Ochrana firemní sítě před vnějšími hrozbami

Protection of the enterprise network against the outer threats

Martin Hvožďara

Bakalárska práca
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Martin HVOŽĎARA**
Osobní číslo:	**A07710**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Ochrana firemní sítě před vnějšími hrozbami.**

Zásady pro vypracování:

1. **Vypracujte literární rešerši dané problematiky.**
2. **Popište možnosti útoku na data firmy.**
3. **Stanovte možnosti ochrany těchto dat.**
4. **Popište metodiku penetračních testů a jejich vyhodnocení.**
5. **Realizujte praktickou ukázku penetračního testu.**
6. **Vypracujte bezpečnostní doporučení.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. BOTT, Ed, SIECHERT, Carl. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Brno : Computer Press, 2004. ISBN 80-7226-878-3.
2. JAŠEK, Roman. OCHRANA ZNALOSTÍ A DAT V PODNIKOVÝCH INFORMAČNÍCH SYSTÉMECH. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. ISBN 80-7318-095-2.
3. FRYE, Douglas. Network Security Policies and Procedures. USA : Springer Science+Business Media, LLC, 2007.
4. NORIS, Ivan. Bezpečnosť servera v sieti. [online]. 2007 [cit. 2010-02-08]. Dostupný z WWW: http://deja-vix.sk/sysadmin/security.html.
5. WACK, John, TRACY, Miles, SOUPPAYA, Murugiah. Guideline on Network Security Testing : Recommendations of the National Institute of Standards and Technology. USA, WASHINGTON : U.S. GOVERNMENT PRINTING OFFICE, 2003. Dostupný z WWW: http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

Vedoucí bakalářské práce: **Ing. Pavel Vařacha**
Ústav informatiky a umělé inteligence

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

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
LS.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Ako už názov tejto práce naznačuje, je zameraná na počítačovú sieťovú bezpečnosť. Na začiatku predkladá rozbor kľúčových literárnych zdrojov, z ktorých práca čerpá. V teoretickej časti spočiatku rozoberá základné pojmy bezpečnostných hrozieb v sieti. Ďalej sa zaoberá najčastejšími spôsobmi sieťových útokov na dáta. Nasledujúca kapitola je venovaná prevencii a ochrane dát pomocou dostupných prostriedkov ako sú antivírusy, firewally či šifrovanie dát. V poslednej teoretickej časti sa práca venuje problematike penetračných testov. Praktická časť tejto práce je orientovaná na praktickú ukážku penetračného testu. Táto časť sa prevažne zameriava na získavanie informácií o cieľovom serveri. Obsahuje tiež bezpečnostné odporúčanie pre zvýšenie bezpečnosti servera.

Kľúčové slova: hacker, malware, útok, antivírus, firewall, kryptografia, penetračný test, nmap

ABSTRACT

As the title of this work suggests, it is focused on computer network security. At the beginning it presents the analysis of the key literary resources, from which work gathers. In a theoretical part it first analyses basic ideas of the security threats in the network. Next it deals with the most frequently methods of network data attacks. Following chapter is dedicated to prevention and protection of data with using the available resources like the antivirus software, firewall or the data encryption. In the last theoretical part, the work is dedicated to penetration testing methods. Practical part of this work is focused on the practical demonstration of the penetration test. This part is mainly oriented to gathering the information about the target server. It also contains the security recommendation in case of increasing the server security.

Keywords: hacker, malware, attack, antivirus, firewall, cryptography, penetration test, nmap

Poďakovanie

Poďakovanie patrí vedúcemu mojej bakalárskej práce Ing. Bc. Pavlovi Vařachovi, ktorý mi počas vypracovávania poskytol rady a pripomienky. Ďalej ďakujem mojej rodine a priateľke za ich ochotnú podporu pri štúdiu.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Človek aj spoločnosť sa každý deň stávajú závislejšími na správnych funkciách počítačových systémov. Či už ide o zamestnanie alebo osobný život, narušenie činnosti týchto systémov môže mať na nás negatívny dopad. S pribúdajúcimi technológiami a zabezpečovacími systémami úmerne vzrastá aj počet hrozieb. Firmy, ktoré pracujú s počítačovými systémami často krát venujú príliš malú pozornosť bezpečnosti a neuvedomujú si cenu funkčnosti systémov a informácií v nich. Neuvedomujú si ani, že v sieťovom prostredí sa nekontrolovane pohybuje obrovské množstvo nebezpečných faktorov, ktoré môžu mať za následok aj úplné zlyhanie činnosti firmy. Či už ide o krádež alebo deštrukciu informácií, na ktorých firma stavia svoju činnosť, nikdy nemožno podceňovať riziká prichádzajúce zo siete. A preto je na mieste zaujímať sa o bezpečnosť svojich dát a venovať ich zabezpečeniu náležitú pozornosť. Existuje veľa nástrojov ako chrániť dáta. Jedná sa hlavne o programové vybavenie, ale dôležitá je tiež bezpečnostná politika. Len striktné pravidlá môžu zabrániť alebo zmierniť negatívne dopady mimoriadnej udalosti vyvolanej bezpečnostným incidentom. Aj ten najlepší zabezpečovací systém je zraniteľný, pokiaľ nie je dostatočná pozornosť venovaná jeho aplikácii na konkrétny systém a preto je dobré niektoré záležitosti v zabezpečení prenechať odborníkom. Treba si však uvedomiť, že psychika človeka je najzraniteľnejší článok bezpečnosti informácií a z toho dôvodu je informovanosť tou najlepšou prevenciou.

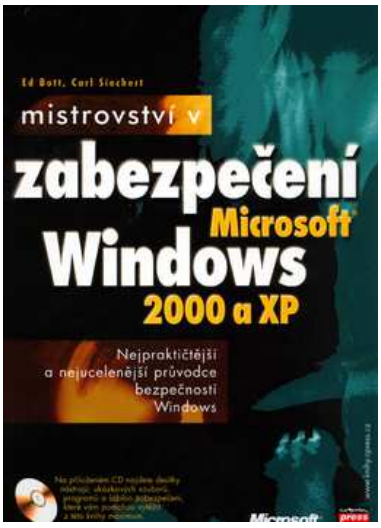
I. TEORETICKÁ ČASŤ

1 LITERÁRNA REŠERŠ POUŽITÝCH ZDROJOV

Nakoľko je problematika počítačovej bezpečnosti veľmi rozsiahla, je veľakrát ťažké sa v takom obrovskom množstve informácií orientovať. Pre vašu lepšiu orientáciu predkladám literárnu rešerš kľúčových zdrojov, z ktorých som čerpal informácie pri písaní tejto bakalárskej práce.

1.1 Tlačené zdroje

1.1.1 Mistrovství v zabezpečení Microsoft Windows 2000 a XP



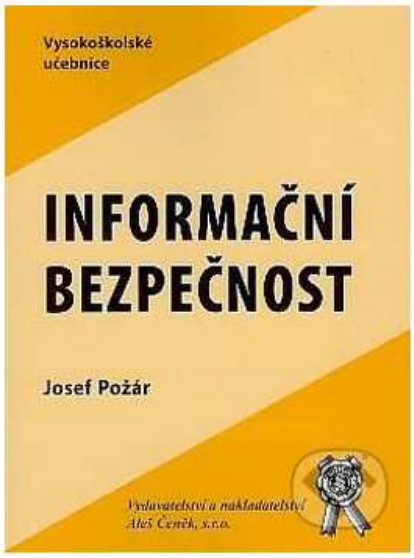
Obr. 1 Mistrovství v zabezpečení Microsoft Windows 2000 a XP

Autori Ed Bott a Carl Seichert túto knihu predstavujú ako praktického sprievodcu princípmi a jednotlivými nástrojmi pre zabezpečenie systémov Windows XP Professional, Windows XP Home Edition a Windows 2000 Proffessional. Vďaka zrozumiteľnosti a komplexnosti je táto kniha určená pre všetkých administrátorov aj domácich užívateľov, ktorí chcú zabezpečiť svoju sieť. Kniha ozrejmuje, čo je potrebné urobiť pre ochranu systému a má za úlohu naučiť sa brániť proti hackerským útokom, škodlivému softwaru a ďalším bezpečnostným hrozbám.

Kľúčové témy

- Základy zabezpečenia systému Windows
- Ochrana osobného počítača
- Ochrana počítačovej siete

1.1.2 Informační bezpečnost



Obr. 2. Informační bezpečnost

Autor Josef Požár v knihe vyjadruje rastúci význam výpočtovej techniky a s ním aj ďalšie možnosti využitia tejto techniky v bežnom živote. S tým prichádza do popredia aj nutnosť ochrany dát pred poruchami, kriminalitou, neoprávneným prístupom a celkovo zneužitím dôležitých informácií. Osnova textu je koncipovaná tak, aby sa čitateľ zoznámil s problematikou informácií a ich ochranou. Obsah je zameraný univerzálne na informácie a ich ochranu v počítačových systémoch.

Kľúčové témy

- Informačná bezpečnosť
- Ochrana dát
- Počítačová kriminalita

1.1.3 Ochrana znalostí a dat v podnikových informačních systémech

doc. Mgr. Roman Jašek, Ph.D. vytvoril skriptá, ktoré reagujú na vzrastajúci význam bezpečnosti v informačných systémoch. Ich cieľom je zvýšiť pojem o cene informácií a naučiť sa ich chrániť v rámci dostupných možností. Skriptá sa venujú širokému rozsahu informačnej bezpečnosti a to tak, aby čitateľ získal komplexný prehľad o všetkom, čo informačná bezpečnosť v dnešnej dobe ponúka.

Kľúčové témy

- Informačná bezpečnosť
- Počítačový vírus
- Kryptografia
- Elektronický podpis

1.2 Elektronické zdroje

1.2.1 www.SecIT.sk

Odborný portál zameraný na IT bezpečnosť, sieťovú bezpečnosť a programovanie, rozoberá odborné témy a prinášal odborný pohľad na mnohé zaujímavosti a novinky vo svete IT bezpečnosti. Mnoho odborných článkov, recenzií a komentárov k aktuálnemu dianiu. Súčasťou portálu je aj fórum kde zadarmo a ochotne radia skúsení odborníci.

1.2.2 deja-vix.sk/sysadmin

Príručka systémového administrátora, ktorá obsahuje veľké množstvo praktických rád a ukážok nastavení rôznych bezpečnostných sieťových prvkov. Autor stránky ponúka bližší pohľad na veľa dôležitých faktorov, s ktorými sa systémový administrátor môže stretnúť.

1.2.3 www.viry.cz

Stránka venuje pozornosť najnovším počítačovým infiltráciám. Každodenne sa aktualizuje a tak ponúka prehľad o novinkách vo svete škodlivého softwaru. Ďalej sa zaoberá ochranou, prevenciou a likvidáciou malwaru. Na stránke sa čitateľ môže stretnúť

s vysvetlením základných pojmov v oblasti ochrany dát, ako aj rôzne recenzie na zvýšenie dátovej bezpečnosti.

1.2.4 www.securityrevue.com

Stránka vytvorená akademickými a odbornými pracovníkmi bezpečnostnej komunity. Sú tu publikované články a diskusie o problémoch nielen počítačovej bezpečnosti.

2 BEZPEČNOSTNÉ RIZIKÁ V SIETI

V tejto kapitole práca vysvetľuje pojmy týkajúce sa dátovej bezpečnosti a bude sa zaoberať najznámejšími spôsobmi útokov na počítačové siete. Tieto útoky na sieť majú predovšetkým za úlohu získať dáta, prístupové údaje, prípadne vyradiť či obísť zabezpečenie siete.

2.1 Hacker, Cracker

Verejnosť hackerov príliš nerozlišuje. Berie ich ako ľudí, ktorí sa snažia získavať, meniť alebo ničiť dáta za účelom vlastného obohatenia. Pojmy hacker a cracker sa však od seba odlišujú. V hackerskom svete platí, že označenie hacker znamená určité ocenenie schopností a vedomostí človeka, zatiaľ čo cracker je označenie pre zločinca – osoba, ktorá sa chová ako násilník alebo zlodej.

Základným deliacim znakom je motivácia osoby pri jej konaní. Hacker preniká do systému za účelom získania vedomostí o ňom, zatiaľ čo cracker útočí na systém za úmyslom škodiť, prípadne sa obohatiť.

Obe osoby, hacker aj cracker majú expertné znalosti počítačových systémov a princípov fungovania sieťových mechanizmov. V USA je nelegálna činnosť v oblasti internetových prístupov do systémov najrozšírenejšia. Verejnosť postupne prestala používať pojem cracker začala deliť hackerov na tri skupiny.

White Hats (biele klobúky) – etickí hackeri, počítačoví odborníci, vďaka ich vedomostiam často uznávaní v hackerských komunitách. Ako špičkoví špecialisti bývajú zamestnávaní vládnymi agentúrami alebo súkromnými spoločnosťami. Ich náplňou práce je odhaľovať chyby, zraniteľné miesta systémov a chrániť ich pred útokmi ostatných hackerov.

Grey Hats (šedé klobúky) – hackeri, ktorí svojou činnosťou nikomu neškodia ani nepomáhajú. Ich motiváciou nie je trestná činnosť, systémy napádajú len z recesie či pre zábavu.

Black Hats (čierne klobúky) – protiklad bieleho klobúku, má výborné programátorské zručnosti a znalosti informačných technológií, využíva nedokonalosti

zabezpečenia systému, pácha trestnú činnosť, kradne, mení alebo ničí dáta, najčastejšie za účelom vlastného obohatenia. [1]

2.1.1 Dôvody útokov hackerov na počítačové systémy

Keďže biele klobúky sa dajú skôr považovať za bezpečnostných technikov, analyzuje sa konanie šedých a čiernych klobúkov. Táto činnosť sa dá rozdeliť do štyroch kategórií rozdelených na základe ich motivácie útoku na počítačový systém.

1. **Prienik do systému „pre zábavu“** – hackeri v tejto skupine berú prienik do systémov ako súťaž s ostatnými hackermi. Obvykle systémy neničia, len dajú ostatným najavo, že to dokázali – zanechajú svoj „podpis” ako dôkaz ich prítomnosti v systéme.
2. **Prienik z recesie –** Takto sú napádané hlavne servery či systémy rôznych inštitúcií, často vládnych, armádnych a pod. Hacker prelomí obranu systému a nejakým spôsobom pozmení obsah informácií v ňom tak, aby inštitúciu zosmiešnil. Ich ciele by sa dali nazvať „politicko-fylozofickými”. Ako príklad sa dajú uviesť rôzne zosmiešňujúce heslá a obrázky na stránkach politických strán pred voľbami.
3. **Ilegálny vstup do systému za účelom získania informácií** – Toto je skutočná podstata hackerov, ktorí svojim jednaním vedome páchajú protiprávnu činnosť. Hacker získava neprístupné informácie, v systéme často nič nemení. Snaží sa dostať k zabezpečeným dátam, získať prístupové práva, meniť heslá a parametre ochrany systému. Po všetkých jeho činnostiach v systéme zostávajú stopy, z ktorých sa dá identifikovať prítomnosť nežiaducej osoby.
4. **Útok na systém za účelom skreslenia obsiahnutých informácií** – Táto skupina sa dá považovať za najnebezpečnejší druh hackerov, ktorí do systému prenikajú za účelom pozmeniť originálne dáta. Týmto spôsobom sa snažia ublížiť subjektu, ktorému systém patrí. Ide o tzv. počítačovú sabotáž, o získanie a väčšinou aj zneužitie získaných dát. Útočník po sebe síce dokáže zahladiť stopy po prieniku do systému, ale jeho prítomnosť sa dá vydedukovať na základe nelegálne pozmenených dát v systéme. [1]

2.2 Malware

Pojem malware je odvodený od slov malicious software (škodlivý software) – jedná sa o súbor programov ohrozujúcich počítače a údaje v nich uložených. Malware sa do počítača dostáva zvyčajne cez internet, email a hlavne pri prezeraní nezabezpečených stránok. Často však môže byť zámerne umiestnený útočníkom do cieľového počítača. V napadnutom počítači môže poškodzovať, pozmeňovať alebo odosielať dáta tretej strane, prípadne sa šíriť na ďalšie počítače. Niektoré druhy malwaru dokážu deaktivovať zabezpečenie počítača obete a tak do neho útočníkovi umožnia prístup. Existujú aj škodlivé programy, ktoré dokážu zničiť niektoré hardvérové časti počítača. [2]

Počítačové systémy sú zraniteľné najmä z týchto dôvodov:

- **Homogenita systémov** - väčšina počítačov v sieti pracuje s rovnakým operačným systémom, rovnakým Internetovým prehliadačom a emailovým klientom. Toto umožňuje malwaru, aby sa rýchlo šíril, pretože ak narazí na jednu bezpečnostnú dieru, je pravdepodobné, že ostatné počítače budú mať túto slabinu tiež.
- **Chybovosť programov** - väčšina softwaru môže obsahovať bezpečnostné chyby. Niektoré sú tak závažné, že malware dokáže jednoducho vniknúť do systému a spôsobiť mu tak nemalé škody.
- **Nepotvrdený kód** - pri vložení prenosného média ako je napr. CD, DVD, USB disk alebo iné, sa ihneď aktivuje spúšťací program, ktorý môže obsahovať malware. Jedným z riešení je zakázať automatické spustenie prenosných médií po vložení CD alebo DVD do mechaniky.

2.2.1 Klasické počítačové vírusy

Škodlivé programy, ktoré sa spúšťajú na určitý podnet. Majú zväčša väzbu na čas, alebo dátum, spúšťajú sa a pôsobia v určitých hodinách, dňoch. Existuje niekoľko typov klasických vírusov

Súborové vírusy sa spúšťajú spolu so spustením bežných programov, najčastejšie s koncovkami .exe, .com, .sys, .dll, prípadne sú implementované do súborov balíka MS Office.

Boot vírusy bývajú uložené v boot sektore, čo je prvý sektor diskety alebo pevného disku, kde sa nachádza spúšťacia časť operačného systému. Tieto vírusy sa spúšťajú pri každom čítaní z infikovanej diskety a tak isto pri každom spustení operačného systému v infikovanom počítači. Existujú aj kombinované vírusy nachádzajúce sa naraz v súboroch i v boot sektoroch, označujú sa tiež ako multipartitné vírusy.

Stealth vírusy majú schopnosť skryť sa pred užívateľom, preto ich niektoré antivírusové programy nie sú schopné odhaliť.

Polymorfné vírusy dokážu meniť časť svojho kódu, to znamená že dve kópie toho istého vírusu nie sú totožné. Detekcia takýchto vírusov je oveľa ťažšia.

Prejavy klasických vírusov môžu byť napríklad vypisovanie nečakaných hlásení, najčastejšie však ide o deštruktívnu formu. Napádajú a mažú systémové súbory, menia adresáre a obsah súborov, následkom čoho je zhoršený chod, prípadne znefunkčnenie systému. Niektoré sú schopné poškodiť hardware počítača. [2]

2.2.2 Červy

Samostatný program ktorý sa sám veľmi rýchlo aktívne šíri. Súčasťou červa môže byť ďalší malware. Po aktivácii na infikovanom počítači sa snaží rozoslať na všetky ostatné počítače v dosahu. Rozdeľujú sa na dve hlavné skupiny podľa cesty, ktorou sa šíria po internete.

E-mailové červy využívajú masívne šírenie elektronickej pošty. Môžu sa nachádzať v prílohe emailu alebo v odkaze obsiahnutom v emailovej správe. Spustením ich používateľ na infikovanom počítači aktivuje a následne sa tieto červy snažia rozoslať všetkým kontaktom v emailovej schránke.

Sieťové červy sa šíria pomocou infikovaných paketov v internete. Sú to samostatné programy, ktoré zvyčajne nepotrebujú hostiteľa, teda nosné médium. Na infikovanom počítači sa často spúšťajú bez impulzu zo strany používateľa. Infikované pakety sú rozosielané na všetky dostupné počítače v sieti, kde sa snažia využiť bezpečnostné chyby zabezpečovacieho softwaru cieľového systému. Sieťový červ sa nedá odhaliť bežnými

antivírusovými technikami, pretože sa na napadnutom počítači nenachádza infikovaný súbor. Okrem ich prioritnej škodlivej činnosti sú schopné kompletne zahltiť lokálnu počítačovú sieť. [3]

2.2.3 Trójske kone

Škodlivý kód, ktorý je pribalený k neškodnému, zdanlivo užitočnému programu. Na rozdiel od červov a obyčajných vírusov sa trójsky kôň nereprodukuje, to znamená že sa sám nerozposiela ďalej. Trójske kone majú rôzne funkcie, napríklad môžu mazať súbory, prepisovať dáta alebo pravidelne vpúšťať do systému ďalší malware. Ten napadne sieť z vnútra a potom je ťažké odhaliť zdroj nákazy.

Najčastejšou akciou, ktorú trójske kone vykonávajú, je otvorenie tzv. **backdoor** (zadné vrátka). Prostredníctvom zadných vrátok je útočník schopný sa nepozorovane dostať do systému bez potreby poznať užívateľské mená a heslá. Zadné vrátka využívajú chyby a nedokonalosti v aplikáciách spravujúcich pripojenie do siete. [2]

Ďalšou nebezpečným typom je tzv. **keylogger** ktorý dokáže v počítači nepozorovane ukladať alebo posielať po sieti súbory, ktoré obsahujú záznamy o všetkých stlačených klávesoch na klávesnici bez toho, aby o tom cieľový užívateľ vedel. Takto sa dá odhaliť heslo, osobné údaje alebo aj sledovať komunikáciu. [6]

2.2.4 Rootkity

Špeciálny typ infiltrácie, ktorý uniká detekcii tak, že má schopnosť skryť svoju prítomnosť v napadnutom systéme. Umožňuje útočníkovi zneužiť zraniteľné miesta v systéme a získať tak plnú kontrolu nad napadnutým počítačom. Rootkit býva často súčasťou iného malwaru, ktorého prítomnosť dokáže ukryť. [6]

2.2.5 Adware

Program spôsobujúci automatické sťahovanie, zobrazovanie alebo prehrávanie reklamných a propagačných materiálov v počítači užívateľa bez jeho vedomia, či za čiastočnej asistencie. Príznakmi sú napríklad o vyskakujúce pop-up okná, vnucovanie stránok (nastavenie ako domovskej stránky bez vedomia užívateľa) a pod. [4]

2.2.6 Spyware

Špionážny software, ktorý jeho autorovi odosiela informácie o používateľovi prostredníctvom internetu bez toho, aby o tom používateľ vôbec vedel. Takým spôsobom môže autor spywaru získať informácie o prehliadaných stránkach, súboroch v počítači, inštalovaných aplikáciách a pod. [3]

3 SPÔSOBY ÚTOKU NA DÁTA

Vo veľmi komplikovanom a sofistikovanom svete sietí existuje množstvo druhov útokov na dáta, počítače alebo aj celé systémy. Komunikácia prebiehajúca medzi počítačmi v sieti obsahuje veľmi veľa špecifických informácií, ktoré môžu byť v nesprávnych rukách veľkou hrozbou. Tieto informácie nie je možné spozorovať bežným používaním počítača. Pre skúseného útočníka však nie je problém pomocou špeciálnych nástrojov túto komunikáciu odpočúvať alebo presmerovať a využiť tak prenášané informácie o počítačoch vo svoj prospech.

3.1 Skenovanie portov

Port by sa dal definovať ako komunikačný kanál, cez ktorý sieťové služby komunikujú. Skenovanie portov nie je priamo sieťovým útokom, ale často predznamenáva záujem útočníka o našu sieť. Je to úkon, pri ktorom sa pomocou špecializovaných programov útočník pokúša zistiť na ktorých portoch prebieha komunikácia, ktoré služby sú v sieti pustené, aké programy a operačné systémy ich obsluhujú a aké sú ich verzie. Tým môže použiť určitý malware, ktorý zneužíva chyby konkrétnych verzií a typov programov a následne zaútočiť na bežiace služby. [7]

3.1.1 Ochrana proti skenovaniu portov

Najlepšou ochranou sú administrátorom určené presné nastavenia pravidiel prevádzky na sieti a častá aktualizácia programov. Nepotrebné služby by mali byť zablokované, aby sa cez ne minimalizovali prieniky do siete. Existujú aj určité programy na ochranu pred skenovaním portov (TCP Wrapper) ktoré pracujú tak, že pri zistení záujmu skenovacieho programu útočníka mu neodošlú žiadne informácie o službách. Dôležité je aj nastavenie pravidiel firewallu, ktorý ignoruje požiadavky z IP adries, ktoré nepozná. [7]

3.2 Odchytávanie sieťovej prevádzky - Sniffing

Väčšina sietí dneška je typu ethernet, na ktorých sa používa prenosový protokol TCP/IP. Všetky dáta rozdelené na menšie časti do tzv. paketov (balíčkov) sú po takejto sieti posielané a prijímané prostredníctvom sieťových kariet na jednotlivých počítačoch. Sieť tohto typu funguje tak, že ak chce jeden stroj odovzdať informáciu inému stroju, vysiela pakety do siete. Tie obsahujú adresu cieľovej stanice. Paket však v sieti vidia všetky počítače, ale len stroj s požadovanou adresou ho príjme. Ostatné počítače ho jednoducho ignorujú tak, že na svojich sieťových kartách majú nastavený hardwarový filter, ktorý zahodí všetky pakety ktoré mu nie sú určené.

Záškodník môže na svojej sieťovej karte vypnúť hardvérový filter a tým ju prepnúť do tzv. promiskuitného režimu. V tomto režime karta zachytáva všetky pakety, ktoré sa po sieti dostanú až k nemu. Následne je schopný z vybraných paketov poskladať pôvodné informácie. K tomu slúži napríklad program tcpdump. [5]

3.3 Unášanie relácií - session hijack

Unášanie relácií je jeden z najstarších spôsobov na ovládnutie spojenia medzi dvoma počítačmi. Útočník je schopný prevziať kontrolu nad komunikačným kanálom, spraviť požadované operácie a potom zas nepozorovane vrátiť komunikačný kanál do pôvodného stavu. Pri únose relácie nemusí útočník zadávať autentifikačné údaje, ale môže priamo vykonávať operácie s právami, s akými bol pôvodný používateľ prihlásený. [26]

3.4 DoS útoky

Útoky typu Denial of Service, v preklade “odmietnutie služby” sa snažia o zneprístupnenie určitej služby, počítača alebo aj celej siete. V princípe sa útočník snaží vyradiť službu veľmi veľkým množstvom požiadaviek na cieľovú stanicu, ktorá tento nápor neunesie a skolabuje.. Existuje veľa druhov DoS útokov v závislosti na ich poli pôsobnosti. Distribuované DoS útoky sú na cieľ smerované z veľkého množstva malwarom infikovaných počítačov a môžu spolu v jednom momente vyprodukovať obrovské

množstvo požiadaviek či dát a odstaviť tak aj veľmi dobre zabezpečené servery. Najčastejším cieľom DoS útokov je zničenie alebo požadovanie finančnej čiastky pod hrozbou opätovného útoku. [7, 13]

3.5 Sociálne inžinierstvo

Sociálne inžinierstvo využíva nátlakové a lákavé metódy v podobe hroziaceho nebezpečenstva, časového limitu alebo lákavej ponuky. Zámienkou k získaniu dôvery môže byť vyššia autorita alebo dôveryhodný subjekt. Obeť často ani nevie, že sa stala obeťou zneužitia ňou poskytnutých dôveryhodných informácií tretej strane. Sociotechniky na oklamanie obetí sú v prostredí internetu veľmi častými. Existuje aj manipulácia, kedy útočník využije osobný kontakt či iné komunikačné metódy na nalákanie nič netušiacich darcov citlivých informácií. [13]

3.5.1 Phishing

Cieľom phishingu je vylákať z obete heslá alebo prístupové údaje využitím jeho neinformovanosti, alebo prílišnej dôvery. Najčastejšie sa phishingové podvody šíria prostredníctvom podvodných emailov. Útočník si dokáže svojím prejavom a formuláciou správy získať dôveru obete a nalákať ich na zaslanie napr. prihlasovacích údajov do určitého systému z dôvodu aktualizácie databázy užívateľov.

Najlepším spôsobom ako sa vyvarovať takýmto podvodom je informovanosť a nedôverčivosť. Len takto sa dá zabrániť veľmi jednoduchému prístupu neoprávnenej osoby k citlivým informáciám. [14, 15]

3.5.2 Pharming

Tento spôsob je založený na podvodnej internetovej stránke, ktorá na prvý pohľad vyzerá ako pravá. Pre neskúseného užívateľa môže byť problémom na prvý pohľad zistiť, že ide o podvod. Útočník využíva presmerovanie z jedného webu na podvodný napadnutím DNS servera a pozmenením jeho údajov o prekladaní IP adries na webové stránky. Tak docieli to, že obeť zadá do prehliadača napr. webovú adresu banky, ale DNS server ho prepojí na zamenenú IP adresu, na ktorej je podvrhnutá webová stránka s formulárom pre zadanie prihlasovacích údajov.

Ďalšou metódou je presmerovanie na podvodné stránky prostredníctvom trójskeho koňa v napadnutom počítači.

Ochranou pred pharmingom môže byť dostatočná informovanosť užívateľov. Mali by vedieť, na čo si majú dať pozor. Internetové prehliadače a antivírusové systémy sú v dnešnej dobe schopné pharming odhaliť a upozorniť naň užívateľa, prípadne takúto hrozbu zablokovať. [14, 16]

3.6 Rozlúštenie hesla

Heslo slúži ako autorizačný poznávací znak, na základe ktorého nás systém vpustí dovnútra, alebo nie. Neautorizované osoby a útočníci sa rôznymi spôsobmi snažia tieto heslá odhaliť a rozlúštiť. Tak by získali pohodlný prístup do systému. Na rozlúštenie elektronických hesiel sa s pomocou počítačov najčastejšie používajú dve techniky.

3.6.1 Útok hrubou silou

Metóda, ktorá sa snaží uhádnuť heslo postupným skúšaním všetkých kombinácií znakov. Útočník si môže v programe na to určenom vybrať, či sa budú dosadzovať malé alebo veľké písmená, čísla či rôzne iné znaky.

3.6.2 Slovníkový útok

Na internete je k dispozícii množstvo slovníkov a zoznamov slov. Tieto slovníky môžu obsahovať mená, technické výrazy, názvy miest a pod. Pri tomto type útoku sa hádajú heslá dosadzovaním slov z týchto slovníkov. Dnešné počítače dokážu vyskúšať jedno heslo aj bilión krát za sekundu, takže pokiaľ má užívateľ nastavené jednoduché heslo, je veľmi ľahké ho odhaliť.

3.6.3 Silné heslá

Existuje niekoľko pravidiel ako vytvoriť silné a bezpečné heslo.

1. Heslo musí mať najmenej 8 znakov.
2. Musí okrem malých písmen obsahovať číslice, veľké písmená a špeciálne znaky ako otázniky, výkričníky, pomlčky a iné.

3. Heslo nesmie byť jednoduchý, logický reťazec znakov ako meno či dátum narodenia.
4. Malo by byť jednoduché na zapamätanie ale ťažké na uhádnutie.
5. Na každú službu by sa malo použiť iné heslo.

Príklad vytvorenia bezpečného hesla.

Zložité a bezpečné heslá sa dajú vytvoriť napríklad zo začiatočných písmen nejakej vety. Každé druhé písmeno je veľké. Na konci a na začiatku sa zvolia ľubovoľné čísla. Medzi každé štyri znaky sa vloží špeciálny symbol.

„Peter má rád cukrovinky a koláče“

Výsledné heslo vypadá asi takto : **1PmR?cAk9**

Na vytvorenie bezpečného hesla sa tiež dá použiť generátor hesiel, ktorý nám vytvorí bezpečné a zložité heslo, ale takéto heslo sa len ťažko zapamätá. V žiadnom prípade by sme si však nemali heslá poznamenávať do dokumentov vo svojom počítači. [7]

3.7 Fyzický prístup nepovolanej osoby

Najhorším prípadom pre bezpečnosť našich informácií je to, keď je útočník schopný dostať sa fyzicky k nášmu počítaču. Bez ohľadu na to, ako dobre sú dáta v počítači zabezpečené, pokiaľ má útočník dostatok času na skopírovanie alebo zmazanie dát, môžu byť dôsledky jeho počínania fatálne. Ďalšou hrozbou je inštalácia škodlivého softwaru na náš počítač, prostredníctvom ktorého sa môže dostať na ďalšie pracovné stanice alebo si nechať preposielať informácie o tom, čo sa na počítači práve deje. [17]

3.7.1 Bezpečnostné odporúčania k fyzickému zabezpečeniu

- Uchovávajte akýkoľvek počítač, obsahujúci citlivé informácie, za zamknutými dverami.
- V miestach s veľmi rušným pohybom osôb sa dajú použiť externé bezpečnostné zámky, ktoré sa pripevňujú na počítač. Takéto zabezpečenie môže zabrániť krádeži počítača.

- Pri každom odchode od počítača sa treba odhlásiť.
- Je dôležité dávať pozor na zvedavcov „pozerajúcich cez rameno", ktorí takto môžu ľahko odpozorovať prihlasovacie údaje.
- Používajte heslom chránený šetrič obrazovky, ktorý sa zapína pri nečinnosti kratšej ako 10 minút na počítači. Pri obnovení práce šetrič požaduje heslo.
- Pri počítačoch s citlivým obsahom je nutné používať hardwarové šifrované prihlasovacie zariadenia ako sú tokeny alebo biometrické zabezpečenie. [17]

4 PREVENCIA A INFORMAČNÁ BEZPEČNOSŤ

Pojem bezpečnosť systému znamená určitú mieru istoty. Chápeme ju ako zodpovednosť za ochranu informácií a systémov, prístup do týchto systémov a ich funkčnosť. Firmy s nefunkčnými alebo nezabezpečenými informačnými systémami strácajú konkurencieschopnosť. V niektorých prípadoch môže neoprávnené nakladanie s firemnými dátami vyústiť až do takej miery, že firmy naďalej nemôžu vykonávať ich prioritnú činnosť a sú odsúdené k zániku. Je preto dôležité chrániť funkčnosť systémov a informácií, ktoré sa v nich nachádzajú.

Najdôležitejším faktorom zabezpečenia informačného systému je komplexná prevencia. To znamená, že by firmy mali počítať so všetkými možnými rizikami a včas urobiť také opatrenia, aby tieto hrozby minimalizovali. Jedná sa hlavne o prevenciu na softvérovej úrovni a bezpečnostnej politiky firmy.

V tejto kapitole sa bude zaoberať zabezpečením dát, ochranou pred neautorizovaným vstupom do systému a bezpečnostnou politikou firmy.

4.1 Informačná bezpečnosť

Informácie môžu mať určitú trhovú hodnotu a preto je s nimi možné zachádzať ako s majetkom, teda kupovať, predávať ale i kradnúť.

4.1.1 Bezpečný informačný systém

Bezpečný informačný systém môžeme definovať ako systém, ktorý chráni informácie behom ich vstupu, spracovania, uloženia, prenosu a výstupu, proti strate dostupnosti, integrity, dôveryhodnosti a pri ich likvidácii.

Systém sa pred pôsobením hrozieb bráni radou protiopatrení. Tie môžu mať rôzne podoby:

- **Administratívna** (zákaz prístupu alebo manipulácie s dátami),
- **Logická** (nastavenie prístupových práv),
- **Fyzická** (zabránenie fyzického prístupu nepovolaným osobám),
- **Technická** (diskové polia, šifrovanie, zálohovanie). [8]

Základným cieľom je ochrana a **eliminácia hrozieb a ich dopadov**. Hrozbami sú napríklad:

- Kompromitácia,
- Nedovolená modifikácia,
- Deštrukcia častí alebo celého systému,
- Zneužitie citlivých informácií,
- Použitie klamných dát, z ktorých budú odvodené chybné výsledky,
- Neoprávnený prístup k hmotným a nehmotným častiam systému,
- Únik informácií (kopírovanie, krádež). [8]

4.2 Antivírusová ochrana

Antivírusový program je jeden z najpoužívanejších ochranných opatrení, ktorý sa používa proti infiltrácii škodlivého softwaru. Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupno-výstupné miesta, ktorými by prípadná infiltrácia mohla do informačného systému preniknúť. Týmito vstupno-výstupnými miestami môže byť elektronická pošta, webové stránky alebo prenosné záznamové médiá ako napr. CD alebo USB flash disky.

4.2.1 Zloženie antivírusového programu

Antivírusový program sa skladá z niekoľkých častí, ktoré majú rôzne funkcie:

- **on-access scanner** – kontrola dát, s ktorými užívateľ pracuje. Táto ochrana je spustená nepretržite,
- **on-demand scanner** – kontrolný test je vyvolaný na základe požiadavky užívateľa, ktorý dokáže prehľadávať systém podľa definovaných kritérií,
- **sťahovanie aktualizácií** z internetu,
- **kontrola prichádzajúcej a odchádzajúcej pošty**,
- **plánovač udalostí** – umožňuje vo zvolenom termíne otestovať vybranú časť,
- **karanténu** – dočasné uloženie infikovaných súborov. [9, 10]

4.2.2 Aktualizácie

Nedeliteľnou súčasťou antivírusových programov je aktualizácia cez Internet. Môže byť rozdelená na:

- **aktualizáciu programovej časti antivírusového systému** – odstraňuje nedostatky z programovej časti softvéru, prípadne ju rozširuje o nové funkcie,
- **aktualizáciu vírusovej databázy** – zaisťuje detekciu nových vírusov, prípadne upravuje detekciu už existujúcich,
- **inkrementálnu (rozdielovú) aktualizáciu** – sťahujú sa len tie časti vírusovej databázy, ktoré na serveri výrobcu pribudli od poslednej aktualizácie vykonanej užívateľom. Jej výhodou je rýchlosť vykonanej aktualizácie. [9, 10]

4.2.3 Vírusová databáza

Vírusová databáza obsahuje informácie, na základe ktorých dokáže antivírusový program vyhľadať známe druhy malwaru. Súbory vírusovej databázy sú obvykle označené dátumom ich vydania. Antivírusový program na základe informácií z vírusovej databázy detekuje väčšinu známych vírusov, ktoré vznikli pred dátumom vydania poslednej vírusovej databázy. Vírusová databáza obsahuje **názov vírusu** a **informácie o ňom**, t.j. signatúry na ktorej základe je možné vírus detekovať. [9]

4.2.4 Spôsoby detekcie infiltrácií

Detekcia známych vírusov – najjednoduchšia technika, ktorá spočíva v odhalení známeho vírusu podľa jeho signatúry v databáze.

Generická detekcia – obecnejšia metóda známych vírusov, využívaná pre rozpoznávanie nových variant. Pokiaľ nie je nájdený známy vírus, hľadajú sa sekvencie typické pre určitý vírus, ktoré sa pri jeho modifikáciách obvykle nemenia.

Heuristická analýza – umožňuje identifikovať vírus, ktorý nie je zaradený vo vírusovej databáze. V priebehu heuristickej analýzy sa používajú dve metódy:

1. **Statická heuristická analýza** – hľadanie podozrivých dátových konštrukcií s kódov,

2. **Dynamická heuristická analýza** – emulácia kódu, to znamená jeho spustenie v chránenom prostredí virtuálneho počítača vo vnútri antivírusového programu a hľadanie typických akcií, odpovedajúcich chovaniu vírusu. [9]

4.2.5 Liečenie infiltrácií

Jedným z krajných riešení odstránenia infiltrácie je zmazanie samotného infikovaného súboru, pričom však môže dôjsť k **strate dôležitých informácií**. Preto je vznikli metódy pre liečenie infiltrovaných súborov. Tieto metódy môžu byť rozdelené do dvoch skupín:

1. **Algoritmické liečenie –** metóda ktorá sa spolieha na všetky informácie, ktoré existujú ohľadom vírusu (napr. dĺžka vírusu, alebo aká je jeho pozícia v súbore). Na základe týchto údajov sa snaží antivírusový program zrekonštruovať infikované dáta do pôvodnej podoby.
2. **Heuristické liečenie –** Vírus sa po svojom spustení pokúša predať riadenie pôvodnému programu, preto ak sa sledujú činnosti od začiatku až po bod predania riadenia, je možné túto časť odstrániť a teda obnoviť súbor do pôvodnej podoby. [9]

4.2.6 Odporúčania k antivírusovej ochrane

Neustály vývoj nových technológií a softwaru vo svete počítačov so sebou prináša aj množstvo nových hrozieb. Každý deň sa čoraz rýchlejšie objavujú nové typy infiltrácií a nástrojov k páchaniu počítačovej kriminality. Mať nainštalovaný antivírusový systém neznamená takmer vôbec nič, ak tento systém nie je neustále aktualizovaný a pripravený čeliť tým najnovším hrozbám. Nasledujúcich niekoľko bezpečnostných odporúčaní týkajúcich sa antivírusového softwaru by malo užívateľom počítačov pomôcť chrániť svoje dáta.

- **Pravidelne aktualizujte vírusový update svojho antivírusového programu.** Aj ten najlepší antivírus so zastaranou vírusovou databázou je na nič. Každý deň sa objavujú nové typy malwaru a jeho mutácií. Len aktuálne informácie o nich môžu pomôcť antivírusom spoľahlivo detekovať a odstrániť nové typy infiltrácií.

- **Nikdy neotvárajte emailové prílohy od neznámeho odosielateľa.** Vo svete je v poslednej dobe veľmi rozšírené posielanie škodlivých súborov prostredníctvom elektronickej pošty.
- **Majte kontrolu nad tým, kto používa váš počítač.** Riziko nákazy vášho počítača stúpa úmerne s počtom jeho užívateľov. Stačí jeden nezodpovedný človek, ktorý navštívi infikovanú webovú stránku, vloží do počítača nakazené CD alebo otvorí emailovú prílohu s vírusom a dáta všetkých ostatných užívateľov môžu byť ohrozené.
- **Inštalujte včas všetky „záplaty" na používaný software.** Existuje malware, ktorý využíva tzv. bezpečnostné diery v operačných systémoch a aplikáciách. Pokiaľ výrobca softwaru takúto chybu zistí, väčšinou na túto chybu ihneď vydá opravu, ktorú je možné na daný software nainštalovať. Vydávanie nových „záplat" je potrebné sledovať. To sa týka hlavne operačných systémov. (Pri operačnom systéme Microsoft Windows XP sa tieto opravy nazývajú Service Pack).
- **Vždy preverujte dátové nosiče a iné médiá pred tým, než ich použijete.** Dáta na nosičoch môžu byť takisto infikované. Pred otváraním dát na nosičoch sa odporúča nosič skontrolovať antivírusovým systémom.
- **Pravidelne zálohujte.** Aj keď toto pravidlo priamo nesúvisí s antivírusovou ochranou, jeho dodržiavanie umožňuje minimalizovať prípadné škody napáchané agresívnym vírusom, nespoľahlivým hardwarom a pod. V porovnaní s cenou stratených dát sú prostriedky vynaložené na zálohovanie zanedbateľné. [8]

4.3 Firewall

Firewall je sieťové zariadenie, hardvérové alebo softvérové, ktorého úlohou je oddeliť a kontrolovať komunikáciu medzi počítačovými sieťami, napríklad Internetom a firemnou sieťou. Slúži na zamedzenie neoprávneného prístupu z vonku. [11]

Firewall kontroluje všetky prechádzajúce pakety. Kontrola prebieha na základe pravidiel, ktoré určujú podmienky a akcie. Podmienky sú stanovené pre údaje, ktoré možno získať z prebiehajúcich paketov (napr. zdrojová a cieľová adresa). Úlohou firewallu je

vyhodnocovať podmienky a ak je podmienka splnená, vykoná sa akcia. Základnými akciami sú "**povoliť dátový tok**" a "**zamietnuť dátový tok**". Po vykonaní takejto akcie firewall prestane paket spracovávať.

Ďalšou vlastnosťou firewallu, ktorá sa často používa, i keď nejde o filtrovanie, je schopnosť prekladu IP adries (Network Address Translation - NAT). NAT umožňuje zmeniť zdrojové a cieľové adresy v paketoch, čím sa najčastejšie umožňuje komunikácia so sieťami s privátnymi adresami. Je to z toho dôvodu, že z vonku sa môže firemná sieť javiť ako jeden počítač, i keď má v sebe veľa ďalších počítačov. Takto sa šetrí verejnými IP adresami, ktorých počet je v internete obmedzený. Aj preklad adries prebieha pomocou pravidiel. [11]

Hlavné výhody firewallu teda sú:

- Izolácia vnútornej siete - jeden prístupový bod
- Znemožnenie zmapovania siete zvonku
- Sledovanie sieťovej prevádzky
- Odtienenie prípadných bezpečnostných dier v softwaroch sieťových služieb

4.3.1 Typy firewallov

1. **Paketové firewally**

Najjednoduchší a najstarší typ firewallu, princíp spočíva v tom, že pravidlá presne udávajú z akej adresy a portu na akú adresu a port môže byť paket doručený. Tento spôsob kontrolovania každého paketu môže spomaľovať rýchlosť siete.

2. **Stavové paketové firewally**

Princíp je podobný ako pri jednoduchých paketových firewalloch, navyše si však ukladajú informácie o povolených spojeniach, ktoré potom môžu využiť pri rozhodovaní, či je paket súčasťou toho istého súboru, pre ktorý už proces kontroly prebehol. Odpadá tým nutnosť kontroly každého paketu a premávka na sieti sa príliš nespomaľuje.

3. Aplikačné brány

Filtrovanie komunikácie už neprebieha na základnej úrovni, ale na úrovni aplikácií a programov na úrovni klient – server. To znamená, že firewall kontroluje spustené aplikácie, služby a internetové stránky, ktoré komunikujú v našej sieti s internetom. Administrátor môže zablokovať všetky služby, ktoré považuje za nebezpečné a firewall ich potom zastaví. (Blokovanie stránok s nevhodným obsahom, chat, online hry).

Použitie firewallu

Ak chceme firewallom zabezpečiť prístup do siete, musí sa hardvérový firewall umiestniť medzi našu a vonkajšiu sieť. To znamená, že všetka komunikácia musí ísť len cez jedinú cestu. Takto je možné zaistiť, že sa do našej siete nikto nedostane vedľajšou cestou. Firewall teda vpúšťa alebo zamedzuje prístup komunikácie našej siete s nežiaducimi zdrojmi. Pokiaľ sú na firewalle nastavené striktné pravidlá, je málo pravdepodobné, aby do našej siete vstúpil niekto, kto nemá.

4.4 Kryptografia

Veda, ktorá sa zaoberá matematickým aspektom bezpečnosti informačných systémov, najmä otázkami ako sú dôvernosť a integrita dát, autentizácia a nepopierateľnosť doručenia apod. V zásade hlavnú časť kryptografie tvorí **symetrické**, **asymetrické** šifrovanie a **jednosmerné hash funkcie**. Kryptografia využíva tieto metódy šifrovania, aby ukryla citlivé údaje a informácie pred nepovoleným prístupom.

Šifrovanie je proces, v ktorom daná kryptografická metóda premení otvorený text (originálny tvar správy) pomocou kryptografického algoritmu a šifrovacieho kľúča do šifrovaného textu (ten potom zvyčajne vyzerá ako náhodný zhluk znakov). Tento text nie je možné dešifrovať bez adekvátneho kľúča. [12]

4.4.1 Symetrické šifrovanie

„Symetrické šifrovanie je postup, ktorým jednoznačne zašifrujeme pomocou kľúča čistý text na zašifrovaný text, pričom z tohto zašifrovaného textu dostaneme pôvodný text len v prípade, že poznáme pri šifrovaní použitý kľúč. Princíp symetrického šifrovania teda

spočíva v tom, že odosielateľ aj príjemca správy zdieľajú tajný kľúč, ktorým odosielateľ správu zašifruje a ktorým príjemca túto správu aj dešifruje.

Jedným z prvých šifrovacích algoritmov bol DES (v súčasnosti sa nepovažuje za bezpečný, používa sa jeho modifikovaná verzia 3-DES). V posledných rokoch vzniklo niekoľko riešení na náhradu šifry DES, napr. IDEA, CAST.“ [12]

4.4.2 Asymetrické šifrovanie

„Problém so symetrickým šifrovaním je v zabezpečení prenosu kľúča, ktorý sa musí preniesť cez nejaké médium. Elektronický kanál je ľahko odpočúvateľný, fyzický prenos je na druhej strane veľmi pomalý. Asymetrické šifrovanie tento problém rieši veľmi efektívne. Je založené na jednoduchej myšlienke: **správa je dešifrovaná iným kľúčom než bola šifrovaná**. Každý z komunikujúcich partnerov vlastní dvojicu kľúčov, jeden tajný tzv. privátny a jeden verejný. Správa je zakódovaná verejným kľúčom, ktorý je distribuovaný všetkým partnerom dotyčnej osoby, ale táto osoba môže správu dekódovať len svojim privátnym kľúčom. Asymetrické šifrovanie sa používa pri **elektronickom podpise**.“ [12]

4.4.3 Jednosmerné hash funkcie

„Symetrické a asymetrické šifrovanie sa zaoberá hlavne problematikou utajovania dát. Ďalším problémom je však integrita (neporušenosť) dát. Na jeho vyriešenie sú používané jednosmerné (hash) funkcie. Tieto transformujú ľubovoľne dlhý reťazec znakov na reťazec pevnej dĺžky (odtlačok, fingerprint). Porovnaním odtlačku pôvodnej a doručenej správy je možné zistiť integritu prenášaných dát. Na hashovacie funkcie sú kladené nasledujúce požiadavky:

- k danému odtlačku (fingerprintu) prakticky nie je možné zostrojiť pôvodný dokument, (matematicky vyjadrené: neexistuje inverzná funkcia k hash funkcii),
- prakticky neexistujú dva dokumenty, ktoré majú rovnakú hashovaciu hodnotu (fingerprint),
- ak bol zmenený jeden bit v dokumente, odtlačok sa oproti pôvodnému zmení viac ako v jednom bite.

Hash funkcie sú dôležité aj pri ukladaní prístupových hesiel do informačných systémov. Z užívateľského hesla sa vytvorí odtlačok, ktorý sa uloží v databáze. Pri ďalšom prihlasovaní systém porovná odtlačok zadaného hesla a hesla v databáze. Pokiaľ sa zhodujú, užívateľ je vpustený do systému. Všetko z tohto má veľmi dôležité miesto v informačných technológiách, hlavne v elektronickom bankovníctve. Sú aj súčasťou tvorby digitálneho podpisu.“ [12]

4.5 Elektronický podpis

Celosvetová snaha o integráciu elektronickej komunikácie do bežného života so sebou priniesla aj potrebu overovania pravosti tejto komunikácie. Úlohou technológie elektronického podpisu je zaručene identifikovať autora dokumentu, ktorý ho podpíše. Tým môže byť nahradený klasický podpis v komunikácii osôb napríklad s verejnou správou, čím pre podnikateľov odpadá nutnosť byť fyzicky prítomný na všetkých úradoch a inštitúciách. Tento proces oveľa zjednodušuje právne úkony a overovanie totožnosti oproti klasickému podpisu, ale má aj oveľa iných výhod.

4.5.1 Výhody elektronického podpisu

- Je takmer nemožné sfalšovať elektronický podpis. Je to vďaka použitiu najmodernejších šifrovacích algoritmov.
- Je veľmi jednoduché overiť pravosť tohto podpisu a následne jednoznačne vyhodnotiť, či je podpis správny alebo nie. U klasického podpisu na papier sa pri porovnávaní môžu prehliadnuť určité znaky pravosti.
- Vždy je zaručená integrita správy. To znamená, že obsah správy je vždy rovnaký ako v dobe podpisu dokumentu.
- Je nepopierateľný, pretože sa nedá podpísať prázdny dokument, ktorého obsah by bol doplnený neskôr. Tým podpisovateľ nemôže poprieť, že nebol oboznámený s obsahom správy v čase jej podpisovania. [8]

4.5.2 Zaručený elektronický podpis

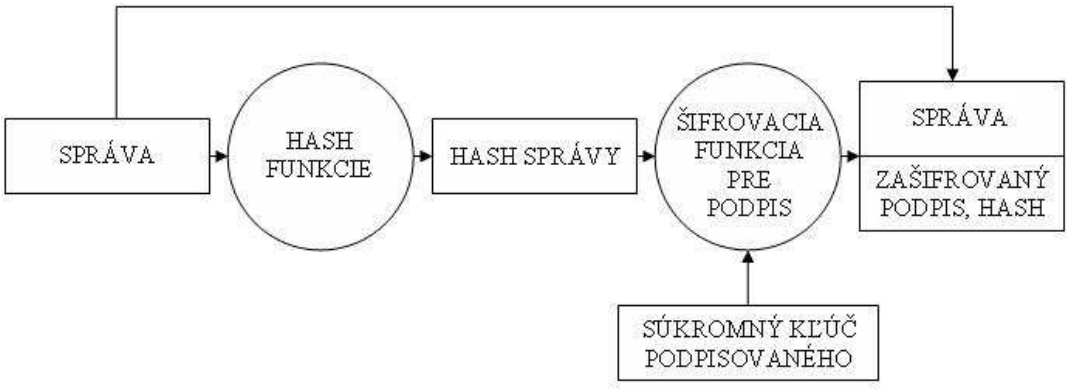
Aby bola naplnená právna podstata uznania elektronického podpisu, hovoríme o tzv. zaručenom elektronickom podpise. Je to podpis, ktorý v ČR spĺňa požiadavky podľa **Zákona o elektronickom podpise č.227/2000 Sb.** Tieto požiadavky sú:

- je jednoznačne spojený s podpisujúcou osobou,
- umožňuje identifikáciu podpisujúcej osoby vo vzťahu k dátovej správe,
- bol vytvorený a pripojený k dátovej správe pomocou schválených prostriedkov, ktoré podpisujúca osoba môže udržať pod svojou výhradnou kontrolou,
- je k dátovej správe, ku ktorej sa vzťahuje, pripojený takým spôsobom, že je možné zistiť akúkoľvek následnú zmenu dát. [8]

4.5.3 Princíp elektronického podpisovania a overovania

Elektronické podpisovanie správy

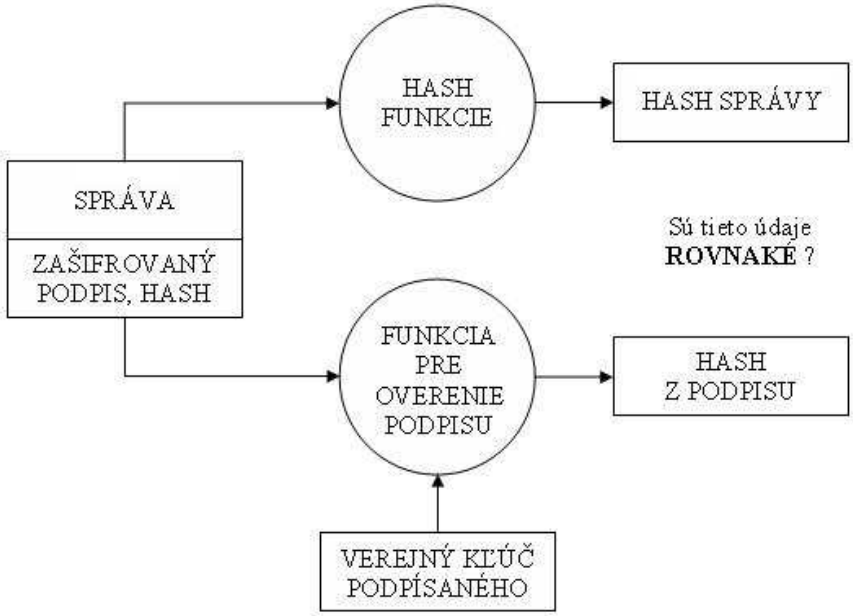
Pomocou šifrovania jednosmernej hash funkcie sa vytvorí odtlačok pôvodnej správy. Podpisovateľ ho zašifruje svojím súkromným kľúčom, ktorý má len on a pripojí ho k správe. Zašifrovaný odtlačok pôvodnej správy neskôr slúži ako kontrola integrity. Princíp je zobrazený na Obr. 3. [8]



Obr. 3. Princíp elektronického podpisovania správy [8]

Overovanie pravosti podpisu

Adresát prijme správu spolu s kontrolným súborom, v ktorom sa nachádza zašifrovaný odtlačok pôvodnej správy. Pomocou verejného kľúča odosielateľa si dešifruje kontrolný súbor a odtlačok v ňom porovná s odtlačkom správy ktorá mu prišla. Ak sa oba odtlačky zhodujú, znamená to, že správa ktorú číta príjemca je rovnaká ako odoslaná správa. Princíp je zobrazený na Obr. 4. [8]



Obr. 4. Princíp overovania pravosti podpisu [8]

Pri používaní elektronického podpisu je možné zabrániť nechcenému poskytovaniu informácií tretej strane. Každý elektronický podpis je schválený a obsahuje informácie o osobe, ktorá ho používa. Pokiaľ medzi sebou komunikujú dve strany, každá s platným elektronickým podpisom, každá zo strán vie, od koho prijíma správy a teda sa dá zabrániť rôznym falošným a navádzajúcim dezinformáciám. Tým sa dá zabrániť tomu, aby obeť poskytovala informácie neautorizovanému subjektu, teda útočníkovi.

5 PENETRAČNÉ TESTY

Väčšina súčasných firiem používa celý komplex rôznych operačných systémov a aplikácií. V podnikových procesoch sú používané aj služby internetu. Softvérové prostredie je teda veľmi komplikované. Komerčný aj voľne šíriteľný software takmer vždy obsahuje rôzne bezpečnostné chyby, ktoré sa objavujú až pri samotnom používaní programov. Každý týždeň sa objaví a zverejní niekoľko nových bezpečnostných chýb v štandardne používanom softvéri.

Zneužitie týchto chýb predstavuje vážne narušenie bezpečnosti, pretože jeho dôsledkom je únik, strata či zmena údajov, strata dostupnosti služieb alebo kontroly nad nimi. Prieniky hackerov z internetu, narušenie dostupnosti firemných služieb či infiltrácia do siete sú dnes vážnou hrozbou. V súčasnosti môže byť potenciálnym útočníkom naozaj ktokoľvek a vďaka ľahko dostupným sofistikovaným programom to môže byť aj osoba bez väčších znalostí „hackovacích“ techník. Je potrebné pravidelne prehodnocovať dostatočnosť, konzistentnosť a vhodnosť použitých bezpečnostných opatrení v sieti. [18, 20]

Z hľadiska miesta, odkiaľ môže útok pochádzať, sa penetračné testy rozdeľujú:

- **Externé penetračné testy** - simuluje sa útok hackera z internetu, ktorý využíva všetky prostriedky a informácie o cieľovom systéme, ktoré sú mu na internete voľne prístupné. Najviac útokov na siete pochádza práve z externého prostredia.
- **Interné penetračné testy** - tester má priamy a úplný prístup do internej podnikovej siete, využíva všetky dostupné informácie o konfigurácii siete a takisto pripojené zariadenia. Môže sa napríklad jednať o nespokojného zamestnanca alebo hackera s priamym fyzickým prístupom.

„Penetračné testovanie je tradičnou a akceptovanou metódou na preverenie stavu informačnej bezpečnosti systému. Penetračný test je realistickou simuláciou aktivít hackera / crackera voči aktívam spoločnosti. Prostredníctvom efektívne realizovaného penetračného testu je možné odpovedať na otázku, aké sú ďalšie potreby v oblasti informačnej bezpečnosti a identifikovať zraniteľné miesta.“ [19]

Najčastejšie bezpečnostné problémy, ktorých pôvod súvisí s používaním internetu, sa týkajú:

- najrozšírenejších operačných systémov - všetkých verzií OS firmy Microsoft a variantov systému UNIX (komerčných i voľne šíriteľných),
- štandardne používaného softwaru poskytujúceho služby cez Internet - WWW servery, internetové prehliadače a programy doručujúce elektronickú poštu,
- počítačových vírusov, červov a iného šíriaceho sa zlomyseľného kódu (malwaru). [18]

Hlavné ciele penetračného testovania sú:

1. Zvýšiť bezpečnosť IT
2. Identifikovať zraniteľnosti IT
3. Nezávislé potvrdenie stavu bezpečnosti IT externou organizáciou
4. Zvýšiť bezpečnosť organizácie a personálnej infraštruktúry [23]

5.1 Metodika penetračných testov

Vo všeobecnosti sa penetračné testy dajú formulovať ako činnosť, pri ktorej sú kontrolovane napádané počítačové siete. Tým sa zisťujú ich slabé miesta. Keďže sa stále objavujú nové bezpečnostné riziká, mali by sa tieto testy vykonávať opakovane. Periodickým testovaním sa dá zistiť, či došlo k zlepšeniu bezpečnosti siete oproti testom minulým.

Penetračné testy, tiež nazývané ethical hacking, umožňujú organizáciám preveriť odolnosť a zabezpečenie ich počítačovej siete proti pokusom o nežiaduci prienik útočníka. Testy včas odhalia, ako by sieť obstála pri reálnom pokuse o neoprávnený prienik. Metodika vychádza z overenej a účinnej kombinácie nástrojov a testovacích aplikácií, ktoré umožňujú poskytnúť množstvo poznatkov o reálnom stave bezpečnosti siete. Z výsledkov testov je tiež možné vydedukovať, aký veľký a ochromujúci dopad by na organizáciu mal nežiaduci prienik útočníka. [20]

Na základe objemu informácií, ktoré má testovaní subjekt o cieľovom systéme k dispozícii, existujú dva druhy penetračných testov:

- **Black-box** - test začína bez akýchkoľvek informácií o systéme (reálne simuluje prístup hackera, ktorý si najskôr musí zistiť všetky informácie o danom systéme).
- **White-box** - test má k dispozícii všetky informácie, vrátane konfigurácie systému (reálna simulácia prístupu útočníka - zamestnanca, ktorý disponuje detailnými informáciami o systéme).

Keďže sa penetračné testy skladajú z viacerých úkonov, preto aby sa nezabudlo na niektoré kroky, vznikli viaceré metodiky, ktoré majú určený presný postup testovacích techník. Najznámejšie a najpoužívanejšie metodiky sú OSSTMM (Open Source Security Testing Methodology Manual), a OWASP (Open Web Application Security Project), potom napríklad ISSAF (Information Systems Security Assesment Framework) a ďalej dokument inštitútu NIST - Guideline on Network Security. [22]

OSSTMM je univerzálna metodika, ktorá opisuje postup a podmienky testovania a definuje rozsah výslednej správy. Cieľom tejto metodiky je zabezpečiť kvalitné vykonávanie testov, pokrytie všetkých zraniteľných kanálov, merateľnosť a opakovateľnosť výsledkov.

OWASP sa zameriava všeobecne na bezpečnosť webových aplikácií a obsahuje dnes už značne veľkú skupinu samostatných podprojektov. Na implementáciu penetračných testov je dôležitá metodika OWASP Testing Guide, ktorá dnes predstavuje najrozsiahlejšiu a najkomplexnejšiu voľne prístupnú metodiku k bezpečnostným testom webových aplikácií. [21]

5.2 Fázy penetračného testovania

Penetračné testy najčastejšie pozostávajú z troch fáz. Najskôr sa zisťujú informácie o zariadeniach v sieti, ktoré sú dostupné z internetu. Ďalej sa odhaľujú bezpečnostné slabiny na týchto miestach, ktoré by mohol útočník využiť. Nakoniec sa vyhodnotia všetky hrozby a vypracujú sa bezpečnostné odporúčania.
Celý priebeh penetračného testu by sa dal zhrnúť do týchto krokov:

1. Zisťovanie informácií o cieľových systémoch
2. Skenovanie cieľových systémov na identifikáciu poskytovaných služieb
3. Identifikácia systémov a aplikácií
4. Zisťovanie zraniteľností
5. Využitie zraniteľností na prienik do systémov [23]

5.2.1 Zber informácií

„Pre potreby penetračného testu sa zisťuje maximálne množstvo informácií z verejne dostupných zdrojov o cieľovej oblasti testovania (napr. registračné databázy, atď.). Testy sú plánované tak, aby nedošlo v prípade nájdenia slabiny k ohrozeniu skúmaného systému, tj. sú nedeštruktívne.“ [20]

Prebieha identifikácia napríklad:

- voľne prístupných účtov (ftp, telnet),
- aktívnych komponentov internetového pripojenia (ping scan),
- aktívnych služieb na týchto komponentoch (port scan),
- užívateľských účtov a ich využívania (finger, smtp),
- používaných komunikačných protokoloch,
- potencionálnych únikov informácií z cieľovej stanice,
- smerovania elektronickej pošty,
- zistenia podporovaných / používaných autentifikačných metód. [20]

5.2.2 Prienik do systému

Nadväzujúca fáza penetračného testu, ktorá má za úlohu testovať rôzne spôsoby prieniku do siete. Na základe prvej fázy sa tu využívajú najmä bezpečnostné chyby v operačných systémoch alebo aplikáciách, o ktorých sme sa dozvedeli zo získaných informácií v prvej fáze. Patrí sem:

- Využitie exploitov
- Skúšanie defaultných prístupových hesiel,
- Využitie chýb konfigurácie firewallu a web serverov,
- Obchádzanie autentifikačných mechanizmov, hádanie a lámanie hesiel a kľúčov,
- Odstavenie sieťových služieb (DoS útoky).

5.2.3 Vyhodnotenie testov

V tejto fáze sú sumarizované všetky zo získaných informácií o systéme, jeho slabinách a zneužiteľných bezpečnostných dierach, prevedených útokoch a ich následkoch. Všetky slabiny a bezpečnostné hrozby sú ohodnotené podľa stupňa závažnosti, ktorý predstavujú. Zároveň sú formulované odporúčania o možnostiach odstránenia týchto hrozieb. Všetky informácie o penetračnom testovaní sú zhrnuté do záverečnej správy, ktorá obsahuje:

- dokumentáciu vykonaných bezpečnostných penetračných testov,
- podrobné vysvetlenie penetračných testov, ak bol ich výsledok pozitívny (odhalili sa zneužiteľné chyby),
- klasifikácia výsledkov pozitívnych penetračných testov podľa ich významu,
- odporúčania postupov, ktoré vedú k odstráneniu zistených bezpečnostných nedostatkov v zabezpečení cieľového systému.

„Informácie o bezpečnostných chybách sa objavujú prakticky nepretržite a situácia v tejto oblasti sa dynamicky mení. Z tohto dôvodu je vhodné vykonávať penetračné testovanie periodicky (napríklad raz za 6 mesiacov).“ [18, 24]

II. PRAKTICKÁ ČASŤ

6 UKÁŽKA PENETRAČNÉHO TESTU

Cieľom praktickej časti bakalárskej práce bolo predviesť praktickú ukážku penetračného testu. K testovaniu bolo potrebné mať k dispozícii aspoň dve pracovné stanice. Jedna pracovná stanica bola určená k vykonávaniu penetračného testu a na druhej pracovnej stanici sa simulovali spustené sieťové služby, ktoré boli predmetom testovania. Penetračné testy sa dajú rozdeliť na externé, teda vykonávané z prostredia Internetu a interné, kedy je tester priamo pripojený vo vnútri firemnej siete, na ktorej sú servery so spustenými cieľovými sieťovými službami. Praktická časť je viac zameraná na interný penetračný test. Zaoberá sa prevažne mapovaním a vysvetlením ďalšieho postupu penetračného testu na pracovnej stanici so spusteným serverom a sieťovými službami. Táto práca bola vykonaná v experimentálnej sieti, v ktorej boli zapojené dva počítače. Jeden počítač bola testovacia stanica s operačným systémom BackTrack Linux a na druhom počítači s operačným systémom Microsoft Windows XP Professional bol aktívny server so spustenými bežnými sieťovými službami. Tieto dva počítače boli zapojené v jednej privátnej sieti a teda priamo viditeľné. Takýto penetračný test spadá do techniky white box, kedy sú pre účely testu známe všetky informácie o topológii siete a bežiacich službách v nej. Ďalej práca demonštruje princíp získavania informácií o serveroch pri externých penetračných testoch, teda technikou black box, keď do doby testovania neboli známe žiadne interné informácie o použitých systémoch na serveri. Za týmto účelom sa previedlo mapovanie školského servera Univerzity Tomáše Bati - www.utb.cz. Súčasťou praktickej časti je aj bezpečnostné odporúčanie.

6.1 Popis použitých systémov

6.1.1 Stanica s operačným systémom Microsoft Windows XP Professional

Táto cieľová stanica bola predmetom penetračného testu. Obsahovala operačný systém Microsoft Windows XP Professional so Service Packom 3.Na Obr. 5. sú zobrazené **systémové informácie o testovanej pracovnej stanici:**

Obr. 5. Systémové informácie Windows XP

Sieťové nastavenia systému Windows na Obr. 6. boli nastavené manuálne:

Fyzická adresa	00-0C-F1-D0-C0-72
Adresa IP	192.168.10.80
Maska podsiete	255.255.255.0
Predvolená brána	192.168.10.1
Servery DNS	217.119.121.225
	217.119.113.244

Obr. 6. Sieťové nastavenia

Bola nastavená neverejná IP adresa poskytovaná providerom, kvôli prípadnému prístupu na Internet z dôvodu získavania ďalších informácií pre účely penetračného testovania.

Na tomto počítači bol spustený freeware XAMPP server verzie 1.7.3, ktorý v sebe zahŕňa ľahko spustiteľné použité sieťové služby Apache web server ver. 2.2.14 s OpenSSL

0.9.8l, MySQL databázový server 5.1.41 s PBXT engine, PHP 5.3.1 a FileZilla FTP Server verzie 0.9.33. Ďalej tu bežal freeware Comodo Firewall ver. 4.0.141842.828. Do testovania boli pre porovnanie zahrnuté výsledky so zapnutým aj vypnutým firewallom.

6.1.2 Stanica s operačným systémom BackTrack Linux

Táto testovacia stanica obsahovala spustenú LiveCD distribúciu Linuxu - BackTrack verzie 4 Final, ktorá je určená na bezpečnostné audity siete a penetračné testovanie. Obsahuje veľké množstvo nástrojov, v tomto prípade využité napríklad Nmap, Nikto a metasploit framework. V súčasnosti je táto distribúcia na prvom mieste medzi LiveCD distribúciami zameranými na dátovú bezpečnosť.

Manuálne nastavenie sieťového rozhrania:

```
# ifconfig eth0 192.168.10.88 netmask 255.255.255.0 up
# route add default gw 192.168.10.1
# echo "nameserver 217.119.121.225" > /etc/resolv.conf
```

MAC adresa sieťovej karty na tomto počítači je 00:18:F3:EF:1E:C1. Bola nastavená neverejná IP adresa z rovnakej podsiete ako IP adresa cieľového počítača, ďalej sa nastavila predvolená brána do Internetu a tiež DNS server poskytnutý providerom pre prípadné prístupy do Internetu.

Informácie o operačnom systéme:

```
# uname -a
Linux bt 2.6.30.9 #1 SMP Tue Dec 1 21:51:08 EST 2009 i686
GNU/Linux
```

Verzia jadra systému je 2.6.30.9 z 1. decembra 2009. Distribúcia BackTrack ako aj mnoho iných distribúcií Linuxu je založená na licencii GNU/GPL, čo znamená že sú voľne šíriteľné a využiteľné za akýmkoľvek účelom.

6.2 Zber informácií o cieľovom systéme

Najdôležitejšia fáza penetračného testovania je zber informácií o testovanom systéme. Metódy zberu informácií sú rozsiahle a existuje ich viacero druhov, či už ide o všeobecné informácie o subjekte ako sú napríklad emailové adresy, telefónne čísla alebo údaje získané sociálnym inžinierstvom. V závislosti na charaktere a type penetračných testov sa metódy rôzne kombinujú s cieľom dosiahnutia čo najlepších výsledkov a úspešnosti penetračného testu. V tomto prípade sa práca zaoberá len získavaním informácií prostredníctvom počítačovej siete a nástrojov na to určených, napríklad Nmap a Nikto.

6.2.1 Nmap

Nmap ("Network Mapper") je open-source nástrojom na skúmanie siete a kontrolu bezpečnosti. Používa sa na rýchle scanovanie veľkých sietí, ako aj pri nasadení proti jednotlivým hostiteľom. Nmap používa IP pakety na určenie hostiteľských staníc a služieb v sieti, ktoré tieto hostiteľské stanice ponúkajú a na akom operačnom systéme bežia, aký typ paketových filtrov alebo firewallu je použitý a mnoho ďalších charakteristických informácií. V tejto práci bola použitá verzia Nmap 5.00. [25]

Mapovanie dostupných počítačov v sieti

Nmap v sebe zahŕňa aj nástroj **ping** ("Packet InterNet Groper"), čo je funkcia na overenie funkčnosti spojenia medzi dvomi sieťovými rozhraniami. Ping odosiela IP pakety a čaká na odozvu. Nmap vie urobiť hromadný ping celej podsiete

```
# nmap -sP 192.168.10.0/24

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-16 12:54 UTC
Host 192.168.10.80 is up (0.00032s latency).
MAC Address: 00:0C:F1:D0:C0:72 (Intel)
Host 192.168.10.88 is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 31.41 seconds
```

Takto sa príkazom -sP dá urobiť ping celej podsiete a zisťuje sa, ktoré sieťové rozhrania sú aktívne a pošlú svoju odozvu. Zistilo sa, že sú aktívne dve IP adresy, z toho jedna je cieľová a jedna adresa rozhrania, z ktorého vyšla požiadavka na ping. Okrem toho program vypísal aj hardwarovú MAC adresu cieľového rozhrania a jeho výrobcu.

Nmap spustený na cieľový počítač so zapnutým firewallom

```
# nmap 192.168.10.80

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-16 14:30 UTC
All 1000 scanned ports on 192.168.10.80 are filtered
MAC Address: 00:0C:F1:D0:C0:72 (Intel)
```

Výpis ukazuje, že všetky porty ktoré Nmap scanoval, sú filtrované. To naznačuje prítomnosť firewallu. V tomto prípade bol pre ukážku firewall nastavený, aby neprijímal žiadne spojenia z neznámych lokalít alebo z lokalít, ktoré nie sú nastavené administrátorom ako známe.

```
# nmap -O 192.168.10.80

Running (JUST GUESSING) : Microsoft Windows 2003|XP|2000 (95%), D-
Link embedded (88%), TRENDnet embedded (88%), Xylan embedded
(86%), Juniper Windows 2000 (85%)
Aggressive OS guesses: Microsoft Windows Small Business Server
2003 (95%), Microsoft Windows XP Professional SP2 (firewall
enabled) (92%), Microsoft Windows XP SP 2 (91%), Microsoft Windows
XP SP2 (91%), Microsoft Windows XP SP2 or SP3 (91%), Microsoft
Windows XP Professional SP2 (90%), Microsoft Windows Server 2003
Enterprise Edition SP2 (89%), Microsoft Windows XP Professional
SP2 (German) (88%), D-Link DWL-624+ or DWL-2000AP, or TRENDnet
TEW-432BRP WAP (88%), Microsoft Windows 2000 SP4 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Pokus o presné zistenie operačného systému sa nepodaril. Nmap len hádal o aký operačný systém sa môže jednať na základe charakteristických znakov. V tomto prípade s 95% pravdepodobnosťou určil, že ide o systém Microsoft Windows 2003/XP/2000.

Nmap spustený na cieľový počítač s vypnutým firewallom

Najprv sa prevedie jednoduchý Nmap, ktorý vypíše zoznam bežiacich služieb, portov na ktorých sú spustené a tiež stav portov. Existuje šesť stavov portov:

Otvorený - aplikácia na tomto porte aktívne prijíma TCP spojenia. Zistenie tohto faktu je často hlavným cieľom scanovania portov. Každý otvorený port je prístupom pre útok. Útočníci a testeri preniknutia chcú využívať otvorené porty, zatiaľ čo administrátori sa pokúšajú zatvoriť ich alebo chrániť ich firewallmi bez limitovania oprávnených používateľov.

Zatvorený - port je prístupný (prijíma a odpovedá na pakety testu vykonávaného nástrojom Nmap), ale žiadna aplikácia na ňom nepočúva. Môžu sa zísť pri zisťovaní, či je hostiteľská stanica aktívna na IP adrese (zistenie hostiteľskej stanice alebo ping scan) a ako časť detekcie OS.

Filtrovaný - Nmap nedokáže určiť, či je port otvorený, pretože filtrovanie paketov zabraňuje testom dosiahnuť tento port. Filtrovanie môže pochádzať z osobitného firewallového zariadenia, pravidiel routera alebo hostiteľského softwarového firewallu.

Nefiltrovaný - je zrejmé, že firewall na porte nepočúva ani nie je nastavený.

Otvorený / filtrovaný - je filtrovaný, ale filtrácia prebieha podľa určitých kritérií, niektoré typy prienikov sú cez tento port uskutočniteľné.

Zatvorený / filtrovaný - filtrácia úplne obmedzuje akýkoľvek vstup cez tento port. [25]

```
# nmap 192.168.10.80

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-16 15:03 UTC
Interesting ports on 192.168.10.80:
Not shown: 992 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
80/tcp   open   http
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
443/tcp  open   https
445/tcp  open   microsoft-ds
1027/tcp closed IIS
3306/tcp open   mysql
MAC Address: 00:0C:F1:D0:C0:72 (Intel)
```

Popis jednotlivých služieb

FTP (File Transfer Protocol, protokol prenosu súborov) je TCP/IP protokol určený na prenos súborov medzi počítačmi, či už na internete alebo lokálnej sieti.

HTTP - Hypertext Transfer Protocol je primárna metóda prepravy informácií na world wide, naznačuje že na cieľovom počítači beží web server.

MSRPC - je vzdialené volanie procedúr, používa sa pre rozdeľovanie aplikácií na niekoľko počítačov.

NetBios-ssn - protokol, ktorý vytvára logického spojenia (session) medzi počítačmi a prenos dát týmto spojením, napríklad pre vzdialené tlačiarne.

HTTPS - Hypertext Transfer Protocol Secure je zabezpečená verzia HTTP, komunikačného protokolu WWW, šifruje prenos dát použitím SSL (Secure Socket Layer) protokolu alebo TLS (Transport Layer Security) protokolu a tým zaisťuje primeranú ochranu pred odpočúvaním komunikácie.

Microsoft-ds - služba pre zdieľanie priečinkov a súborov na sieti.

IIS - Internet Information Services / Server je nastavenie serverových funkcií Microsoft Windows. Je to druhý najpoužívanejší server, hneď za Apache HTTP Server. Prieskum hovorí že na IIS beží približne 37.13% zo všetkých webových stránok.

MySQL - databázový server podporovaný na viacerých platformách.

Zistenie verzií bežiacich služieb.

Parameter -sV slúži ako dotaz na zisťovanie verzií bežiacich služieb.

```
# nmap -sV 192.168.10.80

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-16 12:36 UTC
Interesting ports on 192.168.10.80:
Not shown: 993 closed ports
PORT     STATE  SERVICE      VERSION
21/tcp   open   ftp          FileZilla ftpd
80/tcp   open   http         Apache httpd 2.2.14 ((Win32)
135/tcp  open   msrpc        Microsoft Windows RPC
139/tcp  open   netbios-ssn
443/tcp  open   ssl/http     Apache httpd 2.2.14 ((Win32)
445/tcp  open   microsoft-ds Microsoft Windows XP microsoft-ds
1027/tcp closed IIS
3306/tcp open   mysql?

MAC Address: 00:0C:F1:D0:C0:72 (Intel)
Service Info: OS: Windows
```

Použitím príkazu -A sa Nmap pokúsi zistiť verziu operačného systému a ostatné údaje o ňom. Nasledujúci výpis je len koniec výpisu Nmap-u, nakoľko prvá časť je totožná s výpisom s parametrom –sV

```
...
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server
2003
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_ nbstat: NetBIOS name: JANKA, NetBIOS user: <unknown>, NetBIOS
MAC: 00:0c:f1:d0:c0:72
|  smb-os-discovery: Windows XP
|  LAN Manager: Windows 2000 LAN Manager
|  Name: WORKGROUP\JANKA
|_ System time: 2010-05-16 10:29:47 UTC+2
```

Nmap zistil údaje o operačnom systéme, jeho typ, ale nevedel presne určiť o akú verziu sa jedná. Program dokáže odhadovať verziu operačného systému na základe charakteristických znakov a následným porovnávaním s charakteristikami v databáze. Ďalej opäť dokázal zistiť MAC adresu, názov počítača a pracovnú skupinu, v ktorej je zaradený.

6.3 Zhodnotenie získaných informácií

V ďalšej fáze penetračného testovania sa využívajú informácie získané v prvej fáze. Kľúčové sú informácie o otvorených portoch, bežiacich službách a ich verziách. Veľmi často sa stáva, že sa na serveri používajú neaktuálne verzie služieb, čo môže znamenať bezpečnostné riziko, pretože staré verzie pravdepodobne budú obsahovať bezpečnostné chyby.

6.3.1 Identifikácia zraniteľností nástrojom Nikto

Nástroj Nikto sa používa na scannovanie webových serverov. Je to komplexný nástroj na zisťovanie potencionálnych chýb v konfigurácii služby webového servera, hľadá zastarané, neaktuálne verzie jednotlivých modulov (PHP, SSL), prehľadáva adresáre, v ktorých sú umiestnené zdrojové kódy stránok a vyhodnocuje, či by mali alebo nemali byť prístupné, respektíve čitateľné z prostredia internetu. Toto všetko vykonáva a porovnáva na základe špecifikácie databázy zraniteľností OSVDB (Open Source Vulnerability Database).

Pomocou nástroja Nikto bol prevedený test webového servera na adrese 192.168.10.80

```
root@bt:/pentest/scanners/nikto# ./nikto.pl -host 192.168.10.80
- Nikto v2.1.0
---------------------------------------------------------------------
---------
+ Target IP:          192.168.10.80
+ Target Hostname:    192.168.10.80
+ Target Port:        80
+ Start Time:         2010-05-17 18:13:09
---------------------------------------------------------------------
---------
+ Server: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14
OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-
20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
- Root page / redirects to: http:///xampp/
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is
vulnerable to XST
+ OSVDB-0: mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color
PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 -
mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow
which may allow a remote shell (difficult to exploit).
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082,
OSVDB-756.
+ OSVDB-0: Multiple distinct index files found: #1: index.php, #2:
index.html
+ OSVDB-0: mod_ssl/2.2.14 appears to be outdated (current is at
least 2.8.31) (may depend on server version)
+ OSVDB-0: Number of sections in the version string differ from
those in the database, the server reports: 2.0.4 while the
database has: 5.8. This may cause false positives.
+ OSVDB-0: mod_perl/2.0.4 appears to be outdated (current is at
least 5.8)
+ OSVDB-682: /webalizer/: Webalizer may be installed. Versions
lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-
4C7B08C10000: PHP reveals potentially sensitive information via
certain HTTP requests which contain specific QUERY strings.
+ OSVDB-561: /server-status: This reveals Apache information.
Comment out appropriate line in httpd.conf or restrict access to
allowed hosts.
+ OSVDB-3092: /phpmyadmin/: phpMyAdmin is for managing MySQL
databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing is enabled: /icons
+ OSVDB-562: /server-info: This gives a lot of Apache information.
Comment out appropriate line in httpd.conf or restrict access to
allowed hosts.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 3588 items checked: 13 item(s) reported on remote host
+ End Time:           2010-05-17 18:18:13 (304 seconds)
---------------------------------------------------------------------
---------
+ 1 host(s) tested
```

Nikto zobrazil 13 potencionálnych zraniteľností na základe ich porovnania s databázou OSVDB. Napríklad SSL modul sa javí ako zastaralý, takisto aj Perl modul. PHP môže odhaľovať potenciálne nebezpečné informácie. Httpd.conf je konfiguračný súbor webového servera, ktorý nieje zabezpečený a teda je voľne upravovateľný, čo je kritická chyba. Takisto modul phpMyAdmin nieje zabezpečený. Nainštalovaný modul Webalizer nieje aktuálny a je zraniteľný metódou XSS – Cross Site Scripting. Všetky tieto bezpečnostné chyby môžu mať pri pokuse útočníka fatálny následok na funkčnosť webového servera.

6.3.2 Identifikácia zraniteľností programom Nessus

Ďalším skenerom zraniteľností je program Nessus. Vďaka svojej jednoduchej obsluhe patrí medzi najpoužívanejšie bezpečnostné skenery. Pracuje na princípe klient / server. Na klientskej stanici sa okrem zobrazovania výsledkov konfigurujú parametre a podmienky testu, ktorý prebehne na zvolenom serveri. Na základe vykonaných testov a odhalených slabín delí Nessus tieto slabiny do troch kategórií a to nízku, strednú a vysokú, zároveň je každej nájdenej zraniteľnosti pridelený rizikový faktor ohodnotený bodmi od 1-10, teda napríklad slabiny z nízkej kategórie majú pridelený rizikový faktor 1-3. Faktory rizikovosti sú prideľované podľa štandardu Common Vulnerability Scoring System. Na základe tohto hodnotenia je ďalej možné určiť závažnosť hrozieb a vykonať potrebné kroky v závislosti na typu bezpečnostnej politiky.

Výstupom z Nessus-u je kompletná správa obsahujúca informácie o otvorených portoch, spustených službách a ich verziách, operačnom systéme a rizikových miestach v zabezpečení servera. Nessus sa pri testoch zameriava napríklad na zadné vrátka, CGI zneužitie, DoS útoky, firewally, FTP, získanie konzoly, port scan, vzdialený prístup, nasvenia atď. [22, 27]

V praktickej časti nie sú zahrnuté výsledky získané týmto bezpečnostným nástrojom, nakoľko distribúcia BackTrack Linuxu ho neobsahuje.

6.4 Penetrácia

Najzložitejším krokom je samotný prienik do systému. Využívajú sa tu všetky informácie o zraniteľnostiach nazbierané v predchádzajúcich fázach. Cieľom penetrácie je získanie prístupu k cieľovému serveru a jeho ovládnutie, prípadne získanie citlivých dát. Táto fáza vyžaduje perfektnú znalosť sieťovej komunikácie a činnosti systémov. Nedokonalosti v zabezpečení systémov sa prekonávajú buď odstavením určitých služieb využitím ich známej chyby, napríklad buffer overflow (pretečenie zásovníka pamäte programu) alebo použitím exploitu s určitou funkciou, napríklad sprístupnenie administrátorského konta na serveri. Exploity útočník môže vytvárať sám, na čo potrebuje značné programátorské znalosti. Druhým spôsobom je využitie už vytvorených exploitov, konkrétne na zverejnené chyby v sieťových službách. [27]

6.4.1 Metasploit Framework

Metasploit Framework je užívateľské rozhranie pre testovanie počítačovej bezpečnosti. Samotný Metasploit Framework je platforma na tvorbu a vykonávanie exploitov, a zároveň obsahuje ich databázu, v ktorej sa nachádza viac ako 400 predpripravených exploitov a vyše 250 payloadov., čo je kód, ktorý sa vykoná na cieľovom systéme po úspešnom spustení exploitu. Exploity sa napríklad dajú vyhľadávať podľa čísla v databáze OSVDB. Postup pri využívaní frameworku pozostáva z nasledujúcich fáz:

- Zvolenie a konfigurácia exploitu - potrebné zvoliť exploit a nastaviť parametre, ako napríklad cieľová IP adresa a port.
- Kontrola využiteľnosti exploitu proti cieľovému systému - voliteľný krok, slúži na overenie, či je cieľový systém skutočne zraniteľný exploitom s vybranými parametrami.
- Zvolenie a konfigurácia payloadu - zvolenie payloadu, nastavenie vhodných parametrov a kontrola kompatibility payloadu s cieľovým systémom.
- Spustenie exploitu – úspešným spustením exploitu sa vykoná payload a napríklad sa objaví konzola exploitovaného systému. [27]

6.5 Ukážka získavania údajov z externého prostredia

V tejto časti sa práca zameriava na ukážku získavania užitočných informácií z prostredia Internetu. Pre tento účel bolo vykonané na školskom serveri Univerzity Tomáše Bati - www.utb.cz, získavanie informácií, ktoré by mohli predstavovať bezpečnostné riziko. Tieto informácie boli získavané z prostredia Internetu pomocou špecializovaného softwaru obsiahnutom v distribúcii Linuxu BackTrack 4, ktorý v sebe zahŕňa všetky potrebné nástroje pre účely penetračného testovania ako Nmap a Nikto.

Na testovanom serveri je prevádzkovaná webová stránka www.utb.cz. Najjednoduchším spôsobom sa dá dostupnosť webovej stránky overiť zadaním jej názvu do internetového prehliadača. Po zadaní URL www.utb.cz bola stránka zobrazená so zmenenou adresou URL web.utb.cz. To naznačuje, že v systéme DNS existuje viacero záznamov pre doménu utb.cz (tzv. Alias, Canonical name), čo umožňuje prevádzkovanie viacerých webových služieb s rôznymi názvami na jednej IP adrese a na jednom porte.

Nástroj nslookup slúži na vyslanie dotazu na DNS server, či má v databáze konkrétny názov webu a aká je jeho pridelená IP adresa, na ktorú DNS smeruje. Tento nástroj sa dá použiť len na servery, ktoré sú priamo viditeľné z prostredia Internetu.

```
# nslookup www.utb.cz
Server:         217.119.121.225
Address:        217.119.121.225#53

Non-authoritative answer:
www.utb.cz      canonical name = moon.utb.cz.
Name:   moon.utb.cz
Address: 195.178.88.67
```

Týmto spôsobom DNS server poskytol IP adresu, na ktorej sa nachádza webový server www.utb.cz. Použitím nástroja Nmap bol vykonaný portscan na adresu www.utb.cz, čo zodpovedá IP adrese 195.178.88.67. Pomocou parametrov -sS (SYN scan), -sV (Version), -O (Operačný systém), sa zobrazia bežiace služby (daemon) a ich verzie, porty na ktorých sú spustené a verzie a typ operačného systému servera.

```
# nmap  -sS -sV -O www.utb.cz

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-15 20:54 UTC
Interesting ports on moon.utb.cz (195.178.88.67):
Not shown: 985 closed ports
PORT     STATE    SERVICE      VERSION
9/tcp    open     discard?
13/tcp   open     daytime
```

```
21/tcp   open     ftp          PureFTPd
22/tcp   open     ssh          OpenSSH 3.8.1p1 Debian 8.sarge.6
(protocol 2.0)
25/tcp   filtered smtp
37/tcp   open     time?
80/tcp   open     http         Apache httpd 1.3.33 ((Debian
GNU/Linux) PHP/4.3.10-22)
111/tcp  open     rpcbind
113/tcp  open     ident
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
389/tcp  open     ldap         OpenLDAP 2.2.X
445/tcp  filtered microsoft-ds
3306/tcp open     mysql        MySQL 4.0.24_Debian-10sarge3-log
5432/tcp open     postgresql   PostgreSQL DB
Network Distance: 8 hops
Service Info: OS: Linux
```

Z portscanu bolo zistené, že na serveri www.utb.cz sú prevádzkované služby prístupné z internetu ako napríklad FTP server, webový server Apache, MySQL databázový server, ďalej emailový server odchádzajúcej pošty SMTP. Ďalej Nmap v niektorých prípadoch úspešne zobrazil verzie bežiacich služieb. Čo sa týka operačného systému servera, Nmap nebol schopný presne odhadnúť o aký systém ide, len vyhodnotil, že ide o platformu Linux.

Použítím nástroja Nikto sa preverili verzie a iné zraniteľnosti webového servera na addrese www.utb.cz.

```
/pentest/scanners/nikto# ./nikto.pl -host www.utb.cz
- Nikto v2.1.0
---------------------------------------------------------------------
---------
+ Target IP:          195.178.88.67
+ Target Hostname:    www.utb.cz
+ Target Port:        80
+ Start Time:         2010-05-16 21:25:03
---------------------------------------------------------------------
---------
+ Server: Apache/1.3.33 (Debian GNU/Linux) PHP/4.3.10-22
- Root page / redirects to: http://web.utb.cz/
+ OSVDB-0: robots.txt contains 1 entry which should be manually
viewed.
+ OSVDB-0: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is
vulnerable to XST
+ OSVDB-0: Apache/1.3.33 appears to be outdated (current is at
least Apache/2.2.14). Apache 1.3.41 and 2.0.63 are also current.
+ OSVDB-0: Number of sections in the version string differ from
those in the database, the server reports: 4.3.10.45.22 while the
database has: 5.2.8. This may cause false positives.
+ OSVDB-0: PHP/4.3.10-22 appears to be outdated (current is at
least 5.2.8)
```

```
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-
4C7B08C10000: PHP reveals potentially sensitive information via
certain HTTP requests which contain specific QUERY strings.
+ OSVDB-3268: /icons/: Directory indexing is enabled: /icons
+ 3588 items checked: 8 item(s) reported on remote host
+ End Time:           2010-05-16 21:32:36 (453 seconds)
---------------------------------------------------------------
---------
+ 1 host(s) tested
```

Výpis z nástroja Nikto zobrazil informácie na základe porovnania zraniteľností s databázou OSVDB. Celkovo vypísal 8 potencionálnych zraniteľností servera ww.utb.cz. Jedná sa napríklad o zastaralý Apache server verzie 1.3.33, modul PHP môže odhaľovať citlivé údaje, server poskytuje služby GET, HEAD, OPTIONS a TRACE, ktorú môžu predstavovať zraniteľnosť pri metóde XST – Cross Site Tracing. Všetky tieto údaje môžu predznamenávať možné bezpečnostné hrozby. Pri zdarenom útoku skúseného útočníka by tieto bezpečnostné zraniteľnosti mohli mať ochromujúci následok pre univerzitný server www.utb.cz.

6.6 Bezpečnostné odporúčania

V dnešnej dobe je štandardom či samozrejmosťou prevádzkovanie webových stránok, poštových serverov či iných sieťových služieb (web, email, ftp, atď.), ktoré majú za účel prezentovať a podporovať činnosti subjektu, ktorý ich prevádzkuje. Väčšinou sú všetky tieto služby integrované na jednom portáli, čo môže byť pre subjekt potencionálne riziko, nakoľko sú v prípade útoku na server ohrozené všetky služby súčasne. Súčasným trendom znižovania dopadu pri útoku na organizáciu je rozdelenie sieťových služieb na viacero fyzických serverov, čo má v prípade úspešného útoku za následok minimalizovať dopad na komplexnú činnosti organizácie.

Ďalším dôležitý krok v počítačovej bezpečnosti hrajú firewally. Či už ide o hardwarové alebo softwarové, dobre nastavený firewall dokáže odfiltrovať prevádzku a sieti a zabrániť tak možnému úniku informácií. Firewall sa tiež dá použiť tiež proti scannovaniu portov a zisťovaniu tak informácii o serveroch..

Na to, aby bol systém vždy na najvyššej úrovni je nutná neustála aktualizácia všetkých spustených služieb. Staré verzie môžu obsahovať využiteľné chyby.

ZÁVER

Aj keď zabezpečovacie technológie dokážu úžasné veci, dosiahnutie dokonalej počítačovej bezpečnosti nie je možné. Fakt, že sú tvorcovia zabezpečovacích systémov špičkami vo svojom obore ešte neznamená, že takíto ľudia dokážu odvádzať prácu a vytvárať technológie, ktoré budú bezchybné a bezpečné dlhú dobu. V prostredí Internetu je rovnakými odborníkmi stále aktívna snaha o prelomenie týchto bezpečnostných systémov, a tak spolu zvádzajú neustály boj o to, kto bude o krok vpred. Efektívne zabezpečenie vyžaduje využívanie tých najnovších technológií a ich verzií. Dôležitá je aj bezpečnostná politika, nakoľko človek, obyčajný, neinformovaný užívateľ predstavuje najväčšiu bezpečnostnú medzeru. Keďže zabezpečenie počítačovej siete je vysoko odborná záležitosť, v záujme ochrany dát je preto vhodné obrátiť sa na odborníkov, ktorí sú schopní zvýšiť bezpečnosť počítačového systému a minimalizovať tak dopady spôsobené nežiaducim únikom informácií. Táto práca mala za úlohu predstaviť jej čitateľovi možnosti v zabezpečení siete, či už ho informovať o možných rizikách, tak demonštrovať, že každý počítačový systém je viac alebo menej zraniteľný a preto treba dbať na jeho neustálu inováciu.

ZÁVER V ANGLIČTINE

Although security technology can do amazing things, achieving the perfect computer security is not possible. The fact that expert makers of security systems are top of their field does not mean that these people can pay to create jobs and technologies that will be perfect and safe for a long time. Same experts in the Internet enviroment are always trying to break these security systems and they are performing neverending war over who will be step forward. Effective security requires the use of the latest technologies and their versions. Also the security policy is important, because the man, ordinary and not informed user represents the biggest security deficiency. Computer network security is highly technical matter, and in order to protect data is therefore proper to refer to professionals who are able to increase the security of computer systems and minimize adverse impacts caused by leaks. This study sought to introduce the reader to the possibility of securing a network, whether he be informed of potential risks, also to demonstrate that every computer system is more or less vulnerable and therefore need to ensure its continuous innovation.

ZOZNAM POUŽITEJ LITERATÚRY

[1] POŽÁR, Josef. Informační bezpečnost . Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. 309 s. ISBN 80-86898-38-5.

[2] Zodpovedne.sk [online]. [cit. 2010-03-20]. Vírusy. Dostupné z WWW: <http://www.zodpovedne.sk/kapitola3.php?kat=virusy>.

[3] Secit.sk [online]. 16.03.2010 [cit. 2010-03-20]. Rozdelenie malware. Dostupné z WWW: <http://www.secit.sk/sk/content/rozdelenie-malware>.

[4] Eset, s.r.o. [online]. c2010 [cit. 2010-03-22]. Vírusový slovník. Dostupné z WWW: <http://www.eset.sk/virus-info/slovnik?inc=12749#12749>.

[5] BOBRIK , Marian. Programovanie pc.sk [online]. 10.04.2002 [cit. 2010-05-11]. Princíp detekcie odpočúvania na sieti. Dostupné z WWW: <http://programovanie.pc.sk/bezpecnost/bezpecnost/clanok.php?ID=343>.

[6] FRYE, Douglas. Network Security Policies and Procedures. USA : Springer Science+Business Media, LLC, 2007. Dostupný z WWW: <http://www.springerlink.com/content/w75533/?p=9e2b4711f1b34abc839f65d09fd23109&pi=8>. ISBN 978-0-387-47955-2.

[7] NORIS, Ivan. Bezpečnosť servera v sieti. [online]. 21.03.2007 [cit. 2010-02-08]. Dostupný z WWW: <http://deja-vix.sk/sysadmin/security.html>.

[8] JAŠEK, Roman. OCHRANA ZNALOSTÍ A DAT V PODNIKOVÝCH INFORMAČNÍCH SYSTÉMECH. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. ISBN 80-7318-095-2.

[9] LOVEČEK, Tomáš. Informačné systémy a škodlivé kódy od A po Z. Ikaros [online]. 2007, 11, 4, [cit. 2010-03-28]. Dostupný z WWW: <http://www.ikaros.cz/node/4048>. ISSN 1212-5075.

[10] Viry.cz [online]. c2007 [cit. 2010-04-01]. Antivirové systémy. Dostupné z WWW: <http://viry.cz/go.php?p=viry&t=clanek&id=3>. ISSN 1213-4694.

[11] NORIS, Ivan. Firewall. [online]. 26.03.2007 [cit. 2010-03-08]. Dostupný z WWW: <http://deja-vix.sk/sysadmin/firewall.html>.

[12] Prvá slovenská certifikačná autorita [online]. c2005 [cit. 2010-03-15]. Dostupné z WWW: <http://www.psca.sk/gen/faq_slovnik.html>.

[13] PAUKERTOVÁ, Veronika. Elektronická informační kriminalita. Ikaros [online]. 2006, 10, 8, [cit. 2010-03-13]. Dostupný z WWW: <http://www.ikaros.cz/elektronicka-informacni-kriminalita>. ISSN 1212-5075.

[14] CISÁRIK, Pavol. Security revue [online]. 18.05.2007 [cit. 2010-03-10]. Krádež identity a sociálne inžinierstvo. Dostupné z WWW: <http://www.securityrevue.com/article/2007/05/kradez-identity-a-socialne-inzinierstvo/>. ISSN 1336-9717.

[15] PASTIERIK, Július. Inet.sk [online]. 07.08.2007 [cit. 2010-03-17]. Phishing a Pharming – krátke predstavenie 1. Dostupné z WWW: <http://www.inet.sk/clanok/5037/phishing-a-pharming-kratke-predstavenie-1>. ISSN 1336-1899.

[16] HORNÍČEK, Ján. Social engineering [online]. c2009 [cit. 2010-04-12]. Pharming. Dostupné z WWW: <http://www.sociotechnika.ic.cz/web/web/pharming/pharming.html>.

[17] BOTT, Ed, SIECHERT, Carl. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Brno : Computer Press, 2004. ISBN 80-7226-878-3.

[18] Gordias, s.r.o. [online]. c2009 [cit. 2010-04-08]. Externé penetračné testovanie. Dostupné z WWW: <http://www.gordias.sk/produkty/externe-penetracne-testovanie.html>.

[19] Sunflovv [online]. c2010 [cit. 2010-04-21]. Penetračné testovanie. Dostupné z WWW: <http://www.sunflovv.eu/sk/informacna-bezpecnost/penetracne-testovanie/>.

[20] Disig, a.s. [online]. c2008 [cit. 2010-04-07]. Penetračné testovanie. Dostupné z WWW: <http://www.disig.sk/fileadmin/user_upload/pdf/pl/Produkt_list_Penetracne_testovanie.pdf>.

[21] KEFER, Daniel. It news [online]. 30.04.2010 [cit. 2010-05-01]. Penetračné testy – úvod do legálneho hackingu. Dostupné z WWW:

<http://www.itnews.sk/tituly/infoware/free-clanky/2010-04-30/c133372-iw-penetracne-testy-uvod-do-legalneho-hackingu>.

[22] WACK, John, TRACY, Miles, SOUPPAYA, Murugiah. Guideline on Network Security Testing : Recommendations of the National Institute of Standards and Technology. USA, WASHINGTON : U.S. GOVERNMENT PRINTING OFFICE, 2003. Dostupný z WWW: <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>.

[23] Senelin [online]. [cit. 2010-05-01]. Penetračné testy. Dostupné z WWW: <http://www.senelin.sk/index.php?option=com_content&view=article&id=34:penetrane-testy&catid=3:kategoria-sluby&Itemid=46>.

[24] Gordias, s.r.o. [online]. c2009 [cit. 2010-05-01]. Interné penetračné testovanie. Dostupné z WWW: <http://www.gordias.sk/produkty/interne-penetracne-testovanie.html>.

[25] Nmap.org [online]. [cit. 2010-05-02]. Nmap - Referencna prirucka. Dostupné z WWW: <http://nmap.org/man/sk/>.

[26] SPEVÁK, Martin. Útoky z LAN a obrana proti nim [online]. Bratislave : Slovenská technická univerzita, 2003. 12 s. Projekt. Slovenská technická univerzita, Fakulta elektrotechniky a informatiky. Dostupné z WWW: <http://fornax.sk/~singer/si99/skola/8_semester/ps2/projekt.pdf>.

[27] TRGIŇA, Marek. Penetračné testovanie [online]. Brno : Masarykova univerzita, 2008. 35 s. Bakalárska práca. Masarykova univerzita, fakulta informatiky. Dostupné z WWW: <http://is.muni.cz/th/173105/fi_b/bakalarka.pdf>.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

CD	Compact Disc
DVD	Digital Versatile Disc
USB	Universal Serial Bus
MS	Microsoft
TCP/IP	Transmission Control Protocol/Internet Protocol
DoS	Denial of Service
DNS	Domain Name System
NAT	Network Adress Translation
DES	Data Encryption Standard
IDEA	International Data Encryption Algorithm
OS	Operačný Systém
WWW	World Wide Web
IT	Informačné Technológie
OSSTMM	Open Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
FTP	File Transfer Protosol
SSL	Secure Socker Layer
SQL	Structured Query Language
MAC	Media Access Control adresa
GPL	General Public License
HTTP	Hyper Text Transfer Protocol
MSRPC	Microsoft Remote Procedure Call
IIS	Internet Information Services
PHP	Hypertext Preprocessor

OSVDB	Open Source Vulnerability Database
XSS	Cross Site Scripting
URL	Uniform Resource Locator
SMTP	Simple Mail Transfer Protocol
XST	Cross Site Tracing

ZOZNAM OBRÁZKOV