Detekce a prevence počítačového útoku

Detection and prevention of computer's attack

Josef Grygar

Diplomová práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2006/2007

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Josef GRYGAR**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Detekce a prevence počítačových útoků**

Zásady pro vypracování:

1. Analyzujte informační zdroje řešící problematiku počítačových útoků.
2. Analyzujte a stanovte postupy vhodné pro obranné technologie – využijte znalosti útočných metod.
3. Realizujte testy bezpečnosti formou projektu
4. Vyhodnoťte úspěšnost projektu a stanovte závěry pro prevenci počítačových útoků.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1)Carl Endorf, Eugene Schultz, Jim Mellander : Hacking – detekce a prevence počítačového útoku, Grada 2007, ISBN 80-247-1035-8
2) Stuart McClure, Joel Scambray, George Kurtz : Hacking bez záhad, Grada 2006, ISBN 9788024715025
3) Jaroslav Horák :Bezpečnost malých počítačových sítí. Grada 2006, ISBN 8024706636
4) Harold Davis : Bezdrátové sítě Wi-Fi, Grada 2005, ISBN 80-247-1421-3
5) Radek Horský : Bezdrátové sítě Wi-Fi v rekordním čase, GRADA 2006, ISBN 9788024717905

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání diplomové práce: **13. února 2007**

Termín odevzdání diplomové práce: **28. května 2007**

Ve Zlíně dne 13. února 2007

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

V práci je obsažena problematika počítačové bezpečnosti. V úvodní části jsou zmíněny způsoby vyhledávání informací. Jsou popsána hlavní bezpečnostní rizika a způsoby obrany proti nim. Důraz je kladen na silná hesla a ochranu citlivých údajů. Je vysvětlena funkce systémů IDS/IPS a jejich implementace. V práci jsou analyzována bezpečnostní rizika pro uživatele internetu a velké firmy a navrženy způsoby zabezpečení adekvátně k hrozbám. Přitom je kladen důraz na výkon a jednoduchost.

Klíčová slova: Bezpečnost, firewall, síť, antivir, informace, Google, hesla, pharming, phishing, kódování, počítačový útok, DOS, IPS, IDS, analýza

ABSTRACT

The thesis includes the questions of computer security. In the opening there are ways of searching the information mentioned. Described are the main security risks and the ways of protection against it. Emphasis is put on strong passwords and protection of sensitive data. Explained is the function of IDS/IPS systems and their implementation. In the thesis there is analysis of the security risks for internet users and big firms and there are projected ways of securing adequately to the threats. Nevertheless the stress is put on effort and simplicity.

Keywords: Security, firewall, network, antivirus, information, Google, password, pharming, phishing, cryptography, computer attack, DOS, IPS, IDS, analysis

motto: Počítač existuje proto, aby usnadňoval práci, která by bez něj neexistovala.

(z Murphyho zákonů)

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **11**
1 ZÁKLADNÍ POJMY **12**
1.1 HACKER, CRACKER 12
1.2 PROTOKOLY 13
1.2.1 TCP 13
1.2.2 IP 14
1.2.3 UDP 15
1.2.4 ARP 15
1.2.5 DNS 16
1.2.6 HTTP 16
1.3 MALWARE 16
1.4 VIRY 17
1.5 ANTIVIROVÝ PROGRAM 17
1.6 FIREWALL 17
1.7 SPYWARE 18
1.7.1 Projevy spywaru 18
1.8 IDS A IPS 18
1.8.1 Proč je IDS a IPS důležité? 20
1.8.2 Pro a proti IDS respektive IPS 20
1.8.3 Architektura systémů IDS a IPS 22
2 ANALÝZA INFORMAČNÍCH ZDROJŮ NA INTERNETU **23**
2.1 JAK HLEDAT INFORMACE NA INTERNETU 23
2.2 FULLTEXTOVÉ VYHLEDÁVÁNÍ 24
2.3 SPECIALIZOVANÉ VYHLEDÁVAČE 26
2.4 INFORMAČNÍ CENTRA 27
2.5 SROVNÁNÍ FULLTEXTOVÝCH VYHLEDÁVAČŮ 27
2.6 POŽITÍ RSS ČTEČKY 28
2.7 ZÁVĚR 28
II PRAKTICKÁ ČÁST **30**
3 PREVENCE PŘED ŠKŮDCI **31**
3.1 OCHRANA PŘED MALWAREM 31
3.2 KOMPLEXNÍ ŘEŠENÍ 31
3.2.1 Obecné rady pro práci a údržbu softwarových balíčků: 32
3.3 HARDWAROVÉ FIREWALLY 33
3.3.1 Výhody hardwarového firewallu 33
3.3.2 Nevýhody hardwarového firewallu 33

3.4 SOFTWAROVÉ FIREWALLY 34
3.4.1 Výhody Softwarového Firewallu 34
3.4.2 Nevýhody Softwarového Firewallu. 34
3.5 SROVNÁNÍ ANTIVIROVÝCH PROGRAMŮ 36
3.6 ANTI SPYWARE 36
3.6.1 Prevence před spywarem 37
3.6.2 Detekce a odstraňování spyware 37
3.6.3 Shrnutí 38
3.7 ZÁVĚR 38
4 METODY ÚTOKU A OBRANNÉ TECHNOLOGIE 39
4.1 PHISHING A PHARMING 39
4.1.1 Metody phishingu 39
4.1.2 Obrana proti phishingu 40
4.1.3 Metody pharmingu 41
4.1.4 Ochrana před pharmingem 42
4.2 GOOGLE HACKING 43
4.2.1 Hledání hesel 43
4.2.2 Hledání v adresářích 45
4.2.3 Další zajímavé příklady 45
4.2.4 Hledání sériového klíče 46
4.2.5 Ochrana před Google hackingem 46
4.3 ROZLUŠTĚNÍ HESLA 49
4.3.1 Slovníkový útok 49
4.3.2 Útok hrubou silou 50
4.3.3 Získávání hesel 50
4.3.4 Biometrická ochrana 51
4.3.5 Tokeny 51
4.3.6 Obrana před rozluštěním hesla 52
4.4 ODEPŘENÍ SLUŽBY (DOS) 53
4.4.1 Typy DOS útoků 54
4.4.2 Metody záplavového útoku 55
4.4.3 Útoky využívající chybu HW nebo SW 57
4.4.4 Útoky vyčerpáním zdrojů 58
4.4.5 Distribuovaný útok (DDOS) 59
4.4.6 Reflektivní a zesilující DOS útoky 61
4.4.7 Závěr 63
4.5 ZNEUŽITÍ SÍŤOVÝCH PROTOKOLŮ 65
4.5.1 Zneužití ARP 65
4.5.2 Zneužití IP 66
4.5.3 Zneužití UDP 68
4.5.4 Zneužití TCP 68
4.5.5 Zneužití ICMP 70
5 BEZPEČNOST POČÍTAČE 71
5.1 PENETRAČNÍ TEST POČÍTAČE 71
5.1.1 Testování mého počítače 71

5.1.2 Test internetového prohlížeče 72
5.1.3 Závěr 73
5.2 MASKOVÁNÍ IP ADRESY 73
5.2.1 Způsoby skrytí IP adresy: 73
5.2.2 Internetová anonymita 74
5.3 OCHRANA DAT KRYPTOGRAFIÍ 75
5.3.1 Symetrické šifrování 76
5.3.2 Asymetrické šifrování 76
5.4 ANALÝZA DAT 78
5.4.1 Typy detekce: 79
5.4.2 Datová korelace 79
5.4.3 Incidentní odezvy 80
5.5 PROGRAMY NA ZACHYTÁVÁNÍ SÍŤOVÉHO PROVOZU 81
5.5.1 Tcpdump 81
5.5.2 Práce s uloženými soubory 82
5.5.3 Ethereal network analyzer 83
6 VYHODNOCENÍ PROJEKTU 84
6.1 ANALÝZA BEZPEČNOSTNÍCH RIZIK 84
6.2 NÁVRHY ZABEZPEČENÍ 85
6.2.1 Minimální ochrana, maximální výkon 85
6.2.2 Optimální řešení pro domácí použití 85
6.2.3 IDS/IPS Snort 86
6.2.4 Profesionální zabezpečení 86
6.3 IMPLEMENTACE IDS/IPS 87
6.3.1 Celková bezpečnostní strategie 87
6.3.2 Cena IDS/IPS a její odůvodnění 87
6.3.3 Výběr dodavatele 88
6.3.4 Testování a nasazení 89
6.3.5 Závěr 89
ZÁVĚR 90
SEZNAM POUŽITÉ LITERATURY 92
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 96
SEZNAM OBRÁZKŮ 97
SEZNAM TABULEK 98

ÚVOD

V dnešním světě plném elektroniky a digitálních přístrojů je téměř samozřejmostí pracovat doma, nebo v práci s počítačem, nebo notebookem. Asi neexistuje člověk, který by se s tímto fenoménem poslední doby nesetkal. A internet? Před deseti lety bylo jen málo lidí, kteří byli schopni se k této globální síti připojit. Dnes je na něj napojena většina počítačů. Zřízením internetu se nám zpřístupnil celý svět. Bohužel tento fakt má i své stinné stránky. Zapnout počítač umí každý. Ale uvědomuje si také rizika spojené s obrovskou anonymitou a různorodostí lidí, jenž jsou také připojeni?

Mnoho lidí prakticky nic o počítačích neví a přesto s nimi pracuje. Přitom stačí jen několik poučení a použití zdravého rozumu pro bezpečné používání internetu. Bohužel se málokdo sám zajímá o to, co zdánlivě nepotřebuje. Ale škodlivé programy a útočníci tady budou a pokud není nepoužito alespoň základní zabezpečení, které obsahuje každý operační systém, pak je tento počítač vydán doslova napospas. Ve firmách a školách jsou tady správci systémů a bezpečnostní profesionálové, kteří jejich počítače zabezpečují a udržují v provozuschopném stavu. Doma si musí poradit každý sám.

Vybral jsem si téma detekce a prevence počítačového útoku, protože oblast počítačové bezpečnosti je velmi atraktivní. Mnoho firem vyrábí specializovaný software, jenž se snadno nainstaluje, ale pokud nebude správně nastaven ,způsobuje nadměrnou zátěž a přestává být efektivní, nebo naopak není schopen zabránit případným neoprávněným vniknutím. Ať už zákeřných programů, které se snaží nepozorovaně vklouznout do počítače a otevřít například zadní vrátka svým tvůrcům, nebo útočníkům samotným. Zajímalo mě, jak se tyto programy do počítače mohou dostat, co v počítači způsobují a jak se jim bránit.

V televizi je možné vidět filmy, kde se počítačový expert (hacker) dokáže vloupat do jakéhokoli systému během několika vteřin a rozluštit heslo na několik málo pokusů. To lze provést jedině, pokud má napadnutý systém vážné bezpečnostní trhliny a heslem je příjmení majitele firmy. Ale i to je často vidět v reálném životě. Bezpečnost bývá často podceňována i když se o ní pořád mluví. Ale mluvit o něčem a udělat to jsou dvě věci. Jak by jinak bylo možné, že většinou útočníků byly v Americe děti ze základních a středních škol? Ano útočit pomocí již vyrobeného programu je opravdu snadné, ale zabránit tomuto útoku již tak lehké není. Tento problém naráží i na ochranu soukromí, protože pokud by se monitorovala činnost uživatelů, připojených k internetu, zajistila by se mnohem vyšší

bezpečnost, ale na úkor omezení svobody, což samozřejmě v demokratickém státu nemůže být schváleno.

Rozhodl jsem se tedy pokusit napsat práci, která bude obsahovat největší hrozby internetu a způsoby ochrany proti nim. V řadě případů stačí opatrnost a „neklikat“ na všechny reklamy, e-maily a odkazy, které uvidím. Naštěstí existuje spousta užitečných programů, které nám pomohou počítač vyčistit. Větším organizacím a firmám hrozí daleko větší nebezpečí, protože dnešní útočníci nejsou již ti hackeři, kteří pomáhali vybudovat internet a upozorňovali na bezpečnostní chyby. Těmto lidem se říká crackeři a často útočí na servery za účelem zisku, zviditelnění, nebo zábavy. Obrana proti těmto hrozbám je složitější. Mnoho organizací vyvíjí systémy detekce a prevence před těmito útoky. Jsou to poměrně nové technologie, ale znamenají příslib do budoucna.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

V této kapitole zmíním opravdu je ty nejpodstatnější pojmy a jejich popis se pokusím maximálně zestručnit.

Počítačový útok je činnost, kdy se záškodnický program, nebo útočník snaží poškodit, nebo zneužít SW nebo HW druhé osobě.

1.1 Hacker, Cracker

Hacker je člověk, který se vyžívá v bádání po detailech programových systémů a překračování jejich schopností, což je odlišné od jednání většiny uživatelů, kteří se raději naučí jen nutné minimum. Má potěšení z detailních znalostí vnitřních pochodů systému, počítačů a počítačových sítí. Označení "hacker" současně znamená členství v globální komunitě. Je lepší být označován jako hacker ostatními, nežli se tak označovat sám. Od normálních lidí je na ulici nerozeznáte. Chodí do školy, nebo do práce. Může to být váš soused, který vám pomáhá s nákupy.

Hackeři se považují za elitu, což je založeno na jejich schopnostech. Je zde tedy jakási ego satisfakce, když sebe identifikujete jako hackera. Když tvrdíte že jím jste a přesto to není pravda, tak budete bleskurychle označeni za boguse = podvodník. Těmto lidem se také říká wannabee (ti, kteří by rádi byli hackery, ale nejsou jimi).

Věří, že je správné sdílet informace. Je etická povinnost hackerů, aby sdíleli svou odbornost psaním open-source kódů a usnadnili přístup k informacím a počítačovým zdrojům všude tam, kde je to možné. Hacker není ten, kdo se snaží shodit, zničit, nebo smazat systém. Nesnaží se uspokojit své ego DoS útoky, či odesíláním spamu. Bohužel tato fáma mezi lidmi stále panuje, protože jsou hackeři v novinách a hlavně v televizi chybně označováni.

Cracker nebo také Black hat je člověk s výbornými znalostmi počítačů, softwaru a programování. Na rozdíl od hackera využívá cracker získané informace o slabém zabezpečení nebo bezpečnostních mezerách ke kriminálním účelům nebo pro osobní prospěch. Crackeři jsou médii často nesprávně označováni termínem hacker.

Jako cracker může být také označen někdo, kdo se snaží prolomit ochrany většinou placeného softwaru za účelem získat možnost používat jej bez nutnosti ho koupit. (Např.

zjištění způsobu ověřování sériových čísel pro odblokování zkušební verze nebo odstranění kontroly u her, zda je v CD mechanice originální médium.)

1.2 Protokoly

V tak komplexním systému jako je síť internet musí fungovat určitá pravidla, ale musí být taky zajištěna kompatibilita mezi různými operačními systémy a hardwarem. To nám zaručuje rozdělení přenosu dat do více vrstev. Každá vrstva umí komunikovat pouze se svými nejbližšími sousedy. Pro tuto komunikaci jsou požity různé standardizované síťové protokoly. Jako učebnicový příklad se používá model OSI.

Tab. 1 *Transportní protokoly na jednotlivých vrstvách modelu TCP/IP*

Vrstvy modelu OSI	Vrstvy TCP/IP	Protokoly
Aplikační vrstva	Aplikační vrstva (Zpráva)	DNS DHCP FTP HTTP HTTPS IMAP IRC NTP POP3 RTP SIP SMTP SNMP SSH TELNET
Prezentační vrstva		
Relační vrstva	Transportní vrstva (Paket)	TCP, UDP , DCCP ,IL ,RUDP, SCTP
Transportní vrstva		
Síťová vrstva	Síťová vrstva (datagram)	ARP , IPv4 , IPv6 , RARP, ICMP
Linková vrstva	linková(rámec)	Ethernet, FDDI, PPP, Token ring, Wi-Fi
Fyzická vrstva	HW	10Base2, 10Base-T, EIA-422, EIA-485, RS-232

Jak je patrné z tabulky [1]- každá vrstva modelu může mít několik protokolů. Každý používá svoje hlavičky a má pevně stanovenou formu. Linková a Fyzická vrstva je obyčejně sloučena do jedné, takzvané vrstvě síťového rozhraní, ale v praxi se používá model jak jsem jej uvedl v tabulce 1. Pokud bych měl vybrat s každé vrstvy nejčastěji používaný protokol byly : Ethernet, IP, TCP, HTTP .

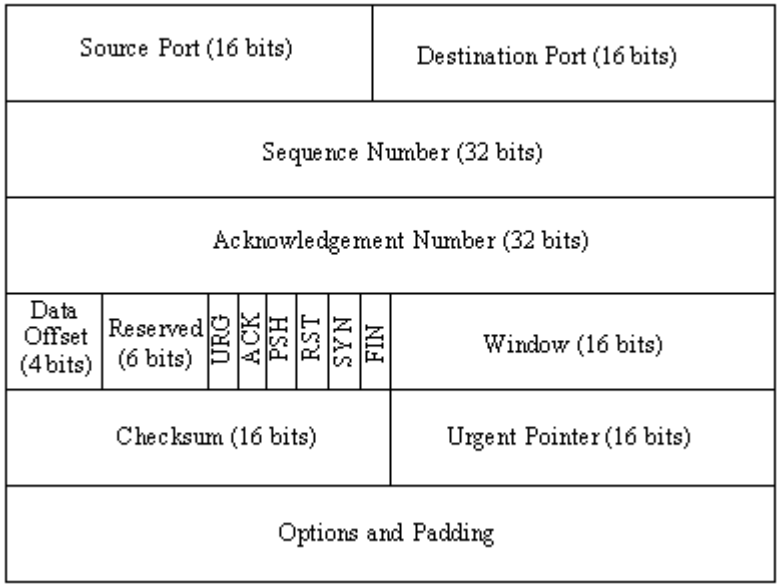
1.2.1 TCP

Protokol TCP je spojovanou službou (connection oriented), tj. službu která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh. Tento okruh je plně duplexní (data se přenášejí současně na sobě nezávisle oběma směry). Přenášené bajty

jsou číslovány. Ztracená nebo poškozená data jsou znovu vyžádána. Integrita přenášených dat je zabezpečena kontrolním součtem.

Konce spojení ("odesilatel" a "adresát") jsou určeny tzv. číslem portu. Toto číslo je dvojbajtové, takže může nabývat hodnot 0 až 65535. U čísel portů se často vyjadřuje okolnost, že se jedná o porty protokolu TCP tím, že se za číslo napíše lomítko a název protokolu (53/tcp)

Cílová aplikace je v Internetu adresována (jednoznačně určena) IP-adresou, číslem portu a použitým protokolem (TCP nebo UDP). Protokol IP dopraví IP-datagram na konkrétní počítač. Na tomto počítači běží jednotlivé aplikace. Podle čísla cílového portu operační systém pozná které aplikaci má TCP-segment doručit.



Obr. 1 *Hlavička TCP*

1.2.2 IP

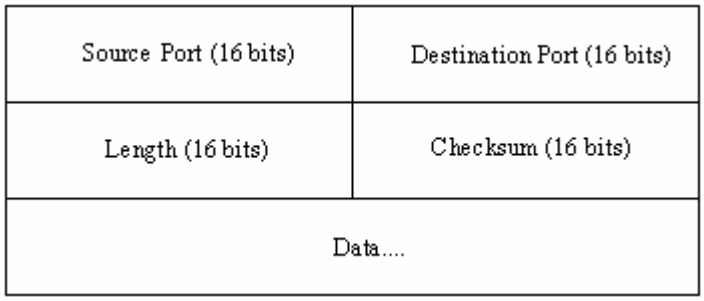
IP protokol v doručování datagramů poskytuje *nespolehlivou* službu, označuje se také jako *best effort* – „nejlepší úsilí". To znamená, že všechny stroje na trase se datagram snaží podle svých možností poslat blíže k cíli, ale nezaručují prakticky nic. Datagram vůbec nemusí dorazit, může být naopak doručen několikrát a neručí se ani za pořadí doručených paketů. Pokud aplikace potřebuje spolehlivost, je potřeba ji implementovat v

jiné vrstvě síťové architektury, typicky protokoly bezprostředně nad IP. Nejčastější je sloučeni TCP-IP.

Dnes se nejčastěji používá verze označovaná číslem 4, nazývaná IPv4. IPv6 je navrhovaný a chystaný nástupce. Verze 0 až 3 jsou buď rezervované nebo nepoužité. Verze 5 (IPv5) byla použita pro experimentální proudový protokol (stream protocol). Nejnovější verze IPv6 nahradí stávající vzhledem k faktu, že adresy IPv4 i přes provedená úsporná opatření díky rozvoji internetu stále ubývají a mezi lety 2010 až 2011 by se mohly všechny vyčerpat. Nový protokol bude klást určité nároky směrem na vybavenost osobních počítačů i jiných zařízení. Moderní operační systémy (Windows XP, Windows Vista, Mac OS X, Linux) jsou již na implementaci připravené, upravit je ale nutné i všechny síťové aplikace.

1.2.3 UDP

V sadě protokolů Internetu poskytuje UDP velmi jednoduché rozhraní mezi síťovou vrstvou pod a aplikační vrstvou nad. UDP neposkytuje žádné záruky doručení a odesilatelova UDP vrstva si u jednou už odeslaných zpráv neudržuje žádný stav. UDP pouze přidává kontrolní součty a schopnost roztřiďovat UDP pakety mezi více aplikací běžících na stejném počítači. Protokol UDP má nejjednodušší stavbu hlavičky.



Obr. 2 *Hlavička UDP*

1.2.4 ARP

Address Resolution Protocol (ARP) se v počítačových sítích s IP protokolem používá k získání ethernetové (MAC) adresy sousedního stroje z jeho IP adresy. Používá se v situaci, kdy je třeba odeslat IP datagram na adresu ležící ve stejné podsíti jako odesilatel. Data se tedy mají poslat přímo adresátovi, u něhož však odesilatel zná pouze IP

adresu. Pro odeslání prostřednictvím např. Ethernetu ale potřebuje znát cílovou ethernetovou adresu.

1.2.5 DNS

Domain Name System je hierarchický systém doménových jmen, který je realizován servery. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a dnes slouží jako distribuovaná databáze síťových informací.

1.2.6 HTTP

Hyper Text Transfer Protocol je internetový protokol určený původně pro výměnu hypertextových dokumentů ve formátu HTML. Používá obvykle port TCP/80, verze 1.1 protokolu je definována v RFC 2616. Tento protokol je spolu s elektronickou poštou tím nejvíce používaným a zasloužil se o obrovský rozmach internetu v posledních letech.

V současné době je používán i pro přenos dalších informací. Existuje také jeho bezpečnější verze HTTPS, která umožňuje přenášená data šifrovat a tím chránit před odposlechem či jiným narušením.

1.3 Malware

Malware je počítačový program určený ke vniknutí nebo poškození počítačového systému.Výraz malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“ a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Pod souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware. V právní terminologii je malware někdy nazýván počítačová nečistota (angl. „computer contaminant“), například v zákonech států Kalifornie, Západní Virginie a několika dalších členských států USA. Malware je někdy pejorativně nazýván scumware. Jako malware by neměl být označován software, který sice obsahuje chyby, ale byl napsán pro legitimní účely.

1.4 Viry

Virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Má podobné vlastnosti jako biologický virus. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Viry jsou jen jedním z druhů tzv. malware, zákeřného software.

Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných, popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů). Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji.

1.5 Antivirový program

Antivirový program je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného záškodného software (malware). K zajištění této úlohy používají dvě techniky:

1. Prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi.
2. Detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů, které si programy pravidelně, nejčastěji z Internetu, stahují. Lepší programy mají také propracované heuristické algoritmy, které se snaží odhalit i neznámé viry.

1.6 Firewall

Firewall je komponenta nebo skupina jednotlivých komponent vložena mezi dvě sítě. Tyto komponenty se skládají z počítačových systémů, routerů nebo skupiny routerů, fungující jako buffer mezi jakýmikoliv veřejnými sítěmi a privátní sítí. Moderní firewall má takové vlastnosti, aby zabránil neautorizovanému přístupu. Rozdělujeme dva základní druhy firewallů. Hardwarový „železná krabička navíc“ a Softwarový „nainstalovaný

program“. Firewall je nezbytnou součástí ochrany počítače. Pokud kupujeme router, rozhodně se zabudovaným firewalem. Je obtížnější ho nastavit, ale chrání celou lokální síť za ním. Na každém počítači by měl být softwarový firewall, který kontroluje přímo aplikace, které se snaží napojit na internet. Dnes bývá Softvarový firewall nedílnou součástí instalace operačního systému. Mezi současné nejlepší firewally patří Outpost, Zone Alarm Pro, Jelico a mezi uživateli je i oblíbený Kerio Profesional (včetně nastavených paketových filtrů).

1.7 Spyware

Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele. Narozdíl od backdooru jsou odcizována pouze data typu přehled navštívených stránek či nainstalovaných programů. Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a legálností spyware. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí.

1.7.1 Projevy spywaru

Přítomnost spyware může vést ke:

Stahování a instalaci dalšího škodlivého softwaru bez vědomí uživatele (backdoory, trojani, viry, "vykrádače hesel"...).

Změně chování Internet Exploreru - běží pomaleji, odkazuje na jiné stránky, než které požadujeme, mění startovací stránku po zapnutí IE, mění položky v oblíbených, obtěžuje s reklamou atd.,

Vyvolání modemového spojení přes draze zpoplatňované telefonní linky (tzv. žluté linky). Tuto činnost provádí speciální program, kterému se obecně říká dialer.

1.8 IDS a IPS

IDS a IPS jsou zkratky pro systémy detekce, respektive prevence proti narušení. Zaznamenávají jak úspěšné, tak neúspěšné pokusy o útoky. Například pokud jsou senzory

před a za firewallem a výsledky se porovnají. Jejich funkce se dá přiblížit následujícím příkladem. V obchodním domě jsou cenné věci. Je zabezpečen zamčenými dveřmi (firewall), bezpečnostními kamerami a alarmem (IDS) a hlídacím psem (IPS). Dveře brání vniknutí útočníkovy ve vstupu, alarm a kamery nás varují, ale v útoku nijak nebrání. A pes je schopen útočníka v některých případech zahnat. Přitom lze říct, že všechny ochrany se vzájemně podporují. Tvrzení že IDS a IPS systémy nahradí firewall jsou nepravdivé. Navíc by měly být zabezpečeny všechny vrstvy, neboť systém je tak bezpečný, jak bezpečný je jeho nejslabší článek.

IDS pracuje v síťové vrstvě OSI modelu.

Rozdělení systémů IDS

HIDS (Host-Based IDS), neboli uzlově orientované IDS. Vyžaduje SW, jenž dokáže skenovat aktivitu všech aktivních uzlů. Zapisuje si aktivitu do bezpečnostní databáze a porovnává tyto události se záznamy ve své znalostní databázi.

NIDS (network-based IDS),česky síťově orientované IDS. Je řazen do sítě sériově a kontroluje procházející pakety.V provozním proudu pak analyzuje přítomnost vzorů závadného chování.

IPS

Tento systém je stále ve vývoji, protože je relativně mladý. Obecně je IPS umístěn v síti a monitoruje ji. Pokud se odehraje nějaká událost, pak přijme opatření dle předepsaných pravidel. IPS se vyvinulo z IDS, ale je to odlišný zabezpečující produkt lišící se ve funkcionalitě a síle.

IDS versus IPS

Tab. 2 *Rozdíly IDS a IPS*

IDS	IPS
instaluje se na uzel(HIDS)a síť (NIDS)	instaluje se na uzel(HIPS)a síť (NIPS)
v síti jsou pasivním prvkem	jsou řazeny sériově(nejsou pasivní)
nemohou analyzovat šifrovaný provoz	vhodnější pro ochranné aplikace
centrální správa řízení	centrální správa řízení
vhodnější pro blokaci hackerských útoků	ideální pro blokaci webových znetvořenin
výstrahu vydávající produkt (reaktivní)	Blokující produkt (proaktivní)

1.8.1 Proč je IDS a IPS důležité?

-Větší účinnost v detekci, než může být dosaženo ručně

-Hluboká báze znalostí z toho vyplývající

-Schopnost vyrovnat se s velkými objemy dat

-Schopnost výstrahy téměř v reálném čase, což pomáhá snižovat potenciální poškození

-Automatizovaná odezva- například odhlášení uživatele, zablokování účtu, nebo nabídka automatizovaných skriptů.

-Silně odstrašující hodnota

-Zabudovaná podpora pro soudní řízení

-Zabudovaná podporo ohlašovacích funkcí

Tři hlavní důvody:

-Právní a řídící vyhlášky. Existuje mnoho vyhlášek a nařízení jenž se týkají bezpečnosti. V kterých sice není podmínkou implementace IDS nebo IPS systémů, ale pomáhají je splnit. Platnost nařízení se vztahuje k velikosti, umístění a povaze firmy.

-Kvalifikace útoků. IDS a IPS poskytuje administrátorovy nástroj pro řízení a příležitost kvantifikovat útoky proti síti organizace.Umožňují vytvářet profily typů těchto útoků.

-Konstituce celkové hloubkové obranné strategie. Obě tyto technologie pomáhají zabezpečovat ochranu sítě a aplikační vrstvy, dále pomáhají korelovat a ohodnocovat platnost informací z ostatních zařízení jako jsou antovirové programy, firewally a routery.

Detekce založená na pravidlech, signaturách a vzorech. (detekce zneužití)

Detekce založená na profilu.(detekce anomálií)

Anomálie je něco. co se liší od normálního stavu. Vytváří se takzvaný profilový systém, který všechny události dlouhodobě zpracovává a odlišnosti předává výstupní rutině. Jde v podstatě o shromáždění statistického (kvantitativní) a charakteristického (kvalitativní) chování.

1.8.2 Pro a proti IDS respektive IPS

Výhody IDS

+ Může detekovat vnější hackery, ale i vnitřní síťově orientované útoky

+ Poskytuje jednoduchou rozšiřitelnost na celou síť

+ Nabízí centralizovanou zprávu korelace distribuovaných napadení

+ Poskytuje hloubkovou obranu

+ Vkládá do rukou systémového administrátora schopnost kvantifikace napadení.

+ Poskytuje dodatečnou vrstvu ochrany

Nevýhody IDS

- Generuje falešné pozitivní a negativní výsledky

- Na útok spíše reaguje, než mu předchází

- Generuje nesmírné množství dat, která musí být analyzována

- Vyžaduje složité zpracování odpovědí na jednotlivé události

- Vyžaduje monitorování na plný úvazek zkušeným personálem

- Náchylnost k „málo četným a pomalým“ napadením

- Nemůže zpracovávat data ze šifrovaného síťového provozu

- Je nákladnou záležitostí

Výhody IPS

+ Chrání aplikační vrstvu

+ Útoku spíše zabraňuje, než aby na něj pouze reagovala

+ Lze použít behaviorální přístup. (na základě analýzy chování)

+ Poskytuje hloubkovou ochranu

+ Umožňuje korelovat události v reálném čase

Nevýhody IPS

- Generuje falešné pozitivní poplachy, které při automatické odezvě mohou způsobit vážné problémy.

- Vytváří v síti úzká místa

- Je to nová a nákladná technologie

1.8.3 Architektura systémů IDS a IPS

-Jednovrstvá (jediná komponenta plní všechny funkce)

-Vícevrstvá používá hierarchické uspořádání (senzory, agenti a manažer)

-Peer-to-Peer (rovnocenné komponenty spolupracují- např. firewally)

Senzory jsou rozmístěny po síti(přímo na trase, nebo v uzlu) a sbírají informace

Agenti vyhodnocují informace ze senzorů, případně od dalších agentů a analyzují je. Potřebují k funkci komunikační rozhraní, odposlouchávače (přijímá data od senzorů a agentů), zasílatele (využívá komunikační rozhraní pro rozesílání dat z odposlouchávače)

Manažer nebo též server- poskytuje řídící a výkonnou funkci. Dohlíží na koordinaci, spravuje data pro statistiky, podává výstrahy, datovou korelaci, tvorbu a distribuci strategie a poskytuje prostředí řídící konzole pro analytika, jenž spravuje IDS a IPS.

Každá komponenta musí být podrobena mnoha rozhodnutím ohledně svého umístění a bezpečnosti. Obecně platí: čím vyšší úroveň daná komponenta zaujímá, tím vyšší bezpečnost vyžaduje. Senzory mohou být rozmisťovány kamkoli. Agenti vyžadují vyšší úroveň ochrany a měli by být umístěny na místo, kde budou pracovat nejefektivněji. Manažer vyžaduje nejvyšší bezpečnost. Je dobré opatřit jej taky fyzickou bezpečností jakou je implementovaná autentifikace a šifrování.

2 ANALÝZA INFORMAČNÍCH ZDROJŮ NA INTERNETU

Internet je zdrojem nepřeberného množství informací všeho druhu. Bohužel různé zdroje nám poskytují odlišné fakta na tutéž informaci. Jak tedy konkrétně postupovat při vyhledávání? Kterým zdrojům můžeme věřit? Na tyto otázky vám odpoví následující kapitola.

2.1 Jak hledat informace na internetu

V dnešní době se těžko hledá člověk, který se nesetkal z internetem. Je však stále mnoho lidí, kteří neví, jak by jim mohl být užitečný. Někteří si jej pletou z teletextem, jiní si myslí, že je to něco jako noviny v elektronické podobě, prostředek pro hraní her a posílání elektronické pošty.

Vzpomínám si, jak jsem poprvé usedl v knihovně před počítač připojený k internetu. Vyzkoušel jsem stránky, které jsem měl napsané na papíru a pak přemýšlel „jak mám najít ty obrázky, jak si psát s jinými lidmi, jak se jmenovala ta zajímavá stránka, kterou mi ukazoval kamarád.“ V té době jsem nevěděl nic o vyhledávání a proto jsem si připadal bezradný.

Na internetu je však spousta serverů, které se specializují na vyhledávání, nebo shromaždování důležitých informací. Většinou za účelem zisku. Rozdělujeme 3 základní skupiny

- **katalogové** : obsahují kategorie s různými tématy a uživatel se „proklikává“ logicky uspořádaným obsahem katalogu. Mezi nejznámější katalogové vyhledávací servery u nás patří: *www.seznam.cz, www.centrum.cz, www.atlas.cz.* Dále například: www.google.cz/dirhp , web.volny.cz/najdito, a spousta dalších. Jejich výhoda spočívá v tom, že stránka je v katalogu registrovaná a její obsah byl shlédnut a prověřen. Bohužel se často stává, že nalezneme něco jiného, než potřebujeme.

- **fulltextové** : Je to vlastně obrovská databáze textů webových stránek. Každý den nechá tento server své roboty pátrat po nových stránkách a aktualizovat ty staré. Zjednodušeně řečeno tento robot nedělá nic jiného, než že zuřivě otevírá stránky a na každé stránce se podívá na každý odkaz, který najde, všechny tyto informace ukládá do databáze

a když zadáte nějaké slovo, server nalezne všechny stránky k danému tématu v databázi

a odkazy na tyto stránky vám zobrazí. Mezi nejznámější patří: *www.Google.com, www.Yahoo.com , www.Altavista.com www.Ask.com, /www.answers.com* a další. Z českých jsou to *www.Google.cz, www.seznam.cz, www.centrum.cz, www.Alenka.cz* a *www.jyxo.cz.*

Výhodou je, že na jakýkoli dotaz vám bude zobrazeno obrovské množství odkazů. Bohužel v tomto množství se skrývá i nevýhoda. Informace vyhledané automatem jsou redundantní a pokud hledáme něco odborného, je velice těžké najít důvěryhodný zdroj. I přesto jsou však nejpoužívanější a při správné formulaci dotazu je možné najít rychle požadovanou informaci. Více v další kapitole.

- **meta vyhledávače** : neudržují vlastní databázi webových stránek a spoléhají se na jiné vyhledávače. Po zadání hledaných slov vyhledávač přejme informace od různých vyhledávačů a zpracují pro vás výsledek. Touto cestou je možné oslovit s dotazem více vyhledávacích serverů, ale problém je v tom, že nikdy nevíte které. Metavyhledávači jsou například: *http://www.kartoo.com http://7metasearch.com/ http://turbo10.com/*

2.2 Fulltextové vyhledávání

Pokud hledáme pouze slovo, stačí jej zadat a stisknout Enter. Fráze se vkládá do uvozovek. Pokud chceme některému slovu přiřadit vyšší prioritu, stačí jej napsat v řetězci vícekrát za sebou.

Příklad:

technology "market share" france germany czech

technology "market share" france germany czech czech czech

Pokud chceme vyhledat číslo z intervalu ve fulltextovém dotazu, provedeme prosté oddělení dolního a horního čísla dvěma tečkami (např. 1..100). Pokud chceme hledat jen v titulcích.

Většina vyhledávačů podporuje vyhledávání podle specifických příkazů. Google patří mezi nejpoužívanější fulltextové vyhledávače a proto se dále budu věnovat jeho funkcím v tomto směru. Ty nejzákladnější jsou uvedeny v tabulce 1.

Tab. 3 *Příkazy fulltextových vyhledávačů*

Příkazy	Definice	Příklad
Filetype	Určuje typ hledaného souboru. Typ souborů vyhledávaných Googlem je umístěn zde	filetype:pdf bezpečnost
Intitle, Allintitle	Hledá v titulkách stránek(<title></title>) Allintitle hledá všechny slova	intitle:databaze allintitle: databáze zákon
Inurl, allinurl	vyhledává slovo v URL stráne nebo v názvu domény. Allinurl hledá všechny slova	inurl:pocitac
Site	vyhledával zadaný výraz pouze ve specifikované webové síti nebo doméně	"Instalace windows vista" site:zive.cz
Link	vyhledávač Google, aby našel všechny odkazy směřující na zadanou stránku	link:google.com
Info	Pokusí se najít informace o stránce	info:utb.cz
intext	Vyhledává zadaný text v obsahu stránky.	intext:prevence
cache	zobrazí kopii webové stránky, kterou si vyhledávač Google stáhl již dříve při indexaci sítě	Cache:seznam.cz

Tyto příkazy se dají kombinovat pomocí operátorů a uvozovek. Proto zde ještě uvedu všechny operátory a jejich praktické využití.

Tab. 4 *Fulltextové operátory*

Operátor	Význam a použití
+ (and)	A. vyhledá oba dva výrazy. + vkládá většina vyhledávačů automaticky místo mezery. Používá se pouze, když nechceme aby u zadaného slova vyhledávač doplnil diakritiku př: +pocitace
| (or)	Nebo. Vyhledá jedno nebo druhé slovo. Nikdy nevyhledá obě.
- (not)	Ne. Používá se pokud nechceme aby daný výraz, nebo slovo bylo obsaženo ve výsledku hledání. Př: novinky -site:novinky.cz. (vyhledá všechny novinky mimo server novinky.cz)

Google ale umí daleko víc. Velmi zajímavá pomůcka je jeho kalkulačka. Stačí napsat výraz včetně závorek, vědeckých funkcí a znamének do kolonky pro hledání a stisknout Enter. Výsledek se objeví okamžitě.

Příklad: ln0.5(5-8)/4+sin5-e^2*

Google dokáže převádět téměř libovolné jednotky, hledá významy slov, telefonní čísla a mnoho dalších užitečných věcí. Ty si každý může nastudovat na následujících třech odkazech:

http://www.google.cz/intl/cs/help/features.html

http://www.google.cz/intl/cs/options/index.html

http://labs.google.com/

2.3 Specializované vyhledávače

Pokud hledáme odborné informace, je lepší použít k hledání specializovaný server. Jsou servery, které hledají informace z oblasti medicíny, vědy, výzkumu, kvalifikačních prací a podobně. Na internetu jich existuje velké množství. Z nich jsem vybral několik zástupců, jež uvedu níže.

Google scholar http://scholar.google.com/

Specializovaný vyhledávač odborných textů (např. článků z časopisů, preprintů, vysokoškolských kvalifikačních prací).

Scirus http://www.scirus.com/

Specializovaný vyhledávač informací z oblasti vědy, výzkumu a vzdělávání. Vyhledává paralelně ve volně přístupných webových zdrojích a zdrojích pro registrované uživatele.

Highware http://highwire.stanford.edu/

Databáze článků z odborných časopisů z oblasti biologických věd, lékařství, fyzikálních věd a společenských věd. Články z časopisů, které má instituce předplacené (v rámci elektronických. databází) jsou k dispozici v plném textu.

OAlster http://oaister.umdl.umich.edu/

Virtuální katalog, který zpřístupňuje vědecky orientované zdroje (i digitální), které běžné vyhledávače (Googole, Altavista) nezaznamenávají.

PubMed www.pubmed.gov/

PubMed, služba National Library of Medicine, obsahuje více než 15 milionů citací článků z lékařských časopisů do roku 1950, patří k nejlepším nástrojům pro vyhledávání v Medline na Internetu. Je volně dostupný.

2.4 Informační centra

Informační centra jsou místa, které se zaměřují na dlouhodobé uchovávání podložených informací. Jsou založeny na profesionálních a komerčních základech a ručí, že jejich data jsou správná. Pokud chceme jejich služby využívat, je nutné nejprve zavázat smluvní vztahy a služby uhradit. Poté vám bude zpřístupněna databáze. Databázová centra vznikala už v -60. letech 20. století a byla i stále jsou přístupná po profesionálních sítích zcela nezávislých na internetu.

Příkladem databázových center jsou:

http://www.dialog.com http://www.lexis-nexis.com, http://www.dimdi.de, http://www.genios.de, http://www.questel.orbit.com, http://www.stn-international.de, http://www.oclc.org a spousta dalších.

2.5 Srovnání fulltextových vyhledávačů

Každý z nás má svůj oblíbený vyhledávací server. Může mít pro to několik důvodů. Rychlost, přehlednost, pokročilé funkce, spolehlivost a spoustu dalších. Pro fulltextové vyhledávání je pro svou velikost databází a propracované vyhledávací algoritmy řazen na první místo vyhledávač Google.com. Odborníci však tvrdí, že pro hledání souborů uložených na lokálních počítačích je lepší použít server Yahoo.com. Důležité je, aby uživatel uměl s vyhledávačem zacházet. Řada jich má pokročilé vyhledávání, kde si uživatel bez znalosti příkazů může zadat i složitý dotaz.

Pro srovnání vyhledávačů při hledání určitého hesla je možné použít odkaz uvedený níže. Jedná se však pouze o orientační informaci, kdy zjistí počet vyhledaných odkazů každým vyhledávačem a vyznačí stránky nalezené oběma.

http://ranking.thumbshots.com

2.6 Požití RSS čtečky

RSS neboli Really Simple Syndication (dříve Rich Site Summary) se řadí mezi technologie, kterým se během relativně krátké doby podařilo změnit využívání webu a Internetu. Rozvoji RSS nesmírně pomohla popularita blogů. Především, všechny blogy jsou nepravidelníky. Za druhé, pro jejich autory by sestavování newsletterů představovalo možná až zbytečnou zátěž. Dále, většina bloggerů má několik kamarádů a chce odkazovat na jejich deníčky. K tomu se původní účel syndikace metadat – vzájemná reklama webů na svých stránkách a odkazování hodí dokonale.

Čtečky mohou být součástí webového prohlížeče, nebo samostatné programy. Existují placené verze i volně šiřitelné verze. Pracují tak, že do čtečky uložíte odkaz na stránku, kterou chcete hlídat cnn.com, novinky.cz a podobně a čtečka bude tyto stránky kontrolovat a na veškeré nové informace upozorní v podobě stručné zprávy. Pokud se uživatel chce dozvědět více, stáhne si zprávu celou. Tím šetří čas hledáním nových informací.

Nejčastěji používané RSS čtečky jsou tyto: rssmad, Abilon ,FeedRead, RapidFeeds

2.7 Závěr

Při hledání informací na internetu máme k dispozici stovky vyhledávacích serverů. Pokud víte, co přesně chcete najít, začněte na specializovaném serveru. Pokud žádný neznáte, použijte fulltextový vyhledávač (www.google.com) pro jeho nalezení. Snažte se využívat pokročilé nastavení vyhledávačů pro dosažení maximálního efektu.

Obecně platí, že většina informací na internetu je psána anglicky. Do češtiny se články a projekty překládají až dodatečně. Spousta odborných textů však nikdy přeložena nebude. Proto doporučuji anglicky zdatnějším hledat v cizím jazyce.

Když nevíte, co přesně chcete najít, je ideální použít katalogový vyhledávač (www.seznam.cz). V něm můžete listovat v jednotlivých kategoriích a načerpat vědomosti, nebo nalézt odkazy, které vám pomohou naleznout potřebnou informaci.

Na internetu se nevyplácí důvěřovat všemu, co se dočtete. Encyklopedie, články, názory na fóru, soubory,.. vše co lze najít na internetu je zatíženo lidskou chybou. Ale tak tomu je ve všech oblastech. Někteří lidé dokonce úmyslně matou ostatní falešnými informacemi. Proto si buď informaci ověřte u více nezávislých zdrojů, nebo využijte

možnost zaplatit si informace u databázových center. Obecně lze doporučit opatrnost a vlastní myšlení.

II. PRAKTICKÁ ČÁST

3 PREVENCE PŘED ŠKŮDCI

Pod tímto pojmem rozumíme základní zabezpečení osobního počítače, připojeného k síti internet, nebo k místní síti. Nebezpečí, které hrozí je často podceňováno. Přitom ani nemusíte mít žádné důležité data, ale viry, červi, nebo trojští koně (malware) navštíví každého, kdo jim nechá otevřené dveře do svého počítače.

3.1 Ochrana před malwarem

V dnešní době řada firem nabízí kompletní ochranu počítače pomocí jejich softwarového balíčku. Jejich výhoda spočívá v tom, že má uživatel méně práce s instalací a jednotlivé programy v balíčku se vhodným způsobem doplňují. Nevýhoda může spočívat v tom, že je těžké vyrobit univerzální software proti malwaru, vyšší výkon i kvalitu. Pro zkušenějšího uživatele je proto vhodnější vybrat si vlastní ochranný software. A to konkrétně: Firewall, antivirový program, antispywarový program. Jednotlivé možnosti si přiblížíme níže.

3.2 Komplexní řešení

Ceny se kompletních bezpečnostních balíčků se pohybují od 1200 do 2000 korun českých. Jejich rozdíly pak jsou hlavně v rychlosti, kvalitě firewallu a schopnosti detekovat všechny viry a spamwery .Zdaleka neplatí, že ten nejdražší bude i nejlepší. Z testu vydaných časopisem PC World jsem vybral dva nejlepší produkty, jelikož jejich cena je dnes 1300 korun českých a dosahují vynikajících výsledků. Na prvním místě se umístil Symantec Norton internet security 2006. Má však složitější ovládání a je pomalejší, než v pořadí druhý McAfee Internet Security Suite 2006. Ten má přehledné a jednoduché uživatelské rozhraní a neobtěžuje uživatele výstražným hlášením na činnost, která je naprosto v pořádku. Proto bych doporučil balíček McAfee Internet Security Suite 2006 s domovskou stránkou: www.mcafee.com/cz

Dokázal odhalit všechny vpuštěné viry a drtivou většinu z 168 523 backdorových programů, zombie a trojských koňů, je výkonný a dokáže nejlépe odstranit nežádoucí Malware a přitom jeho firewall má malé mezery pouze v útoku uvnitř sítě, což se při jinak vynikajících výsledcích dá omluvit.

3.2.1 Obecné rady pro práci a údržbu softwarových balíčků:

1. Pouštějte jen jeden antivirový engine, ne více najednou. Kompletně odinstalujte jeden produkt a restartujte osobní počítač dříve, než začnete instalovat produkt jiný. Vypněte
i Windows Firewall, pokud používáte firewall od jiné společnosti.

2. Před instalací spusťte několikrát utilitu Chkdsk ve Windows, abyste ve svém systému předešli problémům s pevným diskem. Jděte na Start, Spustit a do dialogového okénka napište chkdsk. Klikněte na OK.

3. Aktualizujte. Spusťte Aktualizaci Windows, abyste si byli jistí, že váš systém je aktuální, a to dříve, než nainstalujete bezpečnostní software, který je rovněž třeba aktualizovat, aby byl účinnější. Je potřeba také prodlužovat licence.

4. Pro případ, že byste potřebovali zavolat na linku technické podpory, si poznamenejte datum instalace, číslo série a číslo zákaznické telefonní linky uvedené na vaší bezpečnostní sadě. Tuto informaci budete potřebovat a navíc se telefonát v některých případech platí.

5. Pokud vám to vyhovuje, můžete používat zvláštní antispywarovou utilitu společně s vaší bezpečnostní sadou, ale slaďte rozvrh obou produktů tak, aby se nestalo, že kontrola prováděná aplikací nebo aktualizace různých produktů bude u obou probíhat v tutéž dobu.

6. Osobní počítače připojené k síti, zejména přes VPN (virtual private network) mohou mít uživatelská nastavení. Pokud po instalaci bezpečnostní sady váš systém při bootování zatuhne, odpojte se od sítě. Po novém bootování se opět připojte k síti a nechte sadu, aby nakonfigurovala nastavení vašeho firewallu.

7. Váš firewall by měl mít předdefinované profily, které by měly řídit sdílení souborů a tisku. pokud je nemá, budete si muset stanovit pravidla přímo ve vašem firewallu manuálně. Ta vám pak umožní směrovat vnější aktivitu TCP na port 1 023 a příchozí aktivitu na port 139.

8. Jestliže vás produkt upozorní na nějaký problém - třeba chybovou hláškou nebo výstrahou před malwarem - zapište si celou zprávu v doslovném znění. Ještě lepší je pořídit si snímek obrazovky s touto informací.

9. Setkáte-lí se s podezřelým souborem nebo e-mailem, neotevírejte je a ani se nesnažte je sami prozkoumávat. Pošlete je firmě, která vám poskytuje zabezpečení. Dbejte přitom na to, abyste dodrželi předepsaný postup.

3.3 Hardwarové firewally

3.3.1 Výhody hardwarového firewallu

Integrace s modemem

Spolu s jiným hardwarovým zařízením, jež si pořídíte tak jako tak, neboť bez něj žádný síťový provoz (myšleno především internetový) nezískáte, můžete za jedny peníze získat i poměrně kvalitní firewall v jedné „krabičce". V současné době je naprosto běžné, že specializované modemy pro připojení pomocí technologie ADSL (či příbuzné xDSL) nebo rozvodu kabelové televize již zahrnují funkcionalitu firewallů, a to často na velmi vysoké úrovni. Ve spojení s dalšími možnostmi takovýchto integrovaných krabiček jde o koncepčně velmi dobré řešení: provoz je filtrován již na vstupním bodu do vaší sítě, takže operační systém není vystaven ani potenciálnímu riziku. Pokud potřebujete k internetu připojit více počítačů, ochrana probíhá ještě před rozvedením provozu na všechny stroje a slouží tak najednou všem. Vnitřní, lokální síť je tak zcela oddělena od potenciálně nebezpečného internetového připojení. Pokud jste tedy i z jiných důvodů zvažovali hardwarové řešení, podle způsobu vašeho připojení může být použití jediného zařízení tou nejlepší volbou.

3.3.2 Nevýhody hardwarového firewallu

Další rozhraní navíc

Na jednu stranu je nezávislost a totální odloučení hardwarového firewallů od zbytku sítě či vašeho počítače výhodou, na druhou stranu si žádá oddělenou administraci, a to nemusí patřit mezi jednoduché úkony. Ovládací rozhraní -tedy především jeho logika - bývá většinou dosti odlišné od zkušeností s běžnými aplikacemi v operačním systému. Za zmínku také stojí fakt, že při velkém množství nabízených funkcí jeho uspořádání prostě úplně jednoduché ani být nemůže. Běžným trendem je uplatňovat pro konfiguraci jakési větší, ucelené kolekce nastavení (politik), jejichž organizace je většinou pojata dosti

zeširoka, takže prostě nezbývá nic jiného, než potřebné informace nastudovat a najít dostatek času na seznámení s vrtochy uživatelského rozhraní.

3.4 Softwarové firewally

3.4.1 Výhody Softwarového Firewallu

Vidí a rozpozná aplikace

Integrace softwarového firewallu do operačního systému sice přináší jisté komplikace, avšak umožňuje na druhou stranu jeho nejtěsnější sepjetí s dalšími částmi, především aplikacemi. „Místní" firewall může velmi pozorně zkoumat, která aplikace se pokouší síťové spojení sestavit zahájením své aktivity, či naopak dokáže přesně vymezit, které programy obdrží příchozí spojení. Tato úroveň kontroly je nesmírně důležitým posílením celé koncepce ochrany: velkým nebezpečím jsou totiž především programy, jež bez vědomí uživatele samy zahájí odchozí komunikaci (která je běžně a normálně povolena). Odpovědi na jejich propuštěné výzvy pak často představují onen kanál, kudy útočníci proniknou. Důsledné odepření síťových funkcí programům, jež nebyly výslovně vybrány uživateli, je pak účinnou obranou. Ta by pomocí externího firewallu, jenž si s operačním systémem nemůže „povídat", nemohla být zavedena.

Související výhodou softwarového řešení je pak výrazné zjednodušení konfigurace u příchozích výjimek, tedy u komunikace, kterou povolíte v příchozím směru. Ačkoliv softwarovému firewallu stačí často pouze říci, která aplikace smí na příchozí komunikaci reagovat, externí firewall vyžaduje výslovné nastavení síťových parametrů (čísel portů protokolů TCP a UDP). Právě přesné definování takové komunikace může být velkým problémem u aplikací, jež přiřazují čísla portů dynamicky a často je mění.

3.4.2 Nevýhody Softwarového Firewallu.

Snižuje výkonnost počítače

Již ze své podstaty-softwarový firewall běží jako aplikace - je tato varianta nezbytně zátěží pro váš počítač a operační systém. Ačkoliv se to na první pohled tak nemusí jevit, může docházet i k výrazné ztrátě výkonu a skutečná míra „ukousnutí" strojového času pak záleží na celé řadě podmínek.

Jednou z nejdůležitějších okolností je samotná konfigurace firewallu, přesněji řečeno jeho pokročilé funkce, které je možné zapnout. Je třeba si uvědomit, že základní síťová kontrola provozu, založená na poměrně jednoduchých pravidlech (např. porovnávání síťových adres), je poměrně nenáročná ve srovnání s pokročilou aplikační kontrolou, při níž třeba dochází k prověření kompletního obsahu přenášených webových stránek (protokol HTTP) či stahovaných souborů (protokol FTP.či třeba aplikace systémů BitTorrent či Direct Connect). Důsledná analýza na aplikační úrovni je stále náročnější i proto, že kapacita internetových připojení neustále stoupá, a co bylo při 128 kb/s hračkou, je na linkách s 1 Mb/s již slušný eskamotérský kousek. Dalším významným faktorem může být sdílení internetového připojení více počítači ve vaší síti. Pokud je stroj, k němuž vede internetové připojení, prostředníkem pro sdílení internetového provozu s dalšími počítači, může takto znásobený provoz na jeho síťových rozhraních při důsledné kontrole firewallem opět dosti zatížit operační systém.

Může přinést nestabilitu operačního systému

Ačkoliv technologie softwarových firewallu není žádným novým objevem a příslušné programy jsou již většinou vyvíjeny řadu let, stálé zavádění nových a nových verzí s sebou může přinést výrazné potíže se stabilitou. Jako odůvodnění takto silného obvinění stačí stručné vysvětlení, jak softwarový firewall pracuje, neboť jeho způsob instalace a běhu je shodný s běžnými uživatelskými aplikacemi.

Aby mohl firewall v součinnosti s operačním systémem dobře provádět žádoucí operace, musí být alespoň jeho část instalována a spouštěna takzvaně v režimu jádra systému (též se říká v privilegovaném režimu). Nejedná se o nic výjimečného, neboť takto pracují téměř všechny ovladače (drivery) různých zařízení a i proto se této programové komponentě říká též softwarový ovladač. Tento způsob integrace s operačním systémem s sebou přináší možnost přístupu do oblastí, v nichž je nezbytné kontrolu síťového provozu provádět (má-li opravdu dojít ke smysluplné ochraně), avšak také s sebou nese výrazné riziko provedení fatální chyby. Stejně jako ostatní ovladače různých zařízení může totiž díky popsané skutečnosti softwarový firewall chybou při svém běhu přivést k pádu celý operační systém, což kupříkladu běžné aplikace, jež v takto privilegovaném režimu neběží, nedokáží a operační systém nanejvýše ukončí jejich činnost. Chyba v komponentě firewallu, jež běží v jádře, však může být kritická. Z tohoto důvodu bývá většinou prozíravé vyčkávání na verze softwaru, v nichž byly postupně vychytány „drobné"

chybičky, tradičně se vyskytující v nových zásadních edicích. Konkrétně řečeno, je moudřejší počkat se sice starší a ne tak převratnou, nicméně dobře funkční verzí 1.95 firewallu XY na uvedení poopravené verze 2.05, než za každou cenu den po uvolnění instalovat zcela novou a bezpochyby revoluční verzi 2.0.

3.5 Srovnání antivirových programů

Anglický časopis Virus Bulletin vydává jeden z neuznávanějších nezávislých srovnávacích testů antivirových produktů. Testy probíhají ve většině případů pravidelně každé 2 měsíce a aby výsledky byly co nejvíce použitelné, dochází při každém testu ke změně platformy.

Antivirový program	Počet testů	Neúspěšný	Úspěšný	Procento úspěšnosti
NOD32	43	3	40	93,0 %
Symantec Norton	40	6	34	85,0 %
Norman	47	11	36	76,6 %
Kaspersky AVP	48	13	35	72,9 %
eTrust	35	11	24	68,6 %
BitDefender	19	6	13	68,4 %
F-Secure Anti-Virus	36	12	24	66,7 %
Avast!	38	19	19	50,0 %
AVG	35	21	14	40,0 %

Obr. 3 *Srovnání antivirů*

V dnešní době si počítač bez antivirového programu nedokážu představit. Počítačové viry jsou velmi rozšířené a je potřeba se jim bránit tím nejlepším způsobem. Hodně lidí používá antivirový program Avast a AVG verze 7.5. Ty mají jednoduché rozhraní a pro domácí účely jsou zdarma. Vyšší heurestiku a výkon však má software NOD32, Symantec Norton a Kaspersky AVP. Ke koupi jsou například na stránce www.anti-virus.cz ceny se pohybují od 1000 do 1500 korun českých.

3.6 Anti Spyware

Tyto programy jsou zaměřeny na detekci a odstranění Spyware z vašeho počítače aniž by poškodily funkčnost programů, které používáte. I když je možné, že i neškodný program je vyhodnocen jako nežádoucí. Ale pozorný uživatel si toho jistě všimne a zabrání jeho smazání.

3.6.1 Prevence před spywarem

Nahradit Internet Explorer jiným prohlížečem (browser) je jednou z účinných metod jak se podobných problémů zbavit. Prohlížeče jako Mozilla Firefox (www.firefox.czilla.cz) nebo Opera (www.operacesky.net) jsou totiž z velké části proti této havěti imunní. Hlavním důvodem je skutečnost, že Internet Explorer používá naprostá většina uživatelů a tak je havěť zaměřena právě proti Internet Exploreru. Více na stránce www.noie.wz.cz

3.6.2 Detekce a odstraňování spyware

Na Internetu existuje celá řada nástrojů pro detekci a odstraňování havěti. V praxi se osvědčila například kombinace následujících nástrojů (lze je stáhnout zadarmo ve funkční podobě):

Spybot S&D

Ad-Aware

Spyware Terminator (tento lze navíc použít i jako kvalitní nástroj pro prevenci)

Cool Web Shredder

Oblíbeným u mnoha uživatelů je i komerční Spy Emergenci.

Pro kontrolu registru se doporučují utilitky:IceSword, System Mechanic, Registry Mechanic, a Registry Repair.

Samozřejmě je potřeba všechny produkty aktualizovat a záplatovat.

Pozor! Na Internetu lze stáhnout desítky podvodných programů, vydávajících se za anti-spywarová řešení! Obvykle naleznou v počítači neexistující infekci a snaží se z uživatele vylákat peníze na zakoupení plnohodnotné verze, která již bude schopna neexistující havěť odstranit! Ve stejném stylu existují i některé webové stránky (často vzhledově připomínají oficiální stránky služby Windows Update).

Pokud ani tyto utilitky neodstraní problém existuje nástroj HijackThis, který prohledá váš počítač a vytvoří protokol o jeho stavu. Práce s tímto programem a jeho stažení je možné na stránce odkazu [3.]

3.6.3 Shrnutí

Spyware patří k velmi nepříjemnému hostiteli na vašem počítači. Ať už se jedná o nevyžádanou reklamu, programky, které informace o vás posílají do internetu, nebo se za vás připojí na placené linky a podobně. Mnoho se jich do systému dostane díky Internetovému prohlížeči Internet Explorer. Proto doporučuji nainstalovat jiný webový prohlížeč. Informace proč, naleznete v odkazu [5.] Ale i přes výměnu prohlížeče se k vám stále může škodlivý software dostat a proto je vhodné vyčistit systém pomocí vhodných utilitek, jako jsou: Spybot S&D a Ad-Aware. Více je v bodě 5.4. Detekce a odstraňování spyware. Pokud stále přetrvávají problémy, je nutno vyhledat odbornou pomoc.

3.7 Závěr

Internet svým rozšířením a anonymitou představuje zdroj užitečných informací i velké nebezpečí. Tím může být cílený počítačový útok, nebo jen zákeřný prográmek, nebo pouze pár řádků v Programovacím jazyce. Těmto nečistotám se říká Malware. Před ním nás ochrání opatrnost („neklikat“ na každý odkaz a kontrolovat si názvy souborů, které kopírujeme) a vhodné ochranné prográmky a utility. Nedoporučuje se používání nejrozšířenějšího internetového prohlížeče Internet Explorer, protože právě jeho slabin Malware a útočníci využívají. Jako základní software v každém počítači by měl být Antivirový program a takzvaný firewall. Tyto programy nutné stále aktualizovat, aby byly schopné odhalit a zneškodnit nejnovější škůdce systému. Ale žádný ochranný software není 100% a proto je dobré počítač (jeho pevné disky) zkontrolovat programy, které jsou zaměřeny na vyhledávání nežádoucího softwaru. Jsou to takzvané Anti-Spyware programy. Pokud je pro vás příliš složité instalovat více softwaru a utilitek a nedokážete se v nich orientovat, doporučuji koupi balíčku programů McAfee Internet Security Suite 2006 s domovskou stránkou: www.mcafee.com/cz, kde se vám dostane i zákaznické podpory.

4 METODY ÚTOKU A OBRANNÉ TECHNOLOGIE

Existuje nespočetné množství metod, jak lze zaútočit na vzdálený počítač. Většina crackerů využívá již známé bezpečnostní trhliny v operačních systémech, internetových prohlížečích a aplikacích, jež komunikují přes internet (ICQ,Microsoft outlook a další). Také pomocí nástrojů na skenování internetu hledají slabé, nebo nezabezpečené místa. Lidé, co se zabývají hlavně krádeží hesel a účtů používají také vyhledávač google, nebo přesměrují uživatele na svojí stánku. Dobrý cracker bývá většinou zkušený programátor a pokouší se vyrobit své útočné skripty. Proto v této kapitole zmíním pouze základní metody těchto útoků a způsoby, jak se proti nim dá bránit.

4.1 Phishing a Pharming

Tyto dvě slova jsou spojena s internetovými podvody a získávání hesel od začínajících, nebo nepozorných uživatelů.

4.1.1 Metody phishingu

Phishing se u nás označuje také za rhybaření. Typické pro tento druh počítačové kriminality je využívání nikoli slabin počítačových technologií, ale slabin vlastních samotnému člověku.

V zásadě jsou k rhybaření používány následující tři cesty:

varianta sociálního inženýrství

Vychází ze znalosti lidského myšlení a psychiky, útočník se přitom snaží přesvědčit oběť, aby mu vydala své logovací údaje (jméno a heslo). A to buď telefonicky, nebo prostřednictvím e-mailu, ve kterém se podvodně vydává za zástupce legitimní entity a nějakým způsobem vás nutí prozradit data související s vašimi financemi . Příklad takového "důvěryhodně" vypadajícího e-mailu:

Vážený zákazníku, omlouváme se za výpadek naší služby v průběhu posledních 48 hodin. Pro ověření obnovy funkce Vašeho přístupu Vás žádáme o jeho ověření na stránce http://... vložením vašeho hesla do příslušného pole. S úctou ...

Obvykle již přímo v e-mailu je oběť nasměrována, aby se kliknutím na odkaz dostala na podvodnou webovou stránku.

Varianta využívající keyloggery

Keyloggery jsou programy, které mapují vaše stisky klávesnice a odesílají tyto informace útočníkovi (pochopitelně bez vašeho vědomí). Keylogger se dostane na váš počítač obvykle pomocí trojana, který jste si stáhli z nějakého podezřelého webu, nebo nainstalováním "unikátního" softwaru. Více o těchto programech bude popsáno níže v kapitole Luštění hesel.

Varianta klasického útoku (*Man-in-the-Middle)*

Útočník funguje jako prostředník mezi vámi a bankou a ani jedna strana netuší nic o jeho přítomnosti. Pokud oprávněný uživatel skončí se svým připojením k bance, podvodník v něm pokračuje a samozřejmě ho využije ke svým cílům.

Zneužití osobních údajů

Existují případy, kde útočník využil důvěry majitele stránek a použil z životopisu jeho rodné číslo, adresu a jméno pro založení e-bay účtu. Pak pomocí falešného průkazu založil bankovní konto a prodal fiktivní věci. Na nic netušící oběť pak padaly desítky trestních oznámení. Více zde

4.1.2 Obrana proti phishingu

Většina phishing serverů naslouchá na portu 80. Pokud uživatel bude opatrný (dávat si pozor kam klikám) a používá aktualizovaný antivirový program a firewall, nehrozí mu žádné nebezpečí. Nedoporučuje se používání internet exploreru, u kterého hackeři často objeví trhlinu a umožní její využití ostatním (hlavně nebezpečným crackerům). Důležité je neuveřejňovat své osobní údaje na internetu- ať už v diskusních fórech, na svých osobních stránkách, nebo v nezabezpečené komunikaci. Google umí většinu z těchto údajů vyhledat a útočník je neváhá použít. Existuje několik firem vyrábějící software, který hlídá, aby stránky nebyly přesměrovány. Například na stránce antiphishing. Vhodný je například toolbar pro váš prohlížeč. Pro mozilu více informací zde a pro internet explorer zde. Nebo úplně nový chráněný internetový prohlížeč. Například SeaMonkey.

4.1.3 Metody pharmingu

Pharming funguje tak, že se přihlásíte na naprosto normální stránku banky, vydáte své přístupové kódy k vašim účtům a nemáte možnost si všimnout, že jde o podvodnou stránku.

Pharming může fungovat třemi způsoby:

Modifikace systému DNS v počítači uživatele

Software DNS (Domain Name Server) překládá uživatelem zadaný název domény na skutečnou adresu webového serveru v síti (jeho adresu IP) – přeloží například www.vasebanka.cz na 146.04.04.04. Protože je ale nutné tento překlad udělat prostřednictvím sítě, může to chvíli trvat. Aby se vše urychlilo, váš počítač obvykle uchovává vlastní kopie výsledků překladu DNS, které získal pro dříve navštívené weby. Místo, kde je uchovává, se nazývá "mezipaměť DNS". Tím, že před položením vlastního dotazu v síti hledá nejprve ve své mezipaměti, počítač šetří váš čas a nezatěžuje Internet dotazy, na které již zná odpověď.

Ale takovou místní mezipaměť DNS je také možno zneužít. Lupiči identity se mohou pokusit pomocí kódu trojského koně upravit vaši mezipaměť tak, že když zadáte název své banky online, budete převedeni na falešný web, který bude vypadat úplně stejně jako skutečný web banky. Při přihlašování pak neúmyslně vyzradíte své identifikační údaje. Bude to tak skutečně fungovat, protože váš počítač neumí žádným způsobem zjistit, jestli je adresa v jeho mezipaměti proto, že jste daný web již dříve navštívili, nebo proto, že ji tam zapsal nějaký program se zlými úmysly. Počítač v obou případech najde položku pro vaši banku online a bude jí naprosto důvěřovat.

Metoda Cross-Site Scripting

Modifikace systému DNS v počítači uživatele je nejčastější formou pharmingu, ale crackeři se pokusili narušit také kód legitimních webových serverů. Obvykle to dělají proto, aby do něj vložili skript, který bude manipulovat s návštěvníky daného webu. Může se jednat o jednoduché vložení odkazu do pravé webové stránky, který uživatele, pokud na něj klepne, přivede na falešný web. Jiným způsobem je zobrazení falešného okna prohlížeče (překryvné okno) přes okno legitimního webu. Toto falešné okno může požadovat identifikační údaje předstíráním, že se jedná o přihlášení, o problém s účtem nebo o dotazníkové okno předkládané legitimním webem.

Útočníci mohou také uložit na webový server skript využívající chybu v prohlížeči a tak infikovat počítače uživatelů, kteří procházejí Internet. Toto se již během posledních několika let stalo na několika významných webových serverech. Tato taktika je díky možnosti vlákat do léčky velký počet nevědomých obětí pomocí jediného útoku velice přitažlivá, ale kvůli obtížnosti průniku do vysoce zabezpečených webových serverů relativně málo používaná.

Modifikace systému DNS na serveru

Servery poskytovatele služeb Internetu jsou vysoce zabezpečené a modifikace systému DNS na této úrovni je nejobtížnější a také nejméně běžnou formou realizace pharmingu. Stejně, jak si stolní počítač pamatuje odpovědi na vaše dotazy v systému DNS, tak i server u vašeho poskytovatele služeb Internetu udržuje v mezipaměti překlady často vracené systémem DNS. Mezipaměť je pro tyto servery víc než užitečná věc: umožňuje jejich normální funkci. Když se všichni uživatelé velkého poskytovatele služeb Internetu chtějí ihned po významném utkání dostat na stejný web se sportovními zprávami, server DNS může ušetřit hodně času, když již dopředu zná odpověď. V posledních měsících se podvodníci pokusili modifikovat tyto mezipaměti tak, aby se uživatelé po zadání správné adresy URL dostali na nelegální webový server, který vypadá stejně jako ten pravý. Tyto servery mohou požadovat po uživatelích, aby se přihlásili a tím odhalili svoje identifikační údaje, nebo mohou do počítačů uživatelů zavádět spyware pro zcizování identity, nebo virusy trojského koně.

4.1.4 Ochrana před pharmingem

Nejdůležitější prevencí je používání „selského“ rozumu a také každý měsíc kontrolovat výpisy z banky a z účtu kreditní karty, zda neobsahují podezřelé transakce. Jakákoli ztráta vám bude ve většině případů plně uhrazena, pokud ji okamžitě nahlásíte.

Zkontrolujte adresu URL každého webu, který požaduje identifikační údaje. Přesvědčte se, zda vaše relace začíná na známé pravé adrese webového serveru a nejsou k ní přidány žádné další znaky.

Udržujte účinnou a aktuální antivirovou ochranu.

Používejte důvěryhodného a uznávaného poskytovatele služeb Internetu. Nekompromisní zabezpečení na úrovni poskytovatele služeb Internetu je vaší první linií obrany proti pharmingu.

Kontrolujte certifikáty. K ověření klepněte pravým tlačítkem myši kdekoli v okně prohlížeče a z místní nabídky vyberte Vlastnosti. V okně Vlastnosti klepněte na tlačítko Certifikáty a zkontrolujte, zda daný web používá bezpečný certifikát svého legitimního majitele a zda je stále platný.

4.2 Google hacking

Termín Google hacking je vlastně použití vyhledávače pro získání citlivých informací a hesel. Stránky pro ně sbíraji a indexují roboti - skripty, možná i samostatné počítače, jež hledají webové servery, prolézají zdrojové kódy stránek a logicky zařazují tyto stránky do databáze google. Ovšem sem tam naleznou i nějaký ten soubor, jenž by normálně neměl být uživateli přístupný. Stává se to v případech, kdy tvůrce (webmaster) špatně stránky vytvořil - například se ve zdrojovém kódu nachází odkaz na soubor s hesly

Hackování pomocí Google je užitečná věc a použití některého z níže uvedených příkladů může každému urychlit nelezení požadovaných informací, nebo souborů. Použitím správně upravených vyhledávacích řetězců můžeme leckdy nalézt například: čísla kreditních karet, hesla, software, písničky, dokumenty, hry, obrázky a mnoho dalšího.

4.2.1 Hledání hesel

Pokud chceme vyhledat pomocí Google hesla, je zapotřebí vědět, jaké fráze hledáme. V tabulce uvedené níže je několik příkladů jak by mohl vypadat dotaz na zjištění citlivých údajů.

Tab. 5 Získání citlivých údajů googlem1.

Index of /admin	inurl:admin filetype:txt
Index of /passwd	inurl:admin filetype:db
Index of /password	inurl:admin filetype:cfg
Index of /mail	inurl:mysql filetype:cfg
Index of / +passwd	inurl:passwd filetype:txt
Index of / +password.txt	inurl:iisadmin

Index of / +.htaccess	inurl:auth_user_file.txt
Index of /secret	inurl:orders.txt
Index of /confidential	inurl:"wwwroot/*."
Index of /root	inurl:adpassword.txt
Index of /cgi-bin	inurl:webeditor.php
Index of /credit-card	inurl:file_upload.php
Index of /logs	allinurl:auth_user_file.txt
Index of /config	allinurl: admin mdb

Pokud správce, nebo tvůrce webu povolí na svých stránkách indexaci, pak můžeme pomocí příkazu „index of“ procházet adresáře a hledat v nich jakákoliv data.

Tab. 6 *Získání citlivých údajů googlem2.*

intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"index of" passwd
intitle:"index of" people.lst
intitle:"index of" pwd.db
intitle:"index of" etc/shadow
intitle:"index of" spwd
intitle:"index of" master.passwd
intitle:"index of" htpasswd
intitle:"index of" members OR accounts
intitle:"index of" user_carts OR user_cart
allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:govdsa

Některá nalezené hesla, nebo informace mohou být zašifrované. Například hesla pro uživatele Frontpage, jež nalezne dotaz "# -Frontpage-" inurl:service.pwd, jsou chráněná pomocí DES šifry. Ta se dá překonat použitím programu John The Ripper.

4.2.2 Hledání v adresářích

Pokud chceme hledat pomocí Googlu v adresářích, můžeme využít například následujících dotazů, kde MP3, nebo Kabat můžeme nahradit libovolným slovem, jenž chceme najít :

"parent directory " MP3 -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
"parent directory " Kabat -xxx -html -htm -php -shtml -opendivx -md5 -md5sums

Další metodou je hledání v titulcích. Opět uvedu příklad, kde se poslední slovo může nahradit libovolným řetězcem. Pak slouží pro vyhledání obrázků, hudebních souborů a podobně. Příklad:

?intitle:index.of? mp3

?intitle:index.of? mp3 jackson

Je možné použít ještě
inurl:microsoft filetype:exe

4.2.3 Další zajímavé příklady

"http://:*@www" domainname*
Tímto požadavkem získáte hesla z vyhledávacích enginů (ale ne z google). Místo domainname musíte napsat název domény bez koncovky (.cz, .sk, a podobně)

allinurl: admin mdb
Ne všechny stránky, které google po tomto dotazu vrátí, obsahují uživatelská jména, hesla nebo jiné choulostivé údaje.

allinurl:auth_user_file.txt
Soubor s hesly od DC Fóra. Soubor obsahuje seznam (prolomitelných) hesel, uživatelských jmen a e-mailových adres pro DC Fórum a DC Shop.

intitle:"Index of" config.php
Ukáže stránky používající soubor config.php, který (většinou) obsahuje uživatelské jméno

a heslo pro připojení k SQL databázi. Hodně stránek používá fóra běžící na PHP. Tento soubor vám umožní úplný přístup (administrátorský účet) do databáze.

intitle:index.of.etc

Google vám s tímto dotazem vyhledá "etc" adresáře, kde se nachází spousta typů souborů s hesly. Tento odkaz není spolehlivý, ale procházení "etc" adresářů může být velmi zajímavé.

filetype:bak inurl:"htaccess|passwd|shadow|htusers"

Pro vyhledavaní záloh (souboru *.bak). Tyto zálohy vytvářejí některé editory, někdy i samotní administrátoři. Čehož se pak dá využít.

4.2.4 Hledání sériového klíče

Pokud například potřebujeme sériové číslo pro windows xp professional, můžeme do vyhledávací kolonky google napsat následující řetězec:

"Windows XP Professional" 94FBR

Klíč 94FBR je kódem... ten je přikládán k mnoha kopiím MS Office. Velmi vám pomůže zredukovat množství "podvodných" stránek, které vás chtějí zmást a neobsahují žádný sériový klíč. Jestliže hledáte sériový kód pro winzip 8.1 Zadejte:

"Winzip 8.1" 94FBR

Další informace a použité zdroje jsou k nalezení například na:

www.i-hacked.com/index2.php?option=com_content&do_pdf=1&id=23

http://johnny.ihackstuff.com

http://www.securitydocs.com/pdf/3098.PDF

4.2.5 Ochrana před Google hackingem

Důležité je správné vytvoření stránky. Existuje spousta tvůrců, jenž si nad bezpečností neláme hlavu, nebo neví, že vyhledávač není inteligentní a snaží se vyhledat i data, která jsou osobní a chráněná. Proto je potřeba na stránce použít příkazy, které vyhledávači říkají- tuto část přeskoč- zde nehledej.

České webmastery zajímají hlavně české a největší zahraniční vyhledávače. Mezi nejpoužívanější patří tyto:

- "**Googlebot**" (google),
- "**Jyxobot**" (Jyxo používané též na Atlasu)
- "**Seznambot**" (pro fulltext Seznamu)
- **"Morfeo“** (Centrum)
- "**Slurp**" (Yahoo)
- "**msnbot**" (MSN search, Microsoftí hledání)

První možnost je vytvoření souboru **robots.txt** v kořenovém adresáři webu. Do něj se pak vkládají řádky začínající:

User-agent: zde se píše, pro kterého robota omezení platí, nebo znak * jenž značí, že omezení má platit pro všechny roboty. Bohužel se zde * nedělí a pokud pak použijeme znovu User-agent pro některého robota, pravidlo s * pro něj již neplatí. Více v přikladu.

Disallow: specifikace adresářů a souborů které nemá indexovat

Allow: povoluje indexování- ale funguje pouze na několika vyhledávačích (Google,Jyxo, u dalších je zatím otazník)

Pokud do souboru vloží například následující obsah:

*User-agent: **
Disallow: /bin/
Disallow: /php/

User-agent: Googlebot

Disallow: /bin/ *nebo* *Disallow:/*
Allow:/an/

Příkaz User-agent definuje přímo konkrétního indexovacího robota, který by neměl indexovat adresáře uvedené v robots.txt. Hvězdička značí, že informace platí pro všechny vyhledávající roboty. Těm se pak zakáže adresář bin a php. Při znovu použití příkazu User-agent pro robota googlebot se na něj nebudou vztahovat podmínky z předchozího příkazu,

kde byla použita „*“, proto bude mít přístup do adresáře php, ale nebude mít přístup do adresáře bin- ten je zakázán. Pokud použijeme specifikaci Disallow:/ zakáží se všechny adresáře a soubory v kořenu. Pak můžeme povolovat pouze to, co chceme, aby prohledával. Příkaz Allow:/an/ povolí pro indexování pouze adresář an.

Když Internet Explorer stahuje soubory pro prohlížení offline, tak se dívá na robots.txt
a zdá se, že jeho omezení také respektuje. Pokud chcete, aby si vás čtenáři mohli číst offline, tak nedělejte robots.txt moc restriktivní. Bohužel, ne všechny vyhledávače soubor robots.txt berou jako zábranu, nebo jej nepoužívají správně. Takže pro citlivé informace a hesla je dobré použít více možností ochrany.

Druhá možnost jsou **Meta tagy**. Ty se umisťují přímo do hlavičky HTML mohou zakázat robotům jednak indexování obsahu, jednak sledování odkazů.

Tag může mít následující hodnoty:

noindex:	Obsah stránky nebude indexován
index:	Obsah stránky bude indexován (normální hodnota)
nofollow:	Odkazy nebudou sledovány. Podporují pouze některé vyhledávače
follow:	Odkazy budou sledovány (normál)
all:	Vše povoleno, tedy jako index, follow

Příkladem meta tagu je následující řetězec, který je součástí hlavičky HTML:

<meta name="robots" content="noindex, nofollow">

Třetí možnost je použití **javascriptů.** Vyhledávače totiž většinou znají pouze HTML znaky a neinterpretují JavaScript ani Java applety ani Visual Basic skripty. Proto veškeré texty produkované tímto způsobem nemohou být do databáze vyhledávače uloženy.

Každý vyhledávací robot je specifikován jinak. Proto je vhodné si vyhledat, co který robot vidí a nevidí. Každý server má informace pro webmastery, kde radí, jak specifikovat své webové stránky pro jejich vyhledávací robot. Buď je umisťují na co nejlepších pozicích a „prodají“ obsah svých stránek, nebo si naopak dobře ochrání data, která nepatří do cizích rukou.

4.3 Rozluštění hesla

Asi neexistuje člověk, jenž by se nesetkal s heslem. Hesla používáme každý den. Ať už jako PIN kódy, přihlašovací kódy a podobně. Používáme je k přístupu do míst, kde můžeme jenom my. Pokud by naše heslo bylo vyzrazeno další osobě, může ho použít a ukrást naše peníze, data, nebo informace. To odjakživa lákalo lidi, aby vynalézali techniky, jak uhodnout cizí heslo. Dnes za nás tuto „špinavou" práci může dělat počítač. Při jeho obrovské rychlosti se může stát, že útočník získá přístup téměř okamžitě. Mnoho lidí stále používá krátká či jednoduchá hesla, nebo má své oblíbené a to používá v mnoha případech. Často hesla putují po nekódovaných linkách a je možné je odchytit a zneužít. K ochraně údajů nebo majetku či neautorizovanému vstupu rozlišujeme tři skupiny ochrany:

1. **Znalost** - Uživatel se prokáže znalostí, kterou „by měl" vědět pouze on, typické **heslo**, šifrovací klíč uložený na disku, vstupní PIN...
2. **Vlastnictví** - Autentizovat (ověřit identifikaci)se může pouze ten, kdo vlastní určitý předmět - **token**. Na příklad: autentizační kalkulátor, čipová karta, USB token...
3. **Biometrika** - Měří se tzv. **biometrické vlastnosti** uživatele – otisky prstů, geometrie ruky, oční sítnice, tvar obličeje, rozpoznávání řeči, test DNA...

4.3.1 Slovníkový útok

Na internetu existuje řada slovníků, jež obsahují nejpoužívanější slova, jména, hesla zachycená na internetu, směrovací čísla a podobně. Tento slovník jmen – většinou uložený v obyčejném textovém souboru pak otevře program a jednotlivé slova zkouší zadat jako heslo. Dnešní počítače to dokáží i bilionkrát za vteřinu. K vytvoření vlastního slovníku můžeme použít například utilitu Raptor, ke stažení zde. Existuje však spousta hotových produktů, které mají své slovníky a jsou specializovány na luštění hesel u různých aplikací. Například souborů vytvořených v aplikaci: MS Office, Adobe Acrobat, Archivy (Rar, Arj,Zip Ace)

4.3.2 Útok hrubou silou

Je metoda, která zkouší postupně všechny možné kombinace znaků. Je možné zadat počáteční a koncovou hodnotu. Pokud má naše heslo například 5 znaků, tak při abecedě o m symbolech bude potřeba přesně m^1 + m^2 +.. m^5 kombinací.

Většina hesel na internetu je zakódována pomocí hash kódu. Hash je otisk dat a jeho vlastností je, že nelze z hash kódu zjistit kód původní. Proto se musí přepočítat veškeré jeho kombinace vstupních kódů do takzvaných hashovacích tabulek. Tyto tabulky pak mohou mít řádově desítky Gigabitů a přepočítávají se několik dnů. Výhoda spočívá v tom, že program na prolamování hesel chráněných hash kódem použije tuto tabulku a rozlouskne heslo během několika vteřin. Tomu se říká Rainbow útok.

Tab. 7 Příklady Rainbow cracků pro jednotlivé hash kódy

Název	Platforma	Algoritmus
Rainbowcrack-1.2a-win	win32	LM, NTLM, MD2, MD4, MD5, SHA1, RIPEMD-160, MySQL v.3.23, MySQL SHA1, Cisco PIX
rainbowcrack-1.2-src,	win32, unix	LM, MD5, SHA1
rainbowcrack-1.2_mac.diff	mac os x	LM, MD5, SHA1

4.3.3 Získávání hesel

K získání hesel slouží celé řada HW a SW. Pro odchytávání na lokální síti je nejlepší prográmek Cain@cabel, který je navíc zdarma. Bohužel se mi k němu nepodařilo najít českou dokumentaci a jeho nastavení není nejjednodušší. HW metoda spočívá v zabudování malého zařízení mezi počítač a klávesnici- něco jako redukce pro klávesnici. V něm jsou pak uloženy všechny stisklé klávesy. Takže včetně hesla do biosů a k operačním systémům. Je těžké orientovat se v tak obrovském množství znaků a pokud uživatel použije pro přihlašování token, získáme jen PIN k tokenu. Klávesy jdou odchytávat i SW metodou, ale nejdřív musíte keylogger dostat do cizího počítače pomocí trojského koně.

Pro rozluštění hesla nebo pro prohledání prostoru klíčů ze souborů, bych doporučoval následující programy. Společnost ElcomSoft je díky svému produktu Advanced Office Password Recovery jednou z nejlepších v rekonstrukci hesel pro sadu

MS Office. Její další aplikace jsou zaměřeny na archivy (Advanced Archive Password Recovery) a další software. Dalším výrobcem je VDG Software s produktem Ultimate ZIP Cracker (UZC) jenž slouží k lámání hesel archívů ZIP, ale poradí si také se soubory Word, Excel (oboje verze 97 až 2003) a ARJ.

4.3.4 Biometrická ochrana

Všichni si určitě vzpomenou, jak ve filmu pro vstup na místo s nejvyšším stupněm ochrany potřeboval pracovník vyťukat mnohamístný kód, potom potvrdit svou totožnost otiskem prstu, hlasem, nebo obrazem sítnice. Dnes se tyto prostředky dají pořídit i pro osobní ochranu. Snímání otisků lze zakoupit opravdu levně. Počítače mohou porovnávat i klasický podpis. Mnoho lidí se k tomuto zabezpečení staví spíše s obavami. Tvrdí, že všehoschopní zločinci jim mohou například uříznout prst nebo „vydloubnout“ oko. Otisky se však dají vyrobit a snímače, které zjišťují kapacitanci (a to jen některé), nebo dokonce teplotu, jsou drahé. Navíc potravinářská želatina má stejnou kapacitanci jako prst. Stačí otisk do formely, chvilka v kuchyni a máte duplikát. Z otisku na sklenici nebo na snímači je to jen o málo těžší. Vždy je potřeba vynaložit určité finanční prostředky. Měly by být vyšší, než je cena ochranného systému.

4.3.5 Tokeny

Tokeny, jako například čipové karty, nebo USB tokeny, slouží k uchování důležitých hesel mimo počítač (jako malokapacitní přenosné médium) a k autentizaci. Jejich výrobní číslo je přitom váže na číslo softaru majitele. Cizí osoba tak nemůže token použít ze svého počítače. To je nesporná výhoda oproti uživatelům, kteří si své hesla ukládají na obyčejné USB nebo disketu. Navíc token může být použit pro povolení pro vstup do místnosti, na toaletu a podobně, takže uživatel jej musí při odchodu z místnosti z počítače vyjmout a tím svůj počítač zablokuje a předejde zneužití. Navíc má token neustále u sebe. Mnoho uživatelů se totiž zapomíná odhlásit při vzdálení od počítače.

Autentizace pomocí hesla, by měl být v dnešní době již spíše přežitek. Uživatelé zadávající své username a heslo, jsou noční můrou každého správce sítě, který dbá na bezpečnost.

1. Uživatelé volí hesla typu: 1heslo,12345, rodné číslo, jméno partnera/-ky, telefonní číslo, nápisy poblíž počítače, obyčejná slova, typu domeček, sluníčko, krteček.. Tyto hesla se buď dají uhodnout, nebo lehce rozluštit.

2. Heslo se dá snadno získat odpozorováním , obzvláště u lidí, kteří nepíší všemi deseti a s využitím moderní techniky. S web kamerami, mobily třetí generace, či digitálními fotoaparáty.
3. Pokud odhlédneme od hesel do operačního systému, dají se všechna ostatní hesla (k emailu, informačnímu systému, účetnímu software**...)** odchytit na úrovni klávesnice. Například software iBoss zaznamenává vše, co uživatel na počítači dělá, včetně všech stisknutých kláves s podrobným výpisem, v jaké to bylo aplikaci.
4. Důvodů, proč nepoužívat statická hesla, by se asi našlo více.

Více o této problematice je k nalezení na stránce :

http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=264&clanekID=265

4.3.6 Obrana před rozluštěním hesla

Proti rozluštění hesla se dá bránit pouze jeho vysokou složitostí a dobrým uschováním. Heslo je tím bezpečnější, čím je delší a čím větší je abeceda, kterou používá. Zahrnuje-li m symbolů, pak všech možných slov délky n je m^n

Několik zásad pro silné heslo:

1. Heslo by mělo být alespoň osm znaků dlouhé
2. Heslo v sobě nesmí obsahovat smysluplné slovo (např. computer, pepa2005 apod.)
3. Heslo nesmí být spojeno s informacemi o uživateli (např. rodné či telefonní číslo).
4. Heslo obsahuje malá i velká písmena standardní anglické abecedy.
5. Heslo obsahuje číslice a speciální znaky (např. !, ?, _, # apod.)
6. Heslo by se mělo v určité periodě měnit.

Další typy pro tvorbu hesla:

Heslo by mělo obsahovat nahodilost, chaotičnost (informační entropii)

Je dobré používat asociace, které nás například napadnou. Například k e-mailu na centrum, mě napadnou dvojčata. a heslo by mohlo být teroristickyutok- to je vsak moc jednoduché, ale zapamatovatelné.

Pak stačí mít systém na upravení hesla. Například záměnu některých písmen, nebo doplnění nadbytečných znaků mezi heslo. Zvolil bych změnu každého pátého písmene na číslici, dále přidání za každé 4 písmeno znak „!“ a každé sudé písmeno přepsat na velké, pak bude heslo vypadat takto: tErO!1iSt!I2kY!uT3k!. pro větší nahodilost se můžou ještě některá písmena posunout v abecedě. Pokud však bude pravidlo až příliš rutinní a někdo získá dvě, tři hesla, mohl by si domyslet třetí.

Existují například generátory hesel (Password Generator, SecureSafe Pro). Nevýhoda je potom v tom, že takové heslo není zapamatovatelné. Potom se nabízí možnost tato hesla ukládat do správce hesel (AES Password Manager) a k tomu používat jedno silné heslo spolu s tokenem. Nebo je mít uložené v zaheslovaném textovém souboru a ten mít ještě uložen například na zašifrovaném disku. Lidé, kteří používají kolem 50 ti hesel si je ukládají tímto způsobem do přenosných zařízený typu PDA, které nosí neustále u sebe jako mobil. To by jim pak musel někdo ukrást a ještě zjistit heslo.

4.4 Odepření služby (DOS)

Odepření služby (denial of service) je asi nejznámější počítačový útok. Jeho podstatou je přetížit, nebo vyčerpat fyzické zdroje cílového počítače. Ani sebelepší Antivir , nebo firewall totiž nedokáže zpracovávat neomezený objem dat. A server má omezenou paměť, rychlost CPU, nebo šíři pásma. Pokud některý ze zdrojů vyčerpáme, přestává být bezpečnostní systém efektivní a může i selhat. První DOS útok vytvořil student Robert T. Morris. Napsal de facto prvního červa, který se nyní jmenuje po něm. Nejednalo se o úmysl způsobit škodu, ale o důkaz potenciálních rizik. DOS útoky jsou vzdálené a lokální, kdy musíte mít přístup na počítač, na který se útočí.

Obecně si útočník vyhlédne oběť a zjistí si o ní veškeré informace (typ OS, programy které používá, stránky kam chodí) a zjišťuje, zda v nich není nějaká známá, ještě neopravená chyba. To může například zjistit na stránce http://osvdb.org/ . Zde je každá chyba dobře popsána. K většině chyb je udán i exploit- což je jednoúčelový program, pomocí něhož se útok provádí. Ten bývá na internetu ke stažení v podobě zdrojových kódů (většinou v jazyce C někdy i python, nebo perl). Ty pak používají „script kiddies“, neboli náctiletí, kteří problematice nerozumí a umí jen škodit.

4.4.1 Typy DOS útoků

Základní rozdělení útoků snažící se zahltit a tím ochromit oběť by mohlo vypadat asi takto:

- **Záplavový útok (Flood atack)**

Jeho cílem je zahltit cílovou linku dary, jež není schopna přijmout. Stačí mít pouze rychlejší internetové připojení, než vaše oběť. Pak oběť může nastavit pravidla ve firewalu a stejně bude linka zahlcena. Jediná možnost je zavolat poskytovateli a požádat jej o zablokování zdrojové IP adresy. Bohužel útočník si může změnit port, zfalšovat svoji IP adresu a pokračovat v útoku. Může se jednat o téměř nekonečný boj. V takovém případě se server často odpojí úplně, útok se analyzuje, hledá se útočník a vymýšlí se co nejlepší protiopatření.

- **Útok využívající chybu v SW, nebo HW**

Jedná se o útoky, které - aby dosáhly svého - využívají zranitelnosti v softwaru nebo hardwaru oběti. Nejčastěji se jedná o chyby, jež jsou velmi rychle opraveny, a tyto útoky většinou nemají dlouhou životnost. Na druhou stranu tato kategorie tu s námi bude navždy, jelikož člověk je tvor omylný a chyby dělal a dělat bude. Navíc lze očekávat, že s postupným zvyšováním složitosti softwaru se bude objevovat těchto chyb více.

- **Vyčerpání zdrojů**

Tyto útoky také využívají chyb objevených v softwaru nebo hardwaru. jedná se ale o chyby implementace (tzn. chyby způsobené špatným návrhem). Tyto chyby se projevují například tak, že při určitých speciálně upravených paketech program vytíží procesor více, než je obvyklé, nebo program začne konzumovat více paměti.

Také počet paketů potřebných pro útok vypadá jinak - místo několika paketů již je potřeba větší datový tok, který musí být přítomen po celou dobu útoku. Také zde může sehrát roli rozdíl rychlosti připojení útočníka a oběti.

Ve výsledku tedy útok vypadá tak, že se posílá co největší množství paketů, aby se procesor oběti vytížil na sto procent nebo program zkonzumoval celou paměť a počítač začal swapovat (přepisovat obsah paměti na HDD) a nestíhá obsluhovat legitimní provoz.

- **Distribuovaný záplavový útok (DDOS)**

Jedná se o DOS záplavové útoky, které jsou charakteristické tím, že se jich účastní více než jeden počítač, takže výsledek je mnohonásobně silnější.. Tyto útoky jsou v poslední době asi nejvíce vidět a nejvíce se o nich mluví. Pokud bychom DOS útoky dělili podle počtu útočících počítačů, pak bychom je dělili na obyčejné (o jednom útočníku) a distribuované (o více útočnících).

- **Reflektivní a zesilující typy**

Jedná se o útoky, které se snaží zahltit linku oběti, ovšem k útoku používají jiné počítače (nebo routery) jako prostředníky. Tito prostředníci nemusí být kompromitováni, to znamená, že útočník je nejdřív nepotřebuje napadnout. Tyto útoky se provádí hlavně distribuovaně. Nejstarší reflektivní útok Smurf byl znám již v roce 1998.

Největší výhodou tohoto útoku je minimální možnost vystopování útočníka. Data (použitá k zahlcení) totiž netečou stále stejnou cestou, protože se při útoku mění počítače, od kterých se útok „odráží“ (proto se jim říká reflektivní). Vyhledávání útočníka se provádí tak, že se od oběti postupuje postupně po routerech směrem k útočníkovi. Vždy se na routeru zjistí, ze kterého portu útok přichází, a toto se provede znovu na routeru, který je připojen k tomu portu, a takto stále dokola (z toho důvodu, že útočník téměř vždy falšuje svoji IP adresu).

4.4.2 Metody záplavového útoku

Jedná se vlastně o různé protokoly, které k útoku použijeme.

ICMP záplava (ICMP Flood):

Útok využívá protokolu ICMP, nejčastěji se používají pakety typu ICMP Echo, což jsou pakety, které využívají ping a slouží k zjišťování, zda je vzdálené zařízení dostupné. Podle doporučení (RFC) by měla být maximální velikost ICMP Echo paketu 548 B, ovšem program ping jak pro systémy Windows, tak i pro Linux umožňuje velikost ICMP Echo paketu až 65 kB (největší možný ICMP Echo paket může být 65.535 B, tak to uvádí specifikace).

ICMP Echo funguje tak, že my pošleme ICMP Echo request a cílový počítač posílá zpátky ICMP Echo reply. Přitom zachovává velikost paketu. Toho lze využít tak, že zfalšujeme adresu odesílatele a tím docílíme, že datová linka oběti bude ucpávána dvakrát. Jednou daty směrem tam a podruhé daty zpátky (která budou určena oné zfalšované

adrese). Často však bývá ve firewalech ICMP Echo zakázané. Pokud není, je velmi jednoduché tento útok uskutečnit.

UDP záplava (UDP Flood)

K tomuto útoku se používá transportního protokolu UDP. Výhodou tohoto protokolu je to, že je bezstavový. To znamená, že se u něj nesestavuje spojení jako u protokolu TCP. Používá se zde také zranitelnosti služeb echo a chargen. Služba echo pracuje tak, že veškerá data, která přijdou na její port, jsou poslána zpět. Naproti tomu služba chargen pracuje tak, že na ni pošlete nějaká data a ona vám zpátky pošle náhodná data.

Trik spočívá v tom, že pošleme data oběti na port echo a zfalšujeme zdrojovou adresu a port. Zfalšujeme je tak, že zdrojovou IP nastavíme na nějaký počítač, který poskytuje službu echo nebo chargen, a port nastavíme na tuto službu. Tímto docílíme toho, že tyto dva počítače si budou tato data posílat stále dokola. Má to tu výhodu, že takto se může odstranit server, který je k Internetu připojen daleko rychleji než my. Ovšem tyto služby se v dnešní době již nepoužívají.

TCP záplavy (TCP Flood)

Tyto útoky jsou založeny na protokolu TCP. Na Internetu se můžete setkat s názvy SYN Flood, ACK Flood, RST Flood, FIN Flood, URG Flood, PSH Flood, nebo jejich kombinacemi. Jejich názvy vycházejí z toho, jaké příznaky má TCP paket nastaven. Počítač oběti na tyto pakety obvykle nereaguje. Správně by měl poslat zpátky TCP paket s RST příznakem, ovšem toto nebývá dodržováno nebo je filtrováno firewallem. Výjimkou jsou packety SYN a RST, které patří do skupiny útoků přečerpávající zdroje.

Mass mailing list a E-mail bombing

Tyto útoky spočívají v zahlcení určité e-mailové schránky, aby byla nepoužitelná.. Dnešní schránky jsou sice větší, ale pokud každý den někomu přijde tisíc e-mailů - schránka je nepoužitelná.

Jak vypadá takový útok? Docela jednoduše. Útočník „obejde“ Internet a zaregistruje vybranou e-mailovou adresu oběti na webových stránkách. Například různé konference, novinky, bulletiny nebo navštíví stránky s pornografií odkud navíc bývají e-mailové adresy distribuovány spamerům. Útok je snadný a možnost vystopování útočníka téměř nulová.

U bombingu se k vytvoření e-mailů se používá program. E-maily tedy generuje sám útočník a jejich množství záleží na tom, kolik jich pošle. Pokud se bude jednat o distribuovaný bombing útok, lze se tímto způsobem pokusit ochromit poštovní server. Ten často kontroluje poštu, zda se nejedná o spam nebo o virus. To přispívá k tomu, že pro odbavení jedné e-mailové zprávy je potřeba více procesorového času.

4.4.3 Útoky využívající chybu HW nebo SW

Útočníci většinou sledují bezpečnostní konference nebo nahlíží do databází, které obsahují informace o chybách a čekají, až se objeví nějaká nová zranitelnost, na kterou ještě neexistuje žádná oprava. Poté útočník začne hledat oběť a následně na ni zaútočí.

Útok využívající chybu je jeden z nejnebezpečnějších, protože většinou spočívá pouze ve vygenerování malého množství speciálních paketů a oběť je nedostupná. Takže na rozdíl od záplavových útoků zde nehraje roli rychlost připojení útočníka a oběti. Díky tomu, že k provedení útoku stačí několik paketů, je těžké útočníka vysledovat, a také je velice těžké se tomuto útoku bránit nějakými filtrovacími pravidly.

Ještě větším nebezpečím je to, že než se vůbec o zranitelnosti dozvíte, tak útočníci už pomocí ní dávno útočí. Dalším nebezpečím je například ignorance některých výrobců softwaru, které to, že byla objevena chyba, vůbec neznepokojuje. Například Microsoft jehož systém má obrovské množství počítačů s uvolňováním záplat právě nepospíchá.

Ping of death (Ping smrti)

Jedná se o jeden ze starých útoků, který bývá často zmiňován. Jedná se o útok využívající chyby. Tento útok používá speciálně vyrobený paket, který má větší velikost, než je povolena. Některé operační systémy na to nebyly připraveny a při obdržení této zprávy kolabovaly. Více o něm bude napsáno v další kapitole. Tato chyba byla odstraněna a lze říci, že tento útok již je mrtvý.

Teardrop (slza)

Jedná se o útok podobný útoku Ping of death. Útok spočíval v poslání fragmentovaného IP paketu, u kterého se fragmenty překrývaly. Vlastně by to ničemu vadit nemělo, jelikož informace o offsetech byly v pořádku. Ovšem dříve některé operační systémy měly špatně implementováno sestavování původního IP datagramu. Kvůli tomu se při poslání speciálně fragmentovaných datagramů operační systém cílového počítače

zhroutil. Stejně jako u pingu smrti bude více popsáno v kapitole Zneužití síťovích protokolů.

4.4.4 Útoky vyčerpáním zdrojů

Jelikož na chyby, jež byly u SW a HW objeveny, se výrobce snaží vytvořit účinnou záplatu, mají tyto útoky pouze dočasné trvání. Ne každý počítač má všechny aktualizace a každá nová chyba může být zneužita podobným typem útoku. Uvedu zde proto jen několik zástupců.

Záplava SYN (SYN Flood)

Útok využíval špatné implementace začátku spojení v TCP protokolu. Chyba byla v tom, že když server obdržel paket od klienta s nastaveným příznakem SYN (výzva k začátku spojení a synchronizaci), tak alokoval pro toto spojení systémové zdroje (prostředky), odeslal mu paket s nastavenými příznaky SYN+ACK (potvrzení přenosu) a čekal na odpověď. Když odpověď stále nepřicházela, server (operační systém) si myslel, že se ztratila, a poslal paket znovu.

Po určité nastavené době vzdal čekání na odpověď a alokaci těchto systémových zdrojů (prostředků) zrušil spolu se záznamem o původní inicializaci spojení. Pokud ovšem útočník poslal paketů s příznakem SYN více, vedlo to k tomu, že se vyčerpala všechna možná spojení, která byla otevřena a čekala na potvrzení. Tím se služba zablokovala pro další uživatele.Velikost paketu s příznakem SYN činí pouhých 42 bytů. Z toho vyplývá, že u tohoto útoku nezáleželo na tom, jak rychle je útočník připojen. Další výhodou bylo, že se u útoku dala falšovat IP adresa odesílatele, protože zde není nutná zpětná vazba.

Land Atack

Jedná se o útoky, které posílají oběti zfalšované pakety, kde je nastavena zdrojová a cílová IP adresa na adresu oběti. Těchto útoků existuje hodně variant, kde se mění zdrojové a cílové porty, často bývá nastaven i příznak SYN. Výsledkem tohoto útoku je, že se oběť ocitne ve smyčce, kdy sama sobě posílá data, což vyústí v pád systému. Tyto útoky se dají označit za malou hrozbu, protože firewall je stoprocentní ochranou a takové pakety nepropustí dovnitř.

Fork bomb

Jedná se o speciální lokální DOS útok. K jeho provedení se používá programů, které pouští do nekonečna samy sebe. Jeho jméno vzniklo pomocí funkce `fork()`, která spustí běžící program ještě jednou (vytvoří další instanci). Takovéto spouštění sama sebe do nekonečna vede k vyčerpání systémových prostředků a pádu systému nebo jeho zatuhnutí. Současné operační systémy mají většinou zapnuto omezení na počet zpuštění jedné aplikace.

WinNukes

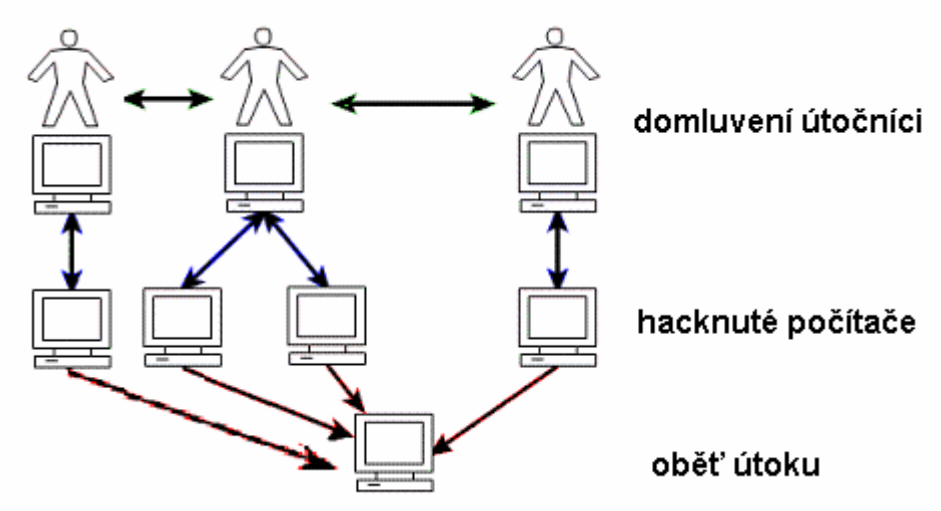
Jedná se spíše o typ nástrojů používaných k útoku. Jako Nukes jsou označovány programy, které slouží k provádění DOS útoků využívajících chyb. Tyto jednoúčelové programy se od exploitů liší tím, že jsou již zkompilovány a spustí je i úplný začátečník. V tom je jejich hrozba. Stačí zadat IP adresu a cílový počítač se zhroutí (pokud je zranitelný vůči chybě, kterou Nuke program využívá). Naštěstí těchto programů existuje jen málo a zkušení hackeři nemají zájem něco takového vytvářet.

4.4.5 Distribuovaný útok (DDOS)

K útoku jsou často použity „zombie“ což jsou již dříve napadené počítače, které má útočník pod kontrolou bez vědomí jejich majitelů. Přitom může být použita libovolná záplavová technika z klasického DOS útoku, nebo i z útoků využívajících HW a SW chybu.

Nejstarší DDO

Už v době prvních záplavových DOS útoků se začaly používat distribuované útoky. Pokud totiž chtěli útočníci zahltit server o větší kapacitě linky, museli se domluvit a útočit spolu. Postupem času se způsob provádění těchto útoků velice změnil. Útočníci většinou jednají za sebe. K útoku používají takzvané zombie počítače, jež útočníci ovládají pomocí botnetů.

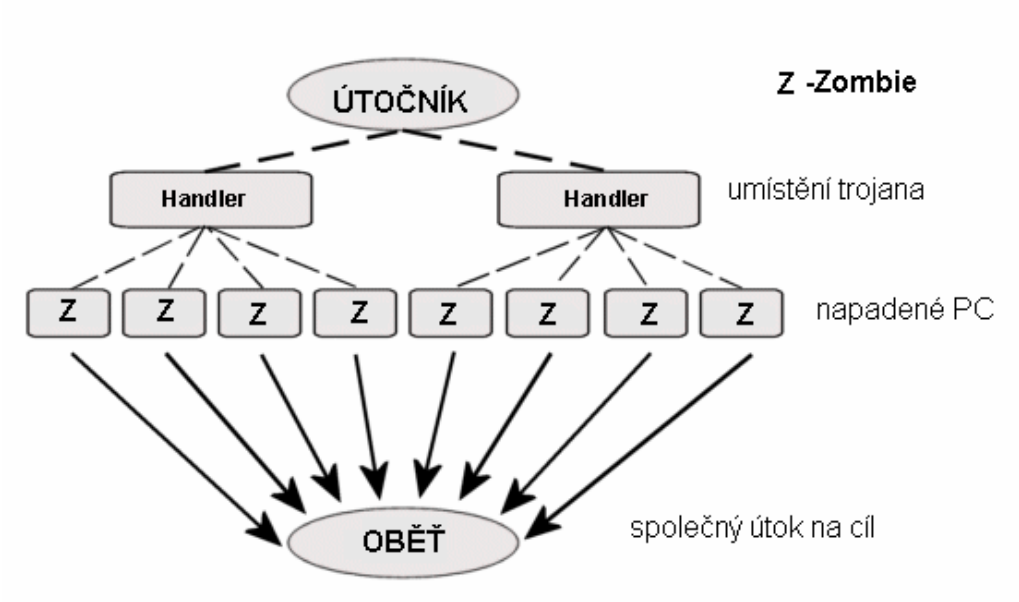


Obr. 4 *První DDOS útoky*

Příklad postupu při DDOS útoku

Útočník naprogramuje nějaký programový kód nebo trojského koně, který např. uloží na stovky serverů (Handler) s tím, že pakliže si jej uživatel stáhne (ať již vědomě nebo nevědomě), tak tento program si v uživatelově PC vytvoří tzv. *backdoors*, nebo-li zadní vrátka, přes která program naslouchá (*echo*) příkazy útočníka (*attacker*).

Všechny PC na světě, které mají v sobě tento zákeřný kód jenom čekají na den D. Ve chvíli, kdy má vše začít, všechny počítače napadané tím kódem (tzv. Zombie PC) zaútočí pomocí různých záplavových technik na cílový server, který se útočník (attacker) snaží ochromit.



Obr. 5 *dnešní DDOS útoky*

Útok pomocí botnetu

Botnety jsou sítě zombie (infikovaných) počítačů, většinou má botnet velikost stovek nebo tisíců počítačů, ve velmi extrémních případech má botnet i více jak milion zombie počítačů. Botnet často vlastní i více útočníků, motivace lidí k vytvoření vlastního botnetu jsou různé. Někdo v tom nachází zálibu a je to pro něj hra, jiný si takto zase vydělává (botnet totiž následně prodá).

Postup je obdobný jak v předchozím případu. Útočníci získávají nové počítače pomocí trojských koní, které se na počítače dostanou většinou využitím nějaké nově objevené chyby. Jakmile se trojský kůň dostane na počítač, otevře na něm zadní vrátka a připojí se na určitý IRC server, kde čeká na rozkazy. Mohou také pátrat po počítačích infikovaných různým malwarem (např. Bagle, MyDoom, Mytob) - ty otevírají některé porty a na nich naslouchají povelům zvenčí. Potom se již útočníkovi stačí připojit přes P2P (Peer to Peer) do sítě či diskusní skupiny, nejčastěji přes chatovací kanály IRC a může všem počítačům rozkazovat. Většinou napíše příkaz, který mají vykonat a na koho útočit a zombie počítače jej vykonají.

4.4.6 Reflektivní a zesilující DOS útoky

Zesilující útoky fungují tak, že pošlete data o určité velikosti a k oběti přijdou data o větší velikosti. Je tedy jasné, že tato data se musí někde "zesílit". Proto jsou zesilující útoky možné pouze u reflektivních útoků, kde se používá nějaký prostředník. Tyto útoky jsou v současné době nejsilnějšími záplavovými útoky.

Smurf

Jeho princip je podobný jako ICMP Flood, ovšem přidává k tomuto útoku zesílení. Toho je docíleno tím, že místo pingu přímo na útočníka je poslán ping na IP adresu sítě s nastavením zdrojové IP adresy na IP adresu oběti. Následně všechny počítače z cílové sítě odpoví paketem "ICMP Echo reply" oběti. Z toho vyplývá, že zesílení závisí na počtu počítačů v dané síti. Dnes existují silnější útoky, ale Smurf je stále použitelný záplavový reflektivní zesilující útok, u nějž se pohybuje zesílení až v desetinásobcích.

TTL Záplava (TTL Expiration flood)

Jedná se o reflektivní útok, jehož použití nevyžaduje si dopředu vytvářet seznam síťových zařízení, která budou využívána. K tomuto útoku se využívá hodnoty TTL (Time

to live) u IP protokolu. Všechna data, která od vás odchází, mají nastavenou hodnotu TTL. Tuto hodnotu určuje operační systém, ale dá se většinou změnit . Její hodnota může být nastavena v rozmezí 1 až 255. Data jdou dále na nějaký router poskytovatele vašeho internetového připojení. Tento router sníží hodnotu TTL o jedna a pošle je dál. Tak to jde pořád dál, než data dorazí k cíli, nebo je hodnota TTL rovna 0.

V normálním případě dorazí data k cíli a TTL je menší průměrně o 10. Jakmile některé zařízení sníží TTL z 1 na 0, tak už data nikam dál nepošle, ale pošle odesílateli zprávu, že během cesty vypršela doba životnosti (vypršel TTL) dat.Tím je ošetřeno aby zbloudilé pakety neputovaly internetem donekonečna. Tuto zprávu vám nemusí poslat všechna zařízení, jelikož jsou tyto zprávy často filtrovány firewallem.

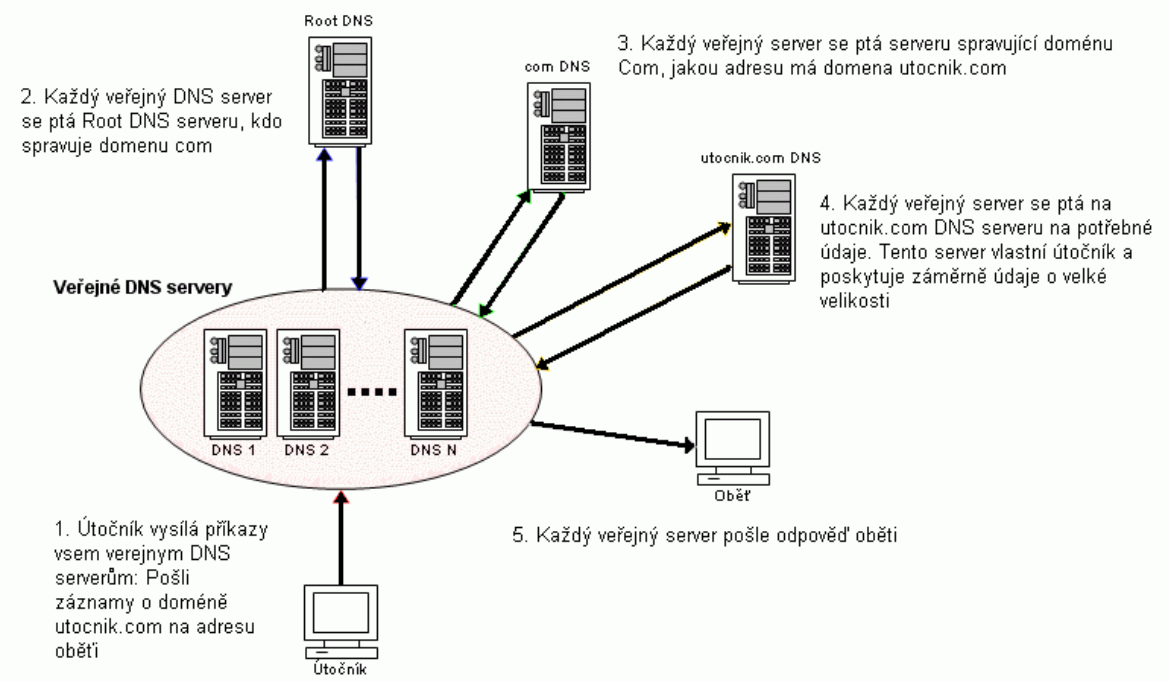
K útoku se TTL využívá tak, že se adresa odesílatele napíše na IP oběti. Jelikož ICMP echo paket, který od nás odchází, má velikost 42 bytů a při nízkém TTL (například 5) bude smazán. Oběti dojde zpráva o vypršení TTL o velikosti 70 bytů. Zesílení je tady minimální, zhruba 1,7krát. Paket kterému nevyprší TTL má po návratu 60 bytů. K vyzkoušení stačí spustit ping –l 0 –i 5 „LIBOBOLNÁ IP ADRESA“. Parametr -l 0 zajišťuje minimální velikost odchozího paketu a parametr –i nastavuje TTL.

DNS zesilující útok (DNS Amplification Attack)

Útok spočívá v posílání DNS dotazů se zdrojovou IP adresou nastavenou na IP adresu oběti. Tento útok se dá považovat za nejsilnější funkční útok, jelikož jeho zesílení může dosáhnout více jak 70 násobku původních dat. Normální DNS server pracuje s protokoly TCP a UDP. Standardně se používá protokol UDP, který umožňuje posílat DNS odpovědi do velikosti 512 B. To znamená, že pokud zažádáte o nějaký překlad, žádost má průměrně velikost 80 B (pokud se ptáte šikovně, můžete se dostat i pod 70 B), můžete dostat odpověď velikou až 512 B. Čímž získáte sedmínásobné zesílení.

Použijete-li EDNS, což je rozšířené DNS, které umožňuje odpovědi větší než 4 KB. Jak zajistit, aby byla odpověď takto veliká? Útočníci většinou nějakou doménu nabourali a vložili si tam svoje záznamy. Především používají dlouhý textový záznam, který normálně slouží jako komentář. Poté útočník vytvoří seznam veřejných relay DNS serverů, které bude využívat. Pak začne těmto serverům posílat dotazy na svoji předem připravenou doménu, u dotazů změní IP adresu odesílatele na IP adresu oběti. DNS servery budou

posílat oběti odpovědi, které budou až 73krát větší než dotazy. Tím dojde k zahlcení linky oběti. Situace je znázorněna na obrázku níže.



Obr. 6 Zesilující útok

4.4.7 Závěr

Pokud si chcete útoky vyzkoušet, dělejte to na své lokální síti. Pokud někomu způsobíte škodu- může ji po vás chtít uhradit. V případě velkých serverů to nejsou malé částky. Proti DOS útokům se brání velmi špatně a ochranný systém je navíc velmi drahý, ale lze zjistit kdo útok provedl. Aplikace NetTools4 umožňuje odzkoušení těchto typů útoků. Je ke stažení například na http://users.pandora.be/ahmadi

Útočníci se často snaží komunikovat s nezabezpečenými porty počítačů. Doporučuje se hlídat a blokovat následující porty:

- 6666 a 6667: používají se pro IRC
- 136, 137, 138, 139: umožňují komunikaci aplikacím na různých PC
- 593: umožňuje komunikaci mezi počítači na Internetu
- 445: umožňuje sdílení souborů (otevřený port zneužívá škodlivý kód Sasser, Agobot, Zotob),

- 1024 a vyšší, které bývají vyhrazeny pro volné použití.

Sledujte podezřelý provoz: celá řada útoků se projeví neočekávaným nárůstem přenášených dat. To platí jak pro datové přenosy z Internetu dovnitř, tak naopak (může jít např. o komunikaci trojských koňů nebo komunikaci botů s IRC servery).

Jeden ze způsobů ochrany je použití SYN cookies. U této metody se počáteční sekvenční číslo ISN (sekvenční číslo u paketu s příznakem SYN) kryptograficky odvozuje od IP adres a čísel portů tohoto spojení a zpět se zasílá paket SYN/ACK s tímto ISN, aniž by byla udržována fronta nevyřízených požadavků. Tím se nespotřebovává žádná paměť jako u polootevřených spojení. Klade však vyšší nároky na CPU. Přijímací strana (která má taktéž implementovánu techniku SYN Cookies) pak vezme tento SYN/ACK paket a provede tentýž kryptografický výpočet. Pokud je výsledná hodnota stejná s ISN přijatého paketu, je spojení považováno za ustanovené a pokračuje normální komunikace.

Další možnost je omezení rychlosti spojení. Uzly mohou zavést software, jenž povoluje pouze určitý počet nevyřízených zpráv v daném časovém rámci. Uzel pak jednoduše odmítá jakoukoli žádost přesahující tento limit. To má velkou výhodu v tom, že systém nebude přetížen a prostředky ochrany budou funkční. Nevýhoda spočívá v tom, že mohou být odmítnuty i legitimní pokusy o získání spojení, ale Protokol TCP se bude pokoušet posílat žádost vícenásobně a některá může projít k příjemci.

Ošetření prošlého spojení. Když se tabulka spojení zaplní právě prošlým požadavkem, některé uzly z obslužné fronty odstraňují náhodně vybrané již prošlé požadavky na spojení. Což elegantně řeší problém, neboť staré požadavky na spojení pochází s nejvyšší pravděpodobností ze SYN záplavy. Pokud je však čas odezvy na spojení, nebo rychlost požadavků na spojení extrémně vysoký- může dojít i k přerušení legitimního spojení.

Dále je potřeba zajistit, aby se samotné bezpečnostní zařízení nestalo první obětí útoku. Při výběru firewallu, eventuálně IPS, je dobré se ujistit, před čím vším dokáží ochránit a jaké na to používají metody. V tomto případě platí, že důležitý je nejen výsledek, ale i cesta k výsledku, dále: jaké metody detekce jsou podporovány, zda se pamatuje na pravidelný upgrade atd. Důležitá je i podpora formování provozu, která umožní omezit a izolovat útok. U velkého výkonu se více doporučují hardwarová zařízení - u gigabitových rychlostí je to dokonce jediná volba.

4.5 Zneužití síťových protokolů

Internet byl původně navržen pro armádu. Jeho hlavním úkolem bylo čelit výpadkům a směrovací protokoly byly vyvinuty k automatickému směrování pro případ, když k výpadku dojde. Návrh byl založen na spolupráci spřátelených uzlů, komunikujících po bezpečných linkách. Otázka bezpečnosti byla tedy druhořadá. Navíc se ani neočekávalo, že by z něj měl vzniknout tak robustní systém jaký je dnes.(problém z nedostatkem IP adres částečně vyřešily proxy servery) A komplexní systémy vždy jsou a budou náchylné k chybám.

Bezpečnostní trhliny se nachází také na síťové úrovni v takzvaném tmavém koutě specifikace. Ačkoli bylo věnováno mnoho úsilí o specifikaci standardního chování účastnických uzlů, v některých oblastech stále existuje spousta vratkého prostoru, který umožňuje různé výklady těchto standardů.

Existují dvě třídy síťových protokolů, o které se útočníci a obranné mechanizmy zajímají.

- síťová úroveň – odpovídající relační, transportní, síťové, linkové a fyzické vrstvě modelu OSI. Útočníci se snaží narušovat, podvracet a získávat informace o transportu dat od zdroje k cíli.
- aplikační úroveň – odpovídající prezenční a aplikační vrstvě. Tu se útočník nesnaží narušovat přenos, ale vytvářet přenos útočných dat k cílovému uzlu, nebo od něj.

4.5.1 Zneužití ARP

ARP Address Resolution Protocol, zajišťuje překlad fyzické adresy uzlu (též HW adresa nebo MAC adresa) na IP adresu. ARP je znám pouze na lokální podsíti, ale pokud má útočník adresu přepínače, jenž odděluje vnitřní síť od vnější, může ARP zneužít.

Záplava ARP

Útočník posílá pakety s falešnými ARP odpověďmi na přepínač. Ten pokud zjistí, že tuto ARP adresu ještě nemá v paměti, tak si ji uloží. Problém je v tom, že ji nemůže ukládat do nekonečna. Až se paměť zaplní, mohou nastat dva případy:

1. může ji buď smazat, pak pracuje v režimu hubu do doby, než zjistí informace o uzlech ve své podsíti a ty si znovu uloží do cash paměti.
2. nebo se přepne do režimu hubu a veškeré pakety, jež ještě v paměti nemá, začne posílat na všechny uzly podsítě.

Ať nastane jakýkoli scénář, útočník tím získá přístup k síťovému provozu a může pomocí slídících aplikací odposlouchávat komunikaci, která nastane uvnitř sítě. Získá adresy jednotlivých uzlů, ale často i hesla a důvěrné informace.

Předstírané MAC

Provoz na síti bude ukončen, jestliže dvě síťové zařízení budou mít stejnou MAC adresu. Aby se to nestalo, má každý dodavatel přidělen blok adres, z něhož každé síťové kartě přiřadí unikátní adresu. Občas se stane, že někteří levní výrobci použijí adresu z bloku jiného výrobce. Existuje však 2^{48} (přes 280 triliónů) možností unikátních adres a požaduje se pouze unikátnost na lokální síti.

Prakticky každý ethernetový adaptér lze přeprogramovat na požadovanou adresu. Útočník pak může přeprogramovat ethernetové adaptéry tak, že se jeden systém v podsíti tváří jako jiný systém, což způsobí ztrátu schopnosti komunikovat na obou stranách. Pokud se bude shodovat některá adresa síťové karty s adresou místního routeru - veškerá komunikace s podsítí bude přerušena.

Předstírání ARP

Předstírané ARP může být použito například k přesměrování nebo přerušení provozu. Například systém A vyšle ARP požadavek a ptá se: „kdokoli má IP adresu uzlu B nechť mi ji zašle“. Útočník sídlící na uzlu C spatří tento požadavek a může předstírat ARP s odpovědí: „já jsem uzel B zde je má IP adresa“ ale vložil by místo toho HW adresu zlu C. Uzel B samozřejmě taky odpoví. Uzel A naváže komunikaci s tím, kdo se ozve dřív. Na uzel B může být navíc použit některý z DOS útoků a tím nebude schopen odpovědět. Jeden z nejlepších nástrojů, který pomáhá proti tomuto útoku je dsniff arpspoof Dug Song.

4.5.2 Zneužití IP

IP je nespolehlivý transportní protokol používaný k dopravě všech protokolů vyšší úrovně. Kontroluje dodávku a transport, ale není schopen zjistit a ověřit, zda datagram z nějakého uzlu pochází právě z něj. Každý uzel má totiž schopnost jednat jako router.

Předstírané IP adresy

Tento problém je možný díky tomu, že poskytovatelé internetu a hraniční routery (mezi vnitřní sítí a internetem) většinou nekontrolují IP adresy které jimi prochází. Respektive neobsahují pravidla, aby adresa, která je určena pro vnitřní síť- například 178.16.12.10. nemohla projít dovnitř ani ven z vnitřní sítě. Bohužel na páteřních linkách je situace ještě horší. Protože v tom okamžiku již zdroj provozu není znám a musí být brán za legitimní. Existuje protokol RFC1918, který říká které adresy by měly být filtrovány.

Útok spočívající v předstírané adrese je útokem „střílet a zapomenout“ , neboť nemá žádnou vazbu na pakety, jež cílový počítač posílá zpátky. Ale útočník je odstíněn a může zkusit provoz mezi falešným útočníkem (předstíraným) a obětí zkusit odposlouchávat.

Daleko horší je útok generován zasláním předstíraných UDP paketů na port 7 nebo 19. Tento útok je nazýván Fraggle a jeho výsledkem je ping pong paketů mezi dvěma oběťmi právě přes výše zmíněné porty. To má za následek zesílení provozu a dává větší prostor a ochranu útočníkovi. Nejlepší obrana je samozřejmě nepovolovat porty, které nejsou potřeba pro internetové aplikace. Což tyto dva 7 a 19nejsou.

Fragmentace IP paketů

Všechny uzly musí akceptovat pakety s minimální délkou 68 bajtů, přičemž maximální velikost IP hlavičky je 60 bajtů a minimální 20 bajtů. na data zbývá minimálně 8 bajtů. IP fragmenty jsou příkladem temného místa v IP specifikaci. Potíže totiž nastávají při jejich sestavování v cílovém uzlu. Problémy nastanou například :

- Jestliže jsou přijaty duplikované fragmenty s různým obsahem. Který zachovat a který zahodit? a nebo zahodit oba?
- Právě přijatý fragment částečně přesahuje již přijatý fragment. Přitom se zde nemusí jednat o narušení. Výpadek některého uzlu mohl způsobit, že se fragment musel zaslat znovu po jiné trase a mohl být jinak fragmentován.
- Fragment má lichou délku. Je velice podezřelé když má paket lichou délku, neboť jsou fragmentovány v násobcích 8mi,. vyjma posledního.
- Fragmentace je použita k vyhnutí se firewallu. Firewall totiž mimo jiné dělá rozhodnutí podle zdrojové a cílové adresy a portu. Ale některé části fragmentů

tyto informace neobsahují a tak se nemůže správně rozhodnout. Některé Firewally to řeší poskládání původního paketu, tím ale vyčerpávají své zdroje a nahrávají útočníkům.

- Útočník vytvoří speciální fragment, který buď po složení překročí maximální velikost paketu (65 535 bajtů), tím došlo k přetečení paměti a systém mohl zkolabovat - tomuto útoku se říká *ping smrti*, nebo naopak je druhý fragment vnořen do prvního- tomu se říká *teardrop*.

Záplaty samozřejmě všechny tyto známé chyby opravily, ale stále je fragmentace hrozbou a skýtá možnost nalezení nové chyby.

4.5.3 Zneužití UDP

Hlavička UDP je velmi jednoduchá a proto se jeví jako odolná vůči zneužití. Obsahuje pouze zdrojový a cílový port, délku paketu a kontrolní součet. Záškodnická strana může napodobit všechno, takže je důležitá autentifikace.

Kontrolní součet UDP

Kontrolní součet UDP se vypočítává pouze volitelně. Pokud je toto 16tibitové pole rovno 0, znamená to, že kontrolní součet nebyl vypočítán a ani cílová strana ho nemá kontrolovat. Dříve se kontrolní součet vypínal pro zvýšení rychlosti, ale za cenu nedetekovatelnosti porušených paketů. Pro dnešní procesory nepředstavuje přepočet kontrolního nijak velkou zátěž. Proto pokud mají UDP pakety které mají kontrolní součet vypnut, jsou sporné a může se jednat o pokusy vyhýbání se detekci.

4.5.4 Zneužití TCP

Protokol TCP zavádí spolehlivou úroveň nespolehlivému IP transportnímu mechanizmu. Zajišťuje například opětovné zaslání poškozeného paketu. Přináší sebou i lepší bezpečnost, neboť je těžké předstírat, nebo napodobit TCP spojení, dokud útočník nevládne kontrolou nad routerem na trase mezi zdrojem a cílem přenosu. Provoz, který cestuje na plně ustanoveném spojení, musí být oboustranně potvrzován. Oblast, která se u TCP zneužívá jsou hlavně její příznaky. Pakety SYN a RST mohou, ačkoli by neměly, obsahovat data. A uzly bývají často zasypávány záplavami pakety SYN, nebo zpětným rozptylem.

Příznaky TCP

Příznaky v TCP hlavičce jsou: URG- naléhavý, ACK-potvrzení, PSH – posuv, RST- reset spojení, SYN- synchronizace spojení a FIN- ukončení spojení. Některé kombinace jsou vzájemně neslučitelné a různé systémy na ně reagují jinak. Tyto reakce mohou zkoumat programy jako Nmap, nebo queso za účelem analýzy náchylnosti. Mohou být použity tyto zvláštní TCP příznaky:

žádný, SYN + FIN, SYN+ RST, SYN+ FIN+ ACK, SYN+ RST+ ACK, všechny příznaky.

Záplavy SYN

Tato problematika byla probrána v kapitole DOS útoků, neboť záplava SYN pakety je jedna z jeho variant. Útok spočívá v tom, že útočník donutí systém otevřít mnoho spojení se zdrojem který neexistuje a než uplyne doba ukončení spojení (obvykle 3 minuty), jsou již vyčerpány všechny paměťové zdroje a systém oběti není schopen přijímat již žádné požadavky, nebo se zhroutí.

SYN s daty RST s daty

Běžné TCP/IP zásobníky nezasílají data v těchto paketech a ani je nemusejí zpracovávat. I když podle RFC 792 přenos dat v těchto paketech zakázán není. IDS předpokládají umělý původ těchto paketů se záměrem vyhnout se detekci, nebo spustit podvratný mechanizmus.

Předpovídání počátečního sekvenčního čísla

Potíže při s předstíraném TCP provozem spočívá právě ve složitosti uhodnout ISN, zvláště pokud paket nemůže být prozkoumán. ISN je na většině operačních systémů 32bitové číslo, které se vybírá v podstatě náhodně. Přesto na některých desktopových OS je ISN pouhou inkrementací toho předchozího. Často i TCP zásobník, jenž je součástí zařízení (například tiskáren), používá předvídatelné ISN. Ve prospěch útočníků pracují ještě dva faktory:

- Mnoho TCP služeb má jednoduše předvídatelné odpovědi a pak lze počet bajtů uhodnout s dostatečnou přesností. Útočník se dokonce může pokusit připojit před útokem a empiricky (se zkušeností) se pokusit stanovit velikost pravděpodobné odpovědi.

- Mnoho systémových prozrazení může být uskutečněno prostřednictvím jediného paketu (bez potřeby odpovědi). Oblíbenou crackerskou technikou je kompromitování náchylné služby injektáží určitého druhu zpětných vrátek. Poté se připojí k portu těchto vrátek, což nemá zpětný vztah k původnímu útoku.

4.5.5 Zneužití ICMP

Tento protokol nejde autentifikovat, takže nelze říct, zda byl přijatý ICMP z údajného uzlu, nebo ne. Útočník například může na uzel poslat paket, jenž tvrdí, že požadovaná síť je nedostupná a tím naruší komunikaci. Podobně lze narušit i komunikaci mezi dvěma uzly. Stačí jednomu (lépe oběma) poslat předstírané ICMP, že druhý uzel přestal odpovídat.

Využití ICMP k získání informací

Útočníci často hledají skulinky k získání informací o systému, na nějž se snaží nabourat. Pomocí ICMP lze například zjistit aktuální čas, nebo maska podsítě. Tyto funkce však nejsou přístupné aplikačním programům a tak je možné tyto požadavky bez následků zakázat na úrovni uzlu, nebo firewallu.

Skryté datové kanály

Tato problematika se týká všech protokolů, ale na ICMP se neprověřuje většina IDS tak důkladně a proto je k nežádoucím činnostem nejvíce využíván. Dokonce existují skryté kanály navržené speciálně jako jistý druh zadních vrátek. V případě linuxu existuje nástroj sucKIT, který tiše čeká na specifický paket na portu 4567, 6543 nebo 8765. Po aktivaci může zahájit shell s právy root na tomto systému. Detekce těchto zadních vrátek je velmi obtížná.

Pro legitimní utajený provoz mohou být data například ukryta na konci paketu. neboť ICMP pakety mají pouze 36 bajtů, nebo i méně. Rychlost datového přenosu je pak nepřímo úměrný detekci tohoto kanálu. Skryté kanály bývají často zašifrovány lehce dostupnými balíky jako PGP a SSL. Někteří zkušení útočníci mohou těchto kanálů využívat jako prostředek k utajení svých aktivit.

5 BEZPEČNOST POČÍTAČE

5.1 Penetrační test počítače

Penetrační test je online test, jenž má za úkol otestovat váš počítač před vnějšími hrozbami. A to pomocí profesionálních testovacích metod. Testovací metody jsou běžným uživatelům obvykle z důvodu vysoké ceny profesionálních penetračních testů těžko dostupné. Pomocí nabízených nástrojů můžete odhalit slabiny vašich systémů, lokalizovat problémy jejich zabezpečení a získat podrobné informace o nalezených slabých místech. To vám umožní účinněji ochránit firemní data před možným zneužitím či poškozením crackery. Řada společností nabízí základní testy zdarma. Protože u uživatelů, kteří počítač zabezpečený nemají najde test slabiny, které vám firma pomůže odstranit. Většina firem je však poměrně drahá a ochrana osobního počítače nemusí být problém ani pro začátečníka.

5.1.1 Testování mého počítače

Můj počítač běžící pod OS Windows XP professional se SP2 a nainstalovanýma záplatami, antivirovým programem NOD32. Omylem jsem nemel zapnutý firewall. Výsledky ve 2 testech byly 100% a v jednom bylo zjištěné napadnutí DNS. Proto jsem se rozhodl nainstalovat Firewall Outpost profesional, a provést testy znovu.

1. Test

Proveden z internetové stránky www.test.bezpecnosti.cz. Tento test je velmi rychlý a prověřil 19 možných napadení. Výsledky byly v obou případech (s vypnutým i zapnutým FW) 100%. Následné prověření na možnost napadení trojskými koni bylo také 100% zabezpečeno. Následovala zkouška antivirového programu na vzorek viru. Ten systém NOD32 zachytil a bránil jeho uložení na disk počítače. Tím jsem odzkoušel všechny testy zdarma na této stránce s vědomím, že mám počítač ochráněn, před hrozbami, které byly testovány..

2.Test

Nyní jsem vyzkoušel test společnosti symantec. (http://security.symantec.com) Je komerčně založen (říká že pouze jejich programy chrání před všemi hrozbami), ale obsahuje testovací metody z mnohaleté praxe v oblasti bezpečnosti a proto je dobré jej vyzkoušet. Všechny 3 částí byly 100% zabezpečeny, ale kontrola antiviru vyžadovala IE 5

a vyšší s nástrojem Aktive X.Tak jsem musel test pustit znova v mém IE 6. A výsledek? Test nebyl úspěšný z důvodů chyby na serveru. S doporučením zkusit test znova později. Tak to děkuji. Společnost symantec nabízí i oline hloubkovou kontrolu virů v počítači. Po hodině prohledávání nalezl několik souborů, které byly většinou dokumenty s povolenými makry, nebo programy, které jsem si nainstaloval na luštění hesel. Jen trojský kůň v souboru total commander by nemusel být planý poplach.

3.Test

Z velkého množství firem nabízející penetrační testy jsem zvolil společnost Paranoia (http://www.paranoia.cz/), jež nabízela velmi zajímavý test, jehož výsledek mi byl doručen na e-mail. Během testu bylo mé internetové spojení na chvíli přerušeno. Test bez zapnutého firewallu, zde nebyl 100%. A bylo nalezeno možné napadení DNS pomocí takzvaného „poinson atack“ přes UDP protokol. Po přečtení možných důsledků mi bylo doporučeno nainstalovat záplatu řešící tento problém. Test dopadl stejně i s firewallem. Proto jsem opakovaně četl problém a došel k závěru, že mě se tento problém netýká. Software bind nepoužívám a veškeré vzdálené přístupy mám zrušeny. Zaujala mě možnost odposlechu mé linky a jestli je možné „odříznout“ mě od poskytovatele internetu.

Na stránkách této společnosti je i několik zajímavých nástrojů na zjištění informací o IP adrese, nebo černý seznam IP adres. Velice jednoduché na ovládání a přitom se dají zjistit zajímavé informace.

5.1.2 Test internetového prohlížeče

Při hledání testů jsem naleznul stránku security (http://www.vyvial.cz/security/index.php) Byly na ní odkazy na mnou již provedené testy a spousta zajímavých informací. Zaujala mě možnost otestovat svůj internetový prohlížeč. První jsem vyzkoušel Mozilu Firefox 1.5. Bylo testováno 12 známých náchylností a žádná nebyla úspěšná. Poté jsem zkusil otestovat Internet Explorer 6. Z 22 známých chyb byly objeveny 2 nezabezpečené. Z toho 1 velmi vážný a jeden střední. Oba se týkaly možného spuštění odkazu a nainstalování škodlivé aplikace při prohlížení stránek, nebo e-mailů. Bylo mi doporučeno stáhnout si aktualizaci IE SP 2.

5.1.3 Závěr

Testy bezpečnosti počítače jsou vhodné pro informativní charakter. Pokud váš počítač používá základní prvky jako jsou antivirový program firewall a aktualizovaný systém, pak vás výsledky jistě mile překvapí. Pokud však dopadnou velmi špatně, je potřeba najít chybu, nebo se poradit s kvalifikovaným pracovníkem.

5.2 maskování IP adresy

Jak souvisí tato činnost s každodenní bezpečností? Firewall vás však ochrání jen (je-li správně nakonfigurovaný) před neschváleným provozem z a do počítače. Nezabrání například, aby při běžném přístupu k webových stránkám zanechal otisk vašeho čtenářského palce slušně širokou stopu v logovacím souboru serveru, na kterém se stránka nachází. Taková vizitka může čítat mnoho desítek řádků s popisem, co a kdy jste četli, odkud jste sem přišli (případně kam dále jdete), verzi vašeho operačního systému, prohlížeče, nastaveném počtu barev a rozlišení... Zejména však vaši IP adresu, která vás jednoznačně identifikuje, ať jste připojeni pevnou linkou, kabelem, wi-fi přípojkou či dial-upem. Proto si myslím, že je potřebné se chránit a poskytovat o sobě na internetu co nejméně informací.To, co lze o vás vyčíst z IP adresy, si můžete zkusit na následujících dvou odkazech.

http://www.ripe.net/fcgi-bin/whois

http://www.2privacy.com/cgi-bin/PC_Browser_Privacy_Test.pl

5.2.1 Způsoby skrytí IP adresy:

-IP spoofing (střílení naslepo)

Všem odchozím paketům je změněna Zdrojová IP adresa a jsou poslány k cílové adrese. Pokud je Změněná IP adresa neplatná, může tento paket být považován za neplatný a zahozen. Pokud existuje - odpověď je poslána na tuto adresu. Nelze tímto způsobem navázat spojení, pouze poslat příkaz, na který dopředu víme odezvu, nebo pro záplavové útoky naslepo. Na tento počin je potřeba stáhnout přímo hackerské nástroje, nebo si napsat svůj. Programy pro změnu MAC adresy jsou například SpoofMac a smac20. Existuje jich samozřejmě více.

-Redirect (přesměrování)

K přesměrování je možné použít například některý z otevřených proxy serverů-těch funguje v internetu veliké množství a není ani velký problém najít stránky, které je evidují, například http://az.ru/tophacker/Proxy.htm nebo http://tools.rosinstrument.com/proxy/. Je však nutné upozornit, že v řadě případů je jejich otevřenost způsobena spíš neznalostí administrátora než záměrem, takže jejich použití lze považovat spíše za zneužití.

Crackeři si samozřejmě najdou více nechráněných, nebo málo zabezpečených serverů, přes které budou své činnosti maskovat. A majitelé těchto serverů nebudou nic vědět.

5.2.2 Internetová anonymita

Pro běžné uživatele jsou zde tři možnosti jak mohou dosáhnout anonymity. Všechny mají své výhody a nevýhody. Princip spočívá v odstranění HTML hlaviček (jež obsahují údaje o zdroji paketu) a změně hodnoty IP adresy. Druhá strana mince může být to, že se může jednat o vládní projekty, které mají ulehčit monitorování různých internetových živlů. A každý server si musí dělat záznam (log) o komunikaci, která přes něj putuje. Navíc poskytovatel internetového připojení, ke komu se připojujeme. Takže naprostou anonymitu můžeme získat možná pomocí notebooku, který připojíme k nějaké nezabezpečené privátní síti. Nebo pomocí připojení přes mobilní operátory. Pokud o vás má váš poskytovatel informace a on je má, tak nikdy nedosáhneme 100% anonymity.

Specializované aplikace – většinou jednoúčelové programy, které se instalují na klientský počítač a dovolují maskovat surfařovu identitu. Patří sem například program JAP (http://anon.inf.tu-dresden.de/index_en.html), GhostSurf 2005 (http://www.tenebril.com/consumer/ghostsurf/ghostsurf_standard.php) , HideIP (http://www.hide-ip-soft.com/),Tor (http://tor.eff.org) a další. Liší se hlavně v rychlosti, úrovni anonymity a ceně. Zda opravdu dokáže zakrýt všechny stopy je diskutabilní. Někdy naopak může anonymita přitahovat více pozornosti. Prohlížeče mají navíc implementované "persistent storage", pak může webmaster každého návštěvníka označkovat a jednoznačně ověřit jeho identitu.

Veřejné proxy brány – volně dostupné servery, jichž lze využít pro surfování Internetem a které pomáhají při utajení. Stačí k tomu mít oprávnění pro změnu konfigurace webového prohlížeče a nastavit odpovídající IP adresu, samozřejmě doplněnou o číslo portu. Aktualizované seznamy si prolistujte například na Publicproxyservers.com či

Samair.ru. Posledně jmenovaný seznam rozlišuje jednotlivé proxy servery na "anonymous" a "elite", které se liší v míře utajení. Lze použít také MultiProxy www.multiproxy.org, avšak si musíte sehnat seznam high-anonymity proxy serverů, tyto se často mění. MultiProxy funguje jako běžná lokální proxy s tím, že má navíc celkem dobrou správu vložených proxy serverů (testování na rychlost a další věci) Ačkoliv jsou seznamy anonymních proxy zpravidla velice obsáhlé a přehledně strukturované, nalezení funkčního a pro příjemné surfování dostatečně rychlého serveru bohužel může zabrat hodnou chvíli. Srovnáme-li míru utajení se specializovanými aplikacemi, veřejné proxy servery sice nevyžadují instalaci žádného programu, nicméně jejich schopnosti odstranění hlaviček jsou zpravidla na mnohem nižší úrovni.

Webové anonymizéry –stránky WWW, které zprostředkovávají anonymní přístup na cílový server. Existují jak zdarma a bez netnosti registrace, které jsou však velmi pomalé a nebo placené verze těchto speciálních serverů. Ty poskytují lepší služby. Mezi webové anonymizéry patří například:

www.Anonymizer.com

www.Proxify.com

www.Anonymouse.org

5.3 Ochrana dat kryptografií

Elektronická komunikace a úschova dat v elektronické podobě patří mezi základní trendy dnešní doby. Vzhledem k tomu, že se jedná často o citlivá data, ať už se jedná o osobní údaje, firemní data apod., je potřeba zajistit jejich co nejlepší ochranu. Používá se kombinace fyzické (zámky, ochranka, ..) a logické (autentizace, šifrování, ..) ochrany. I v té nejlepší ochraně může trpělivý útočník nalézt skulinku a dostat se k našim datům. Pokud však budou zašifrovaná a nebude je moci dešifrovat, budou pro něj bezcenná. V dnešní době existují metody, které lze považovat za nezlomitelné. Šifry rozdělujeme na symetrické a asymetrické. U symetrických šifer je použit jeden univerzální klíč a u asymetrických jsou klíče dva. Šifra je silnější, pokud použijeme delší klíč, ale pak také narůstá čas potřebný pro kódování.

5.3.1 Symetrické šifrování

U tohoto druhu šifrování klíč, který byl užit k zašifrování zprávy na straně odesilatele ,bude užit i na straně příjemce pro dešifrování zprávy. Z toho vyplývá nutnost před začátkem komunikace předat důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji (konkrétní typ algoritmu) druhé straně. Pro tento přenos klíče se používá také asymetrické šifrování. Jedna z pouček říká, že algoritmus založený na tom, že není zveřejněno, jak pracuje, je nedůvěryhodný.

Současná komerčně dostupná výpočetní technika aplikuje tyto algoritmy (např. DES, TRIPLEDES, IDEA) téměř v reálném čase. Na druhé straně i nejmodernější výpočetní technika je schopna dešifrovat data bez znalosti příslušných klíčů jen za relativně dlouhé časové období a s velkými finančními náklady. Volbou délky klíče lze navíc tento výsledek výrazně ovlivnit. Při použití klíče s délkou 40 bitů je možné zdolat šifru za pomocí paralelního algoritmu s použitím 1200 propojených počítačů za necelé 4 hodiny. Doba rozkódování z délkou klíče roste velmi rychle (128 bitů - 1000počítačů a 3.10exp22 let). USA, které jsou na špičce v šifrovacích technologiích většinu algoritmů a technologií patentovala, a tím omezují vývoz. V současné době je povoleno užití délky klíče 56 bitů. Podle mého názoru z důvodů rozšifrovatelnosti americkou vládou.

Použití symetrických algoritmů představuje způsob, jak zabezpečit důvěrnost transakcí definovaným způsobem s možností přesného stanovení hrozeb, kterým toto zabezpečení odolává. Tyto algoritmy však neřeší důležitý požadavek neodmítnutelnosti odpovědnosti. Nelze totiž určit, která strana zprávu odeslala a která přijala. Proto tento způsob není tak populární, jako asymetrické šifrování. Těchto šifer využívají například programy HyperCrypt, ScriptCrypt, TrustPortEncryption a mnoho dalších.

5.3.2 Asymetrické šifrování

Tento způsob šifrování je velmi oblíben. Jedná se o velmi bezpečnou a pohodlnou metodu, kterou podporují mnohé aplikace a uživatel pak „skoro“ nepozná, že komunikace je šifrována. Asymetrické šifrování je úzce spjato z digitálním podpisem pro ověřování totožnosti. Navíc je často kombinováno se symetrickým šifrováním, protože tím se značně urychlí celý proces.

Jak funguje asymetrické šifrování? Zpráva je na straně odesilatele nejprve podepsána (svým privátním klíčem), podepsán je čitelný text zprávy, a potom šifrována

(veřejným klíčem příjemce). Na straně příjemce je zpráva nejprve dešifrována privátním klíčem příjemce, čímž je zajištěna adresnost zprávy a teprve potom je pomocí veřejného klíče ověřena identifikace odesilatele. Tak je zaručena důvěryhodnost (zdroj mohl šifrovat pouze unikátní majitel popisu) i utajenost (zprávu dešifruje pouze příjemce svým privátním klíčem).

V praxi je situace obvykle složitější. A to z důvodů potřeby urychlit velmi pomalý proces asymetrického šifrování. Proto se na zprávu používá takzvaná hashovací funkce, která rychle z jakéhokoli množství dat spočítá jednoznačný řetězec pevné délky. Ten pak spolu s digitálním podpisem slouží k ověření totožnosti a zaručuje neporušenost obsahu. Zpráva se zašifruje symetrickou metodou a až k přenosu důvěrných informací je použita asymetrická šifra.

PGP -Pretty Good Privacy

Tento velmi známý a rozšířený nástroj nám, jak již název vypovídá, zaručuje „velmi dobré soukromí“. Byl naprogramován Hilipem Zimmermannem s pomocí dalších autorů v roce 1990 a je vyvíjený do současnosti. Jeho zdrojové kódy jsou volně ke stažení (OpenPGP). Avšak existuje spousta komerčních, ale uživatelsky přívětivých verzí. Velmi dobrá česká stránka věnující se PGP je (*http://www.pgp.cz/)*

Pomocí nástroje PGP pak můžete jednoduše a pohodlně šifrovat celý svůj disk a veškerou poštu. Důležité je důkladně zabezpečit svůj privátní klíč. Protože při jeho vyzrazení je jakkoli silná šifrovací metoda k ničemu. Váš veřejný klíč si vystavte na webu Váš soukromý klíč si mimořádně pečlivě uschovejte a nikomu jej nedávejte! Tento klíč se nachází uložen na pevném disku. Uživatele linuxu to v tomto případě mají se zabezpečením lepší, protože práva root nemá každý uživatel. Ve windows se pak obvykle klíč nachází ve složce C:\GnuPG\ proto by se složka s klíčem měla lépe zabezpečit a uživatelé by pokud možno neměli pracovat jako administrátoři.

Je také velice vhodné si vytvořit "revoke certificate". K čemu to je? Pokud zapomenete PassPhrase, nemůžete klíč dále používat, nicméně, tento dále zůstává na veřejných serverech. Jedinou možností, jak jej zrušit, je vystavit si "Revoke certificate", a ten potom nahrát na server. K jeho vystavení je potřeba znalost PassPhrase. Revoke certificate (soubor revoke_my_key.asc) si potom pečlivě uschovejte, kdokoliv, kdo k němu má přístup, může totiž příkazem gpg --send-keys Váš klíč znekvalitnit!

5.4 Analýza dat

Aby byla možná alespoň základní úroveň analýzy, je potřeba pakety shromáždit a dekódovat. Fragmentované je potřeba znovu sestavit a také TCP proudy je potřeba znovu sestavovat. U složitějších se potom filtrují nežádoucí vstupy, aplikují se firewallová pravidla, spouštějí se detekční rutiny a procedury.

Záchyt paketů a jejich předání další komponentě.

Filtrování. Není nezbytné zachytit všechny pakety. IDS dokáže zachycené pakety roztřídit podle jisté logiky, založené na charakteristikách, jako je typ paketu, rozsah zdrojových IP adres a další.

Dekódování paketů. Pokud paket nelze správně dekódovat, je zahozen. Jinak lze zjistit, verzi IP, zdrojová a cílová IP adresa a podobně.

Ukládání. Dekódovaná data se ukládají do jednoho nebo více souborů. Ty pak slouží k vyhledání řetězců, nebo rozboru. Problém je v tom, že dat je obrovské množství, což způsobuje nutnost správy volného místa a nutnost třídit data.

Znovusestavení fragmentů. Děje se tak kvůli zamezení mnohých problémů a útoků, jenž fragmentace využívají. Výhodné je použít selektivní sestavování, kde o každý druh protokolu se stará jiná služba.

Opětovné **sestavení proudu**. To znamená narovnat pakety za sebou počínaje SYN a konče RST nebo FIN/ACK. Sestavení proudu je důležité v případech, kdy pakety nedochází v pořadí ,v jakém byli odeslány.

Inspekce stavů. Útočníci se často snaží vyrobit speciální pakety, jenž se tváří jako součástí některé relace, nebo smyšlené potvrzení provozu. Proto IDS a IPS používají tabulky, do kterých ukládají data o ustanovených relací. Pak porovnávají pakety, které se vydávají za součást relace s daty v tabulce. Pokud nenaleznou záznam pro daný paket - je vypuštěn.

IDS a IPS by měl používat vlastní firewall pro ochranu před napadením a vyřazením z provozu. Mnoho detekčních systémů ho však nemá kvůli zpomalení výkonu. Dobré je použití vnitřního hlídacího časovače do systému. Ten pak v určitých intervalech kontroluje jestli IDS/IPS pracuje normálně.

5.4.1 Typy detekce:

Porovnání signatur. Zaměřuje se na vyhledání známých útočných řetězců. Bohužel existují modifikace těchto útoků. Pokud nový útočný řetězec není nalezen v knihovně signatur, pak není detekován. Obrovské databáze signatur se stávají pomalé.

Porovnání pravidel. Tato metoda přináší jistý příslib, neboť je založena na kombinaci určitých pravidel. Například mnohonásobné neplatné přihlášení, nebo opakované zadávání „cd..“ na FTP. Obecně stačí malá množina pravidel na pokrytí mnoha útoků. Jsou dobré na detekci nových variací zneužití (ne na zcela novou metodu).

Porovnání založené na profilu. Vychází z charakteristik uživatelů. Informace o uživateli, jako jsou stránky, na které se připojuje, množství dat, doba kdy je připojen a mnoho dalších zvyklostí. Pokud se některá činnost výrazně liší od obvyklého stavu, pak je vygenerována výstraha o narušení. Opět vhodné na odkrývání nových útoků, ale chytrý a trpělivý útočník může systém obelstít.

Detekce zhoubných kódů. IDS/IPS pracuje podobně jako antivirový program a porovnává známé vzory zhoubných kódů. Avšak jejich spolehlivost není dostačující.

Výstup z IDS/IPS. Systémy ochrany v případě rozpoznání útoku vydají varovná hlášení obsluze a mohou se pokusit o blokující činnost. Systém předá informace do firewallů a filtrů, aby zablokovali veškeré pakety z útočných IP adres. IDS se může pokusit o zrušení relace zrušení relace vysláním RST paketu. Bohužel nemusí k cíly vůbec dorazit. Rovněž hlídá systémové soubory před opakovanými pokusy o přepsání. Útočníci používají většinou falešné IP adresy a ukončování relací a blokování paketů může snadno přejít v DOS v systému, na kterém IPS/IDS pracuje.

5.4.2 Datová korelace

Obecně datová korelace hledá společné vztahy mezi událostmi. Pokud existují, snaží se určit jejich význam. Sdružuje například:zdrojové a cílové IP adresy, identifikovatelná síťová trasa, zadaný příkaz a čas, kdy akce začala a skončila. Tyto události mohou například poukazovat na začínající útok. Útočník totiž nejdříve zjistí slabiny systému a poté začíná útočit na tyto části. Přitom pokud by se jednalo o tutéž IP adresu, byl by to zjevný útok a bylo by potřeba provést příslušná opatření. Existují automatizované metody korelace dat. Bohužel jsme v praxi málo využívány. Přitom pokud

je datová korelace provedena správně, vede k hlubším úrovním pochopení a také usnadňuje proces odezvy na incidenty, které se odehrály. V systému příští generace detekce a prevence proti narušení by neměl chybět nástroj schopný korelovat události pomocí analytických jednotek, které jsou svázány nejen na senzory, ale také s velkými databázemi známých a podezřelých incidentů.

5.4.3 Incidentní odezvy

IDS se dá nasadit do provozu ve dvou případech. Jako detekce útoků - pak jsou senzory umístěny před firewallem. A jako detekce narušení, kdy jsou senzory uvnitř sítě(za firewallem) Existují tři typy odezev:

Automatické odezvy- kde reaguje IDS/IPS pomocí naprogramovaných metod. Jako jsou odstřelení relace (vysílání reset bitu na oba konce spojení), zrušení spojení (konec veškeré komunikace- firewall), přiškrcení spojení (ochrana před skenováním portů), vyhýbání se (odepření přístupu útočícímu systému) a další. Novinkou na poli odezev je IDIP (infuzně detekční a izolační protokol). Dále existuje nástroj DOSTrack, jenž běží na routerech a provádí automatické sledování paketů zpět ke zdroji.

Ruční odezvy- zde je zapotřebí mít platnou metodologii postupu a tým profesionálů, kteří se budou o bezpečnost starat.

Hybridní odezvy- jsou nejlepším a také nejběžnějším řešením. Automatické odezvy jsou sice výborné, ale je stále lepší tyto odezvy přezkoumat lidským rozumem.

Při řešení incidentů je důležité mít vše připraveno předem. Protože rychle vzpomínat, co vše člověk potřebuje a hledat například ochranné nástroje, vede zaručeně ke zmatku a opomenutí některého kroku. Je dobré například vědět, jak dlouho může být systém odpojen od sítě, aniž by došlo k vážným obchodním ztrátám. Mít po ruce SW a utility pro obnovu systému a vlastní odezvu. Všechny důležité informace by se měly zálohovat na jiný server, kdyby se v důsledku útoku jeden stal nepoužitelným. Doporučuje se také vytvoření formuláře, do kterého se zapisují kontaktované osoby, napadnuté systémy a sítě. Důvody a důkazy útoku. Rovněž se doporučuje nahlášení incidentu na *www.cert.org*.

5.5 Programy na zachytávání síťového provozu

Jsou to aplikace, které dokáží všechny pakety zachytit a prozkoumat, výpis mohou provádět na obrazovku v reálném čase, ale to je prakticky nepoužitelné z důvodů obrovského množství dat. Proto je vhodné veškerou vstupně výstupní komunikaci zaznamenávat do speciálních souborů na pevný disk. Což pochopitelně klade vysoké nároky na kapacitu úložného prostoru a výsledná orientace v takovémto souboru také není jednoduchá práce. Existují však programy, které pomáhají výsledky třídit a usnadňují tak namáhavou práci bezpečnostním analytikům.

5.5.1 Tcpdump

Vynikajícím nástrojem je program Tcpdump, jenž je dokonce považován za jeden z prvních IDS. Dokáže zachytávat všechny formy síťového provozu (navzdory jeho názvu). Nástroje z řady Tcpdump pak pomáhají práci z datovými výstupy. Standardně program Tcpdump pracuje v řádkové konzole a je potřeba znát příkazy pro jeho ovládání. Ty jsou přehledně uspořádány v nápovědě *(http://www.tcpdump.org/)* Existuje také modifikace pro windows , jenž se nazývá Windump. Pokud chceme například zaznamenávat veškerý provoz stačí napsat příkaz:

tcpdump –w provoz.cap ukončen bude stiskem kombinace Ctrl+break

Samozřejmě lze napsat dlouhý příkaz plný specifikací na jednotlivé protokoly a včetně ukončovací podmínky. Samotný soubor je však pro uživatele nečitelný a je potřeba jej otevřít například v programu Ethereal.

Velkokapacitní záchyt dat

Ačkoli jsou možnosti jednoduchého nástroje Tcpdump široké, své nejčastější uplatnění nachází právě jako ukladač síťového provozu. Tento záznam se pak může použít například na offline detekci, nebo analýzu. Což má velké výhody hlavně v ušetření zátěže procesoru. Náročné detekční mechanizmy IDS a IPS jsou často vypouštěny, aby se předcházelo DOS útoku. tyto „odlehčené“ systémy pak v případě narušení přijmou opatření a k prošetření se využívá právě zachycený soubor. Navíc slouží jako důkaz o útoku.

5.5.2 Práce s uloženými soubory

Pokud má útok soudní dohru, jsou data z těchto souborů klíčovými důkazy. Je však potřebné je uspořádat do přehledné a zkrácené formy. K tomuto účelu mohou sloužit tři programy.

tcpjoin- umožňuje spojení několika tcpdump dohromady

tcpslice- jenž umí vytvářet menší části

tcpflow- umí vytvořit datový výstup TCP relací ze zaznamenaných souborů

Tcpjoin

Pokud nastane situace, kdy spojení, o něž se zajímáme, začíná v jednom souboru a pokračuje v druhém, je vhodné použít právě tento program. Umí spojit dva soubory s ohledem na časové známky jednotlivých paketů a může výsledek uložit do specifikovaného souboru.

Tcpslice

Na frekventovaných stránkách se velikost zachycených souborů může vyšplhat do stovek Megabajtů, nebo dokonce Gigabajtů, čímž se jakákoli práce s těmito daty stává časově náročnou a nepřehlednou záležitostí. Tcpslice umí v souboru dělit data v závislosti na počáteční a koncové časové známce. Často se totiž stane, že IDS spustí výstrahu například o otevření portu, který má zůstat zavřený (TCP port 1524). Avšak analytik potřebuje vědět, jaká aplikace nebo služba byla zneužita a umožnila přístup na tento port. Navíc musí jednat rychle, protože mohou být napadeny stejným způsobem i ostatní systémy v instituci.

Proto použije program tcpslice a vyhledá v zachyceném souboru část 10 minut před a 5 minut po události, čímž zredukuje množství dat, která bude muset prozkoumat. Tcpslice je díky inteligentnímu vyhledávacímu algoritmu velice rychlý a vytvoří nový soubor, který obsahuje požadované data.

Tcpflow

Při útoku na prezenční a aplikační vrstvu jsou záznamy plné dat ze síťové a transportní vrstvy na obtíž. Tcpflow je navržen tak, aby vytahoval z TCP protokolu pouze datové bajty a rozčleňoval je do souborů. A to tím způsobem, že každý tok je uložen zvlášť pro odchozí a příchozí provoz. Včetně paketů zaslaných vícekrát, překrývajících se

fragmentů a pořadí doručení. Data v těchto souborech nejsou proložena, ale všechna data jedné strany jsou sekvenčně uložena do svého souboru. V mnoha případech je posloupnost událostí zřejmá, ale v některých sporných situacích je možno časové otázky dořešit pomocí časové známky paketu.

5.5.3 Ethereal network analyzer

Další program, jenž jsem vyzkoušel, je Ethereal network analyzer. Monitoruje síťový provoz a utváří různé statistiky. Program pracuje v grafickém rozhraní a má tak přívětivější prostředí pro uživatele. Navíc je k dostání zcela zdarma. A to jak jeho zdrojové kódy, tak již celé aplikace pro systémy unix nebo windows. Na domovské adrese této aplikace *(http://www.ethereal.com/)* je možnost stažení aktuální verze, manuálů a spousta dalších informací. Doporučuje se kombinace tohoto programu s aplikací winPcap, jenž je podobná aplikaci tcpdump.

Program Ethereal je jednoduchý na používání. Je k němu potřebná základní znalost protokolů, s nimiž hodláme pracovat a problém může nastat také při vytváření nových pravidel pro filtry. Použití těch již přednastavených je triviální. Umí otevírat výstupy mnoha zachytávajících aplikací a dále je programově zpracovávat, editovat a konvertovat. Je schopen detekovat a analyzovat přes 450 protokolů. A to díky své volné licenci. Tak mohou uživatelé, kteří pracují a rozumí protokolu, jenž ethereal neovládá, pomoci k jeho implementaci. A stát se jedním z mnoha lidí (disektorů), kteří přispívají k rozvoji této aplikace.

6 VYHODNOCENÍ PROJEKTU

Mým úkolem bylo zpracovat oblast počítačové bezpečnosti se zaměřením na detekci a prevenci. V této kapitole se zaměřím na analýzu bezpečnostních rizik, návrhy zabezpečení pro firmy a jednotlivce. Budu se věnovat i implementaci IDS a IPS systémů, které se nejvíce skloňují s detekcí a prevencí a představují oblast, která se vyvíjí a jednou bude takovou samozřejmostí jako například firewall.

6.1 Analýza bezpečnostních rizik

Tvrzení, že počítačové sítě internetu jsou plné zákeřného kódu, je zajisté pravdivé. Ale do jaké míry se musíme těchto škůdců a útočníků obávat? Největším nebezpečím pro obyčejné uživatele a malé firmy nejsou zákeřní crackeři, nebo ziskuchtivý útočníci. Největším nepřítelem je neznalost. Začínající uživatel snadno ze svého výkonného počítače během několika měsíců udělá neuvěřitelně pomalý stroj. Jak to souvisí z bezpečností? Pomalý je totiž proto, že se mu do systému dostaly viry, červi a další programy, jenž mu odebírají zdroje a tím výkon počítače. Zákeřný kód obyčejně nesmaže disk nebo nezničí HW počítače. Pouze obtěžuje, případně čeká a naslouchá, jestli mu jeho tvůrce nezadá další příkazy. Tvůrci však často tyto programy dělají jako žert a použijí je na své kamarády. Navíc, proč by měl tvůrce z Ameriky mít zájem o přístup do počítače v České republice?

Tím se dostávám k druhému bodu. Tvorbou virů a zákeřného malwere se zabývají hlavně náctiletí. V Americe se jim obecně říká „scrip kidies“ a tento výraz je spíše hanlivého charakteru. V angličtině totiž existuje spousta návodů a nástrojů, které se dají pro tento druh činnosti použít. A tak i ten, kdo s počítačem moc neumí, může nadělat spoustu problémů bezpečnostním expertům. Navíc náctiletí nejsou ještě plně trestně zodpovědní
a mnohokrát ani neví, jaké důsledky jejich aktivity mají.

Obecně však platí, že čím je daný objekt na známější, tím větší pozornost má také od útočníků. Ale velké nadnárodní korporace mají dostatek finančních prostředků pro tu nejlepší technologii a to má i velký odstrašující efekt. A pokud člověk vlastní něco cenného uvnitř svého počítače, měl by jej zabezpečit tak, aby se útočníkovi nevyplatilo zábrany zdolávat.

6.2 Návrhy zabezpečení

Je těžké navrhnout univerzální řešení bezpečnosti. Každý systém má svá specifika a proto je potřeba přizpůsobovat bezpečnostní systémy těmto uživatelským potřebám. Je potřeba si položit základní otázku, jak moc je pro každého bezpečnost důležitá a kolik finančních a časových prostředků je pro ni schopen investovat. Uvedu zde několik možných řešení od těch nejlevnějších a nejjednodušších, až po opravdu silné a drahé komplexní bezpečnostní systémy. Při jakémkoli zabezpečení je potřeba dbát na zálohování. Ať už se jedná o systémové soubory, citlivá data, software, nebo soubory, o které bychom neradi přišli. HW, nebo SW se může porušit, ať už vlivem útoku, počasí, nebo stářím. Zálohu můžeme provést na jiný disk, DVD, magnetickou pásku, nebo jakékoli jiné médium.

6.2.1 Minimální ochrana, maximální výkon

Při zjišťování, co lidé považují za minimální ochranu, jsem se setkal z různými názory. Někteří považují antivir i firewall za zbytečnost, jiní ne. Dříve jsem používal neaktualizovaný operační systém bez firewallu. Před nebezpečím mě chránil pouze antivirový program. Ale protože jsme navštěvoval nedůvěryhodné stránky a odkazy, měl jsme vždy problémy se spywarem. Pokud člověk dodržuje bezpečné zásady pohybu po internetu, může mu opravdu stačit pouze aktualizovaný operační systém Windows XP, nebo lépe Windows Vista, případně Linux. Součástí těchto systémů jsou bezpečnostní balíčky, které jsou jednoduché na obsluhu a poskytují základní ochranu. Čím méně programů do systému nainstalujeme, tím bude pracovat rychleji. Pak si každý bude muset dávat větší pozor při „výletech“ do světa internetu.

6.2.2 Optimální řešení pro domácí použití

Osobně používám následující kombinaci prvků a považuji je za ideální. OS Windows XP proffesional, antivir nod32 firewall Outpost, který má i prvky IDS. Tento firewall mám teprve chvíli a jeho možnosti nastavení jsou opravdu široké. Ani toto řešení samozřejmě není neprůstřelné a jednou za určitý čas je vhodné disk prověřit nástroji na vyhledávání škůdců a provést úklid počítače. Přitom při každodenním aktivním používání, stahování
a instalaci nových programů a brouzdáním internetem se nevyhnete nutnosti přeinstalování

celého operačního systému. Já provádím kontrolu a čištění počítače jednou za měsíc a jeho generálku v podobě zformátování disku (výborný nástroj je System Mechanic) a opětovné instalaci všech programů jednou ročně.

6.2.3 IDS/IPS Snort

Snort je zdrojově otevřený nástroj pro detekci síťových průniků a anomálií. Jednoduše se používá a není nákladný na provozování. Tento detekční nástroj je neustále zdokonalován. Jeho hlavní nedostatky byly velmi četné falešné poplachy, náchylnost na útok typu DOS nástrojem Stick a jeho malá schopnost identifikovat řadu útoků. Databáze pravidel je již mnohem větší a záplaty na nalezené chyby jsou ke stažení na domovské stránce produktu (*snort.org*). Četnost falešných poplachů byla již také snížena a navíc se mohou nepotřebné pravidla odstranit. Snort dokonce funguje efektivněji s redukovanou sadou pravidel.

Snort je založen spíše na pravidlech, než na signaturách a může pracovat ve třech režimech: slídiče (sniffer, shromažďuje paketové hlavičky a data a vypisuje je na obrazovku), v režimu zachytávače paketů (podobně jako tcpdump) a konečně v režimu IDS, kdy pakety neznamenává, ale analyzuje jejich obsah vybranými pravidly. Snort využívá pro záchyt knihovny libpcap, nebo winpcap. Je rovněž potřeba software jako gcc, automake, autoconf, lex a yacc nebo flex a bison.

Jednoduchost a dostupnost Snortu jej předurčuje jako ideální pomůckou k seznámení a experimenty pro studenty a obsluhu. Najde uplatnění i v malých, nebo začínajících společnostech jako jediné IDS. Jeho služby a kvalita se neustále zlepšuje. Může také sloužit jako doplněk k jinému IDS a ohodnocovat tak jeho detekční kvalitu. Lze jej použít jako druhé IDS pro zvýšení celkové efektivity.

6.2.4 Profesionální zabezpečení

Pokud hledáme ochranu pro nadnárodní korporaci, budeme muset pořídit to nejlepší. Velký zájem uživatelů a známost firmy přitahuje útočníky z důvodu zisku a prestiže, kterou získají po úspěšném nabourání systému. Použití placeného a garantovaného IDS/IPS je zde podmínkou. Navíc je lepší použít více detekčních technologií a každou provozovat na jiném serveru pro případ jeho vyřazení, nebo selhání. Použití VPN (Virtuální privátní sítě) je pak další článek oddělující vnitřní síť od vnějších

hrozeb. Firmy, které poskytují tento druh zabezpečení jsou například Real Secure, Cisco secure, nebo NFR Security. Z našich firem je to například AEC (*www.aec.cz*), která dělá kompletní poradenství a zprostředkování těch nejlepších služeb.

6.3 Implementace IDS/IPS

Proces zavedení tak komplexní ochrany jako je IDS a IPS vyžaduje náležitou přípravu a je potřeba vytvořit náležitý postup implementace. To vše s ohledem na celkovou bezpečnostní strategii firmy. Je mnoho důvodů, proč takovýto systém zavádět a také jsou důvody, proč systém IDS/IPS nepořizovat. Tyto otázky se pokusí přiblížit následující kapitola.

6.3.1 Celková bezpečnostní strategie

Je důležité si předem ujasnit, co si od bezpečnosti jako takové slibujeme a jak je pro nás tato bezpečnost důležitá. Protože bude bezpečnost aktiv na prvním místě a budou nasazena nejpřísnější možná opatření, pak tato situace bude mít následky na mnoho prvků v celé firmě. Bude potřeba přijmout řadu změn a to může příliš narušit denní běh. Je potřeba si položit otázku. Je současná situace dostačující? Jaká jsou rizika pro současnou situaci. Jak je možné tuto situaci zlepšit. Je tedy nutné zavádět další stupeň zabezpečení? Určitě se vyplatí investovat do studie, jež nám zhodnotí rizika. Navíc pořizovací i režijní cena systémů IDS/IPS je velmi vysoká a rozpočet vyčleněný na bezpečnost je omezený. Všechny tyto faktory hrají významnou roli při tvorbě bezpečnostní strategie.

6.3.2 Cena IDS/IPS a její odůvodnění

Pokud mluvíme o ceně, je potřeba si uvědomit, že se skládá následujících částí:

Vybudování infrastruktury Je potřeba koupit nový HW a SW. Vyškolit techniky a personál pro práci a údržbu. Zvětšení šíře pásma. Navíc v době, kdy se personál učí ovládat nový produkt, nemůže se věnovat práci na jiných projektech. Jedná se o počáteční položku. Tato cena se pohybuje okolo 300 000 Kč.

Cena podpory zahrnuje aktualizaci HW a SW, čas strávený analýzami a odezvami na události. Cena vyškoleného administrátora, jenž se může setkat se situacemi, kdy bude potřebovat odbornou konzultaci, nebo pomoc. Tuto částku bude muset firma platit každý rok. Pohybuje se okolo 600 000 Kč.

Takže zavedení systému s IDS a IPS a první rok jeho provozu může vyjít firmu na milion korun českých. A každý další rok stojí bezpečnost firemních aktiv zhruba šest set tisíc korun českých. Což rozhodně není málo.

Zdůvodnění ceny

Cena se zde zdůvodňuje pomocí hrubé návratnosti investice (HROI). V tomto případu se jedná o nalezení průměrné roční ztráty (ALE). To se provádí tak, že se zhodnotí ztráta, která by podniku vznikla z případného útoku: zničení dat, ztráta pověsti a ochromení výroby a možné vydírání. Očekávané ztráty se vyjadřují v procentech z veškeré ceny aktiv, jenž jsou pro firmy cenné a může se o ně v jednom útoku přijít (SLE). Dále je důležité stanovit četnost takovýchto útoků ročně (ARO). Pak je stanovení roční ztráty počítáno následujícím způsobem ALE= ARO* SLE. Například pokud si firma své aktiva a pověst cenní na 100 milionů. Hodnota SLE může být například 70%. Četnost útoků je jednou za 4 roky, takže ARO=0,25. Pak ALE = 70*0,25=17,5% z ceny firemních aktiv a pověsti. Což je 17,5*100M= 1,75M. Takže firma za cenu 600 000 ročně ušetří 1,75 milionu. Je však těžké vyčíslit veškeré tyto údaje a také odhadovat například četnost útoků je sporné.

6.3.3 Výběr dodavatele

V této fázi je potřeba uspořádat výběrové řízení, jenž je zaměřeno na naše požadavky, kvalitu poskytovaných služeb a v neposlední řadě cenu. Vyšší cena jednoho produktu, může hodně ušetřit v podobě kvalitního servisu a záruky na produkt. Kdežto u ISD/IPS které jsou levné popřípadě zdarma (SNORT) mohou nastat problémy s aktualizacemi, nebo krizovými případy. Je dobré uvážit finanční stabilitu firmy od které produkt pořizujeme, služby, jaké nám dodavatel nabízí a jak je ochoten vyjít vstříc vašim jedinečným specifikacím a pověst firmy- respektive zkušenosti a reference administrátorů, kteří daný produkt používají. Pomohou i odpovědi na následující otázky: Jaká je cena za aktualizaci a údržbu produktu? Jak je systém rozšiřitelný jako celek? Jak velký provoz a za jakých podmínek je produkt schopen pracovat? (např. pakety za vteřinu). Kolik signatur systém podporuje? Jaké vlastnosti a odezvy produkt má? Jak je využitelná řídící konzole?

6.3.4 Testování a nasazení

Testování produktu pomáhá vyhodnotit jeho výkonnost na vaší síti. Je důležité ověřit dodavatelova tvrzení, nahlédnout do implementace a otestovat výkon. Přitom je důležité otestovat také: počet falešně pozitivních odezev, počet pozitivních detekcí, počet paketů prověřených za vteřinu, diagnostika útoků, dopad na síť. Proto se doporučuje najmout zkušeného nezávislého konzultanta, který vám pomůže z vyhodnocením testů.

Při nasazení je potřeba dbát na naplánovanou politiku a nájem lidských zdrojů. Je možné například mít jednoho experta na údržbu a kontrolu výstrah a část administrace nechat na outsorsingové firmě.

6.3.5 Závěr

Systém IDS/IPS se stává důležitou součástí celkové bezpečnosti firmy. Jako nová technologie však není ještě zcela propracovaná a řada produktů generuje nadměrné množství falešných poplachů. Situace se dá značně zlepšit dobrým vyladěním detekčních procedur. To vyžaduje profesionální administraci. Jeho správa a pořízení je drahá záležitost. Přitom není vždy nutná. Mnohdy stačí vlastní kvalitní reaktivní systém- například firewally reagují a blokují neautorizované činnosti. Při použití IDS a IPS, jenž jsou proaktivní a jsou schopny útok odhalit dříve, než k němu dojde. Tyto systémy se navzájem podporují. IDS/IPS bych tedy doporučil velkým firmám a to v kvalitním a drahém provedení, kdy je systém řádně vyladěn a podporuje všechny metody detekce a druhy analýz dat. Většina úspěšných implementací se odehrává pouze po malých krocích a je to zdlouhavá cesta, ale na jejím konci vlastní firma tu nejlepší ochranu dat jakou lze v dnešní době mít.

ZÁVĚR

Cílem diplomové práce byla počítačová bezpečnost. Pro kybernetický svět neexistují hranice států, úředním počítačovým jazykem je angličtina. Svět bez politických hranic je na jednu stranu krásný, ale přináší také mnoho problémů. Například hledání útočníků je komplikované, je potřeba získat povolení k odposlechům a prohlídkám. Policisté totiž zákony ctít musí. Zločinci ne. Proto se těmto útokům musí předcházet preventivním opatřením a vhodnými systémy, které chrání naší bezpečnost. Amerika se například obává počítačového terorismu. S problematikou počítačové bezpečnosti je spjat také problém ochrany soukromí. Bezpečnostní administrátor zachytává a kontroluje veškeré dění na vnitřní síti včetně důvěrných informací.

Základní obrana před napadením je znát informace, jak se bránit. Běžnému uživateli internetu stačí být pozorný a opatrný, protože jedině vlastní příčinou si může přivodit potíže. Každý by si měl dávat pozor na své osobní údaje, nikde je nezveřejňovat, neklikat na podezřelé odkazy, neotevírat nevyžádanou poštu, nezkoušet podezřelé odkazy a nestahovat programy z neznámých stránek.

Jenom opatrnost ale nestačí. Malware se může dostat do počítače různými metodami. Proto by každý počítač měl obsahovat antivirový program. U operačních systémů windows doporučuji verze XP a Vista se zapnutými aktualizacemi a vnitřním firewallem. Doporučuji používat mozillu firefox místo internet exploreru. Toto zabezpečení je pro soukromé účely naprosto dostačující. Jednou za tři měsíce doporučuji pevné disky prověřit nástroji Spybot S&D a Ad-Aware.Všechny programy je nutné aktualizovat!

Proti neautorizovaným vstupům nás brání hesla, tokeny a biometrické ochrany. Měly by být použity a v systémech s vysokým stupněm zabezpečením kombinovány. Citlivá data je nutné zálohovat a chránit šifrováním. Větší firmy mohou uvažovat o zřízení systému IDS a IPS. Tato poměrně mladá technologie je zaměřena na vyhledávání podezřelých řetězců na základě signatur a pravidel. Bohužel tyto systémy vyžadují důkladnou implementaci a nastavení, jinak vykazují nadměrné množství falešných poplachů, což je činí prakticky nepoužitelnými. Tyto detekční systémy mají také zastrašující potenciál.

Většina útoků je založena na chybách v softwaru. Tyto chyby jsou zveřejňovány na internetu a crackeři, kteří jsou o krok dál, než bezpečnostní firmy, je obvykle zneužijí dřív, než je vydána patřičná náprava. Systémy IDS však detekují také na základě heurestiky. Mnohem závažnější je, když je chyba právě v ochranném sofwaru, nebo je špatně nakonfigurován a útočník jej vyřadí DOS útokem.

Budoucnost detekce a prevence počítačových útoků je vkládána do zdokonalování IDS/IPS. Protokolová analýza může nahradit detekci signatur. Zdokonalení detekce pomocí jednoduchých pravidel. Využití neuronových sítí pro vyhodnocení dat a správnou odezvu. Zavedení celosvětové databáze o nových druzích útoků a nebezpečných IP adresách, z které by ochranný software přijímal nová opatření. Měla by se zlepšit také oblast vyhodnocování dat, kdy určité příznaky mohou nasvědčovat přípravu útoku. Zajímavá myšlenka je použití takzvaných lákadel (honeyspot), kdy se skutečný, nebo virtuální návnadný server chová jako skutečný a monitoruje aktivity útočníků.

Oblast zabezpečení počítačů je velmi široká a poskytuje dostatek prostoru pro další práce, které by se zaměřily na užší oblast a probraly ji více do hloubky, než tomu bylo v mé práci, která je spíše souhrnná. Za půl roku, co jsem se tomuto tématu věnoval, jsem se naučil spoustu užitečných věcí. Ale stále mám spoustu otázek, jenž mě motivují k dalšímu studiu tohoto tématu. Doufám, že svůj zájem a vědomosti uplatním i v budoucím povolání.

ZÁVĚR V ANGLIČTINĚ

The goal of this thesis was computer security. Pro cybernetic world there are no country limits, official computer language is English. The World without political limits is on the one side beautiful, but on the other hand it brings a lot of problems. For example searching for attackers is complicated, it is necessary to have permission for tapping and inspections. That is policemen have to stick with the law. Not the criminals. That's why attacks has to be preempted with precautionary measures and suitable systems, which protects our security. America for example is afraid of computer terrorism. The problematics of computer security is also bound up with problem of privacy protection. Security administrator captures and controls all events in the inner network including confidential information.

The essential protection from attack is to know how to defend. For the common internet user be attentive and careful is enough, because only by own mistake the harm can be done. Each should pay attention to his personal data, don't public them anywhere. don't click on suspicious links and don't download software from unknown websites.

To be just careful is not enough. Malware can get into the computer by different methods. Therefore every computer should have antivirus software included. Concerning OS Windows I recommend XP and Vista versions with actualizations and firewall enabled. I recommend to use Mozilla Firefox instead of Internet Explorer. This security is for personal purposes absolutely enough. I recommend scan hard disks with Spybot S&D and Ad-Aware tools once in a three months. All programs is necessary to actualize!

Passwords, tokens and biometric protections protect us against unauthorized entries. Those should be used and combined in the systems with high protection level. Sensitive data are necessary to backup and protect with encryption. Bigger companies can consider building IDS and IPS systems. This relatively young technology is aimed towards searching suspicious strings based on the signatures and rules. Unfortunately these systems demands complete implementation and settings, or they shows higher amount of false warnings, which makes them practically useless. These detection systems has also intimidating potential.

Most of the attacks are based on the bugs in software. These bugs shown on the Internet for public and crackers, which are one step forward before security companies,

usually exploit them sooner, than the corresponding patch is released. IDS systems detection is also based on heuristics. Much significant is, when the bug is in the protection software itself , or if it is configured wrong and attacker disable it with DOS attack.

The future of detection and prevention of computer attacks is put into the improving IDS/IPS. Protocol analysis can replace detection of signatures. Improving detection with the help of simple rules. Usage of neural networks for data evaluation and the right response. Implementation of the worldwide database of new types of attacks and dangerous IP addresses, from which the protection software would download a new acquisitions. The field of data evaluation should improve too. When some specific symptoms can indicate the preparations for attack. Interesting idea is to use so called honeyspots, which means that the real or virtual tempting server acts as real and monitors the attacker's activities.

The field of computer security is very wide and offers enough room for other jobs, which would aim for the narrower area and examined it more than in my work, which is more than that general. In the half of the year for which I put my brain to, I have learned many useful things. But still I have got a lot of questions, which motivates me for further studies of this topic. I hope that i apply my interest and knowledge in the future occupation too.

SEZNAM POUŽITÉ LITERATURY

[1] Carl Endorf, Eugene Schultz, Jim Mellander : *Hacking - detekce a prevence počítačového útoku*, 1. vyd. Grada 2007. 356 s., ISBN 80-247-1035-8

[2] Blakemanová Karen: Osobní *Blog o novinkách a vyhledávání v Googlu*. [online]. [cit.2007-03-15] Dostupný z URL: <www.rba.co.uk/rss/blog.htm>

[3] *Když se phisheři vyvíjejí a usilují o nezjistitelnost* [online]. [cit. 2007-04-22] Dostupný z URL: <www.symantec.com/cs/cz/home_homeoffice/library/index.jsp>

[4] *Open source vulnerability database* [online]. [cit. 2007-05-15] Dostupný z URL: < http://osvdb.org/>

[5] *Počítačový magazín PC World* [online] [cit. 2006-28-11] Dostupný z URL: <www.pcworld.cz >

[6] Bitto Ondřej: *lamani-hesel-v-praxi-4* [online]. [cit.2007-04-30] Dostupný z URL: < http://www.lupa.cz/clanky/lamani-hesel-v-praxi-4/>

[7] *Johni hack stuff* [online] [cit. 2007-04-25] Dostupný z URL:

<http://johnny.ihackstuff.com/>

[8] *Portál o počítačové bezpečnosti* [online] [cit. 2007-04-18] Dostupný z URL: <http://www.security-portal.cz>

[9] *Zakázání přístupu vyhledávačům* [online] [cit. 2007-04-12] Dostupný z URL: <http://www.jakpsatweb.cz/robots-txt.html>

[10] *Portál o všem kolem sítí* [online] [cit. 2007-03-29] Dostupný z URL: <http://www.svetsiti.cz>

[11] Debasis Mohanty: *Demystifying Google Hacks* [online]. [cit.2007-02-26] Dostupný z URL: < http://www.securitydocs.com/pdf/3098.PDF>

[12] *Kdo je to hacker* [online] [cit. 2007-01-26] Dostupný z URL:

<http://www.security-portal.cz/clanky/kdo-je-to-hacker.html>

[13] Haller Martin: *Seriál útoky typu DOS* [online]. [cit.2007-04-12] Dostupný z URL: http://www.lupa.cz/serialy/utoky-typu-dos/

[14] Bay Robin: *Čipové karty a USBtokeny* [online]. [cit.2007-04-5] Dostupný z URL: <http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=264>

[15] Bay Robin: *Pravdy o elektronickém podpisu a šifrování* [online]. [cit.2007-04-17] Dostupný z URL:

< http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=244>

[16] *Portál zvědavec* [online] [cit. 2007-03-29] Dostupný z URL: <http://www.zvedavec.org >

[17] *PGP* [online] [cit. 2007-03-29] Dostupný z URL: <http://www.pgp.cz>

[18] Dostálek Libor *Velký průvodce Protokoly TCP/IP a systémy DNS* [online] [cit. 2007-05-27] Dostupný z URL:

<http://www.cpress.cz/knihy/tcp%2Dip%2Dbezp/>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CPU Central processor unity

HDD Harddisk – pevný disk počítače

HTML HyperText Markup Language, Je jedním z jazyků pro vytváření stránek v systému World Wide Web, který umožňuje publikaci stránek na Internetu.

HW Hardware - hmotné vybavení PC (obrazovka,mys,grafická karta,procesor...)

IDS Systém detekce narušení

IP Internet protokol

IPS Systém prevence proti narušení

IRC Internet Relay chat Internetový protokol pro komunikaci mezi uživateli v reálném čase

OS Operační systém je SW umožňujících co nejefektivnější využití HW

RSS Really Simple Syndication – čte a třídí informace a novinky z webu

SW Software – nehmotné vybavení PC (programy, OS, data na HD)

TTL Time to live Zivotnost IP paketu. Při průchodu přes routery je snižován o jedničku

SEZNAM OBRÁZKŮ

Obr. 1 *Hlavička TCP* 14
Obr. 2 *Hlavička UDP* 15
Obr. 3 *Srovnání antivirů* 36
Obr. 4 *První DDOS útoky* 60
Obr. 5 *dnešní DDOS útoky* 60
Obr. 6 *Zesilující útok* 63

SEZNAM TABULEK

Tab. 1 *Transportní protokoly na jednotlivých vrstvách modelu TCP/IP*..... 13
Tab. 2 *Rozdíly IDS a IPS*..... 19
Tab. 3 *Příkazy fulltextových vyhledávačů*..... 25
Tab. 4 *Fulltextové operátory*..... 25
Tab. 5 *Získání citlivých údajů googlem1.*..... 43
Tab. 6 *Získání citlivých údajů googlem2.*..... 44
Tab. 7 *Příklady Rainbow cracků pro jednotlivé hash kódy*..... 50