provádí automaticky.



Obrázek 11 – stav před otrávením ARP cache



Obrázek 12 – stav po otravě ARP cache

Obrana

Sofistikovanější přepínače mohou k odhalení útoku použít Dynamic ARP Inspection, službu, která analyzuje ARP provoz na směrovači a pomocí tabulky DHCP Snoopingu[8], za předpokladu, že v síti funguje server DHCP[9], dokáže odhalit podvrženě ARP pakety. Pokud v síti DHCP server není, lze DAI použít ve spojení s ručně vytvořenými ARP access listy. Spolehlivou, ale v praxi jen těžko použitelnou metodou, jak útoku zabránit, jsou statické záznamy ARP. Nekalé manipulace s ARP cahce lze také odhalit například pomocí programu ARPWatch, který podporuje Windows i Linux. (HARPER, a další, 2008)

[8] DHCP Snooping je funkce tvořící, zjednodušeně řečeno, rozhraní mezi DHPC serverem a klienty, jejím úkolem je filtrovat nedůvěryhodné DHPC zprávy.

[9] DHCP server automaticky přiděluje IP adresy uzlům, které si o ně zažádají.

4.4 VLAN Hopping

Technologie VLAN zjednodušuje správu sítě a zvyšuje její výkon, přináší však také možnost zneužití. Touto možností je, mimo jiné, takzvaný VLAN hopping, volně přeloženo jako přeskakování mezi sítěmi VLAN. Útok umožňuje přenést rámce z jedné VLAN do druhé bez použití routeru nebo L3 switche. Útok je veden tak, že útočníkova stanice připojená k přepínači vyjedná, díky většinou aktivnímu automatickému vyjednávání trunků na portu přepínače, trunk. Jak je známo, přes trunk mohou proudit rámce ze všech VLAN, tím pádem může útočník vysílat i přijímat rámce ze všech VLAN na přepínači. Útok lze provést dvěma způsoby.

- Vyjednáním trunku přímo mezi stanicí útočníka a přepínačem.
- Nastrčením dalšího přepínače, který vytvoří trunk mezi ním a legitimním přepínačem v síti. Prostřednictvím tohoto nastrčeného přepínače má pak útočník přístup k rámcům ze všech VLAN.

Obrana

Útoku zabrání vypnutí automatického vyjednávání trunků na všech portech. Například u přepínačů firmy Cisco trunky automaticky vytváří Dynamic Trunking Protocol (DTP), je tedy vhodné ho na portech zakázat. Trunky je pak potřeba na příslušných portech nastavit ručně. Dalším dobrým zvykem je vypnout všechny nepoužívané porty a umístit je do nepoužívané VLAN. (HARPER, a další, 2008)

4.5 STP Manipulation

Útok spočívá ve zmanipulování STP protokolu tak, že dojde ke změně topologie a odcizení root bridge. Za root bridge se v takovém případě vydává stanice útočníka, čímž získává přístup k veškerému provozu v daném segmentu sítě.

Útok je proveden následujícím způsobem. Útočníkova stanice začne do sítě rozesílat BPDU rámce signalizující změnu topologie. Následně se, při volbě nového root bridge, pokusí zmanipulovat volbu tak, že je root bridgem zvolena právě stanice útočníka. Pokud se tak stane, je útok úspěšný a útočník vidí rámce, které by za normálních podmínek nebyly přístupné.

Obrana

Obranu zajistí implementace funkcí BPDU guard a Root guard. BPDU guard slouží k ochraně access portů přepínače. V případě, že na port, kde je aktivována funkce BPDU guard dorazí BPDU rámec, port okamžitě přejde do stavu err-disabled. Je tedy vhodné ji aktivovat na všech uživatelských portech. Root guard určuje, které přepínače jsou vhodnými kandidáty na root bridge. Funkce se aktivuje na portech, které by neměli vést směrem k root bridge. (HARPER, a další, 2008)

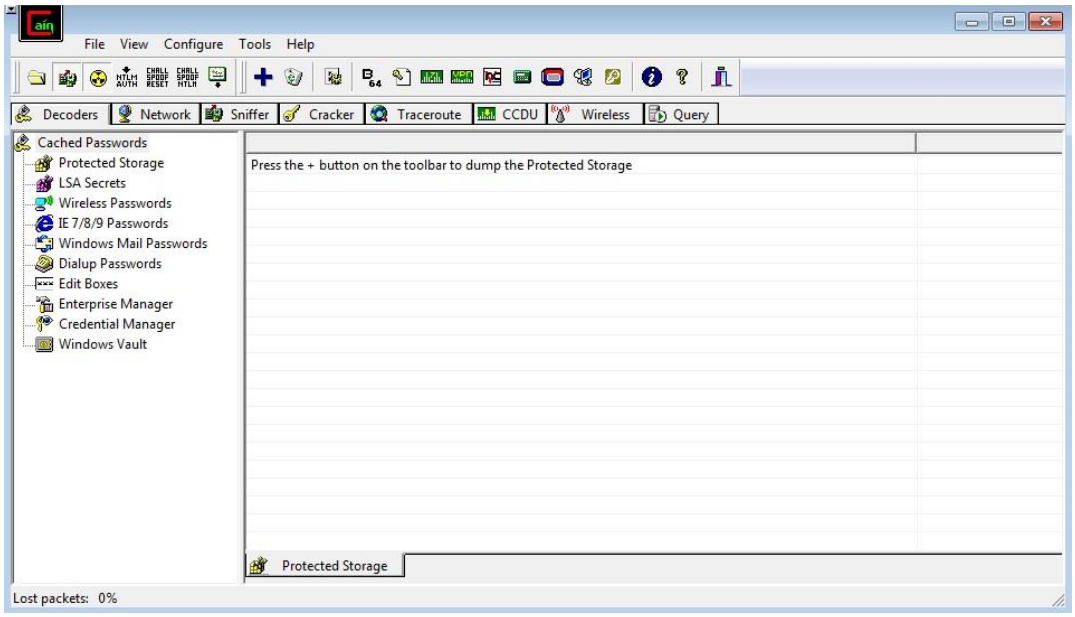
5 Cain&Abel

Tato kapitola představí program Cain&Abel password recovery tools, účel, za kterým byl vytvořen, jeho instalaci a vybrané funkce. Mějte prosím na paměti, že kapitola nemá představovat kompletní manuál k programu, ale popisuje pouze funkce, které jsou využívány v této práci. Kompletní a velmi přehledný manuál napsaný tvůrcem programu (MONTORO, 2001) je volně přístupný na webových stránkách a informace pro tuto práci byly čerpány výhradně z tohoto manuálu.

V první řadě je nutné zdůraznit, že tento program byl vyvinut výhradně pro etické využití. Neslouží tedy k nabourávání se do cizích sítí a následnému působení škod a odcizení citlivých informací. Má být používán administrátory, správci sítí, bezpečnostními konzultanty a dalšími odborníky, kteří potřebují ověřit bezpečnost své sítě a odhalit případně slabiny. Odhalení takových míst pak zpravidla vede k přijetí bezpečnostních opatření pro jejich zacelení a tím zvýšení bezpečnosti celé sítě.

Cain&Abel je nástroj navržený pro operační systémy Microsoft. Umožňuje snadnou obnovu několika druhů hesel pomocí odposlouchávání sítě, prolamování zašifrovaných hesel pomocí slovníkového útoku (Dictionary attack), útoku hrubou silou (Brute-force attack) nebo kryptoanalýzy. Dále umožnuje nahrávat hovory VOIP, analyzovat směrovací protokoly a obnovovat hesla bezdrátových sítí.

Program nevyužívá žádné softwarové slabiny ani chyby, které by nešli snadno opravit. Zahrnuje několik bezpečnostních aspektů/slabin protokolů, autentizačních metod, a mechanismů dočasného ukládání. Jeho hlavním účelem je zjednodušená obnova hesel a pověřovacích listin z různých zdrojů, dále poskytuje několik nestandardních nástrojů pro uživatele systémů Microsoft Windows.



Obrázek 13 – grafické uživatelské rozhraní programu Cain&Abel

5.1 Instalace

Program je poskytován zdarma na oficiálních stránkách výrobce (www.oxid.it) a lze ho odtud stáhnout. Program Cain&Abel se skládá ze dvou částí, část Cain je hlavní aplikace poskytující grafické uživatelské rozhraní, Abel je služba Windows skládající se ze dvou souborů (Abel.exe a Abel.dll).

Systémové požadavky:

- 10MB místa na pevném disku,
- operační systém Microsoft Windows 2000/XP/2003/Vista/7,
- ovladač WinPcap verze 2.3 nebo vyšší,
- ovladač AirPcap pro zpřístupnění funkcí pasivního bezdrátového snifferu a WEP crackeru.

K samotné instalaci programu je použit samoinstalační balík, po jeho spuštění stačí následovat pokyny. Všechny potřebné soubory jsou pak nakopírovány do instalačního adresáře a podadresářů.

Soubory programu Abel jsou také nakopírovány do instalačního adresáře, ale služba jako taková není automaticky naistalována do systému. Je tedy potřeba službu nainstalovat ručně. To je možno provést buď lokálně, nebo na vzdáleně, pomocí programu Cain. Ke vzdálené instalaci je třeba disponovat právy administrátora na cílové stanici.

Abel - lokální instalace

- K instalaci slouží soubor Abel.exe, který se nachází v adresáři, kde je naistalován program Cain. Pokud je použit 64bitový operační systém, použijte soubor Abel64.exe. Tím dojde k nainstalování služby do systému.
- Nyní lze službu spustit pomocí správce služeb (services.msc).

Abel – vzdálená instalace

- Použijte záložku Network v programu Cain, zde vlevo vyberte vzdálený počítač, kam chcete Abel nainstalovat.
- Pravý tlačítkem myši klikněte na ikonu počítače a vyberte „Connect As“.
- Vyplňte přihlašovací údaje k účtu administrátora na vzdáleném počítači.
- Jakmile budete připojeni, klidněte pravým tlačítkem myši na položku „Services“ a zde zvolte volbu „Instal Abel“.
- Tím jsou soubory Abel.exe a Abel.dll zkopírovány do prvního sdíleného adresáře, kam je možné zapisovat. Následně je služba automaticky nainstalována a spuštěna. Při instalaci se program Cain snaží detekovat, jestli hostitelská stanice používá 64bitový operační systém, pokud ano, je nainstalována 64bitová verze služby Abel.

Odinstalování

Odinstalování programu Cain je stejné jako u jiných programů, avšak při odinstalování programu Cain není automaticky odebrána služba Abel. Tu je však možné odebrat právě prostřednictvím programu Cain. Po kliknutí na položku Services se objeví všechny služby běžící na daném počítači, zde vybereme službu Abel a po kliknutí pravým tlačítkem zvolíme její odstranění. Soubory služby je třeba odstranit ručně.

5.2 Konfigurace

Před použitím programu Cain&Abel je zapotřebí nastavit několik parametrů. Kompletní konfigurační menu se skrývá pod položkou Configure na hlavní liště. Menu se skládá z devíti karet, vybrané karty jsou popsány níže.

5.2.1 Karta Sniffer

Zde se nachází seznam připojených síťových karet, kliknutím je vybrána ta, kterou budou nástroje sniffer[10] a APR[11] používat, program podporuje pouze adaptéry pro sítě Ethernet. V informační části karty je uvedena nainstalovaná verze ovladače Winpcap a identifikátor síťové karty. V sekci Options jsou tři zaškrtávací pole, je to

- Start sniffer on startup (zapne sniffer při spuštění programu),
- Start APR on startup (zapne APR při spuštění programu),
- Don't use promiscuous mode.

Poslední volba zakazuje použití promiskuitního módu. Pokud je síťová karta přepnutá do promiskuitního módu, znamená to, že zpracovává i rámce, které jí nejsou adresovány. Zakážeme-li tento mód, není možné při APR používat falšování MAC adresy (MAC spoofing).

5.2.2 Karta APR

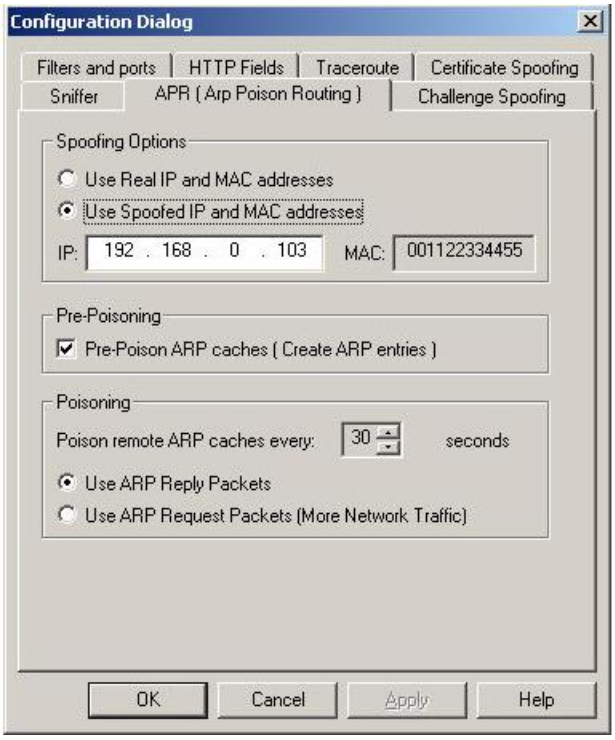
Na této kartě se nachází dialog pro konfiguraci APR (ARP Poison Routing). Cain používá pro posílání otrávených ARP paketů samostatné vlákno, které rozesílá pakety, dle původního nastavení, každých 30 sekund. To z toho důvodu, že nepoužívané záznamy jsou z ARP cache vzdálený hostů průběžně odstraňovány. V tomto dialogu je možné nastavit časový interval mezi rozesíláním otrávených paketů. Nastavení intervalu na několik sekund způsobí nárůst ARP provozu v síti. Naopak, pokud je interval příliš dlouhý, nemusím dojít k požadovanému přesměrování provozu.

V horní části dialogu se nachází kontejner Spoofing Options. Zde je možné nastavit, jaká IP a MAC adresa bude použita v hlavičce rámců Ethernet, paketů APR a přesměrovaných paketů. Při výběru první volby budou použity skutečné adresy zařízení, kde je APR spuštěn. To přináší nevýhodu v podobě možnosti vystopování útoku. Proto je zde druhá volba a to použití adres falešných. Při tom je třeba brát v potaz následující fakta.

[10] Nástroj pro odposlech síťového provozu.
[11] Jedná se o útok ARP cache poisoning (kapitola 4.3).

Falešná IP adresa musí být volnou adresou v dané podsíti. V první řadě, pokud je zvolena adresa již přidělená jiné stanici, dojde ke konfliktu IP adres, který je snadno odhalitelný. Dále, vzhledem k tomu že pakety ARP protokolu neprochází routerem do jiných podsíti ani do jiných VLAN, pokud je použita adresa mimo danou podsíť, vzdálený host pošle odpověď své default gateway[12], tím pádem nikdy nedorazí zpět. Adresa je programem po stisku tlačítka Apply automaticky zkontrolována, a pokud je již v síti používána, program o tom informuje.

Další úskalí se týká adres fyzických (MAC). Tak jako dvě stejně IP adresy v jedné podsíti i dvě stejné MAC adresy působí potíže, přepínače mohou mít problémy s konvergencí. Proto je v případě použití falešných adres ve výchozím stavu nastavena MAC adresa na hodnotu 001122334455, jejíž výskyt u jiného zařízení v síti je minimálně vysoce nepravděpodobný s výjimkou v případě, že by byl v síti spuštěn APR útok prostřednictvím programu Cain na jiné stanici. Je třeba podotknout, že taková adresa působí velmi podezřele a lze podle ní snadno identifikovat útok. Hodnotu adresy není možné měnit přímo prostřednictvím tohoto dialogu. Lze jí však změnit upravením hodnoty registru "SpoofMAC" nacházející se v "HKEY_CURRENT_USER\Software\Cain\Settings". Existují i podmínky, za kterých nelze vůbec použít falešnou adresu MAC. Pokud je na portu přepínače, ke kterému je stanice provádějící APR útok připojena, aktivována funkce Port Security (kapitola 4.1), přepínač odhalí, že na portu operuje zařízení s jinou MAC adresou než by mělo, což vede zpravidla k vypnutí portu.



Obrázek 14 – konfigurační dialog, karta APR

[12] Brána do jiné sítě.

5.2.3 Karta Filters and Ports

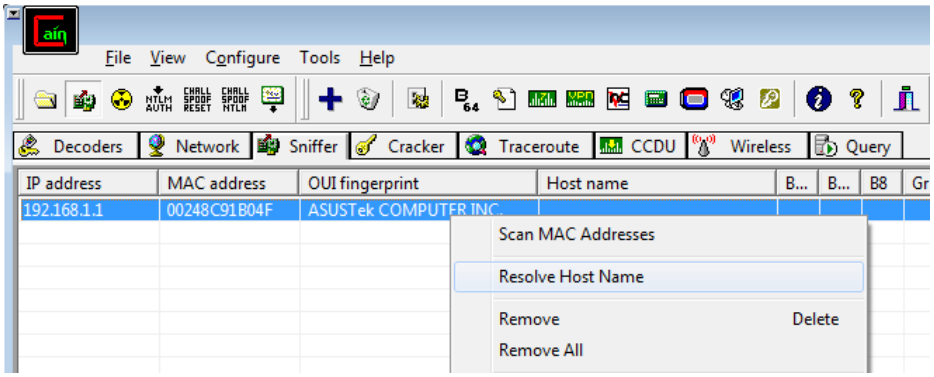
Prostřednictvím této karty je možné zapnout/vypnout protokolové filtry snifferu, případně změnit čísla portů, na kterých program naslouchá. Cain ze zachyceného provozu filtruje pouze přihlašovací údaje, neukládá celý obsah každého paketu. Protokolové filtry snifferu jsou vnitřně uspořádány tak, aby dokázaly fungovat i ve velice nespolehlivém prostředí, jakým je například síť pod útokem ARP cache poisoning.

5.3 Sniffer

Jednou z hlavních funkcí programu Cain&Abel je sniffer, sloužící k odposlechu síťového provozu. Sniffer se zaměřuje zejména na autentizační údaje a hesla putující po síti a neměl by být srovnáván s profesionálními sniffery jako je například Ethereal nebo Observer. Byl vyvinut pro fungování v prostředí přepínaných síti, kde úzce spolupracuje s další funkcí programu, kterou je ARP Poison Routing (kapitola 5.3.2). Aby bylo možné odhalit síťový provoz zajímavý z hlediska autentizačních údajů, dochází k jeho filtrování. Základní úroveň filtrování obstarává filtr BPF (Berkley Packet Filter), jenž zpracovává pouze IP a ARP provoz. Další filtrování provádí filtry autentizačních údajů pro jednotlivé protokoly, jejich kompletní seznam se nachází v příručce (MONTORO, 2001). Tyto filtry mohou být aktivovány/deaktivovány v hlavním konfiguračním protokolu na záložce Filters and Ports (kapitola 5.2.3).

5.3.1 MAC Scanner

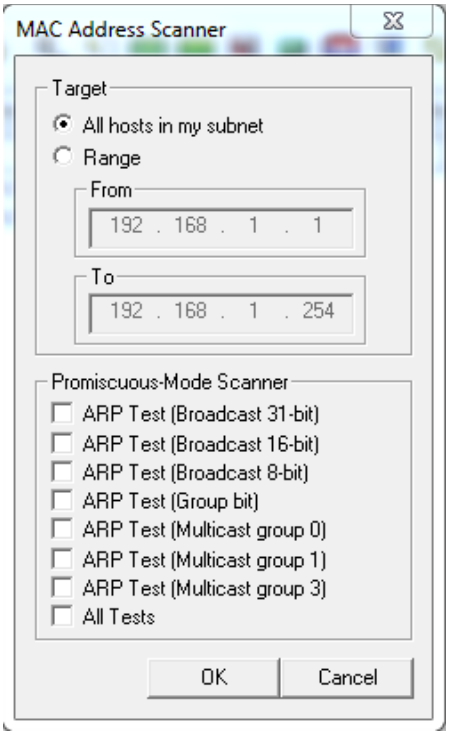
Součástí snifferu je nástroj MAC scanner, ten slouží k nalezení aktivních stanic v lokální podsíti. Jako vstup využívá rozsah adres v dané podsíti, pomocí paketů ARP Request/Reply dohledá k aktivním IP adresám MAC adresy příslušných zařízení, toto je schopen provést velmi rychle. Právě proto, že jsou k hledání MAC adres použity ARP pakety, které nemohou dosáhnout do jiné podsítě ani VLAN, může být hledání provedeno pouze v lokání doméně broadcast. Scanner rovněž zahrnuje databázi OUI, ta poskytuje informace o výrobci v síti nalezených síťových karet. To může být využito k snadnému odhalení aktivních síťových prvků, jako jsou například přepínače, směrovače, firewally, apod. U nalezených zařízení je také možno zjistit jejich název. K jeho zjištění dojde po vybrání volby „Resolve Host Name“ v nabídce, která se objeví po stisku pravého tlačítka myši na vybrané položce nalezených hostů. Scanner je uveden v činnost stiskem klávesy Insert nebo kliknutím na modrý symbol + v panelu nástrojů. Před samotným prohledáním sítě je třeba zadat rozsah IP adres, viz Obrázek 16. Rovněž je nutné mít zapnutý sniffer. Ten se aktivuje druhou ikonou zleva v panelu nástrojů.



Obrázek 15 – odhalená aktivní stanice

Promiscuous-mode Scanner

MAC Scanner dokáže odhalit i jiné sniffery nebo IDS[13] přítomné v lokální síti, pro tento účel je rozšířen o Promiscuous-mode Scanner. K odhalování používá paletu testů založených na paketech ARP. Jednotlivé testy lze aktivovat/deaktivovat v dialogovém okně MAC Scanneru, viz Obrázek 16. Co výsledky jednotlivých testů znamenají, uvádí (MONTORO, 2001).



Obrázek 16 – dialogové okno MAC Scanneru

5.3.2 ARP Poison Routing

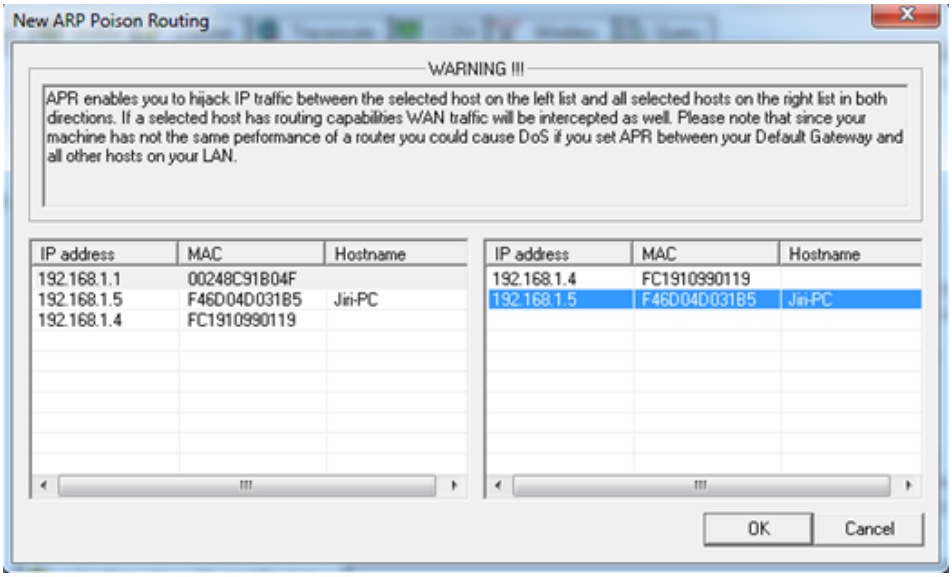
ARP Poison Routing je stěžejní funkcí snifferu programu Cain. Umožňuje odposlouchávání v přepínaných sítích a unášení komunikace mezi hosty. Název ARP

[13] Intrusion Detection System je síťový prvek sloužící k odhalování podezřelých aktivit ohrožujících bezpečnost sítě.

Poison Routing, dále jen APR, je odvozen ze dvou kroků nutných k úspěšnému odposlechnu v přepínané síti. Prvním krokem je vykonání útoku ARP cache poisoning (poison), který přesměruje pakety k útočníkovi a druhým nasměrování paketů (routing) k odpovídajícím hostům.

Princip útoku ARP cache poisoning je popsán v kapitole 4.3. Úkolem snifferu tedy není pouze otrávit ARP cache obětí, ale také obstarat zmíněný routing, tedy přeposílat unesené pakety jejich originálním adresátům, aby útok nebyl odhalen a komunikace mohla dále probíhat. Síťová karta útočníkova počítače musí kromě legitimního provozu zpracovávat také provoz spojený a APR útokem, což může mít, při větším objemu přenášených dat, znatelný vliv na výkon sítě. Aby bylo možné zmíněné přeposílání realizovat, musí sniffer nejprve zjisti dvojice IP a MAC adres obětí. To obstará MAC Scanner, který je potřeba spustit před zahájením útoku APR.

Uživatelské rozhraní pro obsluhu a sledování APR útoku se nachází v záložce Sniffer. Zobrazí se přepnutím na kartu APR v dolní části okna programu. Před spuštěním útoku je třeba z aktivních stanic nalezených MAC Scannerem vybrat dvojici uzlů, mezi kterými bude zachytávána komunikace. Nabídka pro jejich výběr se zobrazí kliknutím na symbol modrého + v panelu nástrojů nebo stiskem klávesy Insert. Zmíněná nabídka je zachycena na obrázku (Obrázek 17). Zde je vybrán uzel s IP adresou 192.168.1.1 a uzel s adresou 192.168.1.5., po spuštění útoku bude tedy zachytávána komunikace mezi těmito uzly v obou směrech. Vybraná dvojice a stav útoku se zobrazí v horní tabulce okna programu. Ke spuštění útoku dojde kliknutím na žlutý symbol v panelu nástrojů, pokud v tu chvíli není zapnutý sniffer, dojde automaticky k jeho aktivování. Útok APR programu Cain byl navržen tak, že dokáže obsluhovat útok na více uzlů zároveň. Po aktivování útoku program vytvoří oddělené vlákno pro rozesílán otrávených ARP paketů v nastavených intervalech.

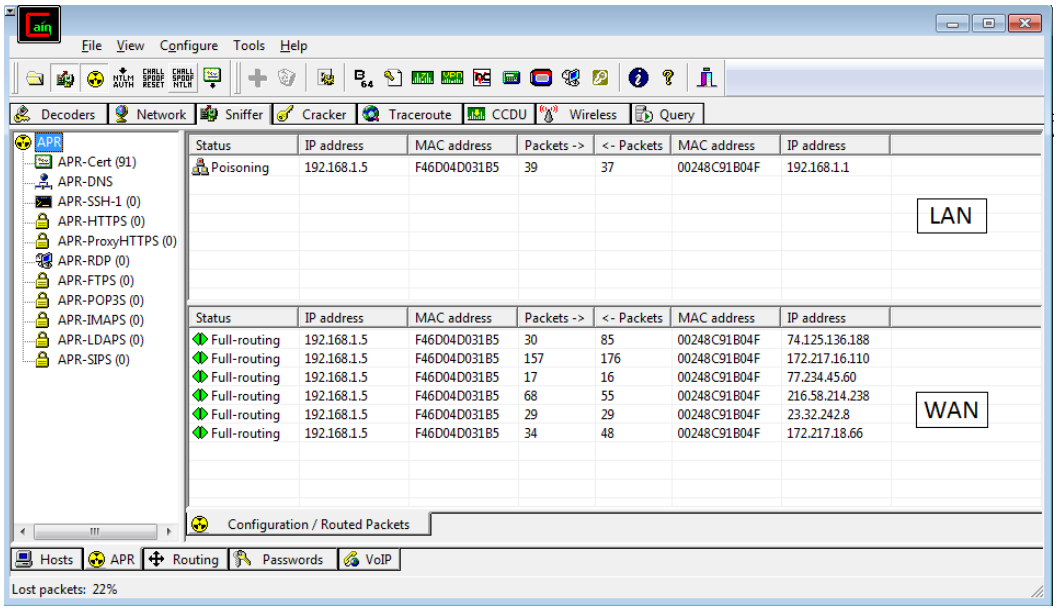


Obrázek 17 – dialog pro vytvoření nového APR útoku

Na dalším obrázku (Obrázek 18) je vidět již probíhající APR útok. Na každém řádku v části LAN se nachází dvojice otrávených hostů, mezi kterými je unášen provoz, kromě jejich adres je zde zaznamenáván i počet úspěšně odposlechnutých paketů. Může nastat situace, kdy roste počet přijatých paketů pouze v jednom směru komunikace, to znamená, že se jeden z hostů útoku úspěšně brání.

V části WAN jsou zaznamenávány počty paketů mířících k hostům ležícím mimo místní síť. Záznamů v této části přibývá rychle zvláště v případě, kdy je odchytávána komunikace mezi stanicí v síti a výchozí bránou. Každý záznam v části WAN může nabývat jednoho ze tří definovaných stavů.

- **Broadcasting** – tento stav značí, že APR obdrželo paket pocházející z jiné sítě adresovaný stanici ležící v doméně broadcast, ve které se nachází stanice, ze které byl útok spuštěn. Takový paket musí být správně přesměrován, ale správná cílová MAC adresa není známa. V takovém případě je paket rozeslán všem stanicím v místní síti.
- **Half-Routing** – v tomto stavu probíhá přesměrovávání pouze v jednom směru. To je zapříčiněno tím, že jedna z napadených stanic útoku úspěšně odolává, čímž nedojde k přesměrování jedné části komunikace a všechny pakety proudící tímto směrem jsou ztraceny. Tím je znemožněno získat některé autentizační údaje.
- **Full-Routing** – v tomto případě se útok zcela zdařil a dochází ke kompletnímu unesení komunikace a odcizení všech dostupných autentizačních údajů.



Obrázek 18 – probíhající APR útok

5.3.3 Passwords

Při odposlechu provozu v síti sniffer filtruje ze zachycených paketů uživatelská jména a hesla, případně jejich otisky (hashe). Tyto zobrazuje na kartě Passwords, kde jsou přehledně tříděny podle protokolů, které je přenesly. Pokud sniffer zachytí heslo přenášené

nešifrovaným protokolem, okamžitě ho zobrazí v podobě čistého textu spolu s dalšími parametry přenosu (uživatelské jméno, IP adresy, čas zachycení, atd.). Nešifrovanými protokoly jsou například protokoly http, ftp, pop3, telnet a další, kompletní seznam uvádí (MONTORO, 2001). Zde se ukazuje největší bezpečnostní slabina těchto protokolů. Uživatel může použít libovolně složité heslo, je-li však takové heslo odposlechnuto při komunikaci, útočník ho obdrží ihned v podobě čistého textu. Oproti tomu, protokoly používající šifrování (https, ftps, pop3s, ssh) posílají hesla v podobě otisku (hashe). Tyto otisky jsou snifferem rovněž zachyceny, avšak získat z nich přihlašovací údaje v podobě čistého textu již není tak triviální jako u nešifrovaných protokolů. V případě použití silného hesla to může být velmi komplikované zvláště z hlediska časové náročnosti. Zachycené otisky jsou rovněž na kartě Passwords zařazeny pod příslušný protokol. K jejich prolomení lze použít lamač hesel Password Cracker programu Cain. Zaslání hesla do Crackeru obstará volba Send to Cracker, dostupná v nabídce zobrazené kliknutím pravým tlačítkem myši na příslušný hash, zde je pak možno na hashe aplikovat postupy pro jejich prolomení (slovníkový útok, útok hrubou silou, atd.).

5.4 Password Cracker

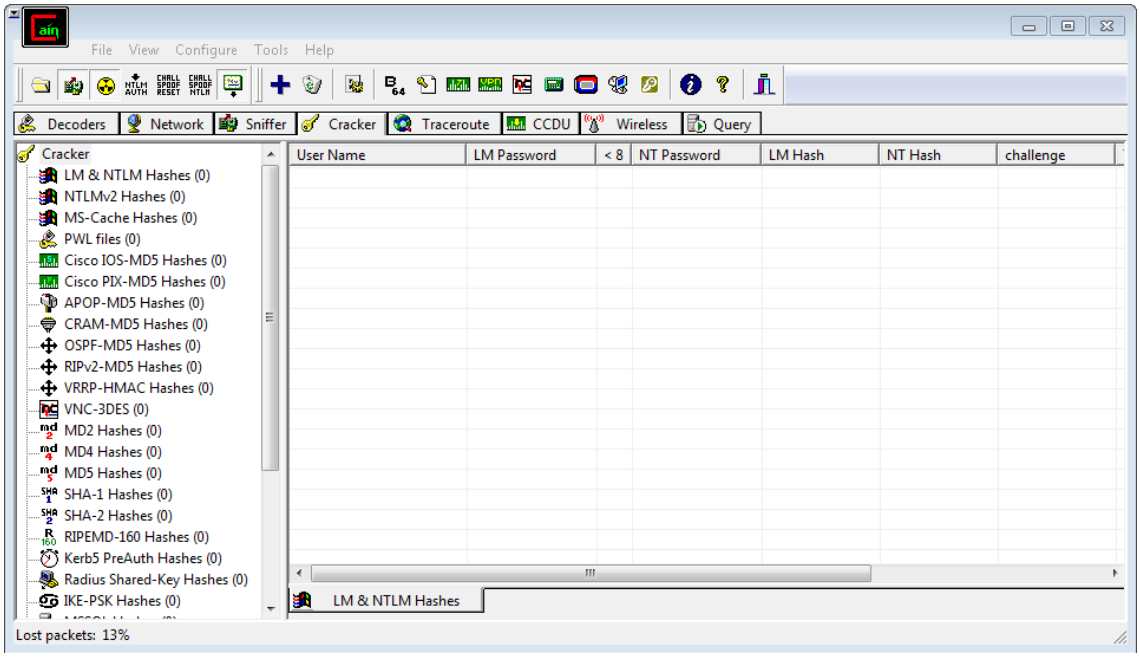
Na kartě Cracker v programu Cain se nachází nástroj sloužící k prolamování hashů a zjištění jejich nešifrované podoby. Nástroj podporuje většinu běžných hashovacích algoritmů a některé na nich založené šifrovací algoritmy.

Podporované typy hashů:

MD2, MD4, MD5, SHA1, SHA2 (256 bit), SHA2 (384 bit), SHA2 (512 bit), RIPEMD160.

Podporované šifrovací algoritmy:

PWL files, Cisco-IOS Type-5 enable passwords, Cisco PIX enable passwords, APOP-MD5, CRAM-MD5, LM, LM + Challenge, NTLM, NTLM + Challenge, NTLM Session Security, NTLMv2, RIPv2-MD5, OSPF-MD5, VRRP-HMAC-96, VNC-3DES, MS-Kerberos5 Pre-Auth, RADIUS Shared Secrets, IKE Pre-Shared Keys, Microsoft SQL Server 2000, Microsoft SQL Server 2005, Oracle, Oracle-TNS-DES, Oracle-TNS-3DES, Oracle-TNS-AES128, Oracle-TNS-AES192, MySQL323, MySQLSHA1, SIP-MD5, WPA-PSK, WPA-PSK-AUTH, CHAP-MD5, MS-CHAPv1, MS-CHAPv2.



Obrázek 19 – Cracker

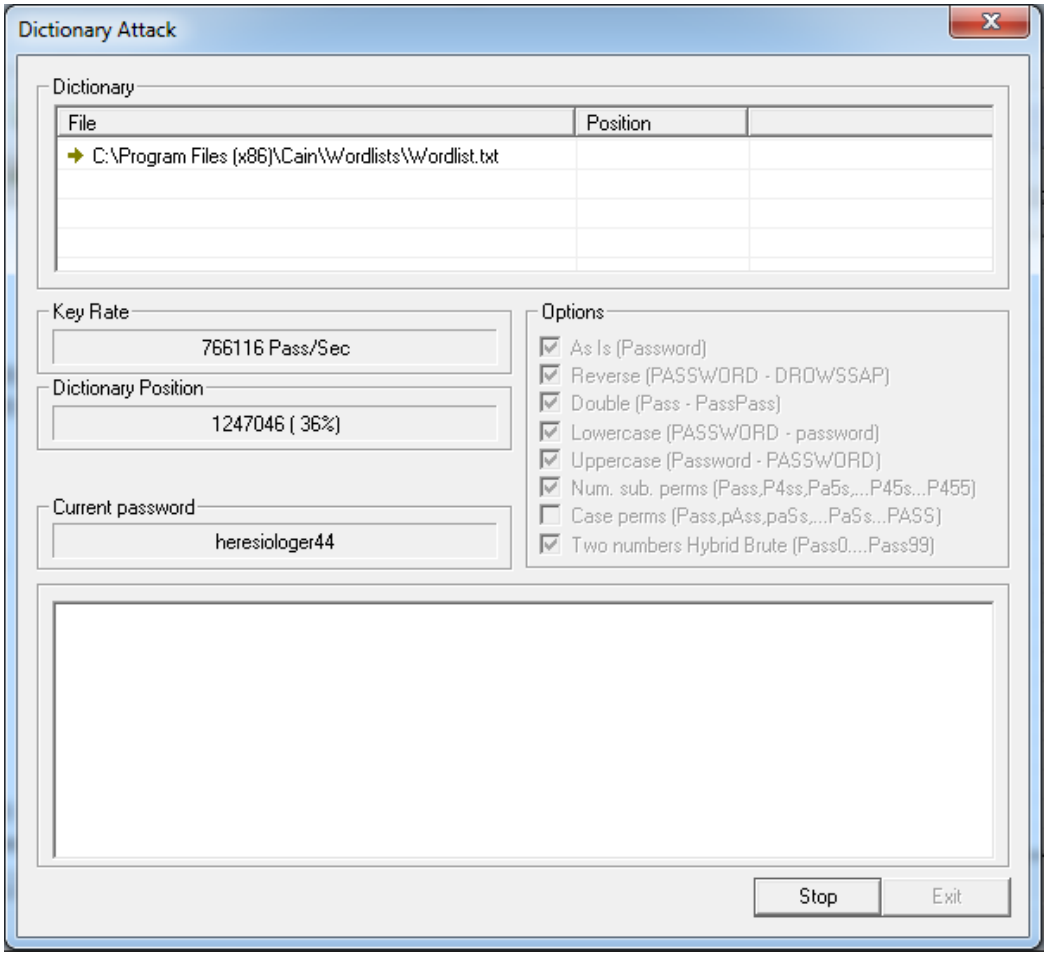
Zašifrovaná hesla poslaná do Password Crackeru se automaticky zařadí pod správný typ hashe nebo šifrovacího algoritmu. Kliknutím na kteroukoli kategorii v levé části okna programu se zobrazí všechny hashe v ní uložené. Na ty je pak možno aplikovat jednotlivé útoky. Cain nabízí tři typy útoků.

- **Slovníkový útok** (Dictionary attack).
- **Útok hrubou silou** (Brute force attack).
- **Kryptoanalýza** (Cryptanalysis attack).

5.4.1 Slovníkový útok

Předpokladem pro úspěch slovníkového útoku je to, že si uživatel zvolí slabé, doslova slovníkové heslo. Heslem je v takovém případě libovolné slovo, například oblíbená značka piva, jméno aktuální přítelkyně, apod. Uživatelé taková hesla často volí proto, že si je dokáží snadno zapamatovat, avšak z hlediska odolnosti proti prolomení jsou slovníková hesla naprosto nevhodná. Útok funguje tak, že se postupně prochází slovník a u každého slova v něm se zjišťuje, jestli právě toto slovo není hledaným heslem. Efektivitu tohoto útoku lze dále zvyšovat a to použitím rozsáhlého slovníku, případně více slovníků, které pokryjí co největší množství výrazů. Případně manipulací se znaky jednotlivých slov, například měnit velikost písmen, zkusit slovo zadat pozpátku, atd.

Dialogové okno pro nastavení a provedení slovníkového útoku se nachází v nabídce, která se zobrazí kliknutím pravým tlačítkem myši na požadovaný hash. Kliknutím na volbu Dictionary Attack se zobrazí zmíněný dialog (Obrázek 20).



Obrázek 20 – dialogové okno slovníkového útoku

V sekci Dictionary v tomto okně, lze přidávat a odebírat soubory slovníků, ve kterých se bude heslo hledat. V sekci Options se dají pomocí checkboxů zakázat/povolit dodatečné úpravy testovaného řetězce.

- As Is – zkusí se použít slovo ze slovníku tak, jak je v něm zapsáno (Heslo).
- Reverse – slovo je zadáno pozpátku (Heslo – olseH).
- Double – použité slovo je zdvojeno (Heslo – HesloHeslo).
- Lowercase – řetězec je převeden na malé znaky (HESLO – heslo).
- Uppercase – opak Lowercase (HESLO – heslo).
- Numbers substitution permutaions – určitá písmena v řetězci jsou nahrazena číslicemi (Heslo – Hes10).
- Case permutations – v řetězci jsou postupně vyzkoušeny všechny kombinace velkých a malých písmen (heslo – Heslo – HeslO – … – HESLO).
- Two numbers Hybrid-Brute – za každé slovo ze slovníku jsou připojeny maximálně dvě číslice (heslo0 – heslo1 – … – heslo9 – heslo00 – … – heslo99).

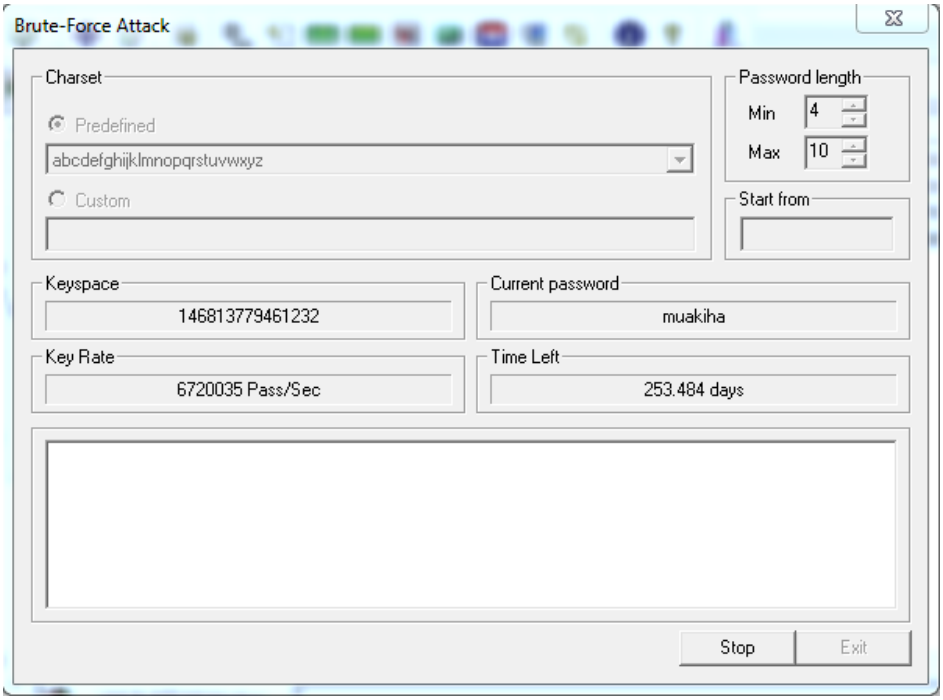
Sekce Key Rate ukazuje kolik hesel je vyzkoušeno za jednu sekundu. O kousek níže, v sekci Dictionary Position je uvedena aktuální pozice ve slovníku a kolik procent slov ze slovníku již bylo otestováno. A nakonec v sekci Current Password se zobrazuje aktuálně testovaný řetězec.

Tato metoda lámání hesel je vhodná spíše pro zjišťování hesel běžných uživatelů, u kterých je stále poměrně vysoká pravděpodobnost, že budou slovníkové heslo používat. Heslo administrátora tento útok pravděpodobně neodhalí. Rychlost tohoto útoku zcela závisí na velikosti slovníku a zvolených modifikacích testovaného řetězce.

5.4.2 Útok hrubou silou

Prolomení šifry pomocí útoku hrubou silou (anglicky Brute force attack) spočívá v postupném zkoušení všech možných kombinací znaků. O vhodnosti nasazení tohoto útoku lze rozhodnout na základě délky klíče dané šifry a výpočetním výkonu útočníkova stroje.

Password Cracker programu Cain postupně testuje všechny možné kombinace znaků z předem definované (Predefined) nebo vlastní (Custom) sady znaků. Dialogové okno útoku na Obrázku 21 zachycuje již probíhající útok. V sekci Charset lze před jeho zahájením, zvolit znakovou sadu, ze které se budou tvořit kombinace znaků pro odhalení hesla. V nabídce jsou různě rozsáhlé znakové sady čítající znaky od pouze malých písmen abecedy až po všechna mála i velká písmena, číslice a speciální znaky. V sekci Password length je možné nastavit horní a dolní hranici délky hesla. Pokud je zvolena znaková sada obsahující všechny znaky hesla a zároveň délka hesla vyhovuje zmiňovaným hranicím, je útoku hrubou silou vždy úspěšný. Je však otázkou, jak dlouho bude hledání hesla trvat. V případě použití silného hesla a lámání na běžném stroji se může jednat o řadu let, která bude počítač k prolomení potřebovat. Například na Obrázku 20 si lze všimnout, že pokud se programu bude snažit najít heslo s délkou 4 – 10 znaků a znaková sada bude obsahovat pouze malá písmena abecedy, bude běžnému počítači trvat zhruba 253 dní, než vyzkouší všechny kombinace. Pokud bude použita znaková sada čítající mala i velká písmena a číslice, doba nutná pro vyzkoušení všech kombinací se prodlouží na těžko představitelné 4000 let.



Obrázek 21 – dialogové okno útoku hrubou silou

5.4.3 Kryptoanalýza

Tento způsob umožňuje dešifrovat hesla pomocí metody Faster Cryptanalyctic timememorytrade off. K tomu je použita sada velkých tabulek s předem vypočítanými hodnotami hashů, čímž je dešifrování značně urychleno. Tyto tabulky se odborně nazývají Rainbow tabulky. Nicméně, tato metoda není vhodná pro lámání odposlechnutých hashů ze síťové komunikace, vhodná je spíše pro dešifrování přímých hashů, používaných pro lokální ukládání hesel. Vygenerování Rainbow tabulky obstará windows utilita „winrtgen“, která je nainstalována spolu s programem Cain a nachází se v jeho instalačním adresáři.

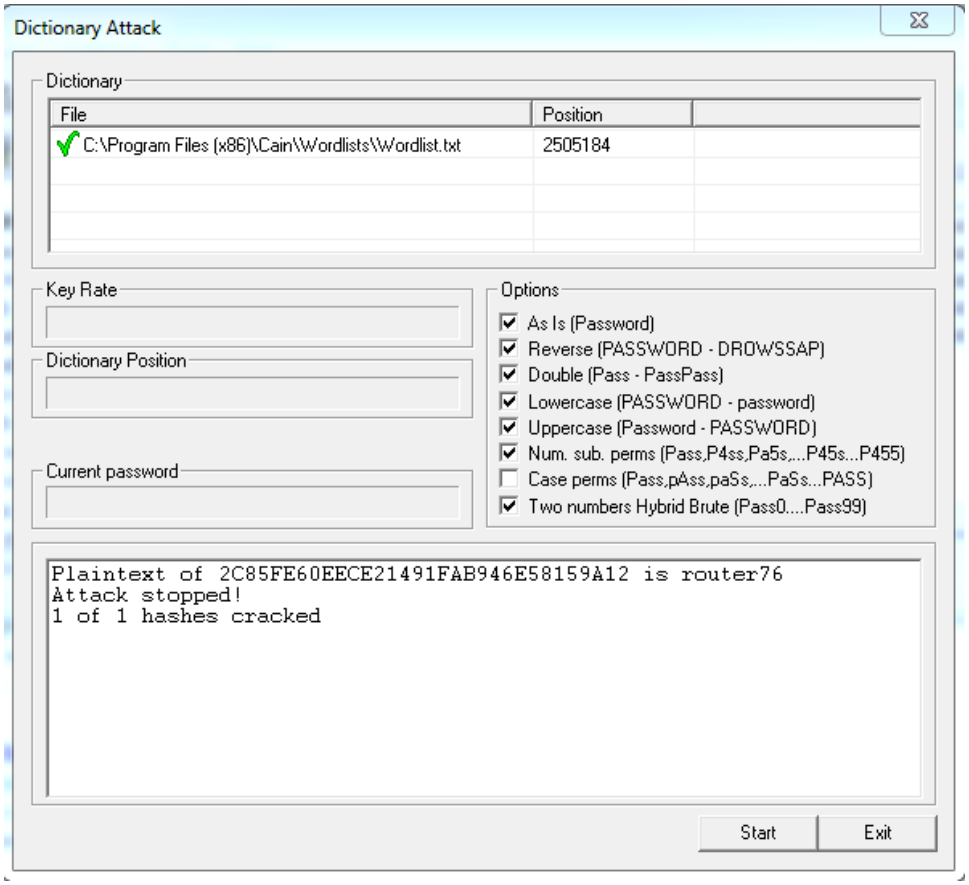
6 Praktická část

Praktická část práce demonstruje konkrétní použití programu Cain&Abel. Všechny příklady byly provedeny v laboratoři, nebyla tedy ohrožena žádná citlivá data. V první úloze je zdokumentováno odkrytí hesla uživatele na lokální stanici, toho lze využít například, zapomene-li uživatel své heslo. Druhá úloha odhaluje, jak snadné je zachytit citlivé údaje pokud jsou po síti transportovány nešifrovanými protokoly. Třetí pak dokládá, že ani šifrované protokoly nejsou naprosto bezpečné a i při jejich použití je třeba dbát na důkladné zabezpečení sítě. U všech třech útoků je popsáno, jak se před nimi efektivně bránit.

6.1 Získání hesla lokálního uživatele

Pokud je z nějakého důvod potřeba odhalit heslo lokálního uživatele, lze k tomu použít program Cain&Abel, konkrétně jeho lamač hesel popsaný v kapitole 5.4. Hesla nejsou v systému Windows uložena jako prostý text, nýbrž v podobě NTLM hashe. Tyto hashe dokáže program načíst z uložiště na pevném disku do Crackeru, kde na ně lze uplatnit metody lámání hesel popsané v kapitolách 5.4.1, 5.4.2 a 5.4.3. V tomto scénáři byl zvolen slovníkový útok z kapitoly 5.4.1. Slovníkový útok je většinou první metodou, která se pro prolomení hesla používá, protože běžní uživatelé často volí slovníková hesla, díky čemuž bývá často úspěšný, pokud selže, je použita jiná, náročnější metoda.

Prvním krokem při odhalování hesla uživatele je načtení otisku hesla z databáze operačního systému, to obstará program Cain automaticky. Od verze operačního systému Windows Vista je pro ochranu hesel defaultně použit NTLM hash, který nahradil starší a snadno prolomitelný LM hash. V Crackeru je tedy potřeba ze stromu v levé části obrazovky vybrat kategorii LM & NTLM hashes, zde se kliknutím na modrý symbol + v panelu nástrojů zobrazí dialog, pomocí něhož se importují hashe hesel z lokální databáze. Lze také importovat hashe z textového souboru nebo SAM databáze. Po načtení stačí vybrat z nalezených uživatelských účtů ten, jehož heslo má být zjištěno. V tomto případě je to účet s uživatelským jménem Victim. Z nabídky, zobrazené po kliknutí pravým tlačítkem myši na řádek uživatele Victim, je vybrán slovníkový útok na NTLM hash. V dialogu slovníkového útoku je třeba vybrat slovník, jehož slova a jejich modifikace budou testována, jestli nejsou hledaným heslem. V adresáři programu Cain v podadresáři Wordlists je uložen základní slovník. Dále lze použít libovolné slovníky třetích stran, případně si vytvořit vlastní. Před spuštěním útoku je vybrán slovník případně slovníky, které budou použity. Import slovníku je proveden stiskem klávesy Insert, v zobrazeném dialogu pak stačí vybrat příslušný slovník. Zde byl vybrán základní slovník programu Cain Wordlist.txt. Dále byly vybrány modifikace řetězce se sekce Options, aby byla zvýšena pravděpodobnost odhalení hesla a nakonec byl útok tlačítkem Start spuštěn. Čas potřebný pro vyzkoušení všech slov ze slovníku a jejich modifikací záleží na velikosti slovníku a zvolených modifikacích, takto nastavený útok (Obrázek 22), používající defaultní slovník trval pouhých 39 sekund.



Obrázek 22 – prolomené heslo

6.1.1 Obrana proti prolomení hesla

Není lepší obrany proti tomuto útoku, než volba skutečně silného hesla. Proto budou v této sekci shrnuty způsoby, jak silné heslo tvořit. Inspirací byly typy uvedené na stránkách pomoci uživatelům firmy Google. (Google.com, 2016)

Začněme obecnými doporučeními jak s hesly zacházet. V první řadě by hesla neměla být nikdy psána na papír nebo do souboru jehož název by prozradil jeho obsah. Pokud není možné si hesla zapamatovat, nabízí se použít důvěryhodný program pro správu hesel. Rovněž by každý důležitý účet, jako je například email, internetové bankovnictví, uživatelský účet na počítači, atd., měl mít vlastní heslo. To z důvodu, že pokud by bylo použito heslo pro všechny účty stejné a útočníkovi by se jej podařilo odhalit, měl by rázem přístup ke všem účtům.

Odolnost hesla určuje jeho délka a použité znaky. Doporučuje se používat hesla s minimální délkou 8 znaků, která by měla ideálně obsahovat velká a malá písmena, číslice a speciální znaky. Nemělo by se také jednat o běžná slova, která by se mohla nacházet ve slovnících pro slovníkové útoky i běžná slova však lze výrazně modifikovat, jak ukazuje následující příklad.

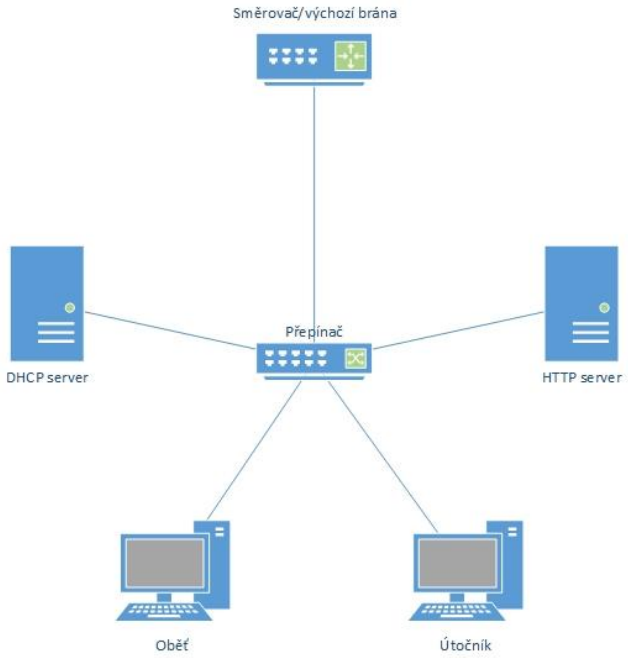
Příklad silného hesla: Un1v3rzit@_ParDu8ic€_§€1

Toto heslo je v podstatě neprolomitelné pro slovníkový útok a i útok hrubou silou na výkonném stroji by zabral velice dlouhou dobu. Avšak správně nastavený útok hrubou silou je vždy úspěšný. Proto je vhodné hesla s několikaměsíční frekvencí obměňovat.

6.2 ARP Poison Routing, útok na nešifrovaný protokol

Tento útok odhaluje největší slabinu nešifrovaných protokolů, kterou je bezpochyby to, že přenáší data, tak jak jsou, tedy například přihlašovací údaje v podobě čistého textu. Pokud se k tomu ještě přidá slabě zabezpečená místní síť, je pro útočníka velmi snadné odcizit citlivá data. Často používaným nešifrovaným protokolem je http, jehož prostřednictvím je přenášen obsah webových stránek včetně přihlašovacích údajů, dnes již bývá často nahrazen šifrovaným protokolem https. V tomto příkladu bude předvedeno, jak z http komunikace odchytit přihlašovací údaje.

Útoku bude proveden na zjednodušené síti, která byla vytvořena čistě pro potřeby demonstrace útoku a následné obrany. Její topologii zachycuje Obrázek 23. Ústředním bodem sítě je přepínač, konkrétně Cisco Catalyst 2960, který propojuje všechny ostatní uzly, dále se zde nachází počítač útočníka a oběti, http server, ke kterému se bude oběť snažit připojit a DHCP server, jehož úloha v síti bude vysvětlena v sekci věnující se obraně proti tomuto útoku (6.2.1). Bránu do ostatních síti znázorňuje směrovač.

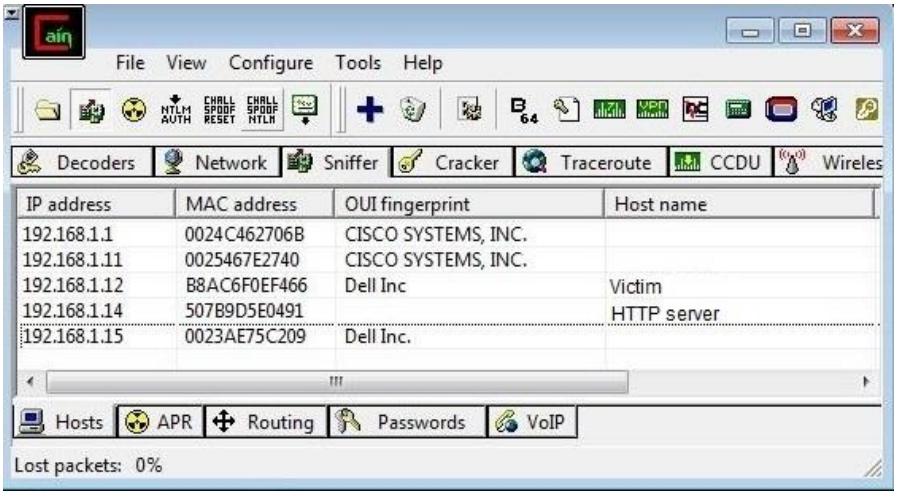


Obrázek 23 – topologie sítě pro testování útoku

Nyní přistupme k provedení útoku. Jedná se o útok popsaný v kapitole 5.3.2 tedy o ARP Poison Routing, dále jen APR. Před zahájením útoku byla pomocí MAC Scanneru (kapitola 5.3.1) prozkoumána místní síť a zjištěny adresy aktivních uzlů, pro identifikaci oběti a http serveru, bylo dále třeba zjistit názvy stanic, které se ukrývají pod nalezenými adresami, viz obrázek 24. Je třeba zmínit, že v reálné situaci se pravděpodobně nebude http

server nacházet ve stejně podsíti jako oběť a útočník. Stačí však odposlouchávat komunikaci mezi obětí a výchozí bránou, čímž bude zachycena i komunikace se vzdáleným http serverem. Po provedení průzkumu lze přistoupit k samotnému útoku. V dialogu pro vytvoření nového APR útoku byl vybrán počítač oběti s IP adresou 192.168.1.12 a http server s adresou 192.168.1.14. Poté už stačilo jen spustit útok příslušným tlačítkem v panelu nástrojů a čekat, až se bude oběť pokoušet na http serveru autentizovat. Obrázky 25a,b a 26a,b dokumentují, jakým způsobem program zmanipuloval APR cache oběti a http serveru. Program v tomto příkladu používá pro pakety sloužící k otravení ARP cache falešné adresy, IP 192.168.1.128 a MAC 00-11-22-33-44-55, problematika použití falešných adres je vysvětlena v kapitole 5.2.2. Jak je patrné z APR tabulek na obrázcích 25b a 26b, oběť i http server mají nastaveny adresy protějšku na 00-11-22-33-44-55, tudíž je splněna podmínka pro úspěch APR útoku a veškerá data v obou směrech putují k útočníkovi, kde je zpracovává filtr programu Cain, který z nich filtruje přihlašovací údaje, nalezené pak zařadí pod protokol, kterým byla přenesena. Na Obrázku 26 jsou zachycené přihlašovací údaje, zařazené ve správné kategorii.

Útok byl tedy zcela úspěšný, došlo přesměrování komunikace a odchycení přihlašovacího jména a hesla, identita útočníka zůstala skryta díky použití falešných adres. Po ukončení útoku po sobě navíc program Cain zamete stopy a uvede ARP tabulky do původního stavu.

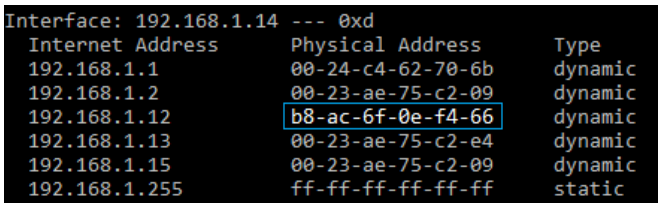


Obrázek 24 – výstup MAC Scanneru

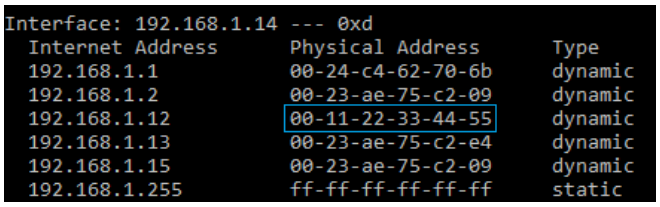
a)

b)

Obrázek 25 – a) ARP cache oběti před útokem b) po útoku

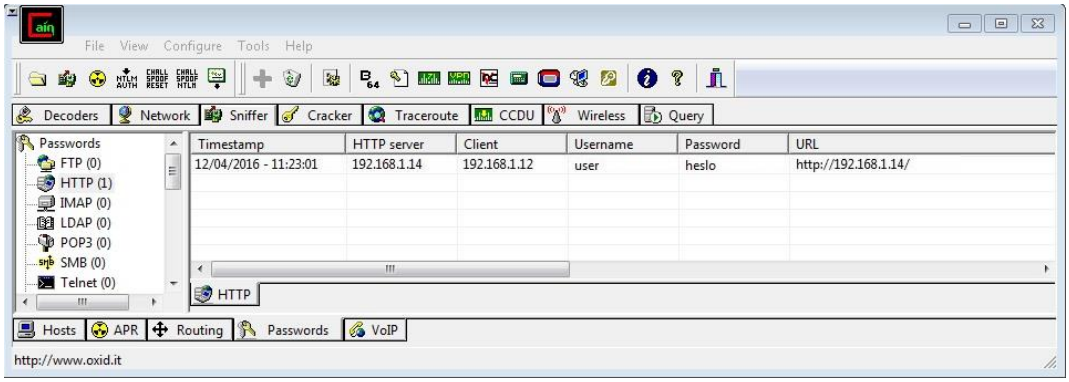


a)



b)

Obrázek 26 – a) ARP cache http serveru před útokem b) po útoku



Obrázek 27 – odcizené přihlašovací údaje

6.2.1 Obrana proti APR

Chceme-li účinně zabezpečit místní síť proti ARP cache poisoningu a v síti použitý přepínač disponuje potřebnými funkcionalitami, jeví se jako nejlepší řešení zabezpečit právě tento přepínač a jeho porty. Pokud bude přepínač efektivně filtrovat ARP provoz a otrávené pakety zahazovat, nelze ARP útok provést.

V ukázkové topologii je použit přepínač Cisco Catalyst 2960 s verzí IOS 15, která disponuje funkcí Dynamic ARP Inspection, která dokáže filtrovat ARP provoz a na základě záznamů z DHCP snooping binding database odhalit otrávené pakety a ty zahazovat. Z toho že DAI pro své fungování potřebuje záznamy z DHCP snooping binding database vyplívá, že na přepínači je nutné nakonfigurovat a spustit i DHCP snooping.

DHCP Snooping slouží primárně k zamezení provozu nelegitimních DHCP serverů v síti. Dělí porty na důvěryhodné (trusted), ke kterým je připojen legitimní DHCP server nebo další přepínač a přes které můžou proudit odpovědi na DHCP žádosti, a nedůvěryhodné (untrusted). Nedůvěryhodné jsou všechny porty, krom těch, které byly nakonfigurovány jako důvěryhodné. Nedůvěryhodný port zahazuje všechny DHCP odpovědi, čímž zamezuje připojení nelegitimního DHCP serveru. DHCP snooping vytváří zmiňovanou DHCP snooping binding database, ve které přiřazuje ke každé zapůjčené IP adrese MAC adresu stanice, které byla zapůjčena. Této databáze pak využívá DAI k ověření legitimity ARP paketů.

Použití DHCP snoopingu je však podmíněno tím, že jsou v síti IP adresy přidělovány DHCP serverem. Pokud tomu taky není, je třeba ručně vytvořit takzvaný ARP access list, který poskytuje stejné informace jako DHCP snooping binding database.

Konfigurace DHCP snooping probíhá následovně:

```
!Zapnutí DHCP snoopingu:
Switch(config)#ip dhcp snooping
!Aktivace DHCP snoopingu na VLAN 10
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#interface FastEthernet 0/4
!k portu Fa 0/4 je připojen DHCP server, označíme jej
!tedy jako důvěryhodný (tzn. propouští DHCP odpovědi).
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
!určení úložiště pro DHCP snooping databázi:
Switch(config)#ip dhcp snooping database flash:/dbdhcp.txt
```

Nyní lze spustit DAI, takto bezpečnostní funkce rovněž využívá důvěryhodné a nedůvěryhodné stavy portů. Nedůvěryhodné by měli být všechny porty, ke kterým jsou připojeny koncové stanice uživatelů. Na těchto portech probíhá kontrola ARP provozu. Jako důvěryhodné lze nastavit porty, ke kterým jsou připojeny další přepínače. Zde je však třeba postupovat s rozmyslem, pokud by například sousední přepínač připojený přes důvěryhodný port nepoužíval DAI, dalo by se přes něj poslat otrávené ARP pakety. Na důvěryhodném portu totiž žádná kontrola neprobíhá. Konfigurace je v tomto případě následující:

```
!zapnutí DAI pro VLAN 10:
Switch (config)#ip arp inspection vlan 10
!port Fa 0/1 lze nastavit jako důvěryhodný, neboť na tento port
!není připojena uživatelská stanice
```

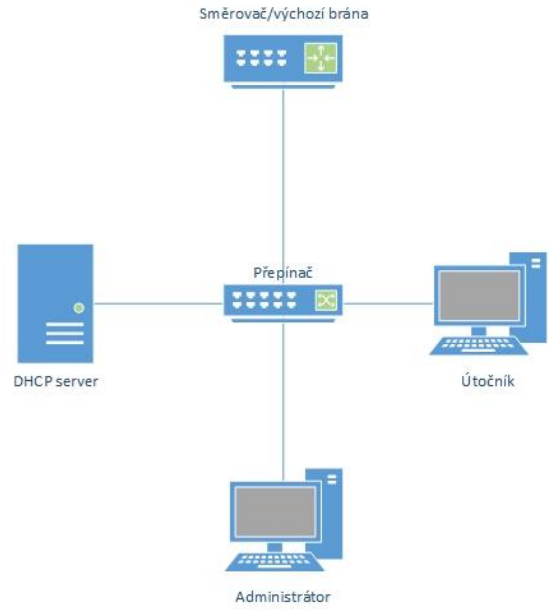
```
Switch (config)#int Fa 0/1

Switch (config-if)#ip arp inspection trust
```

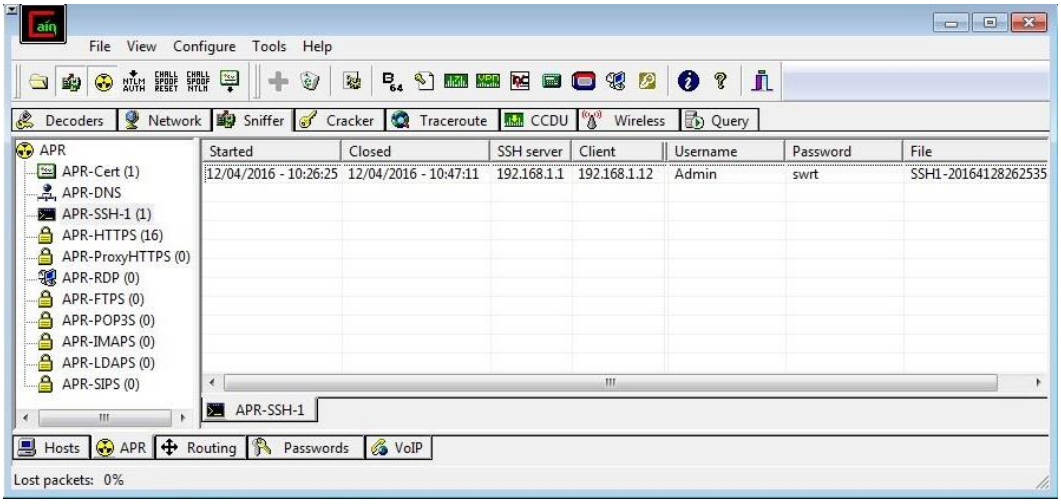
6.3 ARP Poison Routing, útok na šifrovaný protokol SSH

Vůči man-in-the-middle útokům jsou zranitelné i šifrované protokoly, v tomto případě SSH verze 1. SSH by mělo poskytnout silnou autentifikaci a bezpečnou komunikaci skrz nebezpečnou síť, slouží jako náhrada nezabezpečeného protokolu Telnet, který se k podobným účelům používal. Obvykle se používá pro vzdálenou správu počítačů, aktivních síťových prvků nebo jen pro přenos souborů. Program Cain však dokáže pomocí APR útoku zachytávat a dešifrovat SSH provoz mezi stanicemi. Podrobnosti k fungování SSH poskytuje (MONTORO, 2001).

V tomto konkrétním příkladu se jednalo o unesení SSH komunikace mezi administrátorem, který se zde stává obětí útoku, a směrovačem. SSH zde administrátor použil pro vzdálené připojení ke směrovači a k jeho následné konfiguraci, topologii zachycuje Obrázek 28. Díky APR útočník zachytí šifrovací klíče, které si klient, v tomto případě administrátor, vyměňuje se serverem respektive směrovačem, při vytváření bezpečného spojení. Tyto klíče pak program Cain využívá pro dešifrování komunikace, která mezi administrátorem a směrovačem proudí. Proto je třeba nejprve spustit APR útok, který otráví ARP cache směrovače (IP adresa 192.168.1.1) a administrátorova počítače (IP adresa 192.168.1.12), postup je popsán v kapitole 5.3.2. Pokud má být útok úspěšný, musí být dosaženo stavu man-in-the-middle. Po splnění této podmínky stačilo počkat, až se bude administrátor připojovat ke směrovači. Na kartě APR útoku pod položkou APR-SSH-1 v levé části okna programu jsou uloženy zachycené přihlašovací údaje, program ukládá celou zachycenou komunikaci, její obsah zaznamenává do souboru, který je uložen v adresáři programu. Jeho název je rovněž zobrazen v seznamu zachycených přihlašovacích údajů a lze ho odtud také otevřít a prozkoumat. Je možné z něj například zjistit heslo, které administrátor zadával pro přístup do privilegovaného módu a to i v případě, že je na směrovači zašifrované, nebo pokud administrátor zadá příkaz pro vypsání aktuální konfigurace směrovače, celý tento výpis je rovněž zaznamenán do tohoto souboru a útočník by tak mohl případně odhalit další bezpečnostní slabiny.



Obrázek 28 – topologie sítě pro testování útoku



Obrázek 29 – zachycené SSH spojení

6.3.1 Obrana proti odposlechu SSH komunikace

Vzhledem k tomu, že pro přesměrování komunikace je využit APR útok, odposlechu samozřejmě zabrání, pokud je síť zabezpečena proti ARP cache poisoningu. Obrana je tedy shodná s předchozím příkladem 6.2.1. Lze také využít toho, že program Cain dokáže dešifrovat pouze SSH verze 1. Pokud je SSH server nastaven tak že komunikuje jen skrze SSH verze 2. Z důvodu zpětné kompatibility je však možné SSH server za jistých podmínek přinutit k použití SSH verze 1 namísto SSH verze 2. U zařízení Cisco tomu lze zabránit explicitním nastavením použití pouze verze 2. Toho je docíleno zadáním příkazu ip ssh version 2.

Závěr

Cílem této práce bylo zmapovat možnosti programu Cain&Abel pro etický hacking na linkové vrstvé modelu ISO/OSI. Jak je patrné zvláště z praktické části, pokud není síť dostatečně zabezpečená, je poměrně jednoduché odposlechnout hesla a další citlivá data putující sítí. S pomocí tohoto nástroje se může stát hackerem i uživatel, který nedisponuje bohatými znalostmi počítačových síti, síťové komunikace a programování. Tím se zabezpečení sítě stává ještě důležitějším než by bylo bez nástrojů tohoto typu.

V teoretické části práce byla představena problematika hackingu a síťové komunikace. Největší pozornost byla věnována linkové vrstvě, kde byly rozebrány technologie do ní spadající a známe bezpečnostní slabiny. Samostatná kapitola pak byla věnována představení programu Cain&Abel s důrazem na odposlech síťového provozu a jeho následnou analýzu a zpracování zachycených údajů.

Praktická část práce demonstruje schopnosti programu v reálných podmínkách na fyzických zařízeních. Je sestavena ze tří ukázek útoků v rámci přepínané sítě a obrany proti nim. Postupy realizace útoku i obrany jsou podrobně rozebrány a bohatě ilustrovány. První úloha se věnovala odhalení hesla lokálního uživatele prostřednictvím slovníkového útoku. Druhá i třetí úloha se zabývala odposlechem síťového provozu pomocí ARP poison routingu. V druhé úloze byl odposloucháván a analyzován protokol http ve třetí pak šifrovaný protokol SSH. Všechny útoky jsou provedeny na fyzických zařízeních v rámci laboratoře počítačových sítí na Fakultě elektrotechniky a informatiky Univerzity Pardubice.

Vhodné rozšíření práce spatřuji srovnání programu Cain&Abel s dalšími programy zaměřenými na odposlech síťového provozu, jako je například Ettercap. Dále by bylo vhodné věnovat se také útokům na ostatních vrstvách ISO/OSI modelu a komplexnímu zabezpečení sítě.

Literatura

Google.com. 2016. Creating a strong password. *Google.* [Online] 2016. [Citace: 20. 4 2016.] https://support.google.com/accounts/answer/32040?hl=en.

HARPER, Allen, HARRIS, Shon a al., et. 2008. *Manuál Hackera.* Praha : Grada, 2008. ISBN 987-80-247-1346-5.

MONTORO, Massimiliano. 2001. Cain & Abel - User Manual. *oxid.it.* [Online] 2001. [Citace: 11. 10 2015.] http://www.oxid.it/ca_um/.

PALMAR, C., C. 2001. Ethical Hacking. *IBM Systems Journal.* 2001, Sv. 3, stránky 769-780.

PETERKA, Jiří. 1999. Referenční model ISO/OSI. *eArchiv.* [Online] 1999. [Citace: 8. Září 2015.] http://www.earchiv.cz/anovinky/ai1552.php3.

—. 1999. Rodina protokolů TCP/IP. *eArchiv.cz.* [Online] 1999. [Citace: 9. Září 2015.] http://www.earchiv.cz/anovinky/ai1592.php3.

PUŽMANOVÁ, Rita. 2006. *Moderní komunikační sítě od A do Z.* Brno : Computerpress, 2006. ISBN 80-251-1278-0.

SPANGLER, Ryan. 2003. *Packet Sniffing on Layer 2 Switched.* místo neznámé : Packetwatch Research, 2003.

TANENBAUM, Andrew, S. 2003. *Computer Networks, Fourth Edition.* New Jersey : Prentice Hall, 2003. ISBN 0-13-066102-3.