UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

Bezpečnost počítačových systémů na síti

Vladislav Barot

Bakalářská práce
2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vladislav Barot**
Osobní číslo:	**I09069**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Bezpečnost počítačových systémů na síti**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Budou popsány možné útoky na počítačové systémy po síti (např. vnitřní, vnější, sociální, trojské koně, DoS, MITM, ARP spoofing), ale i útoky možné při fyzickém přístupu k počítači. Útoky budou rozděleny do vhodných kategorií a budou popsány možné metody ochrany před nimi.
Několik vybraných útoků (nejméně pět, pokud možno z různých kategorií) budou prakticky vyzkoušeny na zvoleném systému a daný systém proti nim bude zabezpečen.
Budou vypracovány zásady zabezpečení počítačového systému s rozdělením na část určenou správci operačního systému a sítě a část pro jeho uživatele.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

***HARRIS, Shon, et al. Hacking - manuál hackera. 1. vyd. Praha: Grada Publishing, 2008. 400 s. ISBN 978-80-247-1346-5.**
***SCAMBREY, Joel; McCLURE, Stuart; KURTZ, George. Hacking bez tajemství. 2. aktualiz. vyd. Praha: Computer Press, 2002. 625 s. ISBN 80-722-6948-8.**
***VRANÝ, Boleslav. Bezpečnost v digitálním věku [online]. 2004. [cit. 2009-10-21]. S. 2-36. URL: http://www.bolekvrany.cz/downloads/security_cz.pdf.**
***OSTÁLEK, Libor; KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 2 aktualiz. vyd. Praha: Computer Press, 2000. 426 s. ISBN 978-80-251-2236-5.**
***Kolektiv autorů. Linux - Dokumentační projekt. 4. aktualizované vydání. Brno: Computer Press, 2008. 1336 s. ISBN: 978-80-251-1525-1. URL textu: http://www.root.cz/knihy/linux-dokumentacni-projekt-4-vydani/stahnout/961/. URL obsahu: http://knihy.cpress.cz/?p=actions&action=download/file&value=files&id=22019.**

Vedoucí bakalářské práce: **Mgr. Tomáš Hudec**
Katedra informačních technologií

Datum zadání bakalářské práce: **21. prosince 2012**
Termín odevzdání bakalářské práce: **10. května 2013**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 29. března 2013

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 16. 8. 2013

Vladislav Barot

Poděkování

Na tomto místě bych chtěl především poděkovat vedoucímu mé bakalářské práce, panu Mgr. Tomášovi Hudcovi za jeho vstřícný přístup, poskytnuté odpovědi a odborné vedení při vypracovávání této práce. Dále děkuji i mé rodině za trpělivost a podporu při studiu na Fakultě elektrotechniky a informatiky na Univerzitě Pardubice.

Anotace

Bakalářská práce se zabývá bezpečností počítačových systémů na síti. Útoky jsou vhodně rozděleny do kategorií a krátce charakterizovány. Práce obsahuje i souhrn zásad a zabezpečení pro uživatele i administrátory. Práci doplňuje praktická ukázka několika útoků uskutečněných na OS Linux a MS Windows.

Klíčová slova

hacker, počítačový útok, bezpečnost, spam, virus, DoS, antivir

Title

Security of computer systems on the network

Annotation

Topic of this bachelor thesis is a Security of computer systems on the network. Attacks are properly categorized and shortly characterized. The thesis contains a summary of policies and security for users and administrators. The thesis is complemented by a practical demonstration of several attacks which were run on Linux and MS Windows.

Keywords

hacker, cyber attack, security, spam, virus, DoS, antivirus

Obsah

Úvod

Fenoménem posledních let se stává tzv. kyberterorismus, kdy se cílem útoků stávají kromě běžných uživatelů i internetové stránky vládních úřadů, mezinárodních korporací či bank. Počítačové útoky se již neodehrávají za účelem vylepšování si ega či předvádění dovedností jednotlivých útočníků. Ve většině případů jde o to někoho poškodit, ať již finančně či v očích veřejnosti.

Počítačové útoky se stávají čím dál tím více nebezpečnější, avšak existuje proti nim obrana. Vynaložení prostředků na zabezpečení sítě proti útoku či úniku dat může být pro daný subjekt finančně náročné, nicméně je důležité se na eventuální útok připravit. V případě probíhajícího útoku je většinou pozdě, pak se již jedná jen o minimalizaci ztrát. Je také důležité zmínit, že některé útoky může daný subjekt zaregistrovat až s určitým zpožděním.

Tato bakalářská práce se zabývá jednotlivými typy počítačových útoků, se kterými se může setkat jak běžný uživatel, tak i zkušený odborník. Úvodní kapitola se zabývá historií počítačových útoků, typem útočníků a v neposlední řadě také nedávnými útoky v ČR, např. útoky na banky, telefonní operátory nebo na internetový portál Seznam.cz.

Další kapitoly popisují jednotlivé kategorie počítačových útoků. U každé kategorie jsou uvedeny konkrétní příklady útoků, spadajících právě do dané kategorie. V kapitole 7 jsou na ukázku popsány některé nástroje k provedení útoků. Cílem této práce není vytvořit jakýsi návod pro provedení samotného útoku, pouze poukázat na fakt, že v některých případech je realizace takového útoku opravdu banální.

Poslední dvě kapitoly se věnují praktické ukázce některých útoků a případné obraně a zásadám, jak se proti některým útokům bránit. Je pravdou, že útoky, které v nedávné době patřily k těm obávaným, nemusí v současnosti znamenat tak velkou hrozbu. Nicméně i přes tento fakt je důležité vzít na vědomí, že každým dnem přibývá velké množství nových útoků, před kterými nemusí stávající obrana stačit. Všechny uvedené ukázky útoků jsou prováděny lokálně a slouží pouze k testovacím účelům.

1 Počítačové útoky

1.1 Historie

Počítačová bezpečnost byla v počátcích využívání počítačů brána zcela jinak, než je tomu dnes. K ARPANETu, předchůdci současného Internetu, bylo v roce 1972 připojeno asi 50 počítačů, které převážně sloužily k armádním účelům. Tento armádní projekt se však během několika dalších let začal rozrůstat o další uživatele, především z řad akademických pracovníků. Ti však tuto síť používali z velké části jen kvůli e-mailové komunikaci. První počítačový virus se šířil sítí ARPANET 27. října 1980. Ačkoli se jednalo o nehodu, tato událost ukázala na nutnost určitého zabezpečení. [23], [25]

Vůbec prvním člověkem potrestaným za počítačovou kriminalitu byl Ian Murphy (alias Captain Zap), který v roce 1981 pronikl do sítě telefonní společnosti AT&T a pozměnil čas jejího vnitřního systému. Následkem tohoto útoku se hovory s noční tarifní sazbou účtovaly jako denní a opačně. Murphy byl za tento čin potrestán 1000 hodinami prospěšných prací a zkušebním obdobím v délce dva a půl roku. V současné době by byl tento trest několikanásobně vyšší. [31]

Počátkem 90. let minulého století se situace na poli bezpečnosti počítačových systémů začala zhoršovat. Například Vladimir Levin, toho času student Petrohradské univerzity, v roce 1994 spolu se svými kolegy odcizil z účtů americké Citibank přes 10 miliónů dolarů. [23]

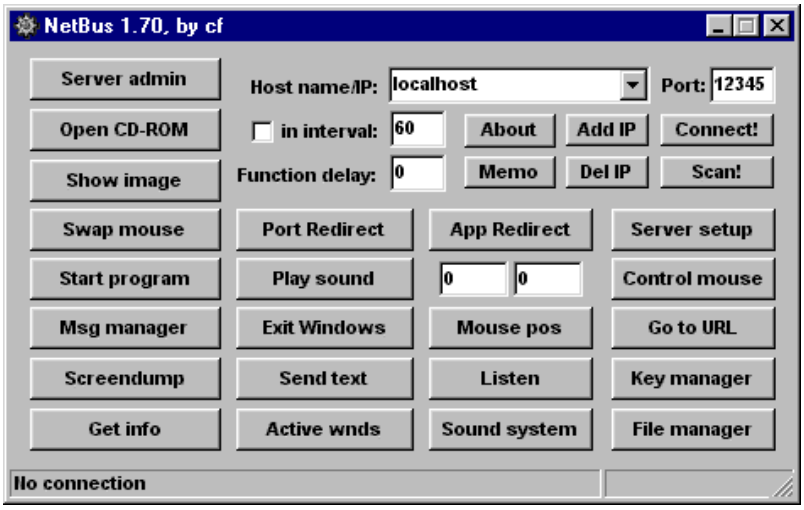
Jedním z nejznámějších hackerů je bezesporu Kevin Mitnick, který se dostal k software firem Nokia, Novell, Motorola, Fujitsu nebo NEC. Ve vězení strávil celkem přes 5 let, po propuštění však Mitnick změnil svůj život. Stal se z něho uznávaný expert na bezpečnost počítačových systémů, založil svou bezpečnostní společnost a vydal knihu (Umění klamu), která se zabývá sociálním inženýrstvím. Mitnick vždy tvrdil, že veškeré útoky prováděl bez úmyslu se finančně obohatit či poškodit danou společnost. Podle jeho slov šlo vždy čistě jen o zvědavost. [26]

1.2 Typy útočníků

1.2.1 Script kiddies

Takto jsou většinou označováni začínající hackeři, kteří k útokům používají předpřipravené nástroje (skripty). Používání těchto nástrojů je velmi zjednodušené, útočníci si většinou vystačí s IP adresou svého cíle a o samotný útok se postará skript. Možnosti takovéhoto útoku jsou široké, od krádeže dat až po úplné poškození systému. [23]

Obr. 1 zobrazuje rozhraní poměrně oblíbeného programu NetBus, který pracuje na principu trojského koně. Útočník nejprve pošle oběti spustitelný soubor, který když oběť spustí, otevře tak pomyslné dveře útočníkovi do svého systému.



Obrázek 1: Program NetBus [35]

1.2.2 Střední třída

Střední třídu představují hackeři s již pokročilejšími znalostmi programování a operačních systémů. Podle typu a úrovně zabezpečení jsou schopni použít vhodný nástroj k prolomení takovéto obrany. Po průniku do systému jsou však obezřetní a snaží se po sobě nezanechávat stopy. Během útoku také získávají informace o okolních systémech pro případný další útok.

Útočníci ze střední třídy provádějí útoky buď pro své pobavení či za účelem získání finančních prostředků. Mohou například data z napadeného systému zašifrovat a požado-

vat po majiteli peníze za jejich odšifrování. Jiná situace může nastat například v rámci konkurenčního boje, kdy si firma najme hackera, aby danou konkurenční společnost poškodil (odcizení dat, znepřístupnění webových stránek, apod.).

1.2.3 Vyšší třída

Do této kategorie se řadí zkušení útočníci s velmi bohatými znalostmi. Vytvářejí a prodávají nástroje, které používají méně zkušení hackeři. Jejich doménou je maximální zakrytí stop po průniku do systému, kde mohou nepozorovaně působit i několik let. Své útoky tak provádí za účelem komplexního ovládnutí napadeného systému. S hackery této kategorie se však běžný uživatel pravděpodobně nikdy nesetká. [23]

1.3 Poslední útoky u nás

1.3.1 DDoS útoky

Začátkem března roku 2013 bylo napadeno několik předních zpravodajských webů masivními DDoS útoky. Jednalo se namátkou o servery iDnes.cz, Novinky.cz, Lidovky.cz a Denik.cz. Tento intenzivní útok mířil na tyto weby současně. Tento útok si dokonce zasloužil pozornost i v zahraničí, kdy o něm informovala také mezinárodní tisková agentura Reuters. [22]

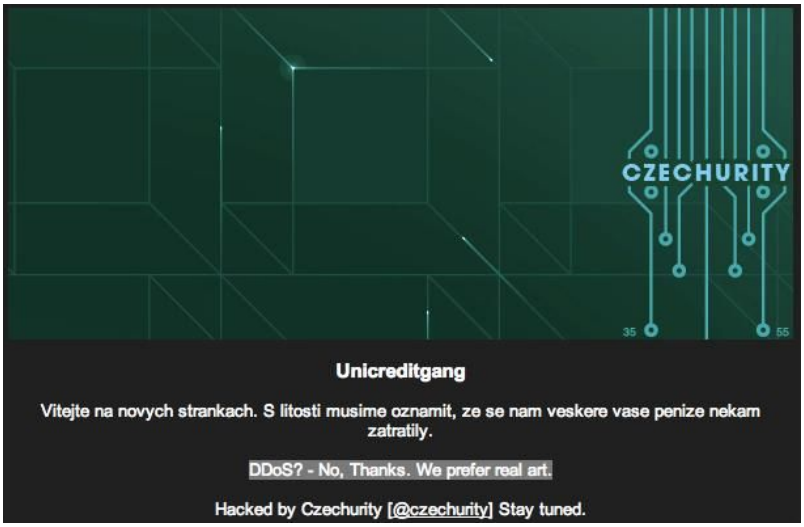
V další vlně útoků, které trvaly prakticky celý týden od 4. března, se útočníci zaměřili i na Seznam.cz. Ten však problém s dostupností vyřešil částečným odstavením konektivity do zahraničí, protože útočníci používali podvržené adresy IP. Zdroje útoku tedy není možné určit jen na základě těchto adres. Tento fakt komentoval na Twitteru technický ředitel Seznamu Vlastimil Pečínka:

„Mapky, odkud procházejí útočníci v současném DDoS útoku, jsou sice mediálně vděčné, ale s ohledem na podvržení IP adres jen úsměvné.“ [5]

1.3.2 Útok na UniCredit Bank

Tentokrát se nejednalo o útok typu DDoS, ale o průnik na webový server UniCredit Bank. K útoku se přihlásila hackerská skupina Czechurity, která na svém Twitteru později

uvedla, že heslo administrátora bylo údajně „Banka123“. Banka samotné stránky vrátila po několika minutách do původního stavu. To, co se návštěvníkům banky naskytlo při vstupu na webové stránky, je zobrazeno na obr. 2. [32]



Obrázek 2: Útok na UniCredit Bank [32]

2 Sociální útoky

Sociální útoky se v některé literatuře interpretují také jako sociální inženýrství, což prakticky znamená způsob manipulace s lidmi za účelem provedení určité akce či získání určité informace. V následujících kapitolách jsou popsány některé typy útoků z této kategorie, kdy se útočník například snaží vylákat z oběti finanční prostředky a podobně.

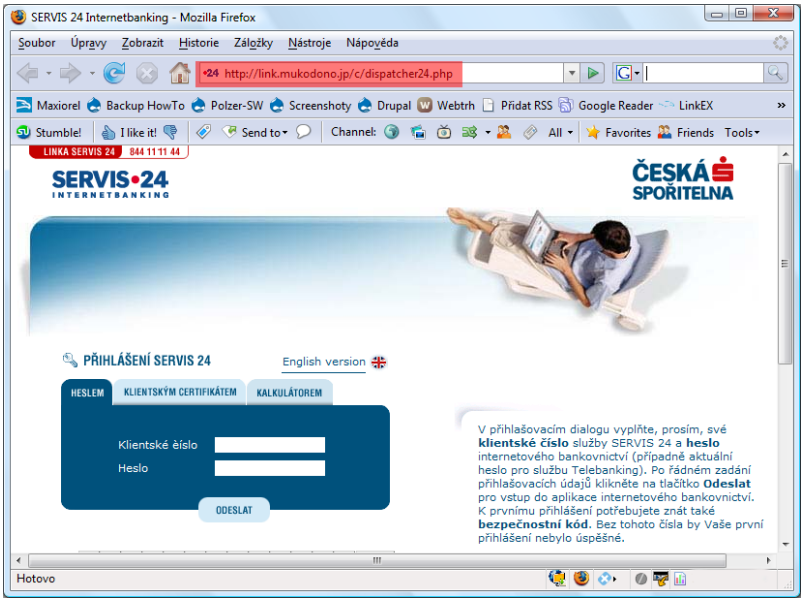
2.1 Phishing

Jedním ze sociálních útoků je vylákání údajů daného uživatele, tzv. **phishing**. Může se jednat například o podvodnou stránku, která se tváří jako formulář k přihlášení do internetového bankovnictví. Uživateli přijde podvržený e-mail, ve kterém se po něm žádá, aby provedl změnu hesla z důvodu zvýšení bezpečnosti. Po kliknutí na odkaz v e-mailu proběhne přesměrování na výše zmíněnou podvodnou stránku, kde uživatel zadá své přihlašovací údaje. Nic nenasvědčuje tomu, že jde o podvod, protože útočník danou stránku navrhl přesně tak, jako ve skutečnosti vypadá originál. Útočník tak tímto způsobem může získat uživatelská jména a hesla, díky kterým může jednotlivé uživatele bez problému okrást.

Banky samozřejmě nikdy po svých klientech takovéto osobní údaje nevyžadují a už vůbec ne pomocí e-mailu. Bohužel i přes tuto skutečnost se podaří útočníkům důvěřivé klienty okrást. Uživatelé by tak e-maily tohoto typu měli vždy ignorovat. Zfalšovat odesílatele e mailové zprávy není v dnešní době žádný problém, proto je důležité zachovat v těchto případech chladnou hlavu. Na obr. 3 je zobrazen příklad podvodné stránky, v tomto případě internetového bankovnictví České spořitelny. Důležité je povšimnout si internetové adresy této stránky. [27]

2.2 Hoaxy

Mezi sociální útoky patří také tzv. hoaxy, česky poplašné zprávy. Jako jeden příklad za všechny může sloužit podvodná stránka na sociální síti Facebook s názvem „Rozdáváme Apple produkty zadarmo“. Tato stránka měla před svým zrušením přes 50 tisíc fanoušků. Autoři této stránky použili obrázky produktů firmy Apple z dalších podvodných stránek



Obrázek 3: Ukázka phishingu [18]

v angličtině. MacBook či iPad 3 „rozdávali“ z prostého důvodu. Šlo o „poškozené krabice“, které bylo dle jejich mínění lepší rozdat než odepisovat. Na obr. 4 je snímek jednoho příspěvku z podobné stránky, který jasně vykazuje známky hoaxu.

Jednalo se samozřejmě o podvod, na který však naletělo několik desítek tisíc uživatelů. Tvůrci stránek slibovali výhru těm, kteří tuto stránku doporučí svým známým a kamarádům. Tím došlo k masovému rozšíření. Po upozornění několika českých médií na tuto stránku vydali autoři prohlášení, že o žádný podvod nešlo. Jednalo se prý pouze o průzkumný projekt. [6]

2.3 SPAM

Pojem spam lze definovat jako nevyžádanou elektronickou poštu. Jedná se ve většině případů o různé nabídky na hubnutí, levné mobilní telefony, řetězové dopisy, apod. Důležitým specifikem těchto nevyžádaných e-mailů je, že nejsou určeny konkrétnímu okruhu vytipovaných uživatelů, nýbrž obrovskému kvantu dostupných e-mailových adres. Spam však není reklamní e-mail, který si uživatel sám vyžádal, protože u těchto typů e-mailů lze svou adresu vyřadit z databáze příjemců na základě odhlášení odběru. [14]

Obrázek 4: Ukázka poplašné zprávy [6]

2.3.1 Prevence

Stejně jako se doporučuje chránit si své citlivé osobní údaje, u e-mailu to platí dvojnásob. Například pokud nějaká firma má na svých stránkách v kontaktech uvedeny e-mailové adresy svých zaměstnanců, jedná se o potencionální nebezpečí, že právě jejich adresy budou zneužity. Takovou stránku totiž může navštívit robot, který hledá emailové adresy a v případě úspěšného nalezení je ukládá do databáze. Proto se pomalu upouští od zveřejňování konkrétních e-mailových adres, pouze se uvádí vzor, jaký se ve firmě dodržuje při vytváření e-mailových schránek zaměstnanců. Takovým příkladem může být adresa ve tvaru jmeno.prijmeni(at)firma.cz.

2.3.2 Filtrování spamu

Za účelem úspěšné eliminace spamu je vhodné filtrovat příchozí zprávy již na straně serveru. Každá příchozí zpráva je porovnána s rozsáhlou databází nevyžádaných e-mailů a na základě tohoto porovnání se určuje výsledné skóre. V případě, že toto skóre překročí určenou hranici, je tato zpráva označena jako spam. Tato metoda však není stoprocentní, filtrování spamu je prováděno heuristicky a výsledkem je pouze podezření. Doporučuje se, aby uživatelé alespoň jednou týdně zprávy označené jako spam zkontrolovali a přesvědčili se, že nedošlo k chybě. [27]

Filtrovat zprávy lze také na konkrétní pracovní stanici. Existuje mnoho specializovaných programů, které takovou službu poskytují. Pokud uživatel na svém počítači má zakoupený a nainstalovaný kancelářský balík MS Office, může využít program MS Outlook. Alternativou může být např. Mozilla Thunderbird, který nabízí poměrně silný a flexibilní spamový filtr a je především zdarma. Pokud uživatel zvolí tuto metodu filtrování, předpokládá se, že má již pokročilejší počítačové znalosti.

3 Hardwarové útoky

Do této skupiny se řadí takové útoky, kdy útočník po síti provádí útok přímo na hardware nebo k takovému útoku využívá hardwarovou chybu. Platí zde předpoklad, že se útočník nachází uvnitř této sítě. Jako příklad lze uvést připojení k přístupovému bodu (Access Point) bez zabezpečení.

3.1 Síťová zařízení

Než útočník přistoupí k realizaci hardwarového útoku, musí mít alespoň základní povědomí o tom, jak taková běžná síť funguje a jaké prvky se mohou starat o provoz v této síti. V současnosti je nejběžnější síť typu Ethernet (s využitím protokolu IPv4). Data se v této síti adresují na základě adresy MAC (spojová vrstva) a adresy IP (síťová vrstva). Pokud chce uživatel navázat komunikaci s jiným počítačem v této síti, musí znát jeho adresu IP. O překlad adresy IP na adresu MAC se poté postará protokol ARP.

3.1.1 Switch (přepínač)

Mezi síťová zařízení patří switch, česky přepínač. Tento aktivní síťový prvek pracuje na spojové vrstvě referenčního modelu ISO/OSI a jednotlivá příchozí data adresuje podle adresy MAC v hlavičce spojového rámce. Podle této adresy MAC data odesílá pouze na port, kde je připojeno cílové zařízení.

Pro snadné rozřazení dat na jednotlivé porty využívá switch vnitřní paměť, do které se zapisuje na kterých portech se objevuje komunikace konkrétních adres MAC. Tato paměť se nazývá tabulka CAM. Tato tabulka má omezenou kapacitu. Při zapnutí switche je CAM tabulka prázdná, ovšem při příchodu prvního rámce se do této tabulky zapíše adresa MAC, odkud tento rámec přišel. Switch poté rozešle rámec na všechny porty vyjma toho portu, odkud rámec dorazil. Obdobně tomu je i poté, co na switch dorazí další rámec. Switch si poznačí adresu MAC odesílatele a zkontroluje, zda v tabulce CAM tato adresa již není. V případě že ne, odešle rámec opět na všechny porty kromě příchozího. V případě zapojení počítače do jiného portu dojde při vyslání prvního

rámce k aktualizaci tabulky CAM.

Záznamy jsou uchovávány v tabulce CAM pouze omezenou dobu. Po uplynutí určitého časového úseku je tento záznam z tabulky odstraněn. Tento časový úsek se liší v rámci jednotlivých switchů od různých výrobců. V případě, že je na určitém portu připojen další switch, je v tabulce CAM k tomuto portu přiřazeno více adres MAC.

3.1.2 Přepínaný a nepřepínaný Ethernet

Důležité je rozlišovat pojmy přepínaný a nepřepínaný Ethernet. Typickým zástupcem nepřepínaného Ethernetu je hub (rozbočovač) a přepínaného Ethernetu switch. Rozdíl mezi těmito aktivními spojovacími prvky sítě je ten, že switch rozlišuje cílový port, na který má přijatá data odeslat (podle cílové adresy MAC). Hub port nerozlišuje, přijatá data odesílá všem připojeným stanicím. Z této skutečnosti pramení poměrně velké nebezpečí toho, že komunikace na této síti může být poměrně jednoduše odposlouchávána. Ovšem i switche mohou být za použití speciálních technik nebezpečné.

3.2 Odposlechy (Sniffing)

Odposlouchávání datové komunikace, anglicky sniffing, je technika útoku, při které dochází k zachytávání určitých dat, která se pohybují po síti. Může se jednat o „neškodné“ odposlouchávání toho, co na síti právě dělá kamarád, například jaké internetové stránky navštěvuje. Může také docházet k situacím, kdy se nejedná pouze o žert, například pokud rozzlobený zaměstnanec odposlouchává počítač svého nadřízeného a získává tak důležitá či tajná data. V těchto případech může být odposlouchávání cizí komunikace trestné a nemorální. Nutno však dodat, že díky odposlouchávání může správce sítě analyzovat celkový provoz na síti, zjistit používané služby či protokoly a v neposlední řadě také odhalit škodlivý software v podobě trojského koně.

3.3 Man in the middle (MITM) útoky

Již z názvu těchto útoků vyplývá, že útočník tvoří jakéhosi prostředníka v dané síťové komunikaci. Cílem je tedy přesměrování síťového datového toku tak, aby procházel přes počítač narušitele. Útočník se tedy může například rozhodnout pro možnost izolování

určitého počtu uživatelů od ostatního okolí. Tento útok je poměrně zákeřný, neboť správce sítě bude pravděpodobně vždy hledat vinu především v hardwaru či v operačním systému. Další možností je například krádež spojení. Útočník počká, až se uživatel přihlásí na server, odstraní ho a převezme jeho spojení s daným serverem. [13] Mezi MITM útoky se například řadí:

- ARP Cache Poisoning,
- DHCP Spoofing,
- ICMP Redirecting,
- Port Stealing,
- DNS Spoofing,
- MAC Flooding.

Některé z těchto útoků jsou popsány v dalších kapitolách. Postupy, jak se bránit proti těmto typům útokům, jsou popsány v kapitole 9.1.4.

3.3.1 MAC Flooding

Útok je založen na principu zaplnění tabulky CAM switche a také na skutečnosti, že pokud se v této tabulce nevyskytuje cílová adresa MAC počítače, pak se rámec rozesílá na všechny ostatní porty. Efektivnost tohoto útoku spočívá především v tom, jak se daný switch zachová při zaplnění jeho tabulky CAM.

Zaplnění tabulky CAM lze provést dvěma způsoby. První možnost lze realizovat tak, že rámce budou mít náhodně vygenerovanou zdrojovou a cílovou adresu MAC. Switch zareaguje tím způsobem, že si pro každou adresu MAC udělá vlastní záznam a rámec odešle na všechny porty. Tímto dojde k infikování dalších switchů v síti (za předpokladu, že nejsou odděleny počítačem nebo routerem). Jak již bylo zmíněno, kapacita tabulek CAM je omezena a pohybuje se v rámci tisíců položek až po statisíce.

Druhou možností je nastavit rámcům cílovou adresu MAC příjemce na adresu MAC útočníka a odchozí adresu generovat náhodně. Jakmile rámec dorazí na switch, dojde k uložení záznamu do tabulky CAM (s náhodně vygenerovanou adresou MAC odesílatele)

a dále se s tím rámcem nepracuje, protože příjemce je na stejném portu. Takový útok je téměř nemožné odhalit, útočník však přijde o možnost napadení okolních switchů.

Po zaplnění tabulky CAM ve většině případů dochází k tomu, že se switch přepne do stavu `fail open`, což způsobí to, že se začne chovat jako hub – začne posílat jednotlivé rámce na všechny porty.

3.3.2 ARP Cache Poisoning

Tento útok využívá nedokonalostí v protokolu ARP, kdy je cílem získat data někoho jiného do útočníkova počítače za účelem jejich analýzy. Útok lze provést na síti, kdy jsou okolní počítače propojeny prostřednictvím aktivního síťového prvku. Samotný protokol ARP byl navržen v době, kdy se s nějakým útokem na síť nepočítalo, proto nemá žádné ochranné mechanismy.

3.3.3 Protokol ARP

Protokol ARP slouží k dohledání adresy MAC k zadané adrese IP. Tento protokol běží stejně jako protokol IP na síťové vrstvě modelu TCP/IP. [3] Princip funkce protokolu ARP je následující:

- Zdrojová stanice hledá adresu MAC cílové stanice podle její adresy IP. Sestaví tedy ARP žádost (request) a odešle ji jako broadcast.
- Jednotlivé stanice přijmou tuto žádost a v případě, že jejich adresa IP neodpovídá hledané adrese IP, tuto ARP žádost ignorují.
- Cílová stanice sestaví ARP odpověď (response) a odešle ji zdrojové stanici.

3.3.4 Útok pomocí ARP Cache Poisoning

Situaci při útoku lze nastínit v podobě tří počítačů v lokální síti. Jeden z počítačů patří oběti, druhý je počítač útočníka a třetí počítač slouží jako brána, který je zároveň připojen k Internetu a veškerá komunikace směrem do Internetu probíhá právě přes tuto stanici. Útok je velmi jednoduchý, útočník pošle oběti rámec, ve kterém oznamuje, že brána má stejnou adresu MAC jako útočník. Obdobně útočník odešle rámec i bráně,

ve kterém sděluje, že oběť má adresu MAC stejnou jako útočník. Díky tomuto triku lze docílit toho, že jednotlivé počítače budou pro vzájemnou komunikaci dosazovat adresu MAC útočníka a switch bude data plynoucí z této komunikace odesílat právě na port útočníka. Jakmile si je útočník prohlédne, odešle je dále, nyní však se správnou adresou MAC.

Úspěšnost tohoto útoku je dána tím, že protokol ARP nekontroluje, zda tato data byla nebo nebyla vyžadována. V případě, že již má záznam vytvořen, jakýmkoliv rámcem ARP `Reply` lze tento záznam změnit.

3.3.5 DHCP Spoofing

Útok vychází z možnosti provozovat na jedné síti více serverů DHCP a také z toho, že regulérní servery nereagují na změny v síti okamžitě. Cílem tohoto útoku je na síti zprovoznit nový server DHCP a v případě připojení oběti do sítě jí podstrčit falešné údaje. Toho lze docílit vyčerpáním veškerých volných adres na straně serveru DHCP. Oběti lze podstrčit také výchozí bránu či server DNS. [12]

Pokud se útočník vydává za výchozí bránu, komunikace směrem do Internetu bude probíhat právě přes něj. Ovšem data vracející se z Internetu směrem k uživatelům již budou směřovat na opravdovou výchozí bránu, která je dále pošle k cílovým počítačům.

3.3.6 Princip DHCP

Protokol DHCP je novějším nástupcem staršího protokolu BOOTP. Používá se k automatické konfiguraci nejdůležitějších síťových parametrů jednotlivých stanic. Jinými slovy, za pomocí serveru DHCP lze jednotlivým klientům přidělit např. adresu IP (z předem definovaného rozsahu), masku sítě, výchozí bránu, apod. [4]

- Po připojení klienta do sítě se vyšle multicast UDP s požadavkem `DHCPDISCOVER`.
- V případě, že v síti existuje server (servery) DHCP, dojde k zachycení tohoto požadavku a odešle se opět multicast `DHCPOFFER`.
- Klient si poté vybere jednu z odpovědí a pošle konkrétnímu serveru `DHCPREQUEST`.

- Tento server buď žádost potvrdí pomocí `DHCPACK` nebo zamítne – `DHCPNAK`.
- Klient si však může svou volbu rozmyslet a odešle zprávu `DHCPDECLINE`.
- Prostředky jsou však klientovi zapůjčeny pouze na určitou dobu (aby nedocházelo ke zbytečné blokaci již volných prostředků), proto klient musí po určité době svou žádost opakovat. V případě, že chce klient své prostředky uvolnit před vypršením uvedené lhůty pro zapůjčení, odešle zprávu `DHCPRELEASE`.

Praktická ukázka útoku DHCP Spoofing je popsána v kapitole 8.2.

4 Softwarové útoky

Softwarové útoky lze souhrnně pojmenovat jako tzv. malware, tedy programy, které slouží ke vniknutí či poškození počítačového systému. Nutno však dodat, že pokud program, který byl napsán pro legitimní účely, obsahuje chyby, které v důsledku jeho používání vedou k poškození systému, nelze tento program označit jako malware.

Softwarové útoky lze také rozlišovat podle chování v počítačovém systému. Mezi ty útoky, které vyžadují zásah od uživatele, aby se mohly dále rozšířit, patří především počítačové viry. Naopak trojské koně mohou v počítačovém systému skrytě působit bez vědomí samotného uživatele i velmi dlouhou dobu. [34]

4.1 Viry

Viry se staly nedílnou součástí slabě zabezpečených počítačů. Historie počítačových virů sahá do roku 1986, kdy osobní počítače začal napadat virus Brain. Od této doby se číslo známých virů rozrostlo na několik desítek tisíc, viry jsou agresivnější a mnohem rychleji se šíří, nicméně existuje proti nim obrana v podobě antivirových programů, které jsou účinnější než před lety.

Počítač napadený virem není nebezpečný jen pro svého uživatele, ale především pro své okolí. Proto do jisté míry záleží na zabezpečení okolních počítačů.

4.1.1 Typy virů

- **Boot viry** — tento typ virů napadává systémové oblasti pevného disku. Vyskytují se častěji i přesto, že je jich méně než souborových virů. Šíření těchto virů probíhá poměrně jednoduchým způsobem. Pokud uživatel restartuje počítač, který má v disketové mechanice vloženou napadenou disketu s boot virem a současně má povoleno zavádění systému z diskety, proběhne spuštění viru a napadení systémových oblastí disku. Takto napadený systémový disk infikuje další diskety, které uživatel použije. V současnosti se však více než diskety používají optická média jako např. CD či DVD.

- **Souborové viry** — tyto viry napadají programy, ve kterých změní část kódu

programu či ke kódu připojí svůj vlastní, škodlivý kód. Ve výsledku tak změní velikost a chování tohoto programu.

- **Makroviry** — útočí na dokumenty vytvořené v kancelářských aplikacích (např. MS Office). Makroviry využívají toho, že takovéto dokumenty neobsahují jen data, ale i makra, které dále využívají ke svému šíření. Při spuštění napadeného dokumentu může dojít např. ke spuštění jiných programů či k odeslání tohoto dokumentu libovolným uživatelům z poštovního adresáře uživatele daného počítače. [21]

4.1.2 Antivirová ochrana

Antivirových programů existuje velké množství, některé z nich jsou zdarma, používání jiných je zpoplatněno. Zakoupení licence antivirového programu je otázkou pro samotného uživatele, nicméně i zdarma nabízené antiviry mohou splnit svůj účel. Nainstalování antivirové ochrany do systému však nezaručuje stoprocentní bezpečnost a ochranu před škodlivými viry. Důležité je u daného antiviru udržovat aktualizovanou virovou databázi. Tato databáze poskytuje antiviru celkový přehled o dostupných virech.

4.1.3 Principy antivirů

- **Porovnání s databází virů** — antivirový program testuje prohledávané soubory na výskyt určité posloupnosti bytů, pomocí které identifikuje vir z databáze. Tato metoda patří mezi nejstarší a pravděpodobně nejrozšířenější způsob detekce napadení virem. Tato metoda je však spolehlivá jen v případě aktualizované virové databáze, v opačném případě antivir nemusí upozornit na nový druh viru.

- **Heuristická analýza** — zde na rozdíl od porovnání s databází virů dochází k analýze kódu souboru a jeho významu. Antivirus tak hledá postupy typické pro viry, na základě kterých může daný soubor označit jako infikovaný virem. Výhodou této metody je možnost nalezení virů, které doposud nebyly vloženy do virové databáze. Může však docházet k omylům, kdy se jako infikovaný označí soubor, který je v pořádku.

- **Sledování změn (kontrola integrity)** — antivirový program pravidelně sleduje změny u souborů v operačním systému. U této metody se využívá skutečnosti, kdy souborové viry mění velikosti či obsah samotných souborů. Při změně velikosti textového souboru je důvod k panice, že daný soubor je napaden virem, nejspíše zbytečný. Pokud ovšem k takovéto změně dojde např. u programu či systémového souboru, může to indikovat právě napadení virem. Princip této metody je založený na tom, že při prvním spuštění antivirového programu dojde k uložení informací o dostupných souborech do své databáze. Při dalších spuštěních dochází k již zmíněné kontrole a k sledování změn. Mezi výhody této metody lze opět zařadit možnost odhalení zatím neznámého viru. Jako nevýhoda se jeví fakt, že antivir nedokáže určit, zda se jedná o vir, pouze nahlásí, že došlo ke změnám. V konečném důsledku záleží na rozhodnutí konkrétního uživatele.

- **Rezidentní kontrola** — v tomto případě dochází k tomu, že v operačním systému je neustále spuštěn proces, který kontroluje prováděné operace. Například před spuštěním libovolného programu nejprve dojde k jeho kontrole, zda neobsahuje virus. Tato metoda rozhodně přispívá k bezpečnějšímu prostředí, nicméně na starších počítačích může docházet ke snížení plynulosti běhu operačního systému, neboť dochází k vyšší spotřebě systémových prostředků. [21]

4.2 Spyware

Jak již z názvu vyplývá, spyware slouží k sledování toho, co uživatel na počítači dělá. Název je odvozený od anglického slova spy, což v češtině znamená špión. V naprosté většině uživatel o tom, že je jeho systém „špehován“, neví, byť si takový program nainstaloval sám, v dobré víře že jde například o důležitý doplněk internetového prohlížeče. Spyware nemusí být nutně nějaký program, vyskytuje se běžně v podobě tzv. cookies, což jsou malé soubory, které se automaticky stahují při navštívení webové stránky. [27]

Spyware se potencionálně nemusí jevit jako přímá hrozba. Nerušeně sbírá a odesílá statistická data, například přehled navštívených stránek či nainstalované programy. Takto získané informace v mnoha případech slouží později pro cílenou reklamu. Tato

činnost však hrubě narušuje soukromí uživatelů. Častým ukazatelem na přítomnost spyware v počítači jsou problémy s připojením internetu.

4.3 Trojské koně

Trojský kůň je program, který na pozadí systému provádí zákeřné akce nebo instaluje nebezpečný software. Tyto škodlivé programy slouží ke skrytému ovládání počítače na dálku. K napadení počítače trojským koněm dochází pomocí triků, kdy potencionálně neškodné programy nebo hry obsahují právě trojského koně, a tak uživatel netuší, že si vytvořil ve svém systému zadní vrátka.

4.3.1 Základní klasifikace trojských koňů

- **Ovládání vzdáleného systému** — útočník v tomto případě může napadený počítač ovládat, ačkoliv k němu nemá fyzický přístup. Tyto počítače mohou být součástí tzv. botnetů, což jsou rozsáhlé sítě již napadených počítačů, které jsou řízeny z jednoho centra. Útočníci pak mohou tyto počítače využívat k nežádoucí činnosti jako je rozesílání spamu, DDoS útoky a podobně.

- **Získávání hesel** -– trojský kůň běží v pozadí systému a zachytává uživatelova hesla, která následně odesílá útočníkovi, například na jeho e-mailovou adresu. Oproti trojským koňům pro ovládání vzdáleného systému, které jsou spuštěny ihned po startu operačního systému, v tomto případě se tyto škodlivé programy spouští pouze při spuštění odpovídajícího souboru.

- **Keyloggery** — neboli aplikace zaznamenávající uživatelem stisknuté klávesy. Tento typ trojských koňů se obdobně spouští ihned po startu systému a stisknuté klávesy se ukládají do speciálního souboru, který může být opět odeslán útočníkovi na jeho e-mailovou adresu.

Mnoho trojských koňů však bývá destruktivního typu, kdy se snaží smazat všechny dostupné soubory. [2]

5 Aktivní útoky

Útoky typu DoS (Denial of Service – odmítnutí služby) se využívají za účelem znepřístupnění určité služby, počítače nebo dokonce celé sítě. Ve většině případů se jedná o zlý úmysl někoho poškodit. K provedení takového útoku nemusí útočník disponovat přílišnými znalostmi, neboť existuje mnoho vhodných nástrojů, které vykonají prakticky všechnu práci za něj. [24]

Motivace k provedení DoS útoku může být různá. Někteří útočníci v rámci žertu provedou útok na kamarádův počítač, aby se jim naskytl vyděšený výraz uživatele, který v danou chvíli nedokáže pochopit, co se s jeho strojem děje. Další důvod k útoku může být takový, že útočník nedokázal daný systém prolomit či obejít, proto se rozhodne server alespoň vyřadit z činnosti. V poslední době se DoS útoky používají také za účelem zviditelnit se, například skupina Anonymous, která provedla bezpočet útoků na různé společnosti, sdružení či vládní weby. V případě takového útoku se o něj začnou zajímat i různá média. [7]

5.1 Ping of Death

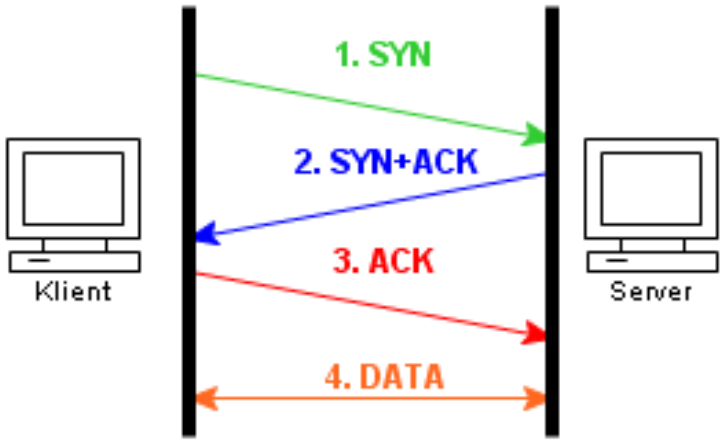
Ping of Death (ping smrti) je jeden ze starých útoků, který využívá chyby v protokolu ICMP. Nástroj ping posílá ICMP zprávy `Echo Request` (a očekává odpovědi typu `Echo Reply`) za účelem zjištění, zda je cílový počítač dosažitelný a jakou dobu paketům trvá, než se vrátí od cíle zpátky ke zdrojovému počítači. Princip tohoto útoku spočívá v tom, že útočník pomocí nástroje ping překročí maximální velikost IP paketu, tedy vyšle paket větší než 65 535 bytů. Systémy na takto veliký paket nebyly připraveny a při obdržení této zprávy zkolabovaly. Tato chyba byla však v operačních systémech již odstraněna, a proto se tento útok dá již považovat za neúčinný. [8]

5.2 SYN Flooding

Tento útok lze zařadit mezi tzv. útoky využívající vyčerpání systémových prostředků. Je zde využito chyby, respektive nedokonalosti navazování připojení v rámci TCP protokolu. Tento protokol pracuje na transportní vrstvě a využívá se téměř pro všechny

webové služby. K navázání spojení dochází například v případech komunikace mezi uživatelem a webovým serverem.

Uživatel zašle webovému serveru TCP paket s příznakem SYN (synchronizovat). V případě, že server nechce přijmout toto spojení, pak tento paket ignoruje a odešle zpět uživateli paket s příznakem RST (reset). V opačném případě dojde ze strany serveru k odeslání paketu s příznakem ACK (potvrzuji). Server k tomuto paketu připojí i příznak SYN, jelikož se předpokládá, že toto spojení bude oboustranné (data si bude uživatel i server posílat navzájem). V případě, že klient od serveru obdrží výše zmíněny paket s příznaky ACK a SYN, odešle zpátky serveru paket s příznakem ACK, čímž dá serveru na vědomí, že navazování spojení proběhlo v pořádku a oba počítače mohou od této chvíle spolu začít komunikovat. Tento způsob navazování spojení je definován jako TCP Handshake (potřesení rukou), ukázka je zobrazena na obr 5.



Obrázek 5: TCP Handshake [9]

Útok využívá toho, že pokud server od klienta obdrží paket s nastaveným příznakem SYN, alokuje pro toto připojení systémové zdroje (prostředky). Jak bylo zmíněno výše, server poté odešle paket s příznaky SYN+ACK a čeká na odpověď od klienta. Pokud klient do určité doby neodpoví, server předpokládá, že o toto připojení přestal mít klient zájem a vyhrazené systémové prostředky uvolní a zruší záznam o původní inicializaci spojení. Problém však nastává, pokud útočník pošle paketů s příznakem SYN více, poté může situace dospět do stádia, kdy webový server disponuje nedostatkem systémových prostředků, protože jsou vyčerpána všechna možná spojení, která jsou navíc otevřená

jen napůl (nedorazila odpověď ACK od klienta – útočníka). [9]

5.3 Smurf Attack

Jedná se o reflektivní zesilující útok, který se snaží zahltit linku oběti pomocí jiných počítačů zasláním dotazu `Echo Request` prostřednictvím nástroje ping (podobně jako útok Ping of Death). Útočník zašle ping na IP adresu sítě a jako zdrojovou adresu nastaví IP adresu oběti. Okolní počítače poté odpovídají oběti paketem typu ICMP `Echo Reply`. Zesílení tohoto útoku závisí na celkovém počtu počítačů v této síti. [10]

5.4 DNS Amplification Attack

DNS Amplification Attack (zesilující útok) spočívá v odeslání DNS dotazů se zdrojovou IP adresou nastavenou na IP adresu oběti. Jedná se o jeden z nejsilnějších DoS útoků, protože zesílení tohoto útoku může dosáhnout více jak 70násobku původních dat. Předpokládá se, že útočník má k dispozici veřejný relay DNS server (server, který provede dohledání záznamu a je dostupný v Internetu). [10]

5.5 DDoS

Distributed (distribuované) DoS útoky se liší od obyčejných DoS útoků především tím, že útok neinicializuje pouze jeden, nýbrž několik útočníků. Tyto útoky jsou v současnosti pravděpodobně nejznámější a nejvíce medializované (velmi oblíbené jsou např. u hackerské skupiny Anonymous). DDoS útoky nejsou však žádnou novinkou, používají již od objevení tzv. záplavových (flood) útoků. Pokud útočníci chtěli provést útok na server s větší kapacitou linky, museli se předem spolu domluvit a útok vést společně.

5.5.1 Botnety

Nutnost využívat k útokům své počítače útočníkům odpadla s příchodem tzv. botnetů. Bot je program, který se do napadeného počítače nejčastěji dostává pomocí trojského

koně. Na tomto počítači je tajně nainstalován a slouží útočníkovi, který jej může plně ovládat. Takto napadené stanici se občas přezdívá „zombie“ (živá mrtvola).

Útočníkovi se tak skýtá možnost sdružovat jednotlivé napadené počítače do jednotné sítě, odtud plyne spojení botnet (bot networks). Tuto síť lze pomocí nástrojů vzdálené správy využívat dále ke koordinovaným útokům bez vědomí jednotlivých uživatelů. Spravovat botnet lze několika způsoby, např. pomocí P2P sítě, mezi hackery je však velmi oblíbený protokol IRC. Napadený počítač se připojí na předem dohodnutý IRC server a čeká na příkazy od útočníka, který je přímo zapisuje do komunikačního kanálu.

Botnet si lze představit jako určitou armádu, která čeká na povel k útoku. Experti se domnívají, že až sedm procent všech počítačů na světě může být součástí různých botnetů, tedy cca až 47 miliónů strojů. V říjnu 2007 byli v Holandsku zatčeni tři muži, kteří dle policie měli mít k dispozici síť o velikosti až 1 500 000 napadených počítačů.

Pomocí botnetů lze provádět velké a v mnoha případech zdrcující DoS útoky či tyto počítače využívat také pro šíření spamu. Skupina Gartner Group uvedla, že až 70 procent spamu je odesláno právě z botnetů. Nedílnou součástí počítače zapojeného do botnetu je také odposlouchávání okolní sítě (sniffing). Data získaná touto činností jsou poté odeslána zpět útočníkovi. [19]

6 Fyzický přístup k počítači

Pokud má útočník přímý, tedy fyzický přístup k počítači, nelze jej stoprocentně zabezpečit. Zde rozhodují faktory týkající se zejména důležitosti či významnosti dat uložených na tomto počítači. Z toho vyplývá fakt, že jinak se zabezpečuje počítač ve velké společnosti obsahující důležitá data, např. plánování další výroby či osobní notebook ženy v domácnosti. Nutno také zmínit, že lépe zabezpečený počítač bude stát také více peněžních prostředků. Fyzickému zabezpečení přístupu k systému se detailněji věnuje kapitola 6.4.

V ideálním případě je tedy cílem to, aby se útočník k počítači fyzicky nedostal. Zkomplikovat mu tento záměr lze několika způsoby:

- Přidělení rozdílných práv přístupu do jednotlivých částí budovy zaměstnancům.
- Zabezpečení pracoviště elektronickými zámky, autorizačními systémy chráněnými hesly nebo čipovými kartami.
- Používání autentizačních systémů na snímání otisků prstů, dlaně, oční duhovky nebo rozpoznávání hlasu.
- Používání auditovacích systémů na sledování a zaznamenávání určitých akcí zaměstnanců – vstup zaměstnanců do místnosti, přihlášení se do systému, kopírování údajů, atd.
- Zabezpečení pracoviště pomocí audiovizuální techniky – kamerové systémy, poplašené zařízení.

Dodržování obecných zásad bezpečnosti ať již kombinací jednotlivých či všech výše zmíněných bodů vede k větší bezpečnosti. Nikoliv však k bezpečnosti úplné, tu zaručit nelze. [36]

6.1 Coldboot Attack

Při tomto útoku útočník využívá toho, že paměti DRAM dokážou uchovávat informace v nich obsažené několik sekund až minut po jejich odpojení od proudu. Délka tohoto

intervalu, kdy jsou data v paměti stále dostupná, přitom závisí především na provozní teplotě paměti. Zkušení útočníci tak mohou z paměti DRAM získat data, která zde byla uložena operačním systémem. V praxi se tento útok využívá k získání šifrovacího klíče k zašifrovaným pevným diskům, který je právě v paměti uchováván.

Předpokladem pro úspěch tohoto útoku tedy spočívá v tom, že útočník má fyzický přístup k zapnutému počítači. Bylo vyzkoušeno, že pozitivní útok byl také na počítač v režimu spánku či hibernace. Poté je potřeba operační paměť vyjmout a získat šifrovací klíč. Aby se zabránilo ztrátě obsahu paměti, ošetří se např. tekutým dusíkem nebo lépe dostupným a přeci plně dostačujícím butanem, který se prodává jako např. plyn do zapalovačů. Útočník poté vyjme zchlazenou paměť DRAM a vloží ji do svého počítače, aby následně získal šifrovací klíč. Vše je otázkou několika minut.

Mezi možnosti obrany před tímto útokem patří zejména:

- **Eliminovat možnost snadného přístupu k paměti počítače** – vybrat takové zařízení, u kterého je nemožné takto snadno přistoupit k vyjmutí paměti. Mezi nevýhody patří neexistující možnost výměny poškozených komponent.
- **Detekování pokusu o průnik ke komponentám zařízení** – možnost detekovat otevření skříně. U tohoto zařízení lze v případě pokusu o otevření klíč přepsat náhodnými daty.
- **Smazání klíče při odchodu od počítače** – jedná se čistě o programové řešení. V samotném důsledku jde o efektivní řešení, ale nutí uživatele při každém příchodu zadat dlouhé heslo k disku. [15]

6.2 Útok nespokojeného zaměstnance

Mezi nejzranitelnější místa bezpečnostní politiky firmy patří útok z vlastních řad, tedy od samotných zaměstnanců. O tom, jak velkou škodu může nespokojený zaměstnanec napáchat, rozhoduje míra jeho privilegií a práv. Je tedy na místě opatřit pracovní smlouvu jednotlivých zaměstnanců o určitou míru odpovědnosti za napáchané škody, bez ohledu na to, zdali zaměstnanec v momentě útoku ve firmě pracoval či již nikoliv. Tuto prozíravost z pohledu vedení společnosti nelze brát na lehkou váhu.

V praxi se lze běžně setkat se situací, kdy zaměstnanec, který právě dostal výpověď, se rozhodne zdemolovat svou kancelář, smazat či ukrást důležité údaje, či popřípadě napadne své kolegy nebo nadřízené. Takovému jednání lze předejít, pokud se mu odepře přístup k firemnímu systému a bezpečnostní služba ho pokojně vyvede z areálu společnosti. V některých případech mohou být taková opatření nutností, zvláště pokud s ním byla pracovní smlouva rozvázána ze zvláště závažného porušení pracovní kázně.

Co může nastat v případě, že společnost podcení takovouto situaci? Fyzické napadení či několik rozbitých počítačů patří spíše do kategorie menších škod. Naopak odcizení velmi důležitých dat (a posléze jejich prodej konkurenční společnosti) by mohlo tuto firmu i existenčně ohrozit. Proto je důležité nespoléhat na tzv. „fair-play“ svých zaměstnanců, ale spíše předvídat ty nejčernější scénáře a firma by na ně měla být připravena. [20]

6.3 Prolamování hesel

Tato kapitola popisuje možné útoky za účelem získání hesla, dále popisuje jak lze heslo zašifrovat. Na tuto kapitolu navazuje kapitola 9.2.1, která se věnuje samotné tvorbě a radám při tvorbě hesel.

Prolamovat hesla lze jak u souborů, u kterých jejich majitel nastavil heslo, tak i u uživatelských účtů operačního systému. Heslo je jeden z nejdůležitějších prvků samotné bezpečnosti systému, proto je důležité ho chránit jako oko v hlavě.

K prolamování hesel lze použít tzv. prolamovače hesel neboli `Password crackers`. Tyto prolamovače lze však použít jen u hesel statických, tedy u hesel, které se v čase nemění. V současnosti se u stále většího množství zařízení začíná využívat hesel dynamických. Prolamovače hesel fungují na principu zkoušení různých kombinací znaků, které jsou v určitých časových intervalech zadávány. O tom, jestli bude útok úspěšný v rozumném časovém horizontu, rozhoduje především délka hesla a jeho složitost. [20]

Na obr. 6 si lze povšimnout toho, jak nebezpečné je si zvolit jednoduché heslo, například 12345. Toto heslo útočník získá za pár minut, případně za pár sekund. Ačkoliv je tato tabulka již staršího data, má určitou vypovídající hodnotu. Uvedená hodnota, počet hesel za minutu, závisí na výkonu počítače, na výkonějších strojích to jsou řádově statisíce hesel za sekundu. Útočníci mohou pro útok využít i více počítačů najednou, díky čemuž mohou tuto hodnotu opět o něco zvýšit.

Použité znaky \ Délka hesla		4	5	6	7	8
		Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec
0-9	10 znaků	**10 000** 2 minuty	**100 000** 16 minut	**1 000 000** 3 hodiny	**10 000 000** 1 den	**100 000 000** 11 dní
a-z; 0-9	36 znaků	**7311616** 5 hodin	**380204032** 7 dní	**2×10^9** 8 měsíců	**8×10^{10}** 25 let	**3×10^{12}** 900 let
a-z; A-Z; 0-9	62 znaků	**14776336** 2 dny	**916132832** 3 měsíce	**5×10^{10}** 18 let	**4×10^{12}** 1000 let	**2×10^{14}** 70 000 let
a-z; A-Z; 0-9; ščáéě... ;@#$^*?!...	85 znaků	**52200625** 6 dní	**443705312** 1 rok	**3×10^{11}** 120 let	**3×10^{13}** 10 000 let	**3×10^{15}** 800 000 let

Obrázek 6: Porovnání složitosti hesla a doby jeho prolomení [29]

6.3.1 Slovníkový útok

Základem slovníkového útoku je zjistit heslo zkoušením hesel z předpřipraveného seznamu pravděpodobných hesel, nazývaným též „slovník“. V praxi se lze setkat s různými druhy slovníků, např. slovník obsahující pouze české či anglické výrazy. Lze tedy předpokládat, že si uživatel mohl zvolit jako heslo nějaké slovo, případně jej doplnit o číslici. Ve srovnání s útokem hrubou silou je tedy slovníkový útok potencionálně efektivnější. [20]

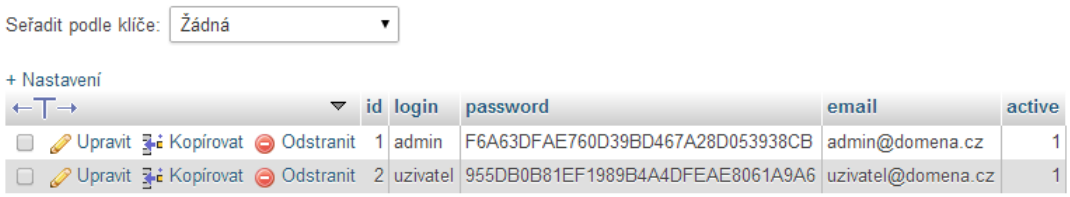
6.3.2 Útok hrubou silou

Jako útok hrubou silou se vyznačuje pokus prolomit heslo tak, že se testují všechny možné kombinace z určité množiny znaků. Jde tedy většinou o neefektivní útok neboť je potřeba na rozdíl od slovníkového útoku vyzkoušet všechny možné kombinace znaků, což je časově náročnější. [20]

6.3.3 Šifrování hesel a jejich následné prolomení

Šifrování hesel se běžně v praxi využívá například u webových aplikací, kdy je potřeba uchovávat přihlašovací údaje uživatelů. Aby se mohlo heslo zašifrovat, je nutné použít nějakou hashovací funkci. Hashovací funkce vytvoří otisk hesla, tzv. `hash`, jedná se o jednosměrné šifrování [1]. Tento otisk hesla je jednoduché vytvořit, ale je prakticky nemožné získat z tohoto otisku původní heslo. Jak takové heslo v zašifrované podobě vypadá je ukázáno na obr. 7. V jazyce PHP se zejména využívají tyto hashovací funkce:

- **MD5** – Pravděpodobně nejpoužívanější hashovací funkce, výsledný otisk obsahuje 32 znaků, existují však způsoby, jak toto šifrování prolomit.
- **SHA1** – Bezpečnější hashovací funkce, hash obsahuje 40 znaků.
- **BASE64/Encode** – Tato funkce šifruje data pomocí MIME base64. Takto zakódovaná data zabírají zhruba o 33% více prostoru než původní data.



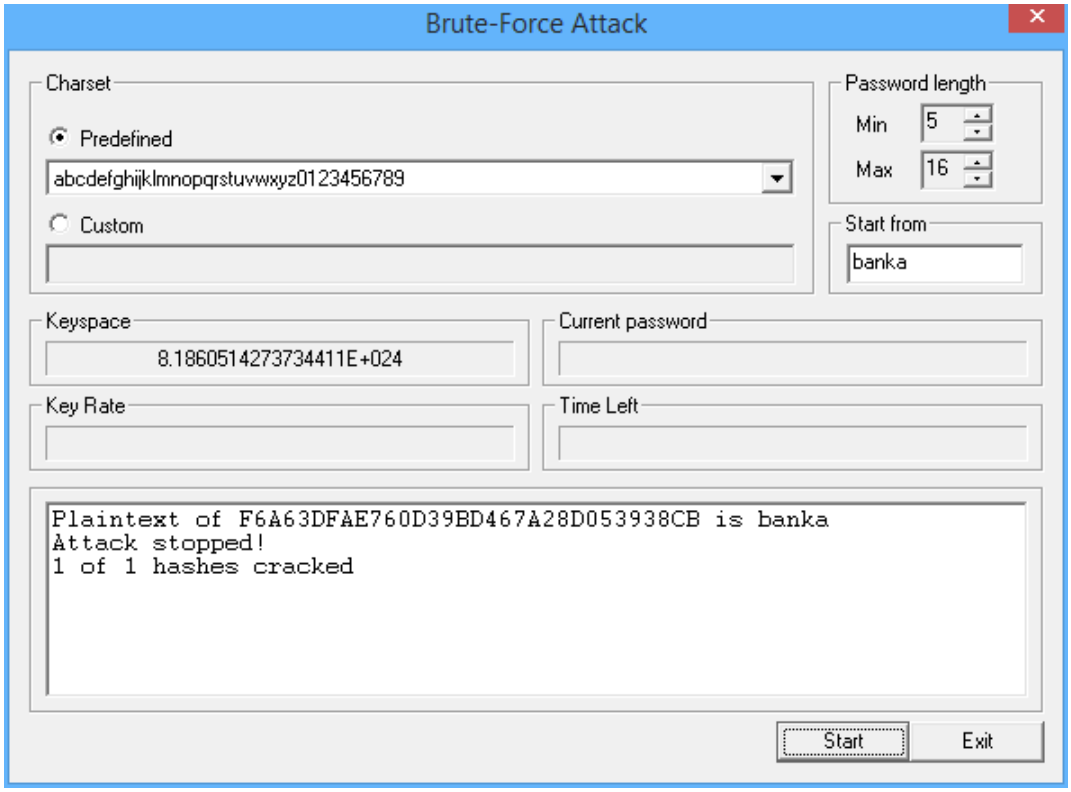
Obrázek 7: Podoba zašifrovaného hesla v databázi

V praxi se ověření správností údajů při přihlášení uživatele provede tak, že se z databáze získá zašifrované heslo, které se porovná se zašifrovaným heslem, které uživatel zadal. Obě hodnoty se Zašifrování hesla lze v jazyce PHP provést následovně:

```
<?php
 $heslo = "tajne_heslo";
 $hash = MD5($heslo);
 echo $heslo; //vypíše původní heslo
 echo $hash; //vypíše hash hesla dlouhý 32 znaků
?>
```

Než se útočník rozhodne pro nějaký útok na prolomení hesla, které je zašifrované, může využít služeb internetového vyhledávače **Google**. Pokud má útočník k dispozici hash (prolomil tedy zabezpečení a má přístup do databáze s hesly, které jsou zašifrované), může tento hash vyhledat. Některé obvyklé hesla (např. 123456, abc123, password apod.) již někdo v zašifrované podobě pravděpodobně hledal, proto je lze snadno vyhledat.

K útoku může útočník využít celou řadu nástrojů, např. oblíbený program **Cain & Abel**, na který je zaměřena kapitola 7.1. Tento program umožňuje vytvořit hash pro libovolné heslo a následně se jej pokusit prolomit, a to jak pomocí slovníkového útoku či útoku hrubou silou, viz obr. 8.



Obrázek 8: Prolomení zašifrovaného hesla v programu Cain & Abel

Ještě větší bezpečnosti lze docílit tím, že se k původnímu heslu přidá tzv. sůl. Počet znaků hashe zůstane stejný, ale zabrání se tomu, že uživatelé se stejným heslem budou mít jiný hash. V tomto případě může být sůl např. uživatelské jméno či email (obecně tedy jedinečný údaj). V konečném důsledku to pro útočníka znamená ztížení útoku, respektive pokles jeho úspěšnosti. Demonstrovat lze tento způsob dodatečné ochrany např. takto:

```
<?php
 $heslo = "tajne_heslo";
 $hash = MD5($heslo."fghjgtzjjhg");
 echo $heslo; //vypíše původní heslo
 echo $hash; //vypíše hash hesla včetně ocásku
?>
```

7 Nástroje k provedení útoků

Následující kapitoly se věnují představení některých nástrojů, které lze použít buď k provedení samotného útoku, nebo k tzv. „přípravě půdy“. Tato kapitola nemá za cíl vytvořit jakýsi „návod“, ale pouze poukázat na možné programy, které útočníci mohou nebo nemusí při útoku využít. Alternativou je využít speciální linuxovou distribuci BackTrack[1], která některé důležité nástroje již obsahuje.

7.1 Cain & Abel

Jedná se o Windows GUI aplikaci známou spíše jako Cain, ukázka je zobrazena na obr. 9. Ačkoliv tvůrci projektu na svých stránkách popisují program Cain & Abel jako „Password Recovery Tool“ (nástroj pro obnovu zapomenutých hesel), ve své podstatě se jedná spíše o tzv. „sniffer“ (zachytávač paketů). Mezi integrované funkce např. patří dump hash, crack hash, hash calculator, WiFi stumbler a další. V případě, že chce útočník poslouchat provoz v rámci bezdrátové sítě, musí mít k dispozici bezdrátovou kartu, která podporuje tzv. „promiskuitní režim“ (karta přijímá všechny datové pakety). Abel je samostatná aplikace, kterou lze pomocí programu Cain nainstalovat na vzdálený počítač. Útočník tak může získat kontrolu na vzdáleném počítači a přímo jej ovládat.[30]

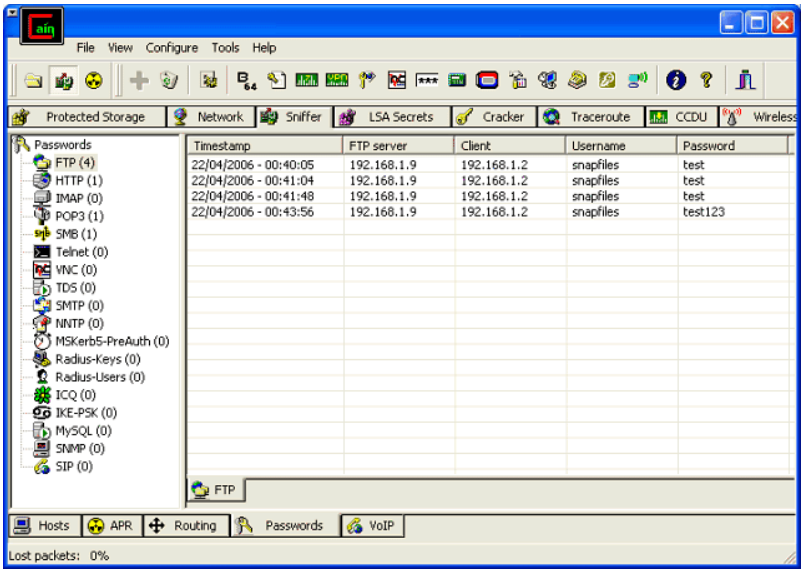
Tzv. hotkeys pro ovládání programu Cain & Abel:

- **ALT + DEL**: schování okna (nejde vidět na systémové liště, pouze v aktivních procesech).
- **ALT + PageDown**: minimalizace do systémové lišty.
- **ALT + PageUp**: obnovení okna.

7.2 NetTools

Tento program slouží spíše k přípravě půdy před samotným útokem. NetTools je sada užitečných nástrojů pro použití na síti, verze 5.0.70 jich obsahuje celkem 175. Všechny nástroje jsou k dispozici z přehledného uživatelského rozhraní. Jde například o:

[1] `http://www.backtrack-linu.org/`



Obrázek 9: Nástroj Cain & Abel

- **NetWatch** (host monitor),
- **WinTools** (podrobné systémové informace o počítačích v síti),
- **NetStat** (seznam připojení k počítači),
- **Network Scanner** (vyhledání všech zařízení z rozsahu IP adres a běžících služeb),
- **Service & Port Scanner** (zjištění otevřených portů a spuštěných služeb).

7.3 Ettercap

Ettercap je další z řady nástrojů, tzv. „snifferů“ a útočníky je oblíben především u útoků typu „man in the middle“. V současnosti podporuje linuxové distribuce Debian/Ubuntu (včetně distribuce Linux Mint) nebo Fedora. Používat jej mohou také uživatelé Mac OSX (verze Snow Leopard a Lion). Ettercap není v současnosti možné používat na OS Microsoft Windows.

7.4 CrackLib

V kapitole 8.3 je ukázka kontroly síly hesla právě pomocí nástroje CrackLib. Pomocí tohoto PAM modulu lze donutit jednotlivé uživatele používat kvalitní a silná hesla.

Nejedná se tedy o nástroj k získání hesla uživatele, nicméně jedním z cílů této práce je i informovat o možné obraně před možnými útoky, což používání silného hesla bezesporu je. CrackLib také kontroluje, zda nové heslo nemůže být prolomeno slovníkovým útokem, dále obsahuje možnost definovat vlastní soubor se slovníkem. V současnosti je nástroj CrackLib možné používat pouze na distribucích Linuxu.

8 Praktické ukázky útoků

V následujících kapitolách jsou vybrány některé z útoků a jsou prakticky vyzkoušeny. Nechybí také nastínění případné obrany a zabezpečení proti nim.

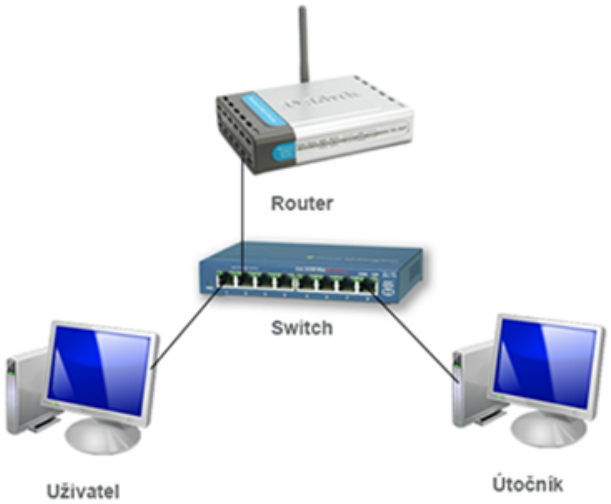
8.1 Útok ARP Cache Poisoning

8.1.1 Nastavení

Tento útok lze prakticky demonstrovat na situaci, pokud se útočníkovi povede připojit do místní sítě. V této síti se nachází kromě útočníka i počítač uživatele, switch a router. Adresace před útokem je zobrazena v tabulce 1. Obě stanice jsou připojeny ke switchi pomocí kabelu UTP. Fyzické zapojení sítě dokumentuje obr. 10.

Název zařízení	**Adresa IP**	**Adresa MAC**
Router	192.168.1.1	00-27-22-55-9C-D0
Uživatel	192.168.1.43	50-46-5D-B2-D6-DD
Útočník	192.168.1.133	E8-9A-8F-FC-57-66

Tabulka 1: Adresace před útokem



Obrázek 10: Zapojení sítě při útoku ARP Cache Poisoning

8.1.2 Ukázka útoku

Pro ukázku útoku lze použít nástroj **Ettercap** (kapitola 7.3), jeho instalace se v distribuci **Debian/Ubuntu** provede tímto způsobem:

```
# sudo apt-get install ettercap-graphical
```

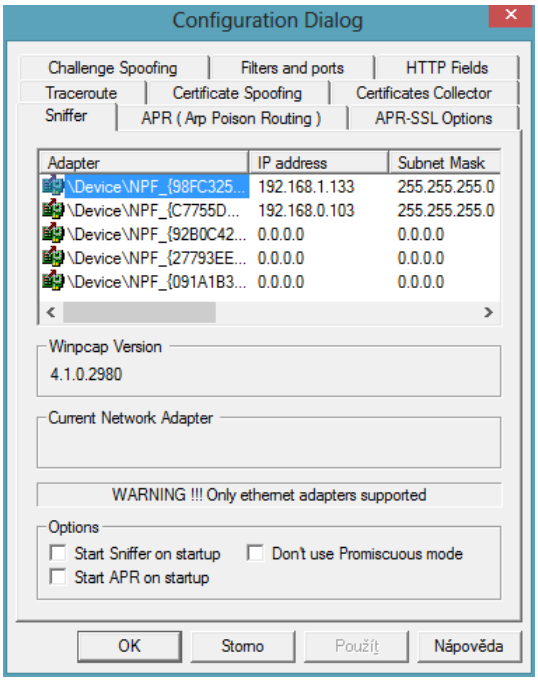
Útok tedy po spuštění programu Ettercap probíhá následovně:

- V hlavním menu se vybere možnost `Sniff` – `Unified sniffing` a zvolí se odpovídající rozhraní (nejčastěji `eth0` nebo `wlan0`).
- Poté se provede prohledání sítě za účelem získání seznamu dalších stanic. Položka `Hosts` – `Scan for hosts`.
- Následuje vybrání cílů pro útok – `Hosts` – `Hosts list`. Adresa IP `192.168.1.1` patří routeru (možnost `Add to Target 1`) a adresa IP `192.168.43` je uživatel (možnost `Add to Target 2`). V případě, že nedojde k vybrání jednotlivých zařízení, aplikuje se ARP Cache Poisoning na všechny počítače v dané konkrétní síti.
- V dalším kroku se provede výběr MITM útoku – `Mitm` – `Arp poisoning` a následně volba `Start` – `Start sniffing`.

Útočit lze tímto způsobem i z prostředí **Microsoft Windows** pomocí nástroje **Cain & Abel**, kterému se věnuje kapitola 7.1. Postup je následující:

- Po spuštění programu je třeba spustit `Sniffer`, to se provede poklepáním na ikonku `Start/Stop Sniffer`.
- Vybere se odpovídající `Adepter`, důležité je věnovat pozornost hodnotě ve sloupci `IP address`, lze tak rozlišit adaptér pro síť Ethernet či Wi-Fi, viz obr. 11.
- Nyní je třeba provést samotné skenování sítě. Toho se docílí zvolení záložky `Sniffer`, kde lze pomocí stisku pravého tlačítka vybrat možnost `Scan MAC Addresses`. Zde lze zvolit sken všech adres v daném subnetu či vybrat konkrétní rozsah.

- Další krokem je zapnout APR útok (ARP Poison Routing). Toho lze dosáhnout kliknutím na ikonku `Start/Stop APR`. Poté je třeba kliknout dole na záložku APR, zde stisknout klávesu `Insert` a vybrat cílový router, na který bude veden útok. Od této chvíle útočník odposlouchává provoz směřující přes tento směrovač.

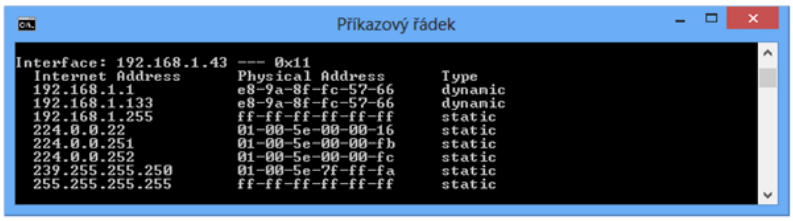


Obrázek 11: Výběr adaptéru pro odposlech sítě v programu Cain

8.1.3 Výsledek útoku

Veškerá síťová komunikace mezi uživatelem a routerem je od této chvíle vedena přes útočníka, který ji může nerušeně zachytávat. Útoku si lze například povšimnout v tabulce ARP oběti (obr. 12) pomocí příkazu `arp -a`.

Fyzická adresa routeru a útočníka je naprosto stejná. V tomto případě byl tedy útok úspěšný. Útočník odposlouchává síťový provoz, tedy například i hesla, které uživatelé zadávají při nezabezpečené komunikaci se servery pomocí protokolu HTTP, proto je velmi nebezpečné zadávat hesla při tomto nezabezpečeném spojení např. v internetové kavárně nebo pokud je uživatel připojen pomocí nezabezpečené Wi-Fi sítě. Existuje reálná hrozba odposlechu.



Obrázek 12: Tabulka ARP z pohledu uživatele

8.1.4 Obrana před útokem ARP Cache Poisoning

Obrana proti tomuto typu útoku spočívá především:

- v používání takového antivirového programu, které dokáže detekovat pokus o ARP Cache Poisoning útok (např. ESET NOD32),
- v zabránění přístupu neoprávněných osob do dané sítě,
- v používání vhodného switche, který provádí inspekci paketů ARP,
- ve využívání statických položek v tabulce ARP (záznam, kterému nikdy nevyprší platnost a systém ho neaktualizuje – a právě to přináší zmíněnou ochranu před útokem). [11]

8.2 DHCP Spoofing

8.2.1 Situace před útokem

Tento útok využívá situace jako v kapitole 8.1 ARP Cache Poisoning Attack, kdy se útočníkovi podařilo fyzicky připojit do sítě. Switch, kterým disponuje administrátor v této síti, neumožňuje síť zabezpečit proti útoku typu DHCP Spoofing.

8.2.2 Útok

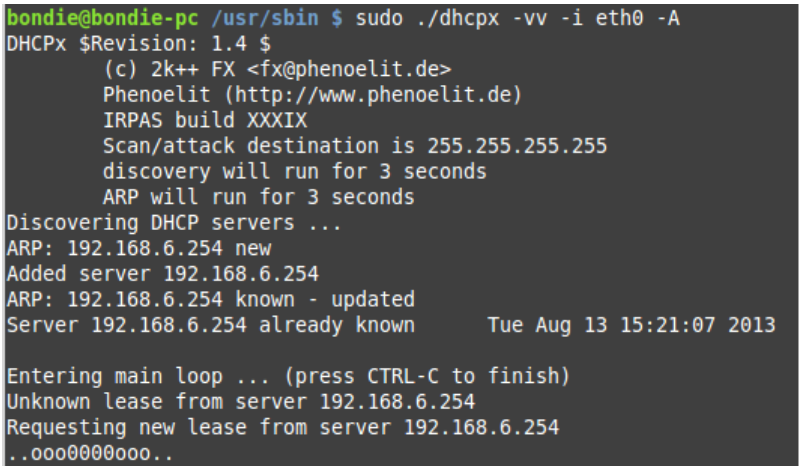
K útoku lze opět použít nástroj `Ettercap`, jeho instalace je vysvětlena v kapitole 8.1. Dále je potřeba nainstalovat balík nástrojů `irpas`, který obsahuje nástroj `dhcpx`. Pomocí tohoto nástroje lze dosáhnout vyčerpání všech volných adres IP na serveru DHCP.

```
# sudo apt-get install irpas
```

Vyčerpání volných adres lze provést příkazy:

```
# cd /usr/sbin
# sudo ./dhcpx -vv -i rozhraní -A
```

Po vykonání tohoto příkazu se spustí program `dhcpx`, který prohledá síť za účelem zjištění serverů DHCP a poté ve smyčce se jich začne dotazovat a žádat o zapůjčení adres (obr. 13).



Obrázek 13: Vyčerpávání volných adres IP

Dalším krokem je spuštění předem avizovaného nástroje Ettercap, následně proběhne výběr volby `Unified sniffing` a v nabídce `Mitm` se vybere volba `DHCP spoofing`. Poté již útočníkovi nic nebrání v tom, aby začal odchytávat data pomocí volby `Start sniffing` [12]

8.2.3 Výsledek útoku

Tento útok by úspěšný, neboť síť (respektive síťové prvky) nebyla jakkoliv zabezpečena proti tomuto útoku.

8.2.4 Obrana

Jako obrana se proti útoku typu DHCP Spoofing používá technologie s příznačným názvem DHCP Snooping. Princip této obrany je založen na rozdělení portů na síťovém

zařízením (v tomto případě se jedná o switch) do dvou skupin:

- **trusted** – pokud se za portem nachází další switch nebo počítač s DHCP serverem,
- **untrusted** – pokud je na portu připojen počítač.

V případě, že je na přepínači spuštěný režim `DHCP Snooping`, na síti běží útočníkův falešný server DHCP a nějaký klient požádá o adresu IP, dojde k situaci, kdy se na přepínači zkontroluje, zda odpověď (`DHCPOFFER`) na klientův `DHCPDISCOVER` byla vyslána z `trusted` portu. Pokud se útočníkovi nepodaří připojit se do `trusted` portu, dojde k zabránění útoku pomocí metody DHCP Spoofing. Úspěch této obrany tedy závisí na správné konfiguraci přepínače, aby jednotliví uživatelé nemohli být připojeni na `trusted` portech.

8.3 SYN Flooding

Tento DoS útok lze demonstrovat na situaci, kdy se útočník rozhodne zaútočit na webový server. Útočník zná adresu IP tohoto serveru a tato služba běží na portu 80.

8.3.1 Nastavení

Útok lze simulovat na místní síti LAN, jako webový server dobře poslouží Apache verze 2.4.9 v balíku Xampp, na server je nainstalován operační systém Windows 8.1, který je chráněn antivirovým programem ESET Smart Security, který obsahuje také firewall. Útočník pro útok využívá operační systém Linux Mint 16.

8.3.2 Útok

Jako nástroj k provedení útoku lze využít `hping3`:

```
# sudo apt-get install hping3
```

Poté útočník může začít zaplavovat daný server pakety s příznakem SYN:

```
# sudo hping3 -i u1 -S -p 80 192.168.1.43
```

8.3.3 Výsledek útoku

V tomto případě se však útok nepovedl, neboť webový server stálé vykonává svou funkci, byť s pomalejší odezvou. Útoky typu SYN Flooding jsou v moderních systémech obvykle neúspěšné. Fungují v případech, pokud server alokuje prostředky pro nové spojení ihned, jakmile obdrží paket s příznakem SYN. Situace by se změnila, pokud by se tento útok vedl z více zdrojů, neboť DDoS útok by znamenal pro konkrétní server daleko větší nebezpečí. Důležité je také uvést, že webový server Apache obsahuje direktivu ListenBackLog, která určuje maximální počet ve frontě čekajících spojení. Tento počet závisí na konkrétním operačním systému.

8.3.4 Obrana před útokem

Obranou proti tomuto útoku je:

- použití tzv. SYN cookies,
- omezení maximálního počtu nových spojení z konkrétního zdroje.

8.4 Útok na webový server pomocí skriptu Slowloris

Další ukázkou bude útok na webový server, který lze zařadit do kategorie DoS útoků. Takovýto útok lze demonstrovat s využitím jednoduchého skriptu s názvem Slowloris, který je mimochodem napsaný v jazyce Perl. Tento útok není úspěšný na všech web serverech, funguje na serverech Apache či dhttpd, s nepořízenou útočník odejde na web serverech lighttpd či IIS 6 a 7 od společnosti Microsoft. Snahou útočníka je vyřadit na určitou dobu webový server z provozu. Útočník může tento útok provést za účelem vyvolání hrozby či odplaty. Velmi často útočníci útočí na internetové obchody, kdy je snahou daný e-shop vyřadit z provozu z důvodu konkurečního boje. Všechny takovéto útoky jsou samozřejmě nelegální a trestné.

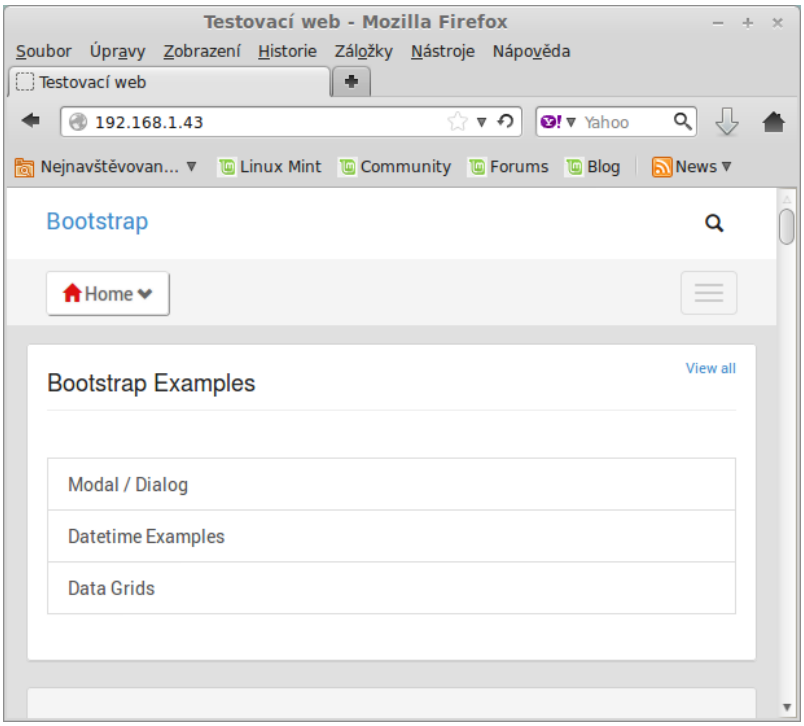
8.4.1 Nastavení

V praxi se v drtivé většině případů útočí přímo přes síť Internet, v této ukázce bude dostačující simulovat tento útok v místní síti LAN. Webový server a útočník jsou ve

stejné síti LAN, oba připojeni pomocí společného přepínače. Na serveru je nainstalován OS Windows 8.1 společně s webovým serverem Apache verze 2.4.9 spravovaný balíkem Xampp. Server je zabezpečen pomocí antiviru s integrovaným firewallem ESET Smart Security 7. Útočník provádí útok z notebooku disponujícím OS Linux Mint 16. Adresace před útokem je uvedena v tabulce 2, webová stránka na serveru je zobrazena na obr. 14.

Název zařízení	**Adresa IP**	**Adresa MAC**
Router	192.168.1.1	00:27:22:55:9C:D0
Server	192.168.1.43	50:46:5D:B2:D6:DD
Útočník	192.168.1.136	74:E5:0B:1F:98:16

Tabulka 2: Adresace před útokem



Obrázek 14: Webová stránka před útokem

8.4.2 Útok

Cílem útoku není vyvinout silný tlak na webový server tak, aby se server samotný pod náporem požadavků zhroutil, jako tomu často bývá. Naopak lze využít potencionálního

nebezpečí toho, že si server udržuje s klientem spojení určitou dobu, respektive pokud klient do vypršení této doby pošle nějaký požadavek, spojení je stále aktivní. Bohužel server už nezajímá, co klient konkrétně zasílá. Skript Slowloris zasílá postupně řádky nekonečné hlavičky, implicitně každých 100 sekund. Webový server Apache má výchozí hodnotu pro dobu čekání na spojení (Timeout) 300 sekund, tedy pět minut.

Útok je velmi jednoduchý, příprava zabere pár minut. Na stránkách projektu Slowloris [2] lze stáhnout samotný skript slowloris.pl, poté stačí spustit příkaz:

```
perl slowloris.pl -dns adresa_serveru
```

V tomto případě tedy:

```
perl slowloris.pl -dns 192.168.1.43
```

Příkaz lze různě modifikovat (existuje i skript pro IPv6), více informací lze zjistit v dokumentaci.

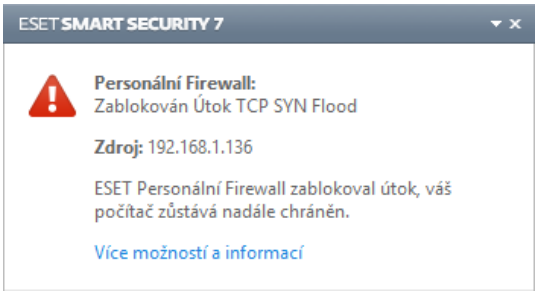
8.4.3 Výsledek útoku

Ačkoliv první zmínky o tomto útoku se objevují již v roce 2009, útok byl přesto úspěšný. Antivirový program zaznamenal pokus o útok a vypsal výstražnou hlášku (obrázek 11). Nezabránil však tomu, že webový server přestal reagovat na jakékoliv dotazy. Webový server Apache ve výchozím nastavení je proti tomuto útoku bezmocný. Prakticky ihned po odeslání příkazu je server nedostupný, útočník si tedy může mnout ruce. Administrátor v tomto případě ani nemusí vědět, že nějaký útok probíhá. Chybové záznamy nic nenapoví, protože k žádnému problému nedošlo. Zatížení serveru je prakticky nulové, nejedná se o DDoS útok, síťový provoz je velmi nízký. Za zmínku stojí jedině velké množství otevřených spojení. Webový server je přesto vyřazen. Výstražnou hlášku firewallu zobrazuje obr. 15, webovou stránku po útoku obr. 16.

8.4.4 Obrana

Jako dostačující obranu nelze považovat samotný firewall (ESET Smart Security) ve výchozím nastavení, protože nezabránil útoku. V praxi se samozřejmě webové servery

[2] http://ha.ckers.org/slowloris/



Obrázek 15: Výstražná hláška firewallu na serveru

neprovozují na obyčejné klientské stanici jako v této ukázce. Pokud by webový server běžel např. na Linuxu, mohlo by se využít IPTables:

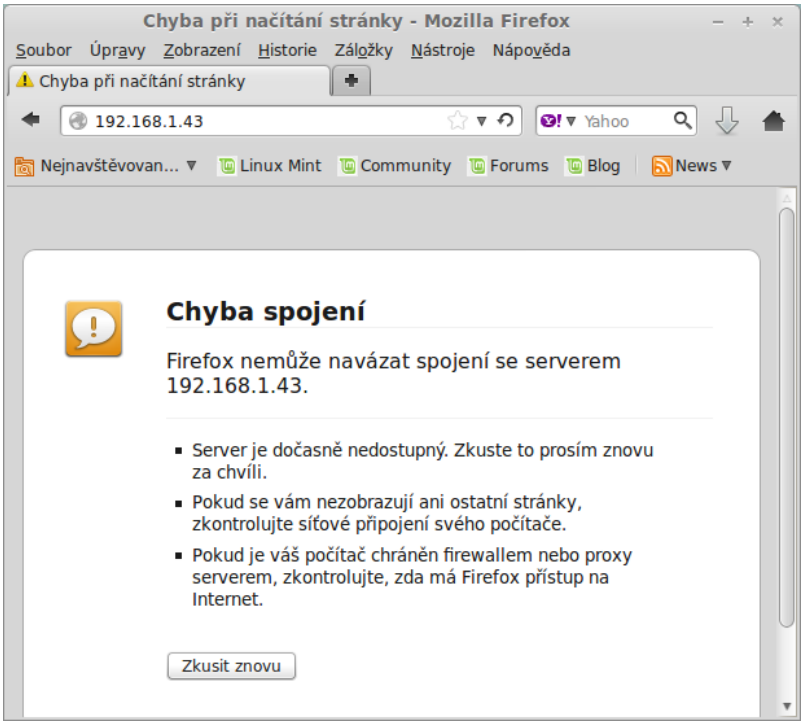
```
# iptables -I INPUT -p tcp --dport 80 -m connlimit --connlimit-above 20
-j REJECT
```

Nevýhodou této konfigurace je zejména to, že se nerozlišuje, co se uživatel snaží přesně získat. Vhodnější je využít modul `mod_limitipconn`, který omezí počet spojení otevřených z jedné adresy IP.

```
LoadModule limitipconn_module modules/mod_limitipconn.so
<IfModule limitipconn_module>
ExtendedStatus On
MaxConnPerIP 10
NoIPLimit images/*
</IfModule>
```

Administrátor v tomto případě musí vzít v potaz skutečnost, že tímto omezí i uživatele, kteří jsou skrytí za sítí NAT (mají tedy společnou veřejnou adresu IP). V předchozím kódu si lze také povšimnout zrušení tohoto omezení, pokud se jedná o obrázky. Pokud je na stránkách obrázků mnoho, prohlížeče si většinou pro jejich zobrazení otevírají další spojení.

Existuje také specializovaný modul, který se snaží přímo bojovat s útokem Slowloris, jeho název je `mod_antiloris`. Jeho úkolem je počítat, kolik spojení z jedné adresy IP je ve stavu `SERVER_BUSY_READ` (ve stavu, kdy server čte data od klientů). V případě, že je toto číslo příliš velké, server další spojení z této adresy již nepřijme. [16]



Obrázek 16: Stav po útoku

8.5 Kontrola síly hesla pomocí nástroje CrackLib

Tato kapitola se nezabývá konkrétním útokem, ale popisuje způsob, jak preventivně zabezpečit hesla jednotlivých uživatelů v systému. Tyto hesla mohou být v nebezpečí tehdy, pokud se útočník rozhodně zaútočit pomocí slovníkového útoku nebo útoku hrubou silou (a například nějakým způsobem získal přímý přístup k počítači). Pokud hesla nebudou dostatečně silná, lze jej slovníkovým útokem jednoduše prolomit. V prvé řadě je nutná instalace nástroje CrackLib (pro distribuce Debian/Ubuntu):

```
# sudo apt-get install libpam-cracklib
```

Poté následuje editace konfiguračního souboru:

```
# sudo nano /etc/pam.d/system-auth
```

Do kterého se vloží následující řádek:

```
password required pam_cracklib.so retry=2 minlen=10 difok=6
```

Kde jednotlivé parametry znamenají:

- **retry = 2**: Nastavení maximálně 2 pokusů o změnu hesla, poté se vrátí chyba.
- **minlen = 10**: Nastavení minimální délky hesla na 10 znaků.
- **difok = 6**: Kolik znaků může být v novém hesle stejných ve srovnání se starým heslem (v tomto případě tedy šest). V případě chyby se vrátí chybová hláška varující, že heslo je podobné starému heslu.

Dále lze mít na uživatele ještě požadavky, aby heslo obsahovalo:

- **dcredit = N**: N počet čísel.
- **ucredit = N**: N počet velkých písmen.
- **lcredit = N**: N počet malých písmen.
- **ocredit = N**: N počet ostatních znaků.

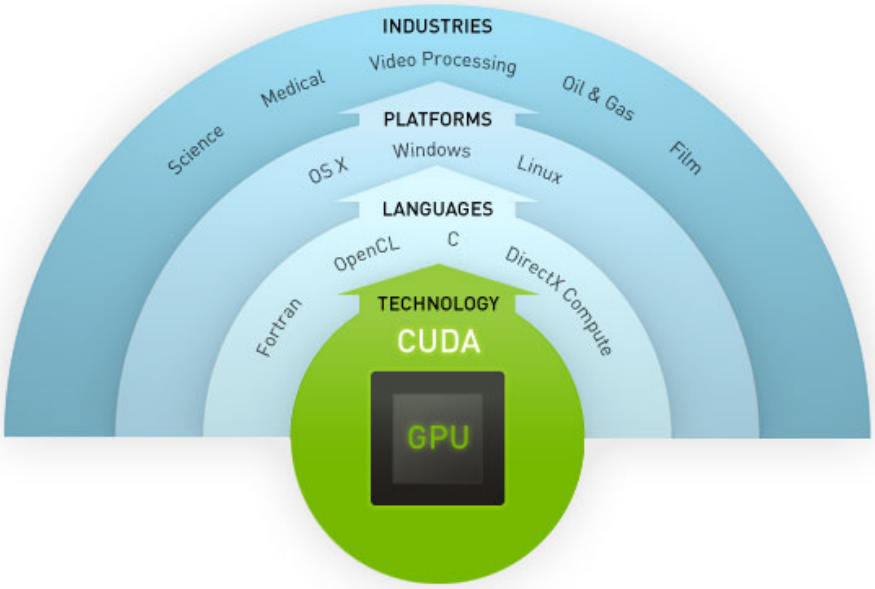
V praxi by například vytvoření hesla, které by uživatel mohl zkusit vytvořit maximálně 3krát, jeho minimální délka by byla 10 znaků, 6 znaků by mohlo být použito i ve starém hesle, dále které by obsahovalo 2 čísla, 1 velké písmeno a 2 symboly, by vypadalo v konfiguračním souboru následovně:

```
password required pam_cracklib.so retry=3 minlen=10 difok=6
dcredit=2 ucredit=1 ocredit=2
```

Je však důležité upozornit na skutečnost, že tyto zásady pro tvorbu hesla platí pouze pro obyčejné uživatele, nikoliv pro uživatele s právy root, ten si heslo může zvolit jakékoliv (nicméně i přesto ho cracklib na tuto skutečnost upozorní). [33]

8.6 Lámání hesel silou grafické karty

V této kapitole je ukázka prolomení několika zašifrovaných hesel, a to jak těch jednodušších, tak i složitějších. Tato kapitola volně navazuje na kapitolu 6.3.3, která se zaměřila na popis šifrování hesel a jejich následného prolomení. Útočníci mohou využít velké výpočetní kapacity nejnovějších grafických karet podporujících architekturu CUDA od společnosti NVIDIA či konkureční architekturu ATI Stream od stejnojmenné společnosti. Tyto architektury podporují spouštění programů napsaných např. v jazycích C/C++ či Fortran přímo na GPU (obr. 17). [28]



Obrázek 17: Architektura CUDA [28]

8.6.1 Nastavení

Útok bude proveden na výkonějším počítači, komponenty jsou uvedeny v tabulce 3. Systémové prostředí je Windows 8.1. Tento útok bude simulovat situaci, kdy útočník získá hesla z databáze, která jsou zašifrovaná hashovací funkcí MD5 a rozhodne se je prolomit pomocí útoku hrubou silou za pomocí výkonu grafické karty. Získaná hesla jsou uvedeny v tabulce 4.

Název komponenty	**Popis komponenty**
Procesor	Intel Core i5-3470 3.20 GHz
Paměť RAM	8 GB
Základní deska	ASUS P8Z77-M
Grafická karta	NVIDIA GTX 660Ti 2G DDR5

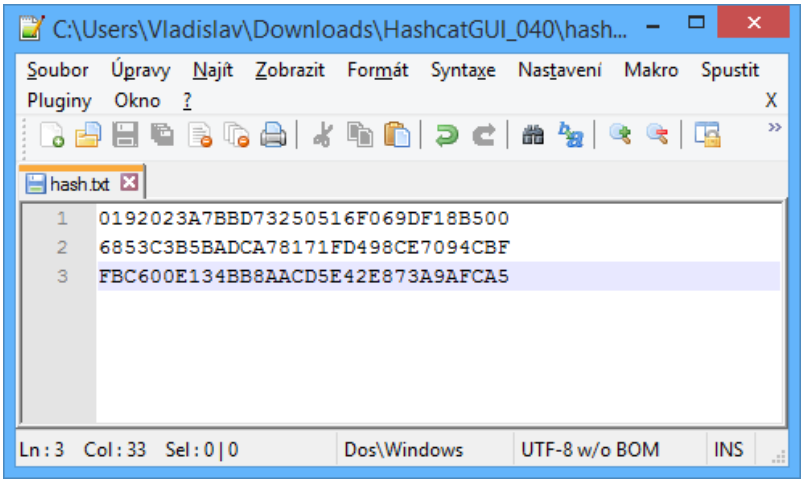
Tabulka 3: Komponenty útočníkova počítače

Uživatelské jméno	Heslo	Heslo v MD5
admin	admin123	0192023A7BBD73250516F069DF18B500
roman	slunicko	6853C3B5BADCA78171FD498CE7094CBF
lucie	lucka.88	FBC600E134BB8AACD5E42E873A9AFCA5

Tabulka 4: Získané hesla zašifrované v MD5

8.6.2 Útok

Nástrojů k provedení útoku existuje několik, v této ukázce bude pozornost věnována nástroji `HashCat`[3]. Tento nástroj lze ovládat buď přímo z příkazové řádky nebo pomocí GUI aplikace (grafické uživatelské prostředí). Útočník v těchto případech většinou disponuje získanými hesly, které má uloženy v textovém dokumentu, jeden řádek odpovídá jednomu záznamu (obr 18).

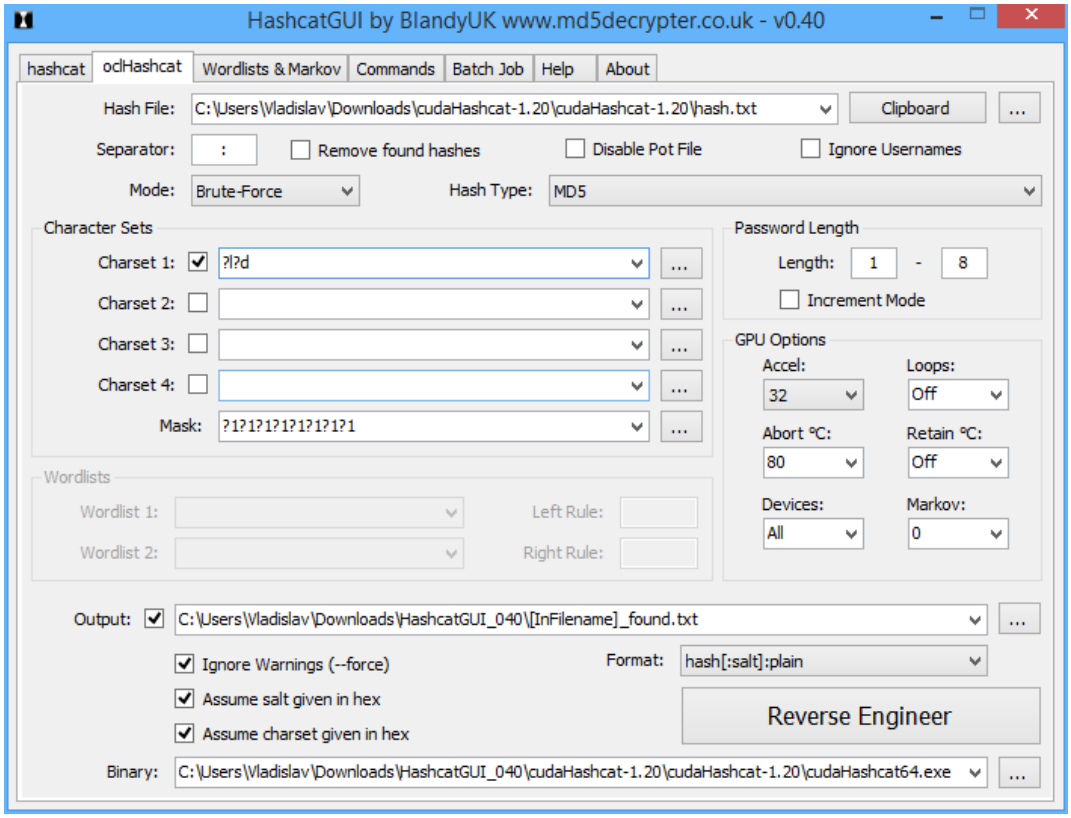


Obrázek 18: Zašifrované hesla v dokumentu

Obr. 19 zobrazuje nastavení programu HashCat. Pozornost je nutné věnovat zejména těmto položkám:

- **Hash File** – Zdrojový soubor se zašifrovanými hesly.
- **Mode** – Výběr typu útoku, v tomto případě útok hrubou silou.

[3]Ke stažení je na adrese `http://www.md5decrypter.co.uk/hashcat-gui.aspx`.

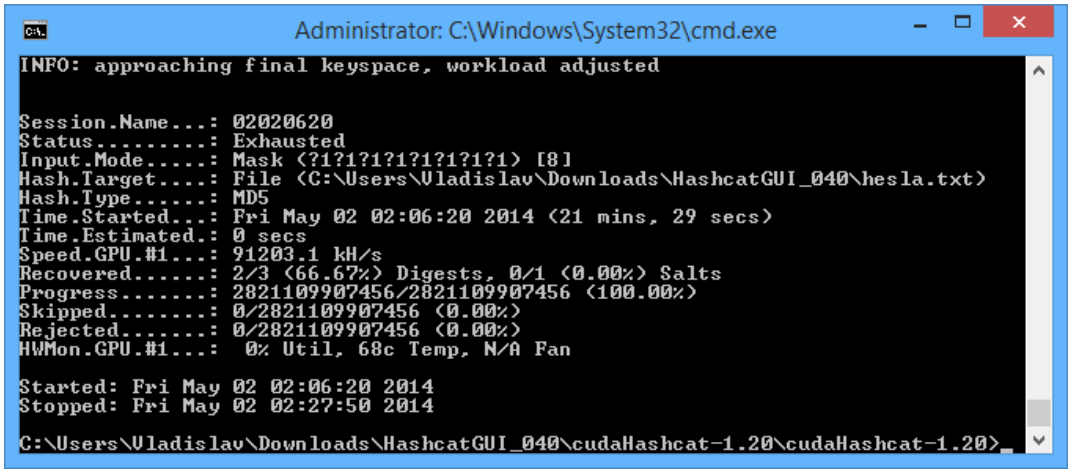


Obrázek 19: Nastavení útoku v programu HashCat

- **Hash Type** – Výběr hashovací funkce či tvaru, pomocí které jsou hesla zašifrována. Na výběr je několik desítek možností (MD5, SHA1, WPA/WPA2, atd.).
- **Character Sets** – Očekávaný formát hesla (l – malé znaky abecedy, u – velké znaky abecedy, d – čísla 0 - 9, s – speciální znaky (!,#,$, apod.), a – kombinace všech možností).
- **Password Length** – Očekávaná délka hesla.
- **Output** – Výstupní soubor s nalezenými hesly.

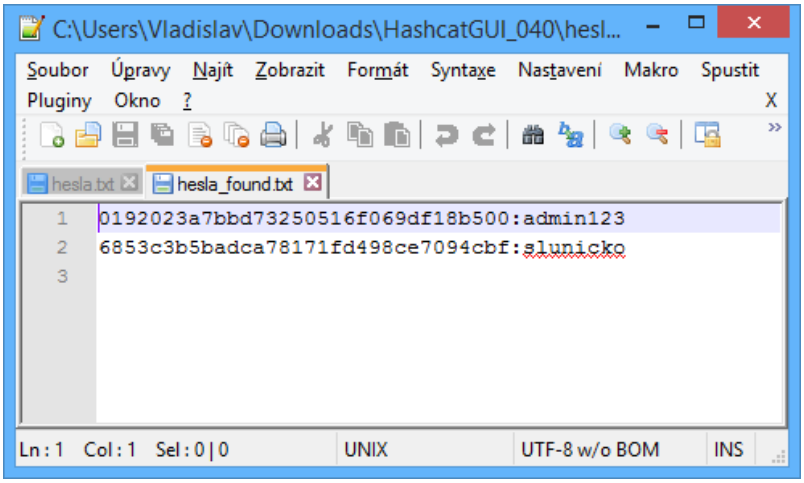
8.6.3 Výsledek útoku

Útok probíhal něco málo přes 20 minut (obr. 20) a podařilo se získat dvě hesla ze tří (obr. 21). První údaj je původní zašifrované heslo v MD5, následuje dvojtečka a prolomené heslo. Heslo uživatele lucie se prolomit nepodařilo, protože je toto heslo ze všech hesel nejsilnější. Pokud by však útočník zvolil možnost testování všech možných



Obrázek 20: Výsledek útoku v programu HashCat

znaků při maximální délce hesla 8 znaků, trvalo by prolomení hesla uživatele lucie maximálně 28 dní. Pokud by měl útočník štěstí, tak samozřejmě i kratší dobu. Lze tedy usoudit, že i heslo uživatele lucie není bezpečné.



Obrázek 21: Získané hesla uživatelů

8.6.4 Obrana proti útoku

Obranou proti útoku je v prvé řadě zabezpečení databáze tak, aby k ní útočník neměl přístup. Toho lze docílit např. povolením přístupu k databázi pouze z vyhrazených adres IP, případně (pokud to situace umožňuje) povolit tento přístup pouze z místní sítě LAN. Těmito způsoby lze omezit možnost anonymního útoku zvenčí.

Nicméně i hesla je třeba volit taková, aby nešly prolomit i za použití útoku hrubou silou. Mnoho uživatelů používá stejné heslo prakticky všude. Existuje reálné nebezpečí, že při získání jeho hesla (společně i s dalšími údaji, jako je přihlašovací jméno, email, apod.), může útočník zneužít tyto údaje jinde. Proto se doporučuje mít různá hesla, ne pouze jedno. Správnému postupu při tvorbě hesla se věnuje kapitola 9.2.1.

9 Zásady zabezpečení

Jedním z cílů této práce je vypracování zásad zabezpečení počítačového systému určených jak pro administrátory takového systému, tak i pro běžné uživatele. Následující kapitola popisuje v prvé řadě základní pravidla, které by měl dodržovat administrátor či správce počítačové sítě, aby samotní uživatelé byli co nejméně ohroženi možnými útoky.

Důležité je však i to, aby všeobecná pravidla dodržoval i konkrétní uživatel. To, co administrátor nemůže ovlivnit, je samozřejmě chování uživatele v síti, např. navštěvování jen důvěryhodných stránek, používání bezpečných hesel, atd. V rámci bezpečnostní politiky firmy však nemusí mít konkrétní uživatel tolik volnosti a může být v používání počítače notně limitován.

9.1 Administrátorská část

Zabezpečení z pohledu administrátora by mělo vycházet z principu „Co není povoleno, je zakázáno“. Jde tedy především o to, aby uživatel nemohl svou činností ovlivňovat bezpečnost počítačového systému či celé počítačové sítě. V případě, že uživatel chce povolit určitou službu, která je momentálně zakázána, měl by informovat administrátora s požadavkem o povolení přístupu k této službě. Administrátor pak na základě svých zkušeností a vědomostí uživateli vyhoví či nikoliv.

Administrátor by tedy kromě samotného zabezpečení počítačů a sítě jako takové měl také jednotlivé uživatele školit, respektive informovat je o možných bezpečnostních hrozbách a podobně.

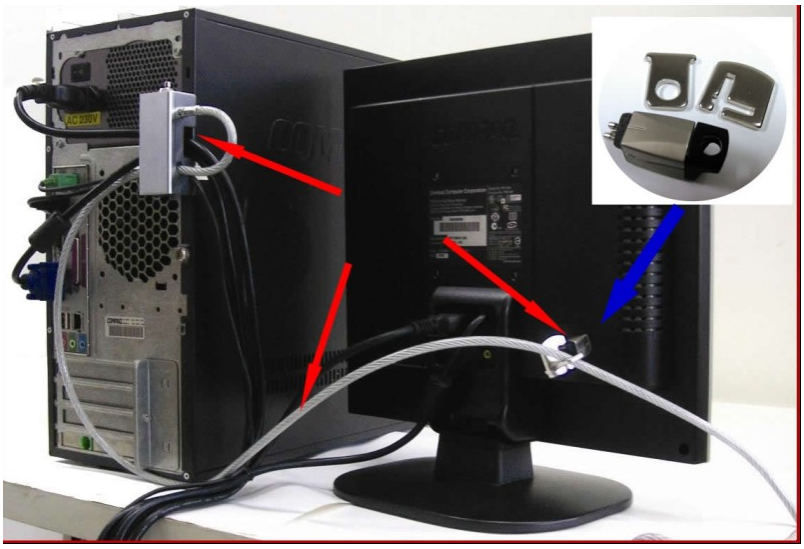
9.1.1 Fyzické zabezpeční počítače

Tato kapitola se zabývá možnostmi fyzického zabezpečení počítačů před neoprávněným přístupem či jinou nežádoucí činností. Před samotnou realizací zabezpečení jednotlivých pracovních stanic a serverů by však měla proběhnout analýza rizik pro daný systém. Podcenění zabezpečení jednoho prvku systému může mít fatální následky, protože takto zranitelný počítač může být tzv. vstupenkou do firemní sítě.

Dalším krokem by mělo být zamezení přístupu nepovolaných osob k důležitým

prvkům systému, ať již se jedná o serverovny, pracoviště správců, apod. Zde je také důležité připomenout, že servery by opravdu měly být umístěny v místnostech jim určeným, a to jak z důvodu ochrany před neoprávněným vstupem, tak i z důvodu ochrany před mimořádnými situacemi (požár budovy, výpadek elektřiny, atd.). S tímto také souvisí ochrana tohoto majetku – záložní zdroj energie, požární čidlo, hasící přístroje, apod. Alternativou může být umístění serverů do jiné budovy nebo pronajímání serverů či virtuálních serverů u specializovaných hostingových společností.

U jednotlivých pracovních stanic by mělo dojít k zabezpečení především tak, aby s nimi nebylo možné jakkoliv manipulovat (krádež jak celé stanice nebo jednotlivých komponent). Toho lze dosáhnout jednoduchým způsobem – např. uzamčení počítačové skříně a periferií pomocí speciálního kabelu se zámkem, viz obr. 22.



Obrázek 22: Fyzické zabezpečení počítače [17]

Pokud se nepodcení zabezpečení jednotlivých počítačů výše zmíněným způsobem, lze poté efektivně využít již konkrétní zabezpečení systému, například:

- šifrování dat (TrueCrypt, BitLocker, FileVault),
- ochrana silným heslem,
- zálohování dat.

9.1.2 Školení uživatelů

Jak již bylo zmíněno, uživatel může ohrozit svým chováním bezpečnost jak svého počítače, tak i související počítačové sítě. V praxi je naprosto běžné, že uživatelé mají tendenci experimentovat, zkoušet nové věci a obcházet to, co je pro ně zakázané. Jen část uživatelů má širší povědomí o nějakých pravidlech či normách týkajících se počítačové bezpečnosti. Proto by mělo být cílem monitorovat a vyžadovat určité základní znalosti po jednotlivých uživatelích ať již menší či větší počítačové sítě.

Vedení společnosti tak může využít zkušeností svých administrátorů a pověřit je školením svých zaměstnanců nebo využít služeb různých školicích středisek. Školicí střediska většinou disponují odborníky s několikaletou praxí a všeobecným přehledem v oblasti počítačové bezpečnosti, což může být jeden z důvodů pro výběr právě této varianty. Díky pravidelnému školení lze zabránit krizovým situacím, které mohou způsobit zaměstnanci s nízkým povědomím o informační bezpečnosti.

9.1.3 Co není povoleno, to je zakázáno

Administrátor by měl povolit pouze ty služby a porty, které jsou bezpečné a které uživatelé používají. Tento postup má pak za následek eliminaci případných útoků pomocí otevřených portů, apod. Uživatel v případě potřeby může administrátora kontaktovat s prosbou o povolení určité služby.

9.1.4 Ochrana proti odposlouchávání

Pokud administrátor zvládne zabezpečit počítače tak, aby uživatelé nemohli instalovat či spouštět žádný nový software, je část jeho úkolu splněna. Problém však může nastat v případě, pokud se útočníkovi podaří připojit se svým počítačem přímo do sítě. Lze uvažovat nad situací, kdy útočník jako vstupní bod použije slabě zabezpečenou firemní bezdrátovou síť nebo se mu podaří připojit svůj notebook do prázdné síťové zásuvky. Pokud není správce na tuto situaci připraven, nebrání útočníkovi nic v tom, aby nerušeně odposlouchával komunikaci na této síti.

Není v silách administrátora, aby fyzicky monitoroval pohyb cizích osob po budově. Jako dostatečné řešení se tedy nabízí nastavit porty na switchi tak, aby na každém

portu mohla být pouze jedna určitá adresa MAC. V případě bezdrátové sítě lze provést podobné řešení, a to povolit připojení pouze konkrétním zařízením (podle jejich adres MAC). Existují také speciální programy, které kontrolují nově připojivší počítače v síti a v případě výskytu takového počítače dovedou na něj správce upozornit, lépe je však cizím počítačům v přístupu do sítě zabránit. [11]

9.2 Uživatelská část

V této kapitole se práce zaměřuje na zásady zabezpečení pro uživatele. Všeobecně platí, že i sebelépe zabezpečený počítač administrátorem může být velmi ohrožen, pokud samotný uživatel není obezřetný a neřídí se základními pokyny. Vše souvisí se vším, proto by uživatelé měli dbát určitých pravidel.

9.2.1 Hesla

Při tvorbě silného a bezpečného hesla by uživatel měl postupovat podle následujících základních pravidel:

- Heslo by mělo obsahovat nejméně 8 znaků a více. Délka hesla potencionálně zvyšuje jeho sílu, záleží však především na kombinaci různých znaků, nikoliv pouze na jeho délce.
- V hesle se nedoporučuje používat české znaky (např. problém v cizině – jiné znaky na klávesnici).
- Uživatel by neměl mít jedno centrální heslo (měl by používat ke každé službě jiné heslo). V případě prolomení hesla by tak uživatel mohl být ohrožen na více místech najednou (e-mail, internetové bankovnictví, atd.).
- Heslo by mělo obsahovat kombinace znaků čísel (0-9), písmen (a-Z, A-Z) a symbolů (@, #, $, &, *, (,), _, +). Heslo (ve většině případů) může obsahovat i mezeru. [20]
- Uživatel by neměl volit takové heslo, které obsahuje slovo či jméno. Takové heslo by bylo zranitelné při slovníkovém útoku (viz kapitola 6.3.1).

- Heslo se rozhodně nedoporučuje mít někde poznamenáno, např. na papírku na monitoru, pod klávesnicí či kdekoliv jinde. Takové heslo je velmi zranitelné. Heslo volíme tak, aby bylo silné, ale i snadno zapamatovatelné. Například věta může znít: „Můj syn Aleš se narodil 17.8.1988.“ Heslo by poté mohlo vypadat následovně: mS4L3$_17/8/1988.

9.2.2 Antivirus a firewall

Při výběru antivirového programu by měl uživatel dbát na rady expertů a volit takový antivirus, který disponuje pravidelně aktualizovanou databází virů a má pozitivní hodnocení v jednotlivých testech. Pokud virová databáze nebude aktuální, může být počítač ohrožen. Také se doporučuje provádět pravidelnou kontrolu všech disků v počítači pomocí tzv. „plánovače“.

Společně s antivirovým programem by tzv. „štít“ měl tvořit také firewall, který může být součástí antivirového programu nebo jako samostatný program. Cílem firewallu je povolit pouze takové spojení (v rámci určitého programu nebo služby), které je bezpečné. Na obr. 23 jsou uvedeny nejpopulárnější antivirové programy spolu s jejich hodnocením, které provedl časopis Virus Bulletin.

9.2.3 Aktualizovaný systém

Bez ohledu na to, jaký operační systém konkrétní uživatel používá, měl by ho udržovat stále aktualizovaný. Někteří uživatelé mohou namítnout, že je to v mnoha případech až obtěžující (ukončení práce a restartování počítače za účelem aktualizace systému). Zde je však potřeba brát v potaz fakt, že bezpečnostní díry se objevují neustále a ve většině případů je záplata vydána pozdě, tedy až proběhne nějaký útok. Těch pár minut čekání se zdá být jako malichernost ve srovnání s případnou škodou způsobenou tímto útokem.

Antivirový program	Počet testů	Neúspěšný	Úspěšný	Procento úspěšnosti
ESET (NOD32)	80	2	78	97,5 %
Symantec Norton	65	8	57	87,7 %
Avira	49	5	44	89,8 %
Sophos	84	18	66	78,6 %
TrustPort	26	6	20	76,9 %
Microsoft Security Essentials	8	1	7	83,3 %
Kaspersky	93	23	70	75,2 %
BitDefender	42	10	32	76,1 %
F-Secure Anti-Virus	58	15	43	74,1 %
CA eTrust	118	39	79	66,9 %
Norman	77	23	52	69,3 %
McAfee	75	24	51	68,0 %
Avast!	70	24	46	65,7 %
AVG	65	23	42	64,6 %

Obrázek 23: Hodnocení AV programů [37]

Závěr

Cílem bakalářské práce bylo popsat možné útoky na počítačové systémy po síti či při fyzickém přístupu k počítači a popsat možné metody ochrany před nimi. Několik těchto útoků jsem si vybral a prakticky je vyzkoušel. Dále jsem vypracoval zásady zabezpečení počítačového systému, které jsou rozděleny na část zaměřenou pro správce operačního systému a na část pro konkrétního uživatele.

Tuto práci lze pomyslně rozdělit na dvě části – část zabývající se počítačovými útoky teoreticky, a část praktickou, kde jsem se snažil vybrané útoky předvést a vyzkoušet. Vypracování teoretické části bylo v některých případech náročné, neboť u některých útoků se využívá chyb jednotlivého hardwaru a tuto problematiku je potřeba alespoň zčásti nastudovat. Dále nesmím opomenout fakt, že s některými útoky jsem se ještě nesetkal, respektive o nich nic konkrétního nečetl. Tento problém při vypracovávání bakalářské práce se mi povedlo minimalizovat i díky několika článkům na serveru Lupa.cz.

Útoky jsem prováděl z počítače, který disponoval distribucí Linux Mint 15 Olivia a Linux Mint 16 Petra. Cílem byl počítač s operačním systémem Windows 8.1. Domnívám se, že výběr počítače s OS Linux je běžnou praxí mnoha útočníků, neboť tento systém poskytuje velkou škálu užitečných nástrojů.

Pokud bych měl možnost někdy v budoucnu v této práci pokračovat, zaměřil bych se pravděpodobně více na praktickou část, tedy na popsání jednotlivých útoků a případné obrany proti nim. Ze zkušenosti vím, že uživatelé v mnoha případech nepoužívají žádnou ochranu a zabezpečení svého počítače, protože jim to nepřijde podstatné. Z tohoto důvodu si myslím, že je potřeba více medializovat možné hrozby, které uživatelům na internetu hrozí.

Vypracování této práce mi přineslo především mnoho nových poznatků a informací týkajících se počítačové bezpečnosti. Je velmi zajímavé sledovat vývoj této problematiky a očekávám, že v krátké budoucnosti se bude klást na počítačovou bezpečnost daleko větší důraz. Tato práce ve mně vyvolala zvětšený zájem o počítačovou bezpečnost.

Seznam zkratek

AP	Access Point
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
BOOTP	Bootstrap Protocol
CAM	Content Addressable Memory
CD	Compact Disc
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DRAM	Dynamic Random Access Memory
DVD	Digital Versatile Disc
GPU	Graphics Processing Unit
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
ISO	International Organization for Standartization
MAC	Media Access Control
MITM	Man in The Middle
NAT	Network Address Translation
OS	Operating System
P2P	Peer To Peer
PAM	Pluggable Authentication Modules
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
Wi-Fi	Wireless Fidelity

Seznam obrázků

Seznam tabulek

Reference

[1] BARÁŠEK, Jan. Hashovací funkce a metody jednosměrného šifrování. In: *Český PHP manuál* [online]. 2013 [cit. 2013-08-13]. Dostupné z: `http://www.php.baraja.cz/index.php?kategorie=navody&page=hashovani`

[2] BITTO, Ondřej. Trojské koně: co jsou zač a jak se bránit. *Živě.cz: O počítačích, IT a internetu* [online]. 2005 [cit. 2013-04-30]. Dostupné z: `http://www.zive.cz/Clanky/Trojske-kone-co-jsou-zac-a-jak-\se-branit/sc-3-a-123708/default.aspx`

[3] BOUŠKA, Petr. TCP/IP - nalezení MAC adresy k IP - ARP. *Samuraj-cz.com* [online]. 2007 [cit. 2013-08-13]. Dostupné z: `http://www.samuraj-cz.com/clanek/tcpip-nalezeni-mac-adresy-k-ip-arp/`

[4] BULÁNEK, Viktor. DHCP. *UNIX-seminář ze správy systému* [online]. 2002 [cit. 2013-08-13]. Dostupné z: `http://www.fi.muni.cz/~kas/p090/referaty/2002-podzim/skupina14/DHCP.html`

[5] ČÍŽEK, Jakub. Včerejší útoky pokračují. Seznam.cz čelí DoS. *Živě.cz* [online]. 2013, 5. 3. 2013 [cit. 2013-04-23]. Dostupné z: `http://www.zive.cz/bleskovky/vcerejsi-utoky-pokracuji-seznamcz-celi-dos/sc-4-a-167853`

[6] DOČEKAL, Daniel. Padesát tisíc lidí věří zjevnému podvodu. Rozdávání produktů Apple se nekoná. *Lupa.cz: Server o českém Internetu* [online]. 2013, 7. 3. 2013 [cit. 2013-04-24]. Dostupné z: `http://www.lupa.cz/clanky/padesat-tisic-lidi-veri-zjevnemu-podvodu-rozdavani-produktu-apple-se-nekona/`

[7] HALLER, Martin. Denial of Service (DoS) útoky: úvod. *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-05-01]. Dostupné z: `http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/`

[8] HALLER, Martin. Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků (1.). *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-05-01]. Dostupné z: `http://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-1/`

[9] HALLER, Martin. Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků (2.). *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-05-01]. Dostupné z: `http://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-2/`

[10] HALLER, Martin. Denial of Service útoky: reflektivní a zesilující typy. *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-05-04]. Dostupné z: `http://www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/`

[11] HALLER, Martin. Bráníme se odposlechu: ARP Cache Poisoning a připojení počítače k síti. *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-08-12]. Dostupné z: `http://www.lupa.cz/clanky/arp-cache-poisoning-a-pripojeni-pocitace-k-siti/`

[12] HALLER, Martin. Odposloucháváme data na přepínaném Ethernetu (4.). *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-08-13]. Dostupné z: `http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-4/`

[13] HALLER, Martin. Denial of Service útoky: man in the middle, distribuované DoS. *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-08-14]. Dostupné z: `http://www.lupa.cz/clanky/denial-of-service-utoky-vyuziti-mitm-utoku/`

[14] HORÁK, Vladimír. Úvod - Co je SPAM a jak se mu bránit. *Ústav výpočetní techniky UK* [online]. 2006 [cit. 2013-04-25]. Dostupné z: `http://uvt1.cuni.cz/email/spam/uvod.html`

[15] HRACH, Jan. Cold boot útok – popis, obrana. *AbcLinuxu* [online]. 2010 [cit. 2013-08-09]. Dostupné z: http://www.abclinuxu.cz/clanky/cold-boot-utok-popis-obrana

[16] KRČMÁŘ, Petr. Útok Slowloris aneb plíživé nebezpečí pro web servery. In: *Root.cz* [online]. 2011 [cit. 2013-16-08]. Dostupné z: http://www.root.cz/\clanky/utok-slowloris-aneb-plizive-nebezpeci-pro-web-servery/

[17] MALANÍK, David. Význam fyzického zabezpečení IT systémů. FAKULTA APLIKOVANÉ INFORMATIKY, Univerzita Tomáše Bati ve Zlíně. *Security Revue: International magazine for security engineering* [online]. 2010 [cit. 2013-08-11]. Dostupné z: http://www.securityrevue.com/article/2010/09/vyznam-fyzickeho-zabezpeceni-it-systemu/

[18] MOHILA, Jaroslav. Phishing dráždí klienty bank. *Owebu.cz: o internetu, počítačích a webhostingu* [online]. 2011, 18.5.2011 [cit. 2013-04-24]. Dostupné z: http://owebu.bloger.cz/Internet/Phishing-drazdi-klienty-bank

[19] NYKODÝMOVÁ, Helena. Botnety: nová internetová hrozba. *Lupa.cz: Server o českém internetu* [online]. 2006 [cit. 2013-05-06]. Dostupné z: http://www.lupa.cz/clanky/botnety-internetova-hrozba/

[20] ORAWSKI, Šimon. *Snížení hrozby neoprávněného přístupu do počítače s OS Windows ve firmě Reci, s.r.o.* [online]. Praha, 2012 [cit. 2013-08-09]. Dostupné z: http://info.sks.cz/www/zavprace/soubory/82050.pdf. Bakalářská práce. Vysoká škola ekonomická v Praze

[21] PEŠA, Radim. Počítačové viry. *Zpravodaj ÚVT MU* [online]. 1999, IX, č. 5 [cit. 2013-04-29]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/articles/160.html

[22] POLESNÝ, David. České zpravodajské weby čelily masivnímu útoku. *Živě.cz* [online]. 2013, 4. 3. 2013 [cit. 2013-04-23]. Dostupné z: http://www.zive.cz/clanky/ceske-zpravodajske-weby-celily-masivnimu-utoku/sc-3-a-167837/default.aspx

[23] RYCHNOVSKÝ, Lukáš. *Počítačová bezpečnost* [online]. Zpravodaj ÚVT MU, 2005, XVI, č. 1, 14. 11. 2011 [cit. 2013-05-01]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/articles/342.html

[24] SCAMBRAY, Joel. *Hacking bez tajemství: Windows, NetWare, UNIX/Linux.* 2. vyd. Praha: Computer Press, 2002, 625 s. ISBN 80-722-6644-6

[25] SHEDDEN, David. New Media Timeline (1980) [online]. 2004 [cit. 2013-04-22]. Dostupné z: http://www.poynter.org/uncategorized/28725/new-media-timeline-1980/

[26] ŠIMEK, Richard. Sociotechnika (sociální inženýrství). *Faklulta informatiky, Masarykova univerzita Brno* [online]. 2003 [cit. 2013-04-23]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm

[27] VRANÝ, Boleslav. Bezpečnost v digitálním věku [online]. 2005. [cit. 2013-04-24]. Dostupné z: http://www.bolekvrany.cz/downloads/security_cz.pdf

[28] ZAORÁLEK, Lukáš. Úvod do technologie CUDA. In: *Root.cz* [online]. 2009 [cit. 2013-08-13]. Dostupné z: http://www.root.cz/clanky/uvod-do-technologie-cuda/

[29] Bezpečné heslo. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2013-08-16]. Dostupné z: http://cs.wikipedia.org/wiki/Bezpečné_heslo

[30] Cain a Abel. In: *Airdump.cz* [online]. 2008 [cit. 2013-08-13]. Dostupné z: http://wiki.airdump.cz/Cain_a_Abel

[31] Captain Zap. Hack Story [online]. 2011, 21. 3. 2011 [cit. 2013-04-22]. Dostupné z: http://www.hackstory.net/Captain_Zap

[32] Hackeři napadli web UniCredit Bank. Administrátor měl prý heslo Banka123. *IHNED.cz* [online]. 2013 [cit. 2013-04-24]. Dostupné z: http://byznys.ihned.cz/c1-59481780-hackeri-napadli-web-unicredit-bank-administrator-mel-pry-heslo-banka123

[33] Linux check passwords against a dictionary attack. *NixCraft* [online]. 2006 [cit. 2013-08-12]. Dostupné z: http://www.cyberciti.biz/tips/linux-check-passwords-against-a-dictionary-attack.html

[34] Malware. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-08-07]. Dostupné z: http://cs.wikipedia.org/wiki/Malware

[35] NetBus: BO's Older Cousin. *Pc-help.org* [online]. 1998, 25. 11. 1988 [cit. 2013-04-23]. Dostupné z: http://www.pc-help.org/www.nwinternet.com/pchelp/nb/netbus.htm

[36] Počítačová bezpečnost. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2013-08-07]. Dostupné z: http://cs.wikipedia.org/wiki/Počítačová_bezpečnost

[37] Srovnání antivirových programů, srovnání antivirů. In: *Antivirové centrum* [online]. 2013 [cit. 2013-08-16]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx