Univerzita Karlova v Praze
Pedagogická fakulta
Katedra informačních technologií a technické výchovy

Útoky na počítače, servery a jejich služby

Autor: Oldřich Bitner
Vedoucí práce: Ing. Jaroslav Novák, Ph.D.
Rok obhajoby: 2011

PRAHA 2011

NÁZEV:

Útoky na počítače, servery a jejich služby

ABSTRAKT:

Teoretická část bakalářské práce je zaměřena na popsání globálních softwarových útoků na počítačové systémy, servery a jejich služby, způsob provedení nelegálních útoků a dělení útočníků podle jejich znalostí uvedené problematiky. Praktická část bakalářská práce je zaměřena na prověření základní bezpečnosti a odolností fakultních softwarových systémů.

KLÍČOVÁ SLOVA:

Útoky, útočník, počítač, server, služba, sociální inženýrství, cizí identita.

TITLE:

Attacks on computers, servers and services.

SUMMARY:

The aim of theoretical part is to describe global software attacks on computer systems, servers and their services. It also describes the way of performing illegal attacks and dividing of attackers according to their knowledge of the issue.Practical part of the theses focuses focucec on an examination of basic safety and durability of university software systems.

KEYWORDS:

The attacks, attacker, computer, server, service, social engineering, foreign identity.

Čestné prohlášení:

Prohlašuji, že jsem tuto práci vypracoval samostatně. Dále, že veškeré použité prameny použité v této práci byly řádně citovány a jsou uvedeny v seznamu použitých informačních zdrojů. Rovněž prohlašuji, že tato práce nebyla žádným způsobem využita k získání jiného nebo stejného titulu.

V Praze dne 7. 04. 2011 ……

Poděkování:

Rád bych tímto velmi poděkoval panu Ing. Jaroslavu Novákovi, Ph.D. za vedení mé bakalářské práce, rady, velkou dávku trpělivosti a cenné připomínky, které mi pomohly při zpracování práce.

Obsah

1. Úvod

Téma, které jsem si vybral pro svou bakalářskou práci, zní „Útoky na počítače, servery a jejich služby“. Stále méně si dovedeme představit svou práci i každodenní život bez počítače a internetu. S tím souvisí veliká propojenost našich osobních či firemních dat, což nám v mnohém život usnadňuje, ale zároveň dává prostor pro zneužití cizími osobami. Je tady jasné, ža tato celosvětová problematika je velmi tíživá nejen pro jednotlivé společnosti, ale i pro běžné koncové uživatele. Tyto subjekty vynakládají nezanedbatelné investice pro to, aby zajistily ochranu nejen svých citlivých dat, ale i funkčnost svých počítačových systémů.

V dnešní velmi uspěchané a nelítostné době převládají dvě veličiny. Tou první jsou informace a tou druhou finance. Tlak civilizace i trend současné společnosti vyžadují, aby jedinec měl co možná nejvíce informací k dispozici - tedy aby bylo možné to, co člověk neví, velmi jednoduše a rychle, nejlépe obratem zjistit prostřednictvím celosvětové sítě internetu.

Boj o co možná největší připravenost nutí společnost k tomu, aby veškeré informace shromaždovala, centralizovala, a logicky tedy i co možná nejvíce zpřístupňovala. Nyní tedy pochopitelně nastává situace, ve které je nutno sice na jedné straně zajistit jednoduchý přístup oprávněným osobám k potřebným informacím, ale na straně druhé bezpodmínečně zabezpečit, aby se tato data nedostala do rukou neoprávněným třetím a dalším osobám.

Teoretická část této bakalářské práce se zaměřuje na popsání globálních softwarových útoků, které mohou vést k získání, omezení nebo kompletnímu selhání systému, a tedy následnému zamezení přístupu k potřebným osobním či firemním informacím.

Praktická část je zaměřená na základní penetrační test, který jsem provedl pod dozorem odpovědné osoby. Za cíl tohoto pseudoútoku jsem si vybral systémy, jichž využívá Pedagogická fakulta UK. Nejedná se samozřejmě o jakýsi kompletní audit softwarové bezpečnosti, ale pouze o několik praktických „útoků“, které předtím popisuji ve své teoretické části bakalářské práce.

Rád bych předem předeslal, že v žádném případě tato práce není psána jako návod pro případné zájemce o zneužití systémů, naopak chci touto prací v rámci svých možností a znalostí upozornit na možné útoky, a tím předejít možnému úspěchu útočníka. Mým hlavním a jediným zájmem je samozřejmě primárně co nejvíce omezit možná rizika, která se vyskytují s používáním počítačových systémů, a sekundárně rozšířit povědomí mezi laickou veřejností o možnosti napadení, jak se útokům bránit a jak hlavně se zodpovědně a efektivně při práci s počítačovými systémy chovat.

2. Teoretická část

V první kapitole se zaměřuji na obecnou charakteristiku útočníků a útoků, popisuji místa, ze kterých je možné útoky provádět a způsob, jakým lze útok provést.

V druhé části popisuji důvody, které vedou útočníky k provedení útoku a zároveň uvádím příklady možné trestní zodpovědnosti jako příklad, která za tyto nelegální útoky je možné uložit.

Poslední, pátá kapitola je nejrozsáhlejší, je těžištěm práce a je zaměřená na uvedení přehledu a rozepsání možných a dostupných technologií směřujících k napadení serveru a jeho služeb.

3. Charakteristiky útoků a útočníků

V této kapitole obecně shrnuji dělení útků, způsob provedení a dělení útočníku dle jejich dosavadních zkušeností a znalostí.

3.1 Dělení útoků

V této kapitole bych se chtěl věnovat odbornému dělení počítačových útoků do několika skupin. Většina dnešních počítačových sítí a stanic je připojena do celosvětové sítě internetu, proto mým prvním dělením je pozice útočníka vzhledem k počítačovému systému, který chce napadnout.

3.1.1 Vnitřní útok

Při vnitřním, interním, útoku se jedná se o útok z počítače, který je připojen do vnitřní sítě. Ve většině případů se jednoduše jedná o zaměstnance, který dobře zná prostředí společnosti, nebo o člověka za zaměstnance se prostě vydávajícího. Proti takovýmto útokům se lze bránit nastavením striktních interních práv v systémech. Zahrnutí této ilegální činnosti do daných směrnic řešící tuto problematiku s přesně vymezenými sankcemi nebo zvýšení fyzické ostrahy u všech vchodových dveří je více než vhodné.

3.1.2 Vnější útok

Při vnějším útoku se jedná o případ, kde jde o útočníka, který nemá fyzický přístup do vnitřní počítačové sítě. Výhodou tohoto útočníka je většinou jeho velká anonymita, neboť zajistit takového pachatele, který ke svým útokům použil již dříve napadenou stanici nebo si zvolí destruktivní útok a v systému nezanechá naprosto žádné nebo minimální a nepostřehnutelné stopy, je téměř nemožná.

3.2 Způsob provedení

Mezi další rozdělení patří způsob provedení daného počítačového útoku. Velmi tedy záleží na tom, s jakým cílem útočník útočí a zda-li jde při útoku o odstavení služby, o zamezení přístupu, záměnu informací nebo jen o nečinné odposlouchávání probíhající komunikace. Toto zpočátku zdánlivě neškodné odposlouchávání může být samozřejmě zneužity mnoha způsoby později.

3.2.1 Aktivní útok

Cílem tohoto útoku je především nějak negativně zasáhnout do systému, a tím ovlivnit jeho správný a bezproblémový chod. Mohu například jmenovat útok na dostupnost služby, změnu již probíhající komunikace, změnu nasměrování toku ve vlastní prospěch nebo prostou záměnu dat. O tom, nakolik všech těchto zásahů lze zneužít, se většina z nás může jen dohadovat.

3.2.2 Pasivní útok

Při pasivním útoku nedochází k modifikaci již probíhající komunikace
nebo aktivní služby. Útočník pouze nečinně odposlouchává určitou službu. Problém pro útočníka může nastat ve chvíli, kdy služba komunikuje šifrovaně.

3.3 Dělení útočníků

V tomto případě chci zohlednit dosavadní znalosti a zkušenosti daného útočníka. Neplatí vždy pravidlo, že útok provádí pouze excelentní programátor skriptů nebo znalec struktury informačních technologií. Bylo by velkou chybou toto předpokládat. Praxe je jiná a často překvapivá. Proto uvádím následující dělení útočníků.

3.3.1 Začátečník

Script Kiddie, Occasionally Script Bunny, Skid, Script Kitty, nebo Similar jsou označení pro takového útočníka, který nemá moc zkušeností a znalostí týkajících se informačních systémů. Převážně se toto tedy týká běžných uživatelů, kteří na internetu narazí pouze na jeden z mnoha článků popisující některé chyby systémů a uvedené si chtějí prostě ověřit. Jeho „problém“ spočívá v tom, že vydané články a zprávy upozorňují na chyby, které jsou již velmi dobře známé a na udržovaných systémech jsou již tzv. záplatované. Útočník-uživatel, nebo chcete-li začátečník, tedy pro většinu svých útoků používá již naprogramované skripty, v nichž je potřeba zadat pouze cílovou adresu serveru nebo počítače, na který bude útok prováděn. Proto se dá s nadsázkou říct, že úspěšnost tohoto útočníka je přímo úměrná možnosti jeho prozrazení.

3.3.2 Pokročilý

Jedná se o útočníky, kteří většinou mají výborné znalosti v topologii sítí, znají většinu úskalí tkvící v útoku, vědí, kde musí po proniknutí smazat stopy, a vědí, kde se mají skrývat pro další případné odposlouchávání sítě. Ke svým útokům většinou využívají – stejně jako začátečníci – již naprogramované skripty, jen s tím rozdílem, že již nic nezkoušejí, ale naopak přesně vědí o možných slabých místech sítě a patřičně je využívají.

3.3.3 Expert

Jde o elitního programátora a znalce topologie sítí. Útoky těchto lidí jsou většinou velmi promyšlené, využívají chyb v systému, které jsou nedávno objevené nebo je objevili dokonce sami útočníci. Skripty, které využívají k útokům, si většinou sami programují nebo je získají za vysoké finanční částky. Cílem útoku už není zničit nějaký systém, ale ve většině případech jde o dlouhodobé parazitování. Útočník přesně ví, co má udělat pro to, aby se dobře skryl. Jeho odhalení a případné usvědčení z tohoto napadení není nijak jednoduché, mnohdy zdánlivě téměř nemožné.

4. Příklady trestné činnosti útočníků

Důvodů, proč jsou počítače, počítačové sítě nebo servery napadány, je nekonečně mnoho. Zpravidla se za útokem skrývá touha získání informací nebo financí, ale ne vždy se útočník musí na úkor nepadnutého přímo obohacovat. Útok může být prováděn také z ješitné či někdy až patologické potřeby zviditelnění onoho jedince nebo celé skupiny útočníků (tento útočník je z mého pohledu nejnebezpečnější, jelikož se nedá dobře odhadnout, jaký je jeho cíl - je pouze hnán touhou udeřit a poškodit systém v co největší míře), z potřeby omezení přístupu legitimním osobám k některé z využívaných služeb. Jeho cílem může být i na první pohled obyčejná snaha ověřit si znalosti a zkušenosti v tomto odvětví. Jedno je však naprosto jisté – vždy se jedná o trestný čin! Celé znění zákona je dostupné v ČÁSTI DRUHÉ: Zvláštní část – HLAVA V, Trestné činy proti majetku[1]. Za velmi důležité považuji vymezení pojmu „Napadení počítačového systému“. Je to neoprávněně nabytý přístup k určité počítačové části, nebo jen k jednomu zařízení. Tím máme na mysli jakýkoliv systémový prvek.

Trestným činem tedy nazýváme[2]:

1. Protiprávní přístup
2. Protiprávní zachycení informací
3. Zásah do dat
4. Zásah do systému
5. Zneužití zařízení
6. Falšování údajů souvisejících s počítači
7. Podvod související s počítači
8. Trestné činy související s dětskou pornografií
9. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

[1] Zdroj: http://www.podnikatel.cz/zakony/zakon-c-40-2009-sb-trestni-zakonik/ [dostuplné: 2011-03-12]
[2] Smejkal, V., *Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku*. Trestněprávní revue, II., 2003, č. 6

4.1 Neoprávněný přístup k počítačovému systému a nosiči informací

Dle mého názoru je neoprávněný přístup k počítačovému systému a nosiči informací nejčastějším trestným činem. Naplnění skutkové podstaty je například obyčejné napadení WIFI sítě a připojení svého počítače do systému. V tuto chvíli se útočník dopouští trestného činu ve smyslu §230 odst. 1 *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“* [3]

4.2 Záměna webové stránky s cílem získat citlivé informace

V poslední době se velmi často setkáváme s technikou, která uživatele internetu, hledajícího určitou webovou stránku, přesměruje na webovou stránku, stejně nebo velmi podobně vypadající. To ho vyzve k zadání jeho citlivých dat. Nemusí být přímo požadováno přímo rodné číslo, jméno, příjmení nebo adresa, ale spíše je řeč o existujícím bankovním kontu společně s heslem či pouze přístup do e-mailové schránky. Jedná se o tak častý útok, že si ho mnoho uživatelů již ani neuvědomuje. Tato technika se nazývá Pharming a její primární podstatou je napadení DNS serveru, kde dochází k překladu jmenného název domény na IP adresy. V tomto případě útočník zamění tyto údaje a uživatel služby je přesměrován na webovou stránku útočníka, která vypadá identicky s legitimní službou. V tomto případě se útočník dopouští trestného *činu „Padělání nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná“* [4] ve smyslu §230 odst. 2 písm. c).

[3] http://www.podnikatel.cz/zakony/zakon-c-40-2009-sb-trestni-zakonik/cast-druha-hlava-v/ [dostuplné: 2011-03-12]
[4] http://www.podnikatel.cz/zakony/zakon-c-40-2009-sb-trestni-zakonik/cast-druha-hlava-v/ [dostuplné: 2011-03-12]

4.3 Denial of Service Attack

V části „Technologie napadení serverů a služeb“ rozebírám také jeden z dalších útoků, kterým je omezení přístupu k určité službě zahlcením komunikační linky nebo přímo celého serveru. I na tento typ útoku zákon pamatuje. V §230 odst.3 písm. b) se tento jedinec klasifikuje jako někdo, „*kdo v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat*“ . Pachateli za tento trestný čin může být udělen trest „*odnětí svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty*“. [5]

4.4 Výroba škodlivého kódu

Mezi posledním a poměrně velice často zneužívaným útokem na počítačové systémy je samotné naprogramování a implementace škodlivého kódu do systému, a tím získání určitého prospěchu. Mezi tyto typy útoků je zahrnut i škodlivý kód, který zdánlivě pouze nečinně odposlouchává komunikaci, tedy nemusí to být pouze program, který systému přímo škodí. V tomto případě odkazuji na zákon §231 odst. 1 písm. b) „*zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části*“ [6]. Za tento trestný čin může být pachateli udělen trest odnětí svobody až na tři léta, zákaz činnosti nebo propadnutí věci nebo jiné majetkové hodnoty.

[5] http://www.podnikatel.cz/zakony/zakon-c-40-2009-sb-trestni-zakonik/cast-druha-hlava-v/ [dostuplné: 2011-03-12]
[6] http://www.podnikatel.cz/zakony/zakon-c-40-2009-sb-trestni-zakonik/cast-druha-hlava-v/ [dostuplné: 2011-03-12]

5. Technologie napadení serverů a služeb

5.1 SQL Injection

SQL zkratka pro Structured Query Language (v překladu strukturovaný dotazovací jazyk). V tomto případě se jedná o standardizovaný dotazovací jazyk v relačních databázích. Podotýkám, že „injection“ znamená v překladu „vstříknutí, injekce nebo také nával“. Jedná se tedy o techniku, při které lze změnit vhodným použitím SQL příkazů smysl původního SQL dotazu. Především se zde využívá základních bezpečnostních chyb, kdy programátoři zapomínají ošetřit veškeré vstupy kontrolou na povolené hodnoty. Díky této chybě se může útočník dostat k citlivým datům v databázi, může nastavovat oprávnění, a tedy i získat přístup do administrační části nebo získat absolutní kontrolu nad veškerým provozem.

Rizikovými místy pro vložení škodlivého SQL dotazu jsou:

1. URL adresy s parametry
2. Formuláře
3. HTTP/XML/SOAP komunikace
4. Importy souborů

Nejčastěji zneužívaná chyba (o čemž svědčí mimo jiné i velké množství návodů na internetu) je naivita některých programátorů, kteří se domnívají, že procesy, které běží skrytě jako služba, se nedají editovat. To je právě osudová chyba – stačí jednoduše uložit a zeditovat indexní přihlašovací webovou stránku a SQL Injection je připravený k použití.

Přiklad SQL Injection[7]

Formulář obsahuje vstupní pole - jméno pro zadání hledaného jména

```
<?php
...
$jmeno = $_GET["jmeno"];
$spojeni = ODBC_Connect("test", "user", "password");
$vysledek = ODBC_Exec($spojeni,
            "SELECT * FROM Zamestnanci
             WHERE Jmeno LIKE '$jmeno%'
             ORDER BY Jmeno");
...
?>
```

Před předáním dat dotazu se testuje, zda řetězec obsahuje jen povolené znaky

```
<?php
...
$jmeno = $_GET["jmeno"];
if (!ERegI("^[a-záčďéěëíóöřšťúůüýž]+$" , $jmeno))
{
  echo "Hledaný text může obsahovat jen písmena.";
  exit;
}
$spojeni = ODBC_Connect("test", "user", "password");
$vysledek = ODBC_Exec($spojeni,
            "SELECT * FROM Zamestnanci
             WHERE Jmeno LIKE '$jmeno%'
             ORDER BY Jmeno");
...
?>
```

[77] Zdroj: http://www.kosek.cz/vyuka/4iz228/prednasky/bezpecnost/foil13.html [dostuplné: 2011-03-12]

5.2 Denial of Service

Denial of Service (v překladu odmítnutí služby) nebo také Distributed Denial of Service (v překladu distribuované odmítnutí služby) je typ útoku, při kterém dochází k zahlcení linky oběti, a tím je způsobený pád systému nebo minimálně jeho zahlcení s následným znemožněním přístupu legitimních požadavků.

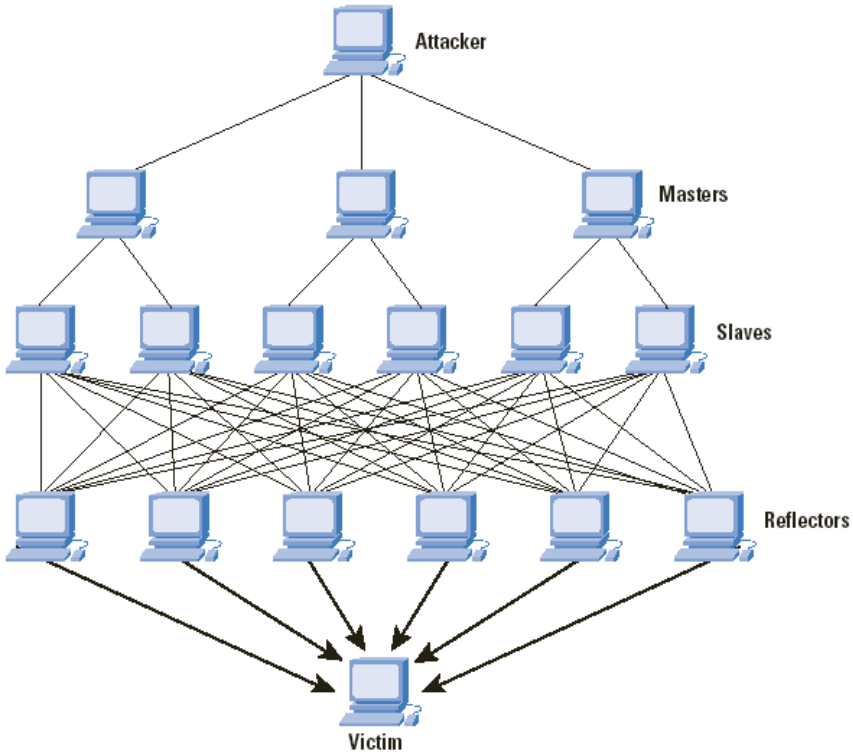
DOS útoky můžeme rozdělit následovně:

1. Reflektivní a zesilující typy
2. Využívající chyb a vyčerpání systémových prostředků
3. Záplavové typy

Projevy tohoto útoku lze sledovat v nadměrném nárůstu časové potřeby na dotaz nebo při náhlé nemožnosti připojit se k službě či webu.

5.2.1 Reflektivní a zesilující typy

Cílem reflektivního a zesilujícího útoku je zahlcení celého přenosového pásma sítě, a tím zamezení vyřizování legitimních dotazů, což vede k odmítnutí služby právoplatným uživatelům. K tomu útoku nejčastěji útočník využívá jiné než vlastní prostředky a to jsou např. již dříve napadené počítačové stanice, servery nebo routery.



Obr. 1: Reflektivní a zesilující útok, zdroj: http://www.cisco.com
[dostupné: 2011-03-12]

5.2.1.1 Smurf Attack

Podstatou tohoto útoku z kategorie reflektivních zesilujících útoků je odeslání Ping dotazu na adresu celé sítě. V hlavičce je pouze změněna IP adresa, a to na IP adresu oběti. V tuto chvíli každá stanice vygeneruje ICMP[8] odpověď (ICMP Echo Replay) a odešle ji oběti. Tento útok je tedy velmi podobný záplavovému útoku ICMP s tím rozdílem, že Smurf je útok učinnější o zesílení, síla útoků je přímo úměrná počtu připojených aktivních prvků v sítí.

5.2.1.2 SYN Flood

SYN[9] Flood je velmi používaný typ útoku. Princip tohoto útoku je v odesílání SYN paketů, u kterých útočník zfalšuje IP adresu odesílatele. Poté, co server obdrží

[8] ICMP zkratka pro Internet Control Message Protocol - protokol, který využívá operační systém k zasílání chybových reportů.
[9] SYN - paket, který obsahuje prázdný TCP segment a má nastavený SYN příznak v hlavičce. TCP je protokol, který slouží k přenosu dat. Oproti UDP je mnohem spolehlivější - zaručuje správné pořadí kompletních předání dat. Tento protokol využívají služby, jako je FTP, SSH, HTTP, SMTP.

SYN paket, tedy výzvu k začátku spojení, alokuje si pro toto spojení místo a odpoví odesláním SYN-ACK, tedy potvrzením započetí přenosu na zfalšovanou adresu a čeká na odpověď, které se samozřejmě nedočká. Tím se zaplňuje prostor tabulky vyhrazený pro kompletaci spojení. Čím více takovýchto neukončených spojení naváže, tím rychleji se potom tabulka zaplní a dojde k zahlcení. S tím je samozřejmě spojená i nedostupnost služby.

Ochrana proti tomuto útoku je sice velmi složitá, ale může spočívat například v odmítání SYN paketů zaslaných z jednoho zdroje, nebo ve snížení časového limitu, potřebného ke kompletaci spojení.

5.2.1.3 DNS Amplification Attack

Tento útok se poprvé na veřejnost dostal v roce 2005. Osobně ho považuji za jeden z nejefektivnějších. Útok spočívá v zasílání DNS dotazů. Jde o zfalšovanou IP adresu na adresu oběti. K jeho provedení potřebuje útočník veřejný DNS server, který za něho dohledá a odešle odpověď na DNS dotaz. Tímto útokem může získat až 50x větší nárůst původních dat, a proto tento útok patří mezi nejúčinnější.

5.2.2 Využívání chyb a vyčerpání systémových prostředků

Jedná se o typy útoku, který využívá systémové nebo hardwarové chyby. Zneužití této chyby se projeví výrazným zvýšením vytížení systémových prostředků. Cílem tohoto útoku je vytížení systému na plný výkon s následným selháním a s nemožností vyřizovat legitimní požadavky. Tyto útoky se postupně přesouvají do pozadí, jelikož rozvoj technologií dává možnost systémové prostředky zvyšovat, nebo úplně celý trafik v době vytížení přesměrovat na jiný systém.

5.2.2.1 RPC Named Pipes

Tento útok je díky velkému rozvoji IT minulostí. Principem je volání služby RPC[10] . Tato služba následně začala využívat enormně systémové prostředky, čímž dochází k selhání systému. Chyba se vyskytuje u Windows NT bez servis packu 4.

[10] RPC je technologie, která dovoluje programu provést určitou proceduru na jiném počítači. Nejčastějším využíváním je odlehčení vlastního systému.

5.2.2.2 Land Attacks

Land (Local Area Network Denial) Attack, nebo také Banana Attacks, je podobný SYN Attacku. Jde tedy o generování náhodných paketů směrovaných do sítě většinou na Port 113 nebo 139 pod zfalšovanou IP adresou uzle nebo napadajícího počítače. Cílem je zahltit provoz a donutit systém k selhání. Ochrana proti tomuto útoku je velmi jednoduchá. Spočívá ve filtrování celého provozu Firewallem, kde dochází k blokování IP adres, ze kterých je směřován útok.

5.2.2.3 Stream a Raped

Další z útoků, jenž byl dříve řazen do kategorie vyčerpávající systémové prostředky, je dnes s přispěním rozvoje systémových prostředků spíše útokem záplavovým. Jeho princip spočívá v zasílání poškozených paketů systému, který při snaze je opravit zcela selže, nebo v danou chvíli nedokáže odpovídat na jiné operace.

5.2.2.4 Fork Bomb

Principem útoku Fork Bomb je vytvoření co možná největšího počtu systémových procesů v co nejkratším čase. Většinou jde tedy o program nebo skript, který spouští sám sebe do té doby, než nedojde k vyčerpání systémových prostředků a k zahlcení systému s následným selháním. Můžeme tento proces také nazvat zacyklením nebo též vytvořením nekonečné smyčky.

5.2.2.5 Unintentional

Osobně tento typ útoku neřadím mezi úmyslné DOS Attaky. Jedná se většinou o webový server, který je ze strany veřejnosti velmi navštěvovaný. Nyní stačí, aby autor článku při uveřejnění na tomto serveru odkazoval na jiný méně navštěvovaný server. Tento server pochopitelně má většinou nižší systémové prostředky pro svůj provoz) i když tomu tak nutně být nemusí). Ve chvíli, kdy se většina čtenářů velmi navštěvovaného serveru proklikne k méně navštěvovanému serveru, může dojít k zahlcení nebo pádu služby. Ve většině případů k tomu skutečně dojde.

5.2.2.6 NetKill

Cílem útoku je vyčerpání maximální velikosti operační paměti. K tomu využívá chyb v protokolu TCP/IP. Tento útok je velmi podobný SYN Floodu, ovšem s tím rozdílem, že v tomto případě opravdu dojde k navázání spojení. Tuto chybu objevil a poprvé využil Stanislav Shalunov[11].

5.2.2.7 Teardrop

Útok Teardrop využívá chyb v implementovaném protokolu TCP/IP, a to přesně při opětovném skládání IP fragmentů. Proč vlastně dochází k IP fragmentaci? Každá počítačová síť má přesně nadefinovanou maximální přenosovou jednotku tedy MTU. Standardní velikost maximální přenosové jednotky je 1500 B. Ve chvíli kdy je obdržen paket větší než MTU na řadu přichází tzv. fragmentace pomocí které, se větší pakt rozdělí na více již přenositelných. Tato problematika je sepsána v RFC 791 z roku 1981. Tento typ útoku je možné uplatnit pouze u operačních systémů Windows NT, Windows 95 a Lunix v. 2.1.63. Ke složení, po přijetí očíslovaných segmentů, které dorazí jednotlivě, nedojde korektně a systém selže.

5.2.2.8 Ping of Death

Tento typ útoku využívá chyby v protokolu TCP/IP. Jde o zaslání Ping dotazu na stanici. V tomto případě se ovšem nejedná o klasický Ping, tedy o zaslání 56 bajtů případně 84 bajtů, což je rovné hlavičce IP, ale zasílá se dotaz větší než 65535 bajtů. Obdrží-li systém takovýto paket, dojde k přetečení paměťového prostoru a systém selže. Budeme-li tento typ útoku chtít aplikovat v dnešní době, s největší pravděpodobností neuspějeme. Jedná se o chybu v protokolu, která byla objevena před rokem 1997. Tohoto roku byla většina systému opravena, hovoříme tedy o velmi zastaralé chybě a již nepoužívaném typu útoku.

5.2.2.9 NBName

Útok od července roku 2000 využíval chybu v NetBIOSu u systémem Windows. Jeho autorem je Sir Dystic ze skupiny Cult of the Dead Cow . Principem zmiňovaného útoku je pomocí služby NetBIOS Name Service zaslat zprávu NetBIOS Name Release

[11] http://shlang.com [dostupané: 2011-03-12]

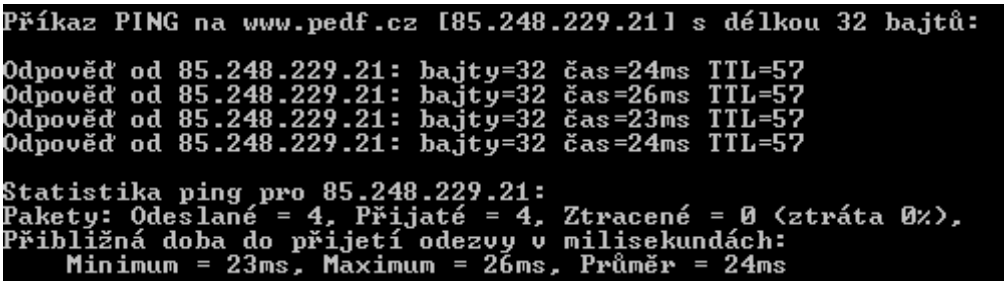
na cílový počítač, který si následně mylně vyhodnotí, že jeho jméno je konfliktní, zamezí jeho používání a vyřadí stanici z připojení do sítě.

5.2.3 Záplavové typy

Jedná se o ryze čistý DOS Attack. V těchto případech dochází ke generování co největšího toku dat a odesílání na adresu oběti. Tento útok je velmi nebezpečný už jen proto, že ho zvládne i úplný začátečník (Script Kiddies). Stačí jen chvilku prohledávat internet a programy pro tyto útoky se nabízejí všem trochu znalým uživatelům s trochou nadsázky opravdu zcela samy. Mohu například zmínit nejjednodušší a velmi často používaný program pro generování paketů na port 80 Attack server, který je běžně dostupný na internetu. V tomto programu stačí pouze zadat IP adresu cílové stanice, na který bude útok prováděn, a stisknout tlačítko Attack.

5.2.3.1 ICMP Flood

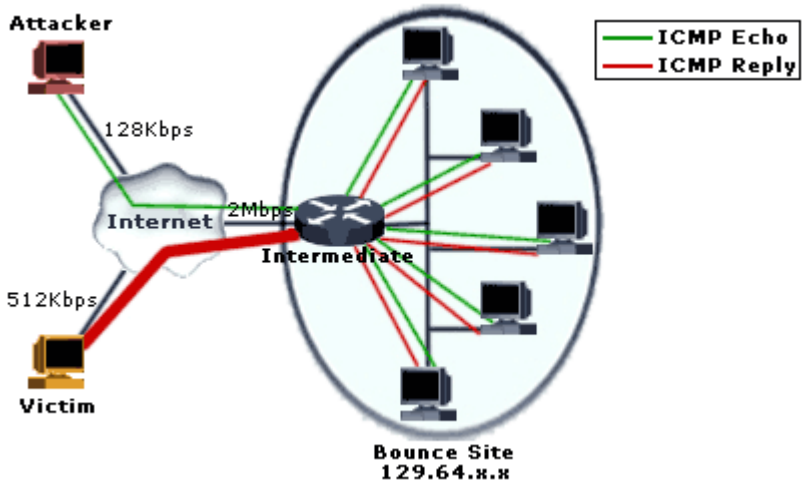
Nejdříve bych chtěl přiblížit, jak vlastně funguje ICMP[12] datadiagram. Mezi nejpoužívanější se řadí Echo, tedy při zaslaní Echo Request dostaneme jako odezvu Echo Replay. Například na obrázku DNS server přeložil webovou adresu www.pedf.cz na IP adresu 85.248.229.21 a začal zasílat Echo Request. Z výsledků můžeme vyčíst průměrný čas 24 ms. Nejdelší je 26 ms a nejkratší 23 ms.



Obr. 2: Ping www.pedf.cz [dostupné: 2011-03-12]

ICMP Flood je tedy útok, kde zasíláme ICMP Echo Request se zfalšovanou IP adresou odesílatele. Tímto útokem docílíme dvojnásobného zahlcení linky. Nejprve při přijímání a následně při odesílání na zfalšovanou adresu oběti.

[12] ICMP je zkratka pro Internet Control Message Protocol. Jde o velmi důležitou službu, která informuje o chybách v systému. Flood je v překladu záplava, zátopa, nebo proud.



Obr.3: ICMP Flood , zdroj: http://www.javvin.com [dostupné: 2011-03-12]

5.2.3.2 UDP Flood

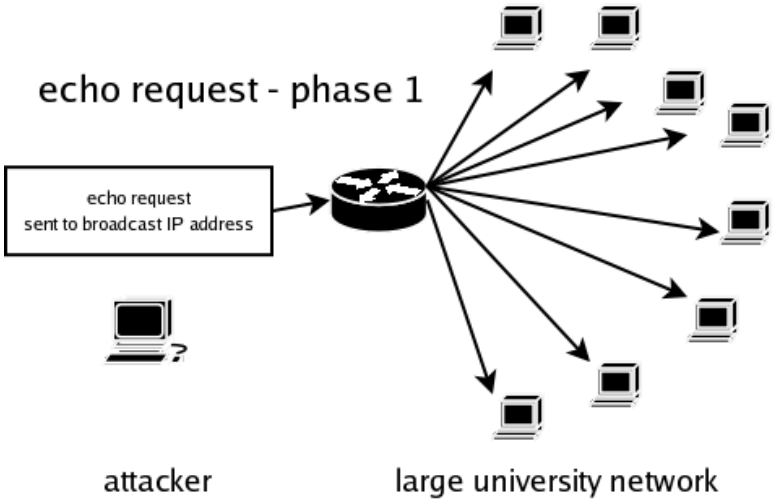
K tomuto útoku se využívají služby určené pro odezvu, tedy Echo nebo Charge. Služby jsou defaultně spuštěné a útok se provádí zasláním Echo dotazu, který má zfalšovanou IP adresu a port. Tyto údaje jsou zaslány na server, který poskytuje službu Echo. Jakmile přijde takovýto dotaz na server, dotaz se následně zpracuje a odešle odpověď na zfalšovanou IP adresu, kde je služba také aktivní. Tímto způsobem dojde k zacyklení a dotaz se stále znovu opakuje.

5.2.3.3 TCP Flood

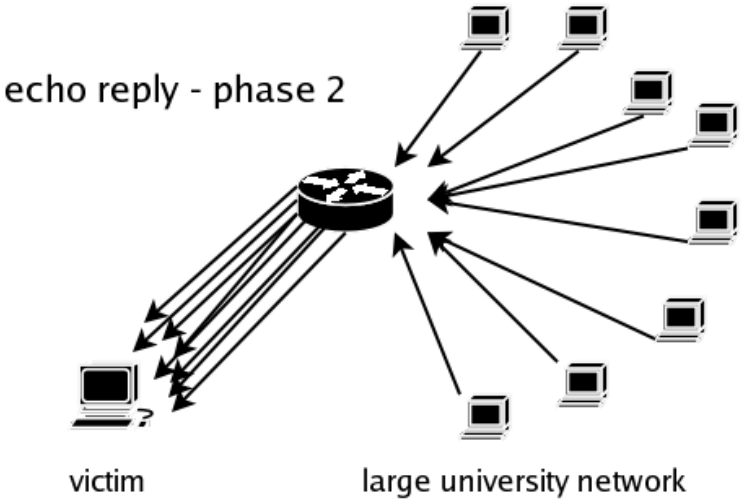
Útok TCP Flood spočívá v zaplavení jedné či více služeb, které využívají nebo mohou využívat služeb TCP, a tím pádem se znemožní vyřizování legitimních dotazů. Nejznámějším představitelem tohoto útoku je SYN Flood.

5.2.3.4 Ping Flood

Tento útok je velmi podobný již zmiňovanému útoku Ping of Death. Jen s tím rozdílem, že Ping Flood nevyužívá systémových chyb, ale pouze zahlcuje linku dotazy typu Ping.



Obr.4: Echo request, zdroj: http://tomicki.net/ [dostupné: 2011-03-12]



Obr.5: Echo replay, zdroj: http://tomicki.net [dostupné: 2011-03-12]

5.3 Sociální inženýrství

„Sociální inženýrství nebo také sociotechnika je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace“ [13]. Je obecným a známým pravidlem, že systém je tak silný, jak silný je jeho nejslabší článek. Musíme přiznat, že toto v sociálním inženýrství platí minimálně dvojnásobně.

[13] Mitnick, Kevin – Simon, William: *Umění klamu*. Helion, Gliwice 2003

„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.”

Albert Einstein

Nižší sociální inženýrství:

1. Zneužití slabších článku kolektivu, nových zaměstnanců
2. Zneužití pozice autority

Vyšší sociální inženýrství:

1. Zneužití dlouholeté důvěry
2. Vydírání

Některé z možností a vlastností, kdy mohou sociotechnikové uspět:

1. **Autorita** – většina z jedinců mají respekt před autoritou, například v pracovním vztahu je autoritou nadřízený. Dostane-li se některý sociotechnik do pozice, kdy se mu podaří manipulovanou osobu přesvědčit, že je tato osoba součásti kolektivu, a sociotechnik je ještě přímo jeho nadřízený, je úspěch téměř zaručen. Z druhé strany ovšem třeba zdůraznit, že nepodlehne-li manipulovaná osoba sociotechnikovi, nesmí být proti ní vyvozena žádná kárná opatření.
2. **Lákavá nabídka** – sociotechnik se dostává do pozice, kdy manipulované osobě předkládá pro něho v různých ohledech velmi lákavou nabídku.
3. **Sympatie** – jednou z velmi důležitých metod je získání náklonnosti manipulované osoby. Například společnou zájmovou činností.

Sociotechnik je tedy schopný využít lidi, se kterými hovoří, případně má pro získání hledaných informací k dispozici dodatečné technologické prostředky a pomůcky, které jsou popsané v dalších kapitolách.

5.3.1 Phising

Phising v českém překladu znamená rybaření. Tato technika je založená na sociálním inženýrství a používá se k oklamání osob a získání jejich citlivých údajů, jako jsou hesla, kontaktní údaje nebo čísla kreditních karet. Principem tohoto útoku je rozesílání podvodné e-mailové zprávy. Obsahem zprávy je sdělení, ve kterém se útočník

vydává za důvěryhodný subjekt, který příjemce zprávy využívá. Nejčastěji se jedná o banku nebo o poskytovateli e-mailových schránek apod. E-mail obsahuje text, jenž po klientovi žádá zaslání přihlašovacích údajů, nebo přímo z e-mailu vede odkaz na podvrženou webovou stránku, která má stejný design jako oficiální web. Po zadání přihlašovacích údajů je příjemce z podvrženého webu přesměrováni na oficiální web s korektním přihlášením. Jen s tím rozdílem, že si útočník přihlašovací údaje ukládá. Phising byl poprvé popsán v roce 1987, ale s masovějším používáním je spjat až rok 1996. V roce 2005 došlo v Kalifornii k přijetí zákona, který řadil činnost phising techniky na listinu trestných činů, za které mohla být udělena pokuta až 250 000 tisíc dolarů nebo 5 let odnětí svobody.

Mezi nejběžnější phising útoky patří[14]:

1. AOL Phising – v roce 1990 se tento útok používal. Kde došlo ke generování čísel ALO a po majiteli požadoval přístupové udaje.
2. Online platby – podvodnou technikou se útočníci snažili vylákat z obětí číslo účtu a jejich heslo a popřípadě PIN kód.
3. Oficiální síť phising – V roce 2006 nejrozšířenější z phising útoků, evidovalo se na 50%.
4. Russian Business Network Phising – příkladem je Phising Virus MySpace. Tento virus napadla stránky MySpace a přesměrovával uživatele na webové stránky, které byly určené k zcizení identity přihlašovacího uživatele.

5.4 Odcizení domény

Případů, kdy dojde k odcizení domény, není nikterak mnoho, ale dojde-li to tak daleko, že někdo doménu odcizí, může se jednat o veliký právní problém. Než-li se pustím do konkrétních popisů, jak vůbec tato situace může nastat, chtěl bych krátce nastínit, jak vlastně probíhá sama registrace.

Prvním krokem je vyhledání volné domény a registrátora. Poté následuje vyplnění jednoduchého registračního formuláře o budoucím vlastníkovi domény. Po ověření, zda-li je doména volná, registrátor potvrdí platnost registrace, novinkou u

[14] Zdroj: http://www.spammers-mgi.com/articles/phishing/index.php, [dostuplné: 2011-03-12]

některých providerů je i potvrzení e-mailu s podmínkami registrace správci domény nejvyšší úrovně v České republice NIC.cz . Po těchto úspěšných úkonech zaplatíte provozovateli náklady spojené s vedením domény a doména se během pár dní aktivuje.

5.4.1 Způsoby odcizení domény?

Způsobů jak odcizit doménu je několik[15]:

a) Vypršení platnosti domény a následné uvolnění

Nejedná se přímo o odcizení domény, ale je s tím spojená jiná technika podvodu, a to je opětovná registrace e-mailu bývalého vlastníka domény a následné přesměrování veškeré e-mailové aktivity. Pozor – nejedná se o domény *.cz – v tomto případě registrátor zasílá expiraci domény i písemně na uvedenou adresu při registraci.

b) Chyba registrátora

Útočník zašle požadavek na změnu vlastníka domény. Při tom využije spoofing e-mailu a změní hlavičku na vlastníka domény. Registrátor vždy musí ověřit věrohodnost tohoto e-mailu. Je ovšem znám případ, kdy registrátor přeregistroval doménu na útočníka bez verifikace pravosti zaslaného e-mailu. Viz odcizení domény www.sex.com Garymu Kremenovi. Jen pro přehlednost: odhadovaná cena domény www.sex.com byla v roce 2006 – 262 milionu korun. Z této domény se rázem stala nejdražší prodaná doména na světě.

c) Zfalšování dokumentů

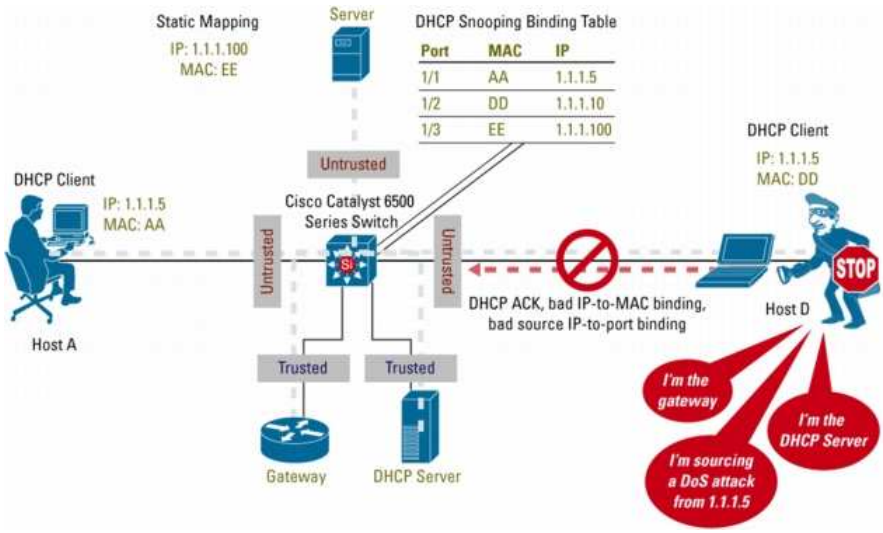
Útočník zfalšuje dokumenty vlastníka domény a odešle písemný souhlas k převedení domény na jinou osobu, spolu s kopií například občanského průkazu. Viz. odcizení domény www.DVDmovies.com v roce 2003, kterou vlastnil Arnold Jones.

Chcete-li překontrolovat vlastníka domény, můžete využít speciální software anebo přímo online databázi dostupnou z http://whois.domaintools.com/. Například po zadání dotazu na doménu http://www.cuni.cz jsem získal patřičný report viz. přílohu „Výpis dotazu WhoIs http://www.cuni.cz“.

[15] Zdroj : http://www.domaintheft.org/ - server s databází a informacemi o odcizených domén [dostupané: 2011-03-12]

5.5 Rogue DHCP

Rouge DHCP[16] je technika vložení falešného DHCP serveru do sítě. Povede-li se takto infikovat síť, počítačové stanice mohou začít přijímat informace pro svůj chod od tohoto falešného serveru. Většinou tato technika klamavého vložení DHPC serveru je doprovázena některým z DOS Attaku. Zaútočením na aktivní verifikovaný DHCP server může dojít k jeho zahlcení pakety a jeho následné selhání. Tímto útokem si útočník při správném nastavení falešného DHCP serveru může zajistit i kontrolu příchozích paketů, kterou doposud neměl.



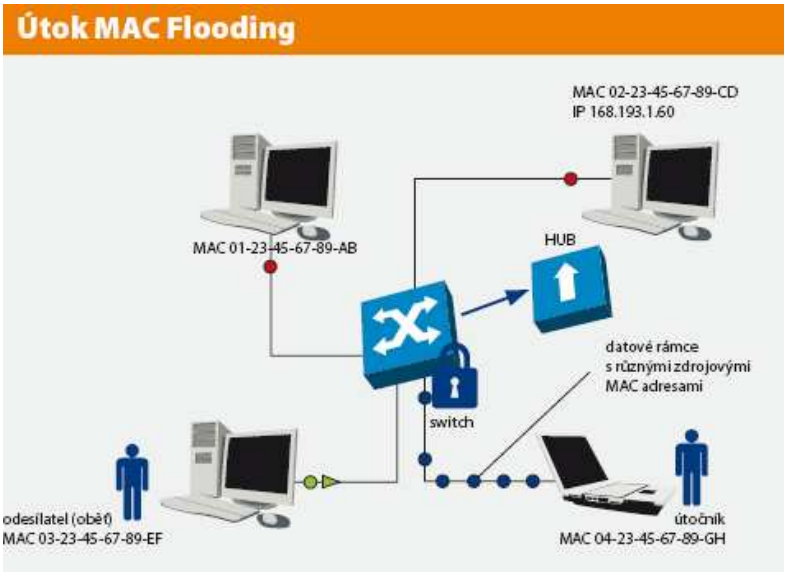
Obr.6: Rouge DHCP, zdroj: http://www.cisco.com [dostupné: 2011-03-12]

5.6 MAC Flooding

MAC[17] Flooding je typ útoku, při kterém dochází k úmyslnému zahlcení vnitřní paměti přepínače. Vnitřní paměť ukládá nové MAC adresy do své několikakilobytové paměti, jakmile se paměť zaplní falešnými adresami, začnou se MAC adresy ukládat i na prostor, kde byly uloženy adresy korektní, a přepínač začne pracovat jako hub. Pro útočníka je pak maličkostí zachytit a analyzovat data.

[16] DHCP je zkratka pro anglické Dynamic Host Configuration Protocola. Tato služba je využívaná pro automatické přidělování IP adres počítačům v počítačové síti a tím i jejich správu a kontrolu nad nimi.
[17] MAC zkratka pro Media Access Control je jedinečná síťová adresa síťového zařízení. MAC adresa se skládá ze 48 bitů a nejčastěji se zapisuje se ve tvaru 01:23:45:67:89:ab.

Ochran proti MAC Floodingu je více. Nejúčinnější ochranou je pevné ukládání MAC adres do vnitřní tabulky bez možnosti neautorizovaného vložení dalších adres nebo omezení počtu MAC adres společně s limitem nastaveným na zadání nových MAC adres z jednoho zařízení. Tímto způsobem je možné nežádoucí zaplavení.



Obr.7: MAC Flooding, zdroj: http://connect.zive.cz/node/714 [dostupné: 2011-03-12]

5.7 Malware

Název Malware vznikl spojením částí dvou anglických slov, a to *mal*icious, v překladu škodlivý, a soft*ware*. Jde o souhrnné označení veškerého úmyslně naprogramovaného softwaru za účelem poškození počítačových systémů. Zde bych chtěl zdůraznit, že se skutečně musí jednat o zcela úmyslné (naprogramování škodlivého softwaru. V případě chybně naprogramované aplikace, která se sice může chovat jako Malware, nelze tuto chybu označovat za skutečný a úmyslný Malware, jde pouze o selhání lidského faktoru. Do skupiny Malware patří viry, Spyware, Adware, Dialer a trojské koně.

Poslední aktuální hrozbou je dle serveru www.hoax.cz zejména Malware s názvem „Facebook online“. E-mail osahuje text a přílohu, ve které je soubor Adobe_Player11.exe. Pochopitelně jde o trojského koně Agent_r.LC (viz přílohu Adobe_Player11.exe).

5.7.1 Viry

Virus je program, který se dokáže samovolně šířit a provádět škodlivou činnost v operačním systému. Vir neodmyslitelně patří k nástroji, který usnadňuje útočníkovi jednorázové napadení, ale i dlouhodobější parazitování na počítačových systémech. Viry tedy mohou být vytvořené z mnoha důvodů, mohou pouze mazat soubory na úložištích, odposlouchávat komunikaci, tvořit zadní vrátka do systému nebo mohou pracovat na principu Logica Bomb, to znamená, že virus se projeví, jakmile dosáhne nějakého matematicky popsatelného výkonu. Virus se nedokáže šířit ve všech zdrojích. Například bezpečný obsah je takový, který nevyužívá makra - tedy například *.JPG nebo *.BMP obrázky apod. Prvním virem uváděným v odborných publikacích je Virus Brain, který byl vytvořen v roce 1986 a napadal boot sektory 360KB disket.

5.7.1.1 Druhy virů:

Viry můžeme třídit podle toho, jak se šíří, jakou část systému napadají nebo také podle toho, jak se virus aktivuje. Zajímavá statistika vznikne při sledování způsobu šíření virů z roku 1999, kde na vzestupu jsou viry šířící se prostřednictvím elektronické komunikace a naopak do útlumu jdou přenosová média, jako jsou diskety.

Zdroj	1996	1997	1998
Disketa, demoverze a podobně	11%	8.1%	4.4%
Disketa, opravář	3%	3.4%	3.0%
Disketa, správce počítačové sitě	1%	2.7%	0.7%
Disketa, zabalený software	2%	4.4%	1.7%
Disketa, záměrně infikovaná	0%	1.0%	1.0%
Disketa přinesená z domu	36%	42.3%	36.0%
Disketa, ostatní	21%	26.5%	20.5%
Distribuční CD	0%	0.7%	1.7%
Stažení z BBS, AOL, CompuServe, Internet	10%	16.1%	9.4%
Stažení odjinud (terminálová emulace, klient server)	2%	2.4%	3.0%
Příloha elektronické pošty	9%	26.2%	32.3%
Automatická distribuce software	0%	1.7%	1.3%
Prohlížení WWW	--	5.4%	2.0%
Ostatní	0%	5.0%	0.7%
Zdroj není znám	15%	7%	5.4%

Obr.8: Zdroj nákazy, zdroj: http://www.ics.muni.cz/ [dostupné: 2011-03-12]

5.7.1.1.1 Boot viry

Tento druh viru útočí na Boot Sektory disku, MBR neboli Master Boot Record nebo napadá přímo FAT tabulku, takže napadá systémovou část disku. Jeho šíření probíhá pomocí povoleného bootování v BIOSu. Stačí následně mít vložené médium v mechanice a boot virus se aktivuje a nakopíruje na systémovou část pevného disku. Při jakémkoliv dalším restartu počítače se boot virus aktivuje.

5.7.1.1.2 Souborové viry

Jedná se o jednodušší verzi viru – oblastí, kterou tento virus napadá, je pouze aktuálně prováděný program. Tento virus následně soubor nahradí vlastním škodlivým kódem, tedy většinou použije sám sebe, nebo virus přepíše program jen z části. Tím dojde k jeho znefunkčnění a následné možné chybové hlášky.

5.7.1.1.3 Multipartitní viry

Jak sám název napovídá, jedná se o virus, který napadá jak systémovou oblast disku, tak jeho souborovou oblast. Je to tedy kombinace viru, který dokáže naráz napadnout jak zavádějící stopu boot sektoru tak i soubor.

5.7.1.1.4 Makroviry

Tento druh viru je velmi zákeřný. Pro své šíření využívá makra, která jsou běžnou součástí většiny kancelářských aplikací, především tedy Microsoft Office. Mezi velmi zákeřné patřil i virus W97M/Melissa[18]. Vir po aktivování, nejčastěji to byla určitá operace v Office 97, sáhl do adresáře Outlook a vytáhl náhodně 50 e-mailových adres, na něž odeslal dokument, se kterým pracujete.

5.7.1.1.5 Stealth viry

Jak jméno tohoto viru napovídá, jedná se vir, který se snaží svou přítomnost v systému zamaskovat (Stealth znamená v překladu tajnost, tajné jednání). Tento virus kontroluje veškerou komunikaci, která je směřována na infikovaný soubor. Dojde-li na komunikaci, kde je volán, infikovaný soubor vrací hodnotu souboru před jeho

[18] Zdroj : http://service1.symantec.com/sarc/sarc.nsf/html/w97m.melissa.w.html [dostuplné: 2011-03-12]

infikováním. Tato technika virů se již naštěstí tolik nešíří, protože na něj antivirové programy velmi rychle zareagovaly a hlídají si každé přerušení či nežádoucí zdržení.

5.7.1.1.6 Polymorfní viry

Na rozdíl od Stealth viru, který upravuje komunikaci přímo za provozu, polymorfní viry se uloží do napadeného souboru po částech, tzn. ani jedna kopie polymorfního viru nikdy nebude stejná. To velmi komplikuje vyhledávání tohoto druhu viru obyčejným antivirovým programům.

5.7.1.1.7 Rezidentní viry

Rezidentní druh viru je neustále přítomný v paměti a aktivně ovlivňuje veškeré programy, se kterými uživatel pracuje. Jakousi výhodou tedy je, že virus nemusí aktivně hledat svůj cíl k napadení.

5.7.1.2 Detekce virů

V této době není na trhu dostupná technologie, jež naprosto neomylně dokáže detekovat každou hrozbu, které můžeme čelit z celosvětové sítě internetu. V každém případě doporučuji mít antivirový program například ještě spojený s Firewallem, který by podle mého názoru měl být nainstalovaný na každé stanici.

5.7.2 Trojský kůň

Název „trojský kůň“ pochází z antiky z dob dobytí Tróji. Je to název velmi příhodný. Většinou se jedná o samostatný program nebo aplikaci, která se tváří jako neškodná, tedy například jako hra nebo spořič obrazovky, po jeho spuštění se ovšem podle druhu trojského koně začnou například otevírat „zadní dvířka“ do počítače. Tyto otevřené porty následně využívají útočníci ve svůj prospěch. Funkce trojského koně nemusí být jen v otevírání, a tudíž ve sdílení portu pro případný DDOS Attack. Trojský kůň může také sloužit jako keylogger, sniffer, URL redirect nebo FTP server.

5.7.3 Spyware

Spyware je označení pro veškerý software, který odesílá vaše data bez vašeho vědomí. Spyware bývá velmi často spojován s nechtěným zobrazováním reklam tzn.

pop-up okna. Zde hovoříme o Adwaru. Spyware ale nejčastěji odesílá statistiky návštěvnosti, čísla kreditních karet nebo nešifrované hesla. Může také sledovat, co píšete, tedy může se chovat jako keylogger a také zaznamenávat pohyby a stisknutí myši. Výskyt tohoto škodlivého kódu poznáte podle určitých signálů, jako jsou zpomalení počítače, zobrazení nechtěných nových ikon na ploše, častý výskyt chyb Windows nebo zvýšený počet vyskakujících oken a podobně.

5.7.3.1 Keylogger

Keylogger nebo také keystroke logger v překladu logování úhozů klávesy. Jedná se o proces, při němž dochází ke snímání stisknutí kláves a ukládání nebo přímé odesílání útočníkovi. keylogger se řadí mezi virus-spyware a antivirus by měl takovéto hrozbě odolat a upozornit na něho. Jedná se tedy o variantu případu, kdy je keylogger na softwaru. keylogger se ovšem může vyskytovat i v hardwarové podobě.

Obr.9: Hardwarový keylogger Zdroj: http://www-cs-faculty.stanford.edu [dostupné: 2011-03-12]

V tomto případě se jedné o samostatné zařízení (průchozí redukce), které se připojí na kabel klávesnice v podobě PS2 nebo USB konektoru. Následné stisknutí klávesnice se ukládá do integrované paměti keyloggeru. Detekce takového zařízení je velmi složitá, většinou se zjistí při ověřování napětí nebo případným časovým zpožděním způsobeným tím, že uložení stisku klávesnice do interní paměti keyloggeru si vyžádá určitou dobu. Ochrana proti keyloggeru je v používání antiviru. Pokud je počítač volně přístupný veřejnosti, tak v pravidelných kontrolách počítače je nutno zjišťovat, není-li na něj napojeno nějaké další, neznámé zařízení. Prvotní myšlenka keyloggeru byla pouze v zachycování stisku kláves počítače, dnes tomu tak není moderní keyloggery

svedou i logování pohybů myši, zachycují online komunikaci například komunikátorů jako je ICQ nebo Skype, síťový provoz nebo i různé klávesové zkratky.

Exploit je druh programu, který využívá chyby v operačním systému. Je velmi rozšířený, pro operační systém Windows. Program v tomto systému spouští bez vědomí uživatele následně po nějaké chybě další programy, samozřejmě nejčastěji škodlivého původu. Ochrana proti těmto Exploitům je v pravidelném aktualizování bezpečnostních chyb – Microsoft na své chyby upozorňuje pomocí záplat, tzn. servis packů.

5.7.3.2 Adware

Adware je reklama, která se zobrazuje při práci s nějakou aplikací. Mezi nejznámější Adware patří reklamní banner v aplikaci ICQ, který si miliony uživatelů této aplikace instalují dobrovolně do svých počítačů.

Obr.10: Spodní část ICQ

Adware reklama se tedy může vyskytovat v řadě od těchto nenáročných bannerů až k vyskakovacím oknům, která mohou velmi obtěžovat uživatele počítače při práci. Jistou výhodou je, že Adware neshromažďuje a neodesílá žádné informace o uživateli, pouze se pohybuje v mezích zobrazování reklamy.

5.7.3.3 Hijacker

Tento druh viru napadá přímo internetové prohlížeče a následně mění domovskou stránku. Jedním ze signálů, které mohou uživatele upozornit na přítomnost Hijackera v počítači, je kromě změněné domovské stránky (k přenastavení může dojít i jiným způsobem než virem) také to, že má uživatel v nastavení internetového prohlížeče domovské stránky znepřístupněnou jakoukoliv změnu. Ochrana proti Hijackerům je používání osobních antivirů a pouze uvědomělá instalace programů, tedy využívání programů striktně pouze od výrobce.

5.7.3.4 Browser Helper Object

Pod zkratkou BHO se skrývá DLL knihovna, která ovlivňuje činnost internetového prohlížeče. Nejčastěji se jedná o shromaždování osobních údajů, čísel kreditních karet a hesel s následným odesíláním útočníkovi. Tento druh Spywaru napadá pouze Internet Explorer. Nejjednodušší ochranou proti BHO je využívání alternativních internetových prohlížečů nebo spíše zákaz jakékoliv manipulace s DLL knihovnami.

5.8 Spoofing

Jde o techniku, při které útočník úmyslně maskuje svou identitu pro získání výhody. Spoofing měl a v některých případech má ještě i stránku, která napomáhá administrátorovi[19]. Jedná se například o případ rozsáhlých sítí. Mám na mysli objemnou síť, která je skládá z malých, navzájem propojených sítí mimo jednu budovu. V tomto případě jsou sítě navzájem propojené určitým spojením a za toto spojení se platí. Pro kontrolou spojení existuje například kontrola aktivity Ping. Při každé takovéto kontrole je zapotřebí navázat spojení, což je drahé a za určitých okolností zbytečné. V tomto případě se dá využít Spoofingu, kdy se generují automaticky odpovědi typu „Ano, prvek je na příjmu“.

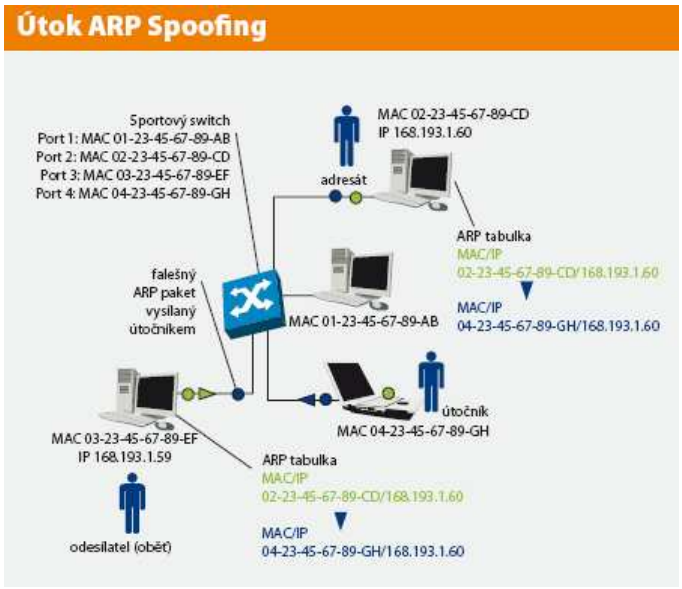
5.8.1 IP Spoofing

IP Spoofing spočívá v úmyslném vytvoření falešné IP adresy a následném zakrytí skutečné IP identity. IP Spooffing se nejčastěji využívá v kombinaci s DOS Attacku, při skenování sítí nebo k proniknutí do sítě, která využívá autentizaci na základě IP adresy – například připojíme-li se vzdáleně k síti a vydáváme se za stanici, která je lokální. V tomto případě nás systém může přihlásit bez zadání přihlašovacích údajů. Ochran proti IP Spoofingu je hned několik. Osobně preferuji zavedení povinného šifrování a autentizaci IPsec[20] pro IP vrstvu, které je například již zahrnuta v novém internetovém protokolu IPv6.

[19] Zdroj : http://www.earchiv.cz/a96/a606k130.php3
[20] IPsec je rozšíření Ip adresy o bezpečnostní prvek a to autorizace a šifrování

5.8.2 ARP Spoofing

ARP Spoofing je technika, při které dochází ke zneužití ARP protokolu. ARP, neboli Address Resolution Protocol, je protokol v síti TCP/IP. Jeho činnost spočívá v přiřazování IP adres fyzickým adresám linkové vrstvy. Celý proces probíhá následovně: chce-li stanice navázat spojení s jiným počítačem, u něhož zná jen IP adresu, zašle ARP protokol celé síti povel k přiřazení MAC adresy k dané IP adrese a v tuto chvíli může přijít na řadu ARP Spooffing, který přiřadí IP adrese podvrženou MAC adresu.
Ochrana proti tomuto útoku je jediná: použití vnitřní statické ARP tabulky.



Obr.11: ARP Spoofing , Zdroj: http://connect.zive.cz/node/714 [dostupné: 2011-03-12]

5.8.3 E-mail Spoofing

E-mail Spoofing se využívá v případech, kdy odesílatel e-mailu potřebuje zakrýt svou identitu. Změna tkví ve změně hlavičky, a tedy zároveň identity odesílatele. E-mail Spoofing se nejčastěji využívá v sociálním inženýrství při Phisingu. Tedy dojde k odeslání e-mailu, kde po příjemci požadujete jeho přístupové údaje například k bankovnímu účtu.

```
Return-Path: <jan.novak@al23.cz>
Delivered-To: jan.novak@al23.cz
Received: (qmail 508 invoked by uid 89); 25 Nov 2010 14:08:05 -0000
Received: by simscan 1.3.1 ppid: 474, pid: 480, t: 0.2808s
          scanners: clamav: 0.95.1/m: spam: 3.2.5
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on
mxavas4.forpsi.com
X-Spam-Level: *
X-Spam-Status: Yes, score=1.0 required=1.0 tests=BAYES_50,RDNS_NONE
autolearn=disabled version=3.2.5
X-Spam-Report:   *  1.0 BAYES_50 BODY: Bayesian spam probability is 40 to
60% *      [score: 0.4131] *  0.0 RDNS_NONE Delivered to trusted network
by a host with no rDNS
Received: from unknown (HELO server.cosi.tld) (1.1.1.1)
  by mxavas4.forpsi.com with SMTP; 25 Nov 2010 14:08:05 -0000
To: jan.novak@al23.cz
Received: from PC (PC [10.10.10.10])
          by server.cosi.tld (Server) with HTTP
          for jan.novak@al23.cz;
          Thu, 25 Nov 2010 15:07:05 +0100 (CET)
Date: Thu, 25 Nov 2010 15:08:05 +0100 (CET)
From: =?iso-8859-2?Q?Jan=20Nov=E1k?= <jan.novak@al23.cz>
Subject: *****SPAM*****  =?us-ascii?Q?
Fwd=3A=20Dear=20jan=2Enovak=40al23=2Ecz=20LOVE=20YOU=21?=
Mime-Version: 1.0
Message-Id: <24949.1388.2854-8096-1026270031-1290694085@aaaaa.tld>
Content-Transfer-Encoding: 7bit
Content-Type: text/plain;
          charset="us-ascii"
```

Obr.12: Hlavička emailu, Zdroj: http://kb.forpsi.com/ [dostupné: 2011-03-12]

Příklad odeslání emailu z konzole telnetu:

```
MAIL FROM : email@email.cz
250 OK
RCPT  TO: email2@email.cz
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
TO: email2@email.cz
FROM: email@email.cz
Text emailu
.
250 OK id= ID odeslaného emailu
```

5.8.4 MAC Spoofing

MAC Spoofing spočívá ve změně MAC (Media Access Control) adresy síťového zařízení.

Příklad změny MAC adresy pod Linuxem:

```
/etc/rc.d/network stop
ifconfig ethX hw ether 00:00:00:00:00:00
/etc/rc.d/network start
```

5.9 Fyzické útoky

V této kapitole se zaměřuji na přímé ohrožení, které může nastat případným přímým fyzickým přístupem útočníka do objektu.

5.9.1 Přímý průnik do objektu

Lidé dnes stále více a více času tráví v kancelářském prostředí u svého počítače. Jedná se o prostředí, kde může útočník velice snadno uspět. Na chvilku se vcítíme do role útočníka a pokusíme se shrnout, jaká nebezpečí tkví za podmínek, že útočník má fyzický přístup do vaší kanceláře a že má dostatek času, který může využít ke sběru dat.

1. První a velmi častou chybou uživatele je poznamenávání svých přístupových údajů na samolepící papír, který umístí na okraj monitoru, klávesnice nebo poličky.
2. Uživatel se neodhlašuje a je stále přihlášen, při odchodu neuzavírá svůj profil. Postačí nastavení při přechodu na spořič obrazovky uzamknout profil.
3. Špatná konfigurace PC. Je nutné dbát na správné nakonfigurování, nejlépe mít zabezpečené zaheslování BIOSu, omezení bootování, nastavení nutnost autorizace pomocí přihlašovacích údajů.
4. Další častou chybou je také ponechávání v kanceláři autorizačních čipů, karet nebo USB klíčů (token).
5. Odhazování citlivých dokumentů do odpadkového koše bez skartace. V tomto případě nemusí mít ani útočník fyzický přístup do kanceláře. Stačí si správně vytipovat příslušné místa na sběr odpadu.
6. Citlivá data jsou uložena na přenosných mediích, například na CD, DVD, flash discích nebo na páskách přímo určených na zálohování. Takováto data je potřeba umisťovat do trezoru nebo šifrovat.

7. Poznamenávání citlivých dat do poznámkového bloku nebo volných listů papírů a ponechání volně na desce pracovního stolu.
8. Centralizace citlivých dat na úložné prostory například v serverovně. V dnešní době není problém mechanicky vymontovat pevní disk z počítače a pomocí speciální redukce přímo připojit k donesenému notebooku a data vykopírovat.

6. Praktická část

Během studia jsem měl možnost vyzkoušet pod odborným dohledem některé z výše popisovaných útoků. Zhodnocením těchto zkušeností se budu zabývat v praktické části své bakalářské práce. Mým cílem byl co možná nejvěrohodnější zásah. Neměl jsem žádné informace o počítačových systémech, které jsou využívány.

6.1 Plánování útoku

1. **Cílem je získání fyzického přístupu včetně plných lokálních práv nad počítačem nebo úspěšná autorizace do dané interní sítě.** Před každým útokem se útočník snaží zjistit o daných systémech a jejich zabezpečení co nejvíce informací. Já jsem se rozhodl, i kvůli velké fluktuaci studentů v počítačových učebnách, pro fyzický přístup a pro pokus napadení sítě interně.
2. **Kompletní proskenování interní sítě a získání maximálního přehledu o systémech a aktivních službách.** Po autorizaci nebo případném nainstalování skenerů na interní systémy fakulty získat maximální přehled nad systémy a aktivních běžících službách. Případné zacílení sociálního inženýrství na systémové administrátory fakulty.
3. **Výběr zajímavé služby.** Útočníkovi musí být vždy předem jasné, co chce útokem docílit a co chce získat. Z mé pozice mi šlo samozřejmě pouze o chvilkové znedostupnění služby, jednalo se tedy maximálně o řády jednotek minut anebo o restart služby.
4. **Zaútočení na tuto službu.** Za zřejmě nejméně chráněné a nejméně využívané služby jsem považoval webové stránky jednotlivých kateder. Tedy mým primárním cílem bylo kromě odhalení chyb na uživatelské úrovni i chvilkové znepřístupnění jedné z webové prezentace katedry.

6.2 Průběh útoku

Nyní svůj „útok“ podrobně popíši krok za krokem. Pod odborným dohledem jsem restartoval jeden ze zadních počítačů a s usednutím do židle jsem vsunul CD s bootovacím operačním systémem Linux. K mému velkému překvapení se systém nabootoval velmi rychle, proto zjištění lokálních přístupových údajů pro daný počítač nebylo nijak těžké. Po restartování jsem vysunul CD mechaniku a nechal naběhnout operační systému Windows. Přihlásil jsem se jako lokální administrátor i přes to, že jsem dostal možnost se nalogovat jako anonymní uživatel - „Student“.

Mým dalším cílem bylo ověřit, do jaké míry jsem schopen korektně autorizovat svůj notebook. Chtěl jsem vstoupit do sítě prostřednictvím zfalšované autorizace. Notebooku jsem přiřadil stejnou identitu, jakou měl stolní počítač v počítačové učebně, následně jsem se bez jakéhokoliv problému autorizoval.

Kompletní skenování sítě proběhlo během několika málo minut. Udělal jsem si přehled o síťových službách běžících na serverech a rozhodl se na doporučení dozoru zaútočit na web server, který obsahoval webové prezentace fakult.

Pomocí ARP dotazu jsem zjistil MAC adresu webserveru a již mi nic nebránilo server zahltit množstvím paketů, které měly zfalšovanou MAC a IP adresu odesílatele.

6.3 Doporučené inovace

Na základě svých postřehů bych chtěl doporučit minimální bezpečnostní opatření pro to, aby nedošlo k napadení systémů, a tím způsobené ztrátě, které je možné velmi jednoduše předejít.

6.3.1 Centrální distribuce instalovaného software včetně instalace operačního systému

Současná situace:

Všechny počítačové stanice jsou instalované z předem vytvořené image.

Nevýhody uvedeného principu:

1. Různorodost počítačových sestav, a tedy nutnost mít pro každou sestavu vlastní image.
2. Není-li pro každou sestavu vlastní image, je nutná ruční instalace driveru

a softwaru.

3. Časová náročnost na reinstalaci počítačové učebny.
4. Časová náročnost na instalaci nového softwaru.

Doporučení:

1. Všechny stanice přidat do domény fakulty.
2. Zavést centrální správu stanic a softwaru na nich instalovaných.

6.3.2 Zavedení restrikcí v připojení nového zařízení

Současná situace:

Na fakultě v počítačových učebnách nejsou stanoveny žádné restrikce v připojení nefakultních zařízení do sítě pomocí kabelu.

Nevýhody uvedeného principu:

1. Každý student se připojí se svým zařízením do počítačové sítě fakulty a získá vnitřní adresu.
2. Připojený student je anonymní a může bez problémů provést jakoukoliv operaci.

Doporučení:

1. Znemožnit připojení nefakultních zařízení pomocí kabelu.
2. Pro případy nezbytného připojení nefakultního zařízení do internetu pomocí kabelu doporučuji vybudovat VLAN pouze pro internet.

6.3.3 Nastavení oprávnění uživatelům

Současná situace:

Na stanicích není aplikována žádná politika. Uživatel má možnost na stanici instalovat software, konfigurovat operační systém a BIOS.

Nevýhody uvedeného principu:

1. Student má oprávnění na stanice instalovat jakýkoliv škodlivý software a může z učebny vytvořit stanice pro vzdálený útok.
2. Student má oprávnění nabootovat live distribuce a napadnout nebo zjistit hesla pro lokálního administrátora.
3. Kdokoliv se na stanicích smí přihlásit pod anonymním účtem „Student“

Doporučení:

1. Znemožnit přístup studentům do BIOSu.
2. Znemožnit studentům instalovat na stanice software.
3. Znemožnit spouštět neautorizovaný software.
4. Znemožnit univerzální účet „Student“.

6.3.4 Vytvoření oddělených VLAN

Současná situace:

Většina systémů jsou v jednom rozsahu IP adres.

Nevýhodou tohoto principu je:

1. Zařízení jsou navzájem viditelná a lze na ně přistupovat.

Doporučení:

1. Dodržování normy pro označování zařízení a přidělování jim příslušných adres. Například označení pro počítače PEDFWčíslo_stanice a jim přidělit rozsah adres 10.10.1.1-10.10.2.254, pro tiskárny PEDFPčíslo_tiskárny a jim přidělit rozsah adres 10.10.3.1-10.10.3.254 a pro notebooky PEDFNčíslo_notebooku a jim přidělit rozsah adres 10.10.4.1-10.10.4.254.

7. Závěr

Bakalářská práce se zaměřuje na počítačové útoky na počítače, servery a jejich služby. Primárním cílem každého útoku je omezit, ochromit tyto služby nebo z nich následně profitovat. V práci přehledně popisuji možné druhy útoků s některými příklady možné ochrany proti nim, aby bylo možné následky co nejvíce minimalizovat nebo se jim alespoň bránit8. Protože útoky na servery a jejich služby nejsou jen technologické, je důležité kromě komplexního zabezpečení vědět, o co v případě útoku útočníkovi jde. Toto jsem se snažil shrnout v kapitole „Charakteristika útoků a útočníků“.

Na citlivá data instituce nebo firmy je možné zaútočit z různých míst –
je třeba mít na paměti, že útoky nemusí být vedeny pouze přes počítačovou klávesnici počítače útočníka. Útoky mohou být vedeny i formou sociální, tedy pouze pomocí určité„výřečnosti, všímavosti a empatie“. Tím lze i v dnešní obezřetné době přesvědčit zaměstnance, aby poskytl citlivá data. Jsou známy případy, kdy pomocí podvodných e-mailů jsou zaměstnanci schopni poskytnout kompletní přístup k takovým datům. Výhodou je, že v tom lepším případě je pachatel zachycen na bezpečnostních systémech firmy nebo (v tom horším případě) pouze v pamětích zaměstnanců. Na rozdíl od softwarových útoků je toto první krok v možném dopadení pachatele trestného činu.

U softwarových útoků má útočník (při dostatku času a znalostí) možnost za sebou stopy zničit nebo v případě nouze celý útočný systém smazat, a tím nevratně skrýt jakoukoliv návaznost mezi ním a napadeným systémem.

Podle praxe ovšem můžeme říci, že ani ta nejpropracovanější bezpečnostní počítačová politika nikdy nedokáže kompletně zamezit útokům. Nelze tedy zcela zamezit případným únikům dat nebo dosáhnout zcela kompletnímu omezení přístupnosti. Vždy se může najít slabý článek v zabezpečení systému, kterým může být ať již zmiňovaný zaměstnanec nebo třeba chybně nakonfigurovaný firewall, Cisco, chybně naprogramovaná aplikace nebo jen i nezaheslovaný BIOS.

Čím více se šetří na vybavení a ochraně vnitřní sítě, tím více je potřeba financovat její případné znovuobnovení. Proto se tedy souhrnně doporučuje:

1. *Používat hardwarové a softwarové firewaly* – síťové zařízení, které dokáže řídit a zabezpečit síťový provoz, je v dnešní době snad samozřejmost. I když mnoho

společností nemá finance na zakoupení hardwarového firewallu, určitým nouzovým řešením je alespoň firewall softwarový. Nativní firewall Microsoftu je určitě lepší než nemít žádný.

2. *Používat a aktualizovat antivir na každé stanici* – všechny antivirové firmy se předhánějí v tom, která bude promptněji reagovat na virovou situaci na internetu, jejich reakce jsou někdy opravdu bleskové, tak zpravidla jen stačí mít antivir nainstalovaný a nezapomenout na nejlépe automatickou aktualizaci.
3. *Pravidelně školit systémové administrátory a uživatele* – pravidelná osvěta v této problematice by se měla uchytit v podvědomí lidí. I když v praxi lze jen těžko absolvovat zcela pravidelně školení nebo číst nejnovější publikace a testovat nové inovace v ochranně systému, každý uživatel by přesto měl mít minimální znalosti o počítačové bezpečnosti a ochrany nejen svého soukromí.
4. *Pravidelně zálohovat* – i ze své praxe dobře vím, že nezálohovaný systém, který selže (a tím umožní zaútočit), je velmi složitý. Finančně a časově je velmi náročné jej obnovit a opětovně uvést do chodu.
5. *Šifrovat data* – šifrování nachází oblibu u uživatelů až v poslední době.Uživatelé si začínají uvědomovat, že některá data je možná jednoduše ztratit nebo ve chvíli neopatrnosti o ně přijít. Většina nepoctivých uživatelů, kteří získají zašifrovaná data, situaci vzdávají a ani se nepokoušejí data rozšifrovat. Tím tedy existuje možnost ochránit data nejen při odesílání e-mailem, ale i při případné ztrátě či odcizení.
6. *Pravidelné upgradovat a aktualizovat systémy* – i programátor je jen člověk, který dělá chyby. Bohužel ještě existuje spousta útočníků, kteří tyto chyby vyhledávají a využívají ve svůj prospěch, proto jen aktualizovaný systém je bezpečný systém.

8. Použitá literatura

1. B. Hatch, J. Lee, G. Kurtz : *Hacking bez tajemství: Linux Computer Press*, Brno 2003, ISBN: 8072268694, 645 stran
2. Doseděl, T. *Počítačová bezpečnost a ochrana dat*, Brno, 2004, 190 stran, ISBN: 80-251-0106-1
3. Rychnovský, L., Peša,R., *Deset rad pro zabezpečení MS Windows 2000/XP*. Zpravodaj ÚVT MU. 2004, ISSN 1212-0901,
4. Doseděl, T., *21 základních pravidel počítačové bezpečnosti* , Computer Press, Brno 2005, 52 stran, ISBN: 80-251-0574-1
5. Harper, S., Eagle, Ch., Ness, J., Lester, M., *Hacking – manuál hackera*, Grada Publishing, Praha 2008 ,ISBN: 978-80-247-1346-5
6. http://www.isotf.org/news/DNS-Amplification-Attacks.pdf [dostupné: 2011-03-12]
7. www.kiv.zcu.cz/~ledvina/ds/~DoS.doc [dostupné: 2011-03-12]
8. http://reboot.cz/howto/hacking/denial-of-service-attack/articles.html?id=18 [dostupné: 2011-03-12]
9. http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm [dostupné: 2011-03-12]
10. http://service1.symantec.com/sarc/sarc.nsf/html/w97m.melissa.w.html [dostupné: 2011-03-12]
11. http://www.lupa.cz/clanky/branime-se-odposlechu-specificke-utoky/ [dostupné: 2011-03-12]
12. http://www.cs.vsb.cz/grygarek/SPS/projekty0405/IDS/ids.html#tear [dostupné: 2011-03-12]
13. http://knihy.cpress.cz/DataFiles/Book/00002741/Download/kap._7_%20K1443.pdf [dostupné: 2011-03-12]
14. http://www.ics.muni.cz/bulletin/ [dostupné: 2011-03-12]

9. Přílohy

9.1 Výpis dotazu Whois http://www.cuni.cz

domain: cuni.cz
registrant: SB:CUNI
admin-c: VH14
nsset: NSS:CUNI:2
registrar: REG-GENREG
status: paid and in zone
registered: 10.03.1996 01:00:00
changed: 27.12.2006 12:45:00
expire: 10.10.2011

contact: SB:CUNI
org: Univerzita Karlova v Praze
name: Vladimír Horák
address: Ovocný trh 5
address: Praha 1
address: 116 36
address: CZ
phone: +420.224491235
fax-no: +420.224491588
e-mail:
registrar: REG-GENREG
created: 10.08.2001 22:13:00
changed: 11.07.2009 16:39:01

contact: VH14
name: Vladimir Horak
address: CZ
phone: +420 224491235
fax-no: +420 224213392
e-mail:

registrar: REG-GENREG
created: 10.08.2001 22:13:00
changed: 21.12.2003 20:20:00

nsset: NSS:CUNI:2
nserver: ns.ces.net
nserver: golias.ruk.cuni.cz (195.113.0.2)
tech-c: SB:CUNI
tech-c: VH14
registrar: REG-GENREG
created: 01.10.2007 02:00:00

9.2 Adobe_Player11.exe

Originál emailu :
Personal Message To You From your friends at facebook video server:
Subject: " Review - My family invite you out for lunch, don't hesitate!"

Read Description for a link to part 1 Original Video added by group member.
You will see a link to Open Your Personal Message Manager.
Selecting this link will take you to the log in page where you can browse new messages.

Proceed to open full message text:

http:// login.facebook .efsonline.videomessageid-rvd8liwtc .scanerdownload .com / home . htm? / privacy / LOGIN=acnjrfnff3d6eaw

Sincerely, Antoinette Woody.
Facebook 2009 Message Center.