Úvod

História počítačových útokov a hackerstva siaha iba do nedávnej minulosti, ale aj napriek tomu je veľmi bohatá a mohla by konkurovať iným vedným disciplínám s niekoľkostoročnou tradíciou. Počítačové útoky sa vo výraznejšej miere začali objavovať s novým fenoménom doby - počítačovými sieťami. Najprudší rozvoj zaznamenali počítačové siete od roku 1985 a od tohto roku môžeme hovoriť aj o histórii počítačových útokov. Počas tejto krátkej doby sa mnoho jednotlivcov aj organizovaných skupín, poháňaných rôznymi pohnútkami pričinilo o nespočetné množstvo menších, ale aj väčších počítačových útokov na rozmanité ciele. Hackeri sa neraz dokázali svojou činnosťou zapísať do histórie.

Miera nebezpečenstva odcudzenia, alebo zničenia údajov na samostatnom počítači nepripojenom k sieti je nízka, lebo takýto čin si vyžaduje fyzickú prítomnosť páchateľa na mieste činu, čo preňho predstavuje veľké riziko. V prípade počítača pripojeného k Internetu je situácia celkom iná. Vo virtuálnom svete počítačových sietí sa nachádzajú jednotlivci, ktorí z nenásytnosti, alebo iba z čistého pôžitku z klamania a ničenia, využívajú nedostatočné zabezpečenie sietí, nahrávajú si osobné informácie a kradnú alebo ničia údaje. V masmédiách vo všeobecnosti týchto jednotlivcov nazývajú „hackermi". Hackermi môžu byť jednotlivci motivovaní ekonomickým ziskom alebo potrebou ničiť, prípadne tzv. „dobrí" hackeri, ktorí sa pokúšajú nabúrať do vašej siete pre vlastné potešenie a ich jedinou motiváciou a zároveň aj cieľom je túžba po dobrodružstve a prekonávaní bariér. Nezáleží na tom, kto je hackerom alebo aké sú jeho úmysly, hacker predstavuje nebezpečenstvo a je nevyhnutné chrániť pred ním svoje údaje.

Zabezpečenie sietí je dnes a denne vystavované skúške ohňom. Správna otázka ale je, kto ju skúša. Pokiaľ sme to my sami, je všetko v poriadku, ale zo všetkých strán na nás útočia aj cudzie „elementy“. Systémy zapojené na Internet (teda systémy s verejne dostupnou IP adresou) zaznamenávajú denne mnoho pokusov o útok, často sú ich stovky i tisíce. Mnohé z nich sú jednoduché prípady skenovania siete či skúmania, proti ktorým sa brániť vieme, ale iné nás vedia neraz zastihnúť nepripravených.

Pri budovaní siete je preto jej neoddeliteľnou súčasťou aj jej bezpečnosť. V našej práci sa snažíme rozobrať problematiku bezpečnosti LAN sietí. Povieme si niečo o najčastejších útokoch na počítačové siete, uvedieme konkrétne príklady

útokov a oboznámime sa so zabezpečením obrany sietí proti nim. Hlavnou ambíciou našej práce je preto vytvoriť hlbší a kompaktnejší prehľad informácií dôležitých pre hlbšie porozumenie rizikám, zraniteľným miestam a hrozbám, ktorým musia počítačové siete čeliť takpovediac denne.

1. Kategorizácia útokov na počítačové siete

V tejto časti práce sa venujeme priblíženiu najrozšírenejších druhov a spôsobov hackerských útokov na počítačové systémy. Rozdelíme jednotlivé techniky, vysvetlíme princíp činnosti, na ktorom sú založené a spôsob, akým ich hackeri zneužívajú.

Z hľadiska zabezpečenia počítačových systémov pred napadnutím môžeme ohrozenie bezpečnosti počítačových systémov rozdeliť na štyri základné okruhy :

zraniteľnosť údajov,

zraniteľnosť softvéru,

zraniteľnosť fyzického systému,

zraniteľnosť pri prenose.

Dokonalá ochrana si vyžaduje do značnej miery paranoidný prístup k otázkam bezpečnosti. Aby sme boli pripravení na útoky, musíme predpokladať, že narušiteľom môže byť ktokoľvek, skrývajúci sa kdekoľvek a chce využiť väčšinu z týchto zraniteľných miest na to, aby odkryl naše údaje, alebo poškodil systém.

Ako príklad môže poslúžiť pripojenie LAN k Internetu, ktoré môže otvoriť bezpečnostné trhliny, cez ktoré môžu neoprávnení používatelia (votrelci) pristupovať k zdrojom lokálnej siete. Hackeri môžu napadnúť internetovský server a zmodifikovať súbory, ktoré sú na ňom uložené. Hackeri môžu zachytiť mail, zmodifikovať ho a prostredníctvom neho sa môžu z Internetu do systému dostať vírusy, alebo iné záškodnícke programy umožňujúce hackerovi nebadane manipulovať systémom (tzv. trójske kone). Tieto príklady naznačujú, aké nebezpečenstvo hrozí systémom po pripojení k Internetu a prečo netreba podceňovať otázky zabezpečenia lokálnych sietí pred napadnutím.

Jestvuje veľa spôsobov (tisíce), akými môžu hackeri zneužiť počítačový systém a ktorých podrobné zdokumentovanie by si vyžiadalo niekoľko takýchto prác. S rastúcim množstvom nového softvéru, novými verziami operačných systémov a zavádzaním nových technológií vznikajú nové zraniteľné miesta, ktoré sa môžu stať cieľom útokov a umožňujú hackerom zneužívať napadnutý systém. Metódy, spôsoby a ciele hackerov môžeme rozdeliť podľa rôznych kritérií:

Medzi najčastejšie ciele hackerov môžeme zaradiť:

- vlámanie sa do systému a nepozorované získanie absolútnej kontroly nad ním,
- ukradnutie dôležitých informácií (komerčných alebo osobných),
- manipulácia poskytovaných informácií za účelom nezákonného obohacovania sa, šírenia dezinformácií alebo vandalizmu (napr. prostredníctvom WWW).

Metódy môžeme rozdeliť:

Metódy umožňujúce prístup do systému:

útoky na heslá,

útoky založené na monitorovaní siete,

útoky založené na predstieraní IP adresy,

útoky založené na únose spojenia,

útoky zneužívajúce bezpečné pripojenia,

útoky založené na pretečení zásobníka,

útoky na Firewally,

útoky založené na spoločenskom plánovaní.

Metódy umožňujúce získanie kontroly nad systémom:

útoky využívajúce zdieľané knižnice,

útoky založené na pretečení zásobníka,

útoky prostredníctvom formátovacích reťazcov,

útoky využívajúce nahrávateľné moduly jadra operačného systému.

Metódy umožňujúce zmanipulovanie údajov

útoky na WWW *(World Wide Web)* stránky.

Tieto jednotlivé spôsoby a techniky napadnutia sa v praxi používajú vo vzájomnej kombinácii v jednotlivých fázach útoku, vo všeobecnosti aktívnemu útoku predchádza pasívne monitorovanie siete. Kombinácia týchto metód potom hackerom umožňuje napadnutie a únos telnetového spojenia, odcudzenie osobných informácií napadnutím WWW stránok a mnohé iné spôsoby manipulácie s údajmi.

1.1 Útoky na heslá

Cieľ útoku: získanie nelegálneho prístupu k počítaču pripojenému k počítačovej sieti (najčastejšie Internetu), zneužitím konta legálneho používateľa. Táto technika sa najčastejšie používa pri získavaní vstupu do unixových systémov a systémov Windows NT/2000.

Základný popis útoku: Princípom takéhoto druhu útokov je „hádanie" prístupového mena a hesla používateľa v online sieťach. Spočiatku sa hackeri pokúšali nabúrať do sieťových systémov opakovaným vkladaním jedného prístupového mena a hesla, hacker skúšal uhádnuť heslo pokiaľ nenašiel to správne. Vylepšením tohoto spôsobu je napísanie a použitie jednoduchého programu, ktorý automaticky generuje heslá na online systémoch namiesto hackera.

Charakteristické pre tieto programy je, že cyklicky skúšajú všetky heslá, pokiaľ nevyskúšajú všetky heslá zo slovníka obsahujúceho potencionálne heslá. Tieto rýchle automatizované útoky sa nazývajú aj **slovníkové orientované útoky** *(dictionarased attacks).* Slovníkovo orientovanými útokmi sú ohrozené hlavne systémy založené na unovskom základe, pretože niektoré verzie Unixu neuzamknú konto používateľa po určitom počte neúspešných pokusov o prihlásenie sa do systému. Väčšina ostatných operačných systémov (napr. Windows 2000) uzamkne používateľské meno (konto používateľa) po presne danom počte pokusov o prihlásenie a zadanie správneho hesla. Hacker sa môže pokúšať napríklad tisíckrát neúspešne prihlásiť do neošetreného systému Unix bez toho, aby systém ukončil spojenie alebo aspoň upozornil administrátora na podozrivé správanie.
Jedným zo spôsobov, ako môže hacker získať súbor hesiel je použitie štandardných služieb Unixu - Telnet a FTP pomocou ktorých sa dostane k normálne čitateľným súborom v ktorých sú uložené heslá používateľov, pretože systém štandardne šifruje heslá do verejne prístupného súboru. Každý unixovský systém šifruje svoj súbor s heslami podľa rovnakého algoritmu (matematickými funkciami), čo predstavuje ďalšiu príležitosť pre hackera, ktorý môže obísť heslo dešifrovaním súboru hesiel algoritmom, ktorý je prístupný na Internete. Tento algoritmus patrí medzi základné pomôcky hackera, pomáhajúce mu pri nabúravaní sa do systémov, ktoré sú rozšírené medzi hackerskou spoločnosťou.

Ochrana pred útokom: spočíva vo vhodnom nastavení parametrov servisov alebo

démonov zabezpečujúcich prihlasovanie do systému. Administrátor by mal parametre nastaviť tak, aby umožňovali používateľovi iba obmedzený počet neúspešných pokusov o prihlásenie sa do systému a potom konto nekompromisne uzamkli.

1.2 Útoky založené na monitorovaní siete

Cieľ útoku: odcudzenie informácií prenášaných údajovým tokom počítačovej siete (najčastejšie Internetu) vo forme paketov. Tento druh počítačového útoku je nezávislý od použitého operačného systému.

Základný popis útoku: Každý paket prenášaný Internetom môže putovať cez veľké množstvo počítačov (uzlov siete) predtým, ako dorazí k svojmu adresátovi. Odpočúvaním paketov môžu hackeri zachytiť pakety cestujúce medzi jednotlivými miestami Internetu, ich obsah skopírovať a vydolovať z neho dôležité informácie. Tieto zachytené pakety môžu obsahovať napr. používateľské mená a heslá, prenos čísiel kreditných kariet, časti mailov, atď. Keď hacker zachytí paket, môže ho otvoriť a ukradnúť meno počítača, používateľské meno a heslo pridružené k paketu. Klasickým scenárom hackermi používaného útoku je získavanie informácií monitorovaním siete odpočúvaním paktov a následný útok predstieraním IP adresy.

Ochrana pred útokom: môže byť realizovaná napríklad šifrovaním informácií prenášaných prostredníctvom počítačovej siete, čo síce hackerovi nezabráni skopírovať prenášané pakety ale ich obsah bude preňho ťažko dostupný.

1.3 Útoky predstieraním IP adresy

Cieľ útoku: získanie neoprávneného prístupu k počítaču pripojenému k počítačovej sieti (najčastejšie Internetu), uvádzaním falošnej identifikácie svojho počítača a vydávaním sa za legálneho používateľa. Tento druh počítačového útoku je možné použiť v systémoch Unix a Windows.

Základný popis útoku: Tento druh útokov ťaží zo spôsobu adresovania paketov používaného IP pri prenose údajov. Počítače pri prenose údajov medzi sebou v každom prenose uvádzajú identifikáciu počítača odosielateľa a počítača adresáta. Keď hacker použije predstieranie IP adresy *(IP spoofing)* k napadnutiu siete, znamená to, že poskytuje chybné informácie o svojom počítači. Inak povedané,

hacker tvrdí, že je hostiteľom v rámci internej siete alebo inak chránenej siete tým, že skopíruje TCP/IP adresu skutočného hostiteľa. Predstieranie IP adresy umožní hackerovi získať vnútorný prístup k systému a systémovým službám, odpovede na výzvy a žiadosti nepôjdu k narušiteľovi, ale k hostiteľovi internej siete, ktorého sa narušiteľ snaží emulovať.

Hacker hľadá poradové TCP/IP číslo v dvoch krokoch. V prvom kroku sa pokúsi určiť IP adresu servera. Existuje niekoľko spôsobov ako zistiť adresu servera napr. sledovaním paketov v Internete , postupným skúšaním čísiel uzlov alebo pripojením sa k uzlu WWW prehliadačom a hľadaním jeho IP adresy v stavovom riadku. Ostatné počítače siete majú časť adresy zhodnú s adresou servera, hacker sa preto pokúša nájsť takú IP adresu, ktorá mu umožní prechod smerovacom a zaistí prístup do siete ako internému používateľovi. Napríklad ak má systém IP adresu 192.0.0.15, je to adresa triedy C, hacker vie, že v sieti môže byť pripojených maximálne 256 počítačov, tak vyskúša hádať všetky čísla, ktoré reprezentuje posledný bajt tejto série. Hacker najskôr monitoruje poradové čísla paketov prechádzajúce medzi počítačmi tejto siete. Potom sa pokúsi ďalšie poradové číslo, ktoré server vygeneruje a potom predstiera toto číslo, čo spôsobí že sa vloží medzi server a skutočného používateľa. Keďže hacker pozná IP adresu servera, môže generovať pakety so správnymi poradovými číslami a správnymi IP adresami, čo mu umožní úplne zachytiť vysielanie medzi serverom a legitímnym používateľom. V súčasnej dobe zdĺhavú a komplikovanú manuálnu prácu hackera nahradili automatické programové nástroje, schopné previesť tento druh napadnutia v priebehu dvadsiatich sekúnd.

1.4 Útoky založené na predpovedaní poradových čísiel

Základný popis útoku: Táto technika je určená k predstieraniu IP adresy v sieťach založených na systémoch Unix. Pri začatí každého TCP/IP spojenia si obidva navzájom prepojené počítače vymenia štartovací paket, ktorý obsahuje *poradové čísla (hand shakeing).* Počítače vygenerujú poradové čísla na základe interných hodín každého počítača a používajú ich ako súčasť každého prenosu počas pripojenia. V niektorých verziách Unixu sú poradové čísla určované podľa modelu, ktorý je napodobiteľný podľa známeho algoritmu (matematickej funkcie). Po odvodení modelu algoritmu tým, že sa zaznamená určitý počet poradových čísel

legálnych pripojení v rôznych chvíľach počas dňa, môže hacker s určitou pravdepodobnosťou získať poradové číslo potrebné k výmene štartovacieho paketu *(hand shakeing)* a k vytvoreniu neautorizovaného spojenia.

Ochrana pred útokom: Najjednoduchší a najúčinnejší spôsob ochrany pred útokmi založenými na predstieraní IP adresy môžeme zabezpečiť nastavením plnej ochrany auditným záznamom v každom použitom smerovací, firewalle a serveri, v systéme. Používanie auditného záznamu nám umožňuje sledovať, kedy sa hacker pokúša dostať cez smerovač a firewall aby získal prístup k serveru. Hlásenie *Prístup zamietnutý. Neznáma IP adresa. (Access denied. IP adress uknown)* sa vyskytne v zázname vtedy, keď hackerov počítač vygeneruje nesprávnu hodnotu poradového čísla. Použitím d'alšej služby operačného systému môžeme nastaviť záznamník udalostí tak, aby automaticky poslal výstrahu, alebo aby zakázal útočníkovi prístup v prípade, že sa v audiom zázname zistí opakovaný výskyt uvedených položiek.

1.5 Útoky založené na únose spojenia

Cieľ útoku: útok slúži k získaniu nelegálneho prístupu ku kontu používateľa, ktorý je práve pripojený a pracuje so svojim kontom. Táto technika sa využíva pri útokoch na operačné systémy Unix a Windows používajúce komunikáciu Client to Server.

Základný popis útoku: Tento druh útoku sa radí medzi populárnejšie útoky ako predstieranie IP adresy. Táto skutočnosť vyplýva čiastočne s toho, že únos spojenia dovoľuje import aj export údajov zo systému. Únos spojenia predstavuje technicky menej náročný druh hackerského útoku, lebo si nevyžaduje predpovedanie poradových čísiel a únos TCP umožní hackerovi obísť jednorázové heslo v systémoch výzvdpoveď a následne skompromitovať aj uzol s vysokým stupňom zabezpečenia. Obídenie hesla môže hackerovi umožniť prienik aj do ďalších operačných systémov. Pri tomto spôsobe napadnutia nájde útočník existujúce spojenie medzi dvoma počítačmi, vo všeobecnosti medzi klientom a serverom. Sledovaním siete môže útočník zistiť príslušné poradové čísla (čísla TCP/IP adries) počas výmeny medzi počítačmi. Ako náhle sa podarí útočníkovi získať adresu legitímneho používateľa, unesie používateľove spojenie tým, že simuluje číslo adresy používateľa. V momente únosu spojenia odpojí hostiteľský počítač legitímneho používateľa a hacker získa voľný prístup k súborom, ku ktorým má prístup legitímny

používateľ.

Ochrana pred útokom: Ochrana spojenia pred únosom je veľmi obtiažna a detovať únos spojenia je takmer nemožné, lebo únosca sa javí systému ako legálny (unesený) používateľ. Vlastná ochrana pred únosom spojenia spočíva v ochrane oblastí systému, z ktorých by útočník mohol spustiť únos. Vhodným riešením je napr. použitie šifrovania , odstránenie nepotrebných, implicitných účtov, patchovanie zraniteľných miest systému.

1.6 Útoky založené na pretečení zásobníka

Cieľ útoku: táto skupina hackerských techník sa vyznačuje širokým rozsahom praktického použitia. Jednotlivé modifikácie tejto skupiny metód slúžia hackerom na získanie neoprávneného prístupu k vzdialeným systémom, ale aj na získanie úplnej kontroly nad napadnutým systémom. Útoky založené na pretečení zásobníka môžu byť namierené proti počítačom založeným na operačnom systéme Unix, ale aj Windows.

Základný popis útoku: Tento druh útokov predstavuje v súčasnosti asi najväčšiu a najprepracovanejšiu skupinu hackerských techník. Táto technika využíva nedostatky programového vybavenia pri práci s údajovou štruktúrou zásobník *(stack)* a môže byť zneužitá pri získaní neoprávneného prístupu k serveru, ako aj pri získaní kontroly nad aplikáciami a systémom. Hacker úmyselne spôsobí pretečenie zásobníka napr. zadaním nevhodného vstupu, čím vyvolá nepredpokladané správanie sa programu alebo jeho zrútenie, ktoré využije vo svoj prospech a postihnutý program odovzdá riadenie hackerom podstrčenému programu.

Zásobník je LIFO údajová štruktúra premenlivej veľkosti umiestnená v operačnej pamäti, na jej používanie slúžia špeciálne príkazy. Štandardne je zásobník využívaný dvoma spôsobmi: slúži CPU v prípade potreby na rýchle odkladanie údajov, pretože CPU má obmedzený počet registrov a slúži programom na vytváranie dynamických údajových štruktúr slúžiacich na dočasné uchovanie údajov napr. pri vstupe a výstupe.

Pred vykonávaní akejkoľvek procedúry CPU uloží do zásobníka návratovú adresu a keď procedúra skončí, CPU predá riadenie na danú návratovú adresu. Ale ak procedúra zapíše do lokálnej premennej väčšie množstvo bajtov ako je jej

veľkosť, prepíše aj hodnotu návratovej adresy a vznikne tzv. **pretečenie zásobníka.** Vhodnou manipuláciou lokálnej premennej v procedúre môže hacker prepísať pôvodnú návratovú adresu novou adresou, ktorá ukazuje na miesto v pamäti, kde umiestnil svoj vlastný program, ktorý prevezme riadenie po ukončení procedúry.

Existuje mnoho spôsobov zneužitia pretečenia zásobníka, medzi najčastejšie patrí získanie neautorizovaného vzdialeného prístupu k serveru a získanie autorizácie správcu systému. Odolnosť programov voči takémuto druhu útokov závisí hlavne od robustnosti operačného systému, správneho použitia programovacích techník a dodržania zásad tzv. bezpečného programovania.

Ochrana pred útokom: Ochrana pred napadnutím systému technikami využívajúcimi pretečenie zásobníka spočíva hlavne v pravidelnom sledovaní novo objavených dier, ktoré bývajú prezentované napr. na WWW stránkach výrobcov softvéru a ich opravovaní súbormi výrobcu, prípadne nahradením používaného softvéru inou verziou alebo produktom iného výrobcu.

1.7 Útoky na firewall

Cieľ útoku: techniky umožňujú hackerovi získať prístup k počítačom a prostriedkom firewallom chránenej siete. Použitie tejto skupiny techník priamo nezávisí od používaného operačného systému, ale skôr od samotných aplikácií a technickej realizácie firewallu.

Základný popis útoku: jestvujú štyri základné postupy umožňujúce hackerovi prekonať ochrannú bariéru firewallu:

- hacker zneužije osobu, ktorá má prístup k počítačom za bariérou a s jej pomocou (vedomou alebo nevedomou) umiestni „zadné vrátka" do ochrannej bariéry.
- hacker zneužije zraniteľné miesta servisov. Aj keď firewally sa snažia minimalizovať prevádzku medzi chránenou a nechránenou časťou siete musia poskytovať priestor základným službám (servisom), ako sú napr. mail, WWW, DNS a pod. Tieto servisy sú často umiestnené na ochrannom počítači, na ktorom je umiestnený aj softvér firewallu, čiže v „rizikovej oblasti", čo pre hackera predstavuje výborné miesto pre útok.
- hacker zneužije externé zraniteľné počítače v nechránenej časti siete. Ľudia pracujúci na počítačoch za ochrannou bariérou sa často pripájajú k zraniteľným

počítačom mimo chránenej siete. Ak sa hackerovi podarí získať kontrolu nad týmto počítačom môže zneužiť spojenie medzi hacknutým počítačom a počítačom v chránenej sieti na prekonanie ochrannej bariéry.

- hacker použije tzv. trójske kone. Hacker tajne nainštaluje svoj program do aplikácie, ktorá sa používa v chránenej časti siete a umožní mu prechod ochrannou bariérou. Existuje niekoľko spôsobov, ako dostať infiltrovanú aplikáciu (trójskeho koňa) za firewall, napr. modifikovaním novej verzie softvéru používaného firewallom, ktorú si potom používatelia stiahnu a nainštalujú, čoho vedľajším účinkom je aj umiestnenie zadných dvierok pre hackera.

V praxi tieto postupy môžu byť realizované rôznymi hackerskými technikami najčastejšie zneužitím pretečenia zásobníka a zneužitím zraniteľných miest konkrétnych aplikácií použitých v chránenej časti siete. Konkrétna realizácia útoku závisí aj od druhu použitého firewallu a jeho nastavenia.

Ochrana pred útokom: spočíva hlavne v správnom nastavení riadiacich pravidiel prevádzky firewallu a v dostatočnej ostražitosti administrátora siete, ktorý nesmie prehliadnuť žiadne podozrivé aktivity.

1.8 Útoky na bezpečné pripojenia

Cieľ útoku: získanie nelegálneho prístupu k vzdialeným hostiteľským počítačom (serverom) pripojených k počítačovej sieti. Táto technika útokov je použiteľná v sieťach používajúcich operačný systém Unix a Windows NT/2000.

Základný popis útoku: Útok je založený na zneužití mechanizmov dôveryhodného (zabezpečeného, bezpečného) prístupu *(trusteccess)* k serverom. Tieto mechanizmy predstavujú veľké bezpečnostné riziko hlavne v niektorých verziách operačného systému Unix. V týchto unixovských operačných systémoch môžu používatelia vytvárať *trusted host* súbory (napr. *.rhost* súbory v domovskom adresári), ktoré obsahujú mená hostiteľov (serverov) alebo adresy, z ktorých môže používateľ získať prístup k systému bez nutnosti zadávania používateľského hesla. Keď sa používateľ pripojí z bezpečného *(trusted)* systému, stačí ak použije príkaz *rlogin,* alebo obdobný príkaz s príslušnými parametrami. Takýmto spôsobom sa môže hacker získať prístup k používateľskému systému, ak zistí meno dôveryhodného počítača, alebo uhádne kombináciu používateľského mena a servera. Správcovia unixovských systémov

stále vytvárajú súbory *.rhost* v koreňovom adresári, aby sa mohli používatelia rýchlo premiestňovať medzi servermi.

Ochrana pred útokom: Postupným zvyšovaním popularity tohoto druhu útokov si správcovia systémov uvedomujú veľké nebezpečenstvo pre ich systémy a realizujú potrebné ochranné opatrenia.

1.9 Útoky využívajúce zdieľané knižnice

Cieľ útoku: táto skupina techník umožňuje hackerovi nepozorovane získať úplnú kontrolu nad postihnutým operačným systémom. Zdieľané knižnice predstavujú potencionálne bezpečnostné riziká najmä v operačných systémoch Unix a Windows.

Základný popis útoku: Cieľom tejto skupiny útokov sú zdieľané knižnice (*.DLL a *.so.lib). Zdieľaná knižnica je množina bežných programových funkcií, ktoré operačný systém nahráva zo súboru do operačnej pamäte pri štarte príslušného programu. Túto skutočnosť sa môže pokúsiť zneužiť hacker, ktorý nahradí programy v zdieľaných knižniciach novými programami, ktoré slúžia potrebám hackera, napr. inštalácia zadných dvierok alebo zabezpečenie privilegovaného prístupu k súborom a pod.

Ochrana pred útokom: spočíva v „strážení" systému a pravidelnej kontrole integrity a pôvodu zdieľaných knižníc správcom siete. Pôvod zdieľaných knižníc (ale aj iných systémových súborov) možno overiť kontrolou ich digitálneho podpisu, ktorý autorizovaný výrobcovia softvéru pridávajú k svojim produktom.

1.10 Útoky založené na spoločenskom plánovaní

Cieľ útoku: získanie neoprávneného prístupu k počítačom pripojeným k počítačovej sieti prostredníctvom zneužitia dôvery vytipovaných používateľov. Tieto techniky nie sú obmedzené používaným operačným systémom, ani softvérovým vybavením.

Základný popis útoku: Technika útokov založených na spoločenskom plánovaní *(social engineering)* by mala skôr patriť do skupiny psychologických útokov, ako do skupiny počítačových útokov. Jej princíp je založený na zneužití dôvery vytipovaného používateľa. Pri výbere vhodných kandidátov sa hackeri sústreďujú na určité skupiny s potencionálne nižšou úrovňou vedomostí v počítačovej oblasti, napr. ženy a starší

ľudia. Frekvencia a nebezpečenstvo tejto skupiny hackerských útokov rastie s počtom používateľov pripojených k Internetu a sieťam všeobecne. Klasickým príkladom spoločenského plánovania hackerom je rozposlanie mailov vytypovaným používateľom (tento druh útoku je realizovateľný aj formou telefónneho hovoru), v ktorom sa hacker prezentuje ako systémový administrátor. Text mailu používateľom hovorí, aby odpoveďou poskytli mailom svoje heslo „administrátorovi", lebo z nejakých príčin bez neho nemôže vykonať údržbu systému. Úspešnosť útokov založených na spoločenskom plánovaní závisí hlavne od hĺbky počítačových znalostí a inteligencie používateľov.

Ochrana pred útokom: Najlepšou ochranou je v tomto prípade včasné a pravidelné varovanie používateľov správcom systému.

1.11 Útoky na WWW stránky

V tejto časti práce popisujeme dva z najbežnejších spôsobov napadnutia prostredníctvom WWW stránok. Falšovanie hypertextových odkazov *(hyperlink spoofing)* a manipulácia WWW *(web spoofing)* sú techniky, pomocou ktorých môže hacker napadnúť počítače komunikujúce prostredníctvom HTTP *(Hyper Text Transmision Protocol)* protokolu.

1.11. i. Falšovanie hypertextových odkazov

Cieľ útoku: je manipulácia informácií prezentovaných na WWW stránkach prostredníctvom falošného hypertextového odkazu smerujúceho na hackerom ovládanú WWW stránku.

Základný popis útoku: útok podvrhnutím hypertextového odkazu využíva chybu v spôsobe, akým prehliadače používajú digitálny podpis pre zabezpečenie WWW spojenia. Falšovanie odkazov neútočí na kryptografiu nižšej úrovne, ani na samotný SSL protokol, čo umožňuje útok použiť aj na iné aplikácie zabezpečené certifikátom, v závislosti od toho, akým spôsobom je certifikát použitý.

Hacker sa vloží do toku paketov medzi klienta a server ako tajný sprostredkovateľ *(man in the middle).* Potom sa môže tajný sprostredkovateľ pokúsiť presvedčiť prehliadač, aby sa pripojil k falošnému serveru, ktorý bude mať aj naďalej parametre bezpečného pripojenia. Hacker potom presvedčí používateľa, aby odhalil

svoje dôverné informácie, ako napr. číslo kreditnej karty, osobné identifikačné číslo *(PIN),* podrobnosti o poistení alebo účte v banke, falošnému dôveryhodnému serveru. Medzi ďalšie nástrahy podvrhnutých hypertextových odkazov patrí nebezpečenstvo, že si používateľ (napr. bankový alebo databázový klient) môže v domnienke, že sa jedná o bezpečný server z falošného serveru stiahnuť a spustiť hackerom nastražený javovský aplet. Hacker sa môže po získaní obvyklých certifikačných konvencií vydávať za ľubovoľný server s nastaveným SSL.

Vo chvíli, keď sa používateľ pokúša o vytvorenie SSL spojenia, prehliadač zdieľa so serverom protokol pre autentizáciu servera. Útok falošným hypertextovým odkazom sa sústreďuje iba na autentizáciu servera. Počas úvodného handshakeingu SSL protokolu odovzdá server prehliadaču svoj certifikát. Certifikát serveru je digitálne podpísaná údajová štruktúra, ktorá obsahuje verejný kľúč servera s určitými atribútmi. SSL protokol v certifikáte používa meno domény *(DNS).* Správnym prenosom protokolu a predložením platného certifikátu, ktorému klient dôveruje, server dokazuje prehliadaču, že je vlastníkom príslušného súkromného kľúča. Prehliadač dôkaz akceptuje a verí, že server má právo používať uvedené DNS meno. Pre falošný odkaz nepredstavuje SSL skutočný problém, ale je ním skôr obsah certifikátu a používateľské rozhranie prehliadača.

Útok podvrhnutým hypertextovým odkazom má dosť vysokú percentuálnu úspešnosť spôsobenú tým, že väčšina používateľov nevyžaduje spojenie cez mená DNS alebo URL, ale cez odkazy. SSL verifikuje iba tú časť URL, ktorá zodpovedá serveru, ale nie odkaz, na ktorý klikol používateľ. Cieľom falšovania sa môže stať DNS meno *(DNS spoofing,* DNS server neuvádza svoju pravú internetovú adresu), ale aj URL, keď stránka neuvedie svoje pravé meno pre URL, obidve formy falšovania zavedú používateľa na nesprávne miesto. Z technického hľadiska je falšovanie odkazu jednoduchším spôsobom, ako falšovanie DNS, hacker môže použiť napríklad tento zápis: <A HREF=https://www.hacker.sk /pasca/>Zadarmo - Klikni sem!</A>. Používateľ vidí stránku s hypertextovým odkazom *Zadarmo - Klikni sem!".* Po kliknutí na odkaz sa používateľ dostane na iný bezpečný server (na doméne hacker.sk) do adresára pasca. Samozrejme v uzle pasca nebude nič zdarma, ale cieľ bude pod hackerovou kontrolou a môže sa tam nachádzať dôveryhodne vyzerajúca stránka, ktorá pod nejakou zámienkou z používateľa vymámi dôverné informácie (napr. číslo kreditnej karty). V prípade, že si používateľ skontroluje cez ponuku svojho prehliadača zdroj alebo informácie o dokumente, zistí,

že autentizovaná identita serveru nie je tá, akú očakával, a že sa jedná o podvod.

Ochrana pred útokom: Spoľahlivou ochranou pred falošnými hypertextovými odkazmi na WWW je nenavštevovať neznáme WWW stránky, alebo aspoň nezverejňovať dôverné informácie do siete Internet. Určitá forma bezpečnosti sa dá dosiahnuť v intranových sieťach a v sieťach ochránených firewallmi, z ktorých je zakázaný prístup do Internetu.

1.11. ii. Manipulácia WWW

Cieľ útoku: je manipulácia informácií prezentovaných na WWW stránkach prostredníctvom manipulovania obsahu WWW stránky za účelom nelegálneho získania dôverných informácií.

Základný popis útoku: Manipulácia WWW *(web spoofing)* je ďalším typom útoku na WWW stránky. Pri tomto spôsobe vytvorí hacker presvedčivú kópiu celého WWW uzla. Zmanipulovaná (falošná) WWW stránka vyzerá presne ako skutočná, falošný uzol obsahuje rovnaké podstránky a odkazy ako skutočný uzol. Jediným rozdielom je, že podlieha hackerovmu riadeniu, takže celá komunikácia medzi prehliadačom obete a WWW stránkou ide cez hackera. Tento útok umožňuje hackerovi pozorovať alebo modifikovať všetky údaje smerujúce od obete k WWW serveru a riadiť spätnú komunikáciu od servera k obeti.

Počas útoku hacker zaznamenáva obsah stránok, ktoré obeť navštevuje. Keď obeť vyplní HTML formulár, prehliadač odošle tieto údaje serveru. Do spojenia medzi server a klienta sa nabúral hacker, ktorý je tak schopný zaznamenať všetky údaje vyplnené klientom. Okrem toho môže hacker zaznamenávať aj údaje, ktorými odpovedá server na požiadavky klientovi. Vzhľadom k tomu, že väčšina online obchodov používa formuláre, hacker má možnosť získať čísla účtov, heslá a iné dôverné informácie, ktoré vyplní obeť do formuláru. Hacker môže pozorovanie uskutočniť aj vtedy, keď obeť nadviaže zdanlivo bezpečné spojenie použitím SSL. Hacker je taktiež schopný modifikovať ľubovolné údaje, prechádzajúce v obidvoch smeroch medzi obeťou a serverom. Napríklad obeť si objedná 5 strieborných tanierov, hacker môže zmeniť číslo produktu, množstvo objednávaného tovaru alebo adresu dodávky a nechať si tak poslať na účet obete napríklad 25 zlatých tanierov. Hacker môže modifikovať aj údaje, ktoré server klientovi vracia, takže do dokumentu

o potvrdení obchodnej transakcie vloží obeťou očakávané údaje a obeť si všimne podvod až pri kontrole stavu svojho účtu.

Ďalšou výhodou manipulácie WWW pre hackera je, že v skutočnosti nemusí uchovávať obsah celého WWW servera, podľa definície je všetko prístupné online, takže v prípade potreby hacker príslušnú stránku stiahne zo skutočného servera a používateľovi poskytne falošnú kópiu. Požiadavka o stránku prechádza hackerovým počítačom, takže hacker môže vyhľadať každú novú stránku o ktorú obeť požiada, falošný server potrebuje falošné stránky uchovávať iba v priebehu realizácie útoku.

Nevyhnutným základom útoku je vloženie sa hackera medzi používateľa a WWW server (tajný sprostredkovateľ) podobne ako pri falošnom hypertextovom odkaze. Prvým hackerovým krokom je zmodifikovanie všetkých URL lokátorov na niektorej WWW stránke tak, aby v skutočnosti ukazovali na server hackera a nie na skutočný server. Napríklad hackerov server sa nachádza v doméne hacker.sk. Hacker prepíše URL tak, že pred každú adresu vloží *http://www.hacker.sk/,* zmenená adresa potom môže vyzerať nasledovne: *http://www.hacker.sk/www.obchod.sk/.* V prípade že používateľ klikne myšou na odkaz http://www.obchod.sk/, *jeho* prehliadač v skutočnosti požiada o stránku z *www.hacker.sk,* pretože zmenená URL *začína http://www.hacker.sk,* zvyšná časť adresy povie serveru hackera, kde sa v skutočnosti nachádza obeťou požadovaný dokument. Potom ako hacker vyhľadá požadovaný dokument, zmodifikuje všetky URL v aj v tomto dokumente obdobným spôsobom, doplnením cesty k svojmu serveru pred každú URL na vyžiadanej stránke. Takto upravenú stránku potom poskytne hacker prehliadaču klienta. Vzhľadom k tomu, že na zmodifikovanej stránke ukazujú všetky URL naspäť na hackerov server aj v prípade, že si obeť zvolí ďalší odkaz z novej stránky hackerov server požiadavku opäť zachytí. Takto môže byť obeť uväznená v zmanipulovaných WWW stránkach a môže donekonečna cestovať cez odkazy bez toho, aby opustia falošný WWW server.

Medzi najnepríjemnejšie vlastnosti manipulácie WWW pre používateľa je tá skutočnosť, že útok funguje aj v prípade vyžiadania stránky cez bezpečné spojenie. V prípade, že sa používateľ pokúsi nadviazať bezpečné spojenie s WWW (použitím protokolu SSL) prostredníctvom zmanipulovaného WWW servera, hackerov počítač dodá požadovanú stránku a prehliadač zapne indikátor bezpečného spojenia. Prehliadač informuje o tom, že je pripojený cez bezpečné spojenie, lebo je skutočne pripojený bezpečným spojením, problém je „iba" v tom, že je to bezpečné spojenie so

serverom hakera a nie s požadovanou WWW stránkou.

Aby sa mohol samotný útok začať, musí hacker nejakým spôsobom svoju obeť vlákať na zmanipulovanú WWW stránku. Z predchádzajúcich riadkov vyplýva, že ak obeť raz uviazne na falošnom WWW serveri, je problematické z pasce tohoto útoku uniknúť. Hacker môže použiť niekoľko spôsobov ako podhodiť používateľom svoj odkaz na zmanipulovanú WWW stránku, napríklad:

- hacker vloží odkaz na falošnú WWW stránku do inej populárnej a často navštevovanej WWW stránky,
- v prípade že obeť používa WWW mail klienta, hacker môže obeti poslať od kaz na falošnú WWW stránku mailom,
- hacker môže mailom poslať obeti zmanipulovaný obsah WWW stránok,
- hacker môže oklamať niektorý WWW vyhľadávač, aby zaradil do indexu aj časť zmanipulovanej WWW stránky.

Ochrana pred útokom: ak sa hackerovi podarí vlákať obeť do pasce falošných WWW stránok, je nutné, aby bola obeť neustále presvedčená, že sa nachádza na skutočných (pravých) WWW stránkach. Jestvujú štyri základné postupy, pomocou ktorých sa môže používateľ presvedčiť, či sa nestal obeťou manipulácie WWW.

Stavový riadok prehliadača môže v prípade zablokovania niektorých funkcií prehliadača zobraziť niektoré informácie prezrádzajúce prebiehajúci útok. Zobrazené údaje o stránke môžu poskytnúť náznaky toho, že obeť vstupuje, alebo sa pohybuje vo falošných WWW stránkach. Napríklad, ak používateľ nastaví ukazovateľ myši na odkaz, prehliadač môže v stavovom riadku zobraziť absolútnu adresu odkazu. Ani tento spôsob odhalenia útoku nepatrí medzi spoľahlivé, lebo hacker môže využitím schopnosti stránky riadiť vlastnosti prehliadača, použiť určité programátorské techniky a príznaky útoku eliminovať. Hacker môže použiť napríklad Javu, JavaScript alebo VBScript na manipuláciu so stavovým riadkom prehliadača. Falošná stránka môže zanechávať dva druhy stôp v stavovom riadku prehliadača. Prvým druhom je už spomenuté zobrazenie absolútnej URL odkazu, na ktorej si môže obeť všimnúť, že ju hacker zmodifikoval. Druhou stopou môže byť výpis v momente, keď prehliadač vyhľadáva stránku, stavový riadok na moment zobrazí meno servera, ktorý prehliadač skontaktoval. Obeť si môže všimnúť, že stavový riadok zobrazil *www.hackers.sk*namiesto očakávaného *www.obchod.sk.* Okrem toho, že hackerov

program zmanipuluje obsah stavového riadku, môže byť naviazaný na určité udalosti a vždy ukazovať obeti očakávané informácie zo skutočnej WWW stránky, napr. aj vo chvíli prechodu na novú stránku.

Riadok adresa (address, location) v prehliadači zobrazuje URL práve navštevovanej stránky. Zadaním URL do tohoto riadku používateľ prikáže prehliadaču vyžiadanie zdroja s danou adresou, bez hackerovho dodatočného zásahu by riadok zobrazoval sfalšovanú URL napr. *http://www.hacker.sk/www.obchod.sk/,* čo by takmer určite viedlo k prezradeniu útoku. Ale aj v tomto prípade môže hacker zobrazované informácie manipulovať pridaním špeciálneho programu, ktorý nahradí skutočný obsah falošným. Falošný riadok zobrazuje očakávané informácie a tiež je schopný prijímať vstup z klávesnice a tým používateľovi zadať URL, ako za normálnych okolností. Hackerov program potom zmení zadané URL skôr, prehliadač požiada o prístup.

Zobrazenie zdrojového kódu dokumentu. Vo väčšine používaných WWW prehliadačov sa v hlavnej ponuke nachádza položka zobrazenie zdrojového HTML textu zobrazenej stránky. V prípade, že používateľ nadobudol podozrenie, že sa stal obeťou manipulácie WWW stránok, môže prehľadať zdrojový kód stránky a vyhľadať zmenené adresy. Ako aj v predchádzajúcich dvoch prípadoch, môže hacker použitím záškodníckeho programu skryť riadok z ponuky prehliadača a nahradiť novým obdobným riadkom, ktorý ale otvorí nové okno, v ktorom zobrazí pôvodný (nezmanipulovaný) HTML text.

Zobrazenie informácií o dokumente je posledným spôsobom odhalenia prebiehajúceho útoku. V ponuke WWW prehliadača sa nachádza položka umožňujúca zobraziť informácie týkajúce sa zobrazeného dokumentu, ktoré obsahujú aj URL danej stránky. Hacker môže rovnakým spôsobom ako pri položke zobrazenia zdrojového kódu nahradiť informácie o dokumente použitím falošného riadku ponuky, hacker vytvorí novú ponuku, ktorá zobrazí nové dialógové okno so zmanipulovanou informáciou.

Z predchádzajúcej charakteristiky útoku prostredníctvom zmanipulovanej WWW stránky vyplýva, že sa jedná o nebezpečný a takmer nezistiteľný útok. Pre minimálne zabezpečenie pred týmto útokom by mali používatelia dodržiavať nasledujúcu stratégiu:

I. Vo svojom WWW prehliadači zakázať používanie *Javy, JavaScriptu* a *VBScriptu,*

aby hacker nemohol skrývať príznaky útoku.

2. Presvedčiť sa, či je vo WWW prehliadači riadok uvádzajúci adresu stále viditeľný.

3. Nepretržite venovať pozornosť URL, ktorú prehliadač zobrazuje a presvedčiť sa, že zobrazuje správnu adresu servera.

1.12 Zhrnutie

V tejto časti práce sme sa snažili stručne priblížiť základné okruhy ohrozenia bezpečnosti počítačových systémov, najčastejšie ciele hackerov a metódy, ktoré pri útokoch používajú. Podrobnejšie sme sa venovali jednotlivým typom útokov, popísali sme postup hackera pri útoku, cieľ, ktorý sleduje a taktiež možnú ochranu pred daným typom útoku.

2. Útoky na LAN

Zraniteľnosť LAN sietí narastá každým rokom. Správcovia sietí su stále zmätenejší z úniku informácií kvôli zlej konfigurácií či umožneniu prístupu na zariadenie pomocou implicitných hesiel. V tejto kapitole sa budeme zaoberať tým, ako útočník detekuje sieťové zariadenia, ako ich identifikuje a akým spôsobom k nim získa neautorizovaný prístup.

Takmer všetky sieťové zariadenia budú ihneď po zapojení fungovať, ale pri štandardnom nastavení, bez dostatočného zabezpečenia. A tu práve vzniká príležitosť pre hackera na to, aby získal prístup k zariadeniu. Práve na tejto úrovni dochádza k najčastejšie k prielomu do sytému. Či už sa jedná o defalutné heslá, vady vo fungovaní protokolu či služby alebo aplikácie alebo zlej konfigurácie, vždy sa jedná o chybu spôsobenú ľudským faktorom. V tejto kapitole preto ukážeme, ako sa vyberá ciel útoku, ako sa získavajú o ňom údaje a následne bude napadnutý.

Skoro všetky siete rozposielajú informácie o poskytovateľovi pripojenia, o svojej topológii, konfigurácií, hardvéri a tým pádom aj o potencionálnych bezpečnostných dierach. Je potrebné uvedomiť si, že získavanie informácií o sieti nie je o nič menej poškodzujúce a o nič menej legálne, ako vyskúšať kľučku na dverách, či je otvorené. Záleží na zámere útočníka, ale väčšinou je nemožné toto správanie z právneho hľadiska postihnúť.

Metódy detekcie sú rôzne, najčastejšie sa jedná o metódy, ktoré nevzbudia rozruch v skenovanej sieti. Skenovanie portu je metóda, ktorú môžeme čiastočne využiť pre nepozorované získavanie informácií o sieti. Môže sa realizovať rôznymi nástrojmi, napríklad Strobe, udp_scan, netcat, SuperScan ale najvýznamnejším nástrojom v tejto oblasti je nmap. Je tu však nebezpečenstvo, že niektoré z týchto techník môzu byť zaznamenané systémom pre detekciu prieniku (IDS).

2.1 Identifikácia funkčných systémov

Jeden zo základných nástrojov pri mapovaní siete je automatický hromadný ping na interval ip adries, ktorý umožňuje v rámci tohoto intervalu identifikovať

fungujúce systémy. Program ping zasiela cieľovému systému ICMP pakety ECHO (Typ 8) s tým, že pokiaľ dostane ako odpoveď paket ICMP ECHO_REPLY (Typ 0), predpokladá sa, že testovaný systém je funkčný. Ping sa hodí na použitie v malých až stredných sieťach, ale je značne neefektívny vo veľkých podnikových sieťach. Skenovanie veľkých sietí typu A môže trvať hodiny až dni. Existuje mnoho utilít na vyhľadanie funkčných systémov. Pod Unixom je zrejme najpoužívanejšia nmap. Väčšina tradičných utilít čaká, pokým nedostane odpoveď od testovanej IP adresy. Až potom začne testovať ďalšiu IP adresu v poradí. Nmap odošle na testované adresy viac paketov súčasne a tak je schopný preveriť oveľa väčšie množstvo IP adries za rovnaký čas ako klasický hromadný ping.

```
paluchm@frix:~$ nmap -sP 158.193.1.0/24

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-
05-15 18:22 CEST
Host sw-moy.net.utc.sk (158.193.1.1) appears to be up.
Host 158.193.1.3 appears to be up.
Host 158.193.1.6 appears to be up.
Host proxy.utc.sk (158.193.1.10) appears to be up.
Host gk-utc.utc.sk (158.193.1.12) appears to be up.
Host gk-sanet-dir.voice.sanet.sk (158.193.1.13) appears to be
up.
Host 158.193.1.14 appears to be up.
Host sw-vd-a.net.utc.sk (158.193.1.21) appears to be up.
Host sw-vd-uk.net.utc.sk (158.193.1.22) appears to be up.
Host 158.193.1.25 appears to be up.
Host sw-svf.net.utc.sk (158.193.1.30) appears to be up.
Host 158.193.1.31 appears to be up.
Host 158.193.1.32 appears to be up.
Host 158.193.1.35 appears to be up.
Host 158.193.1.49 appears to be up.
Host 158.193.1.81 appears to be up.
Host 158.193.1.88 appears to be up.
Nmap finished: 256 IP addresses (17 hosts up) scanned in 4.713
seconds
```

Ak sú routery v sieti nastavené tak, aby nešírili ICMP pakety, je možné použiť náhradné metódy. Napríklad môže útočník vyskúšať skenovanie portov. Pokiaľ nájde na testovanej IP adrese otvorený port, je zrejmé, že počítač je funkčný. Táto metóda je časovo náročnejšia a nie je až taká presná ako hromadný ping. Na skenovanie portov môže použiť program nmap, tento program totiž dokáže omnoho viac ako len ICMP pingy. Jednou z týchto možností je TCP ping scan. Po zadaní prepínača -pT a čísla portu, ktorý sa má testovať (najčastejšie je používaný port 80 čiže http). Počas TCP pingu sú do cieľovej siete odoslané TCP ACK pakety. Ak niektorý z počítačov odpovie paketom RST, je považovaný za funkčný.

```
paluchm@frix:~$ nmap  -pT80 158.193.1.0/24

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-05-15 19:28
CEST
Interesting ports on sw-moy.net.utc.sk (158.193.1.1):
PORT   STATE  SERVICE
80/tcp closed http

Interesting ports on 158.193.1.3:
PORT   STATE  SERVICE
80/tcp closed http
  .  .  .
Interesting ports on 158.193.1.81:
PORT   STATE SERVICE
80/tcp open  http

Interesting ports on 158.193.1.88:
PORT   STATE  SERVICE
80/tcp closed http

Nmap finished: 256 IP addresses (17 hosts up) scanned in 4.788 seconds
```

2.2 Ochrana proti Identifikácií funkčných systémov

Včasnou detekciou môžme nielen zachytiť začiatok útoku, ale aj odhaliť útočníka. K detekcii môžeme použiť niektorý z IDS systémov, ako je napríklad snort.

Protokol ICMP môžeme samozrejme filtrovať. Musíme však postupovať veľmi opatrne, pretože tento protokol slúži aj k diagnostike sieťovej premávky. Nemôžeme len tak vypnúť protokol ICMP, pretože by mohlo dôjsť k výpadkom monitorovaných systémov. Tiež je potrebné si uvedomiť, že protokol ICMP používa oveľa viac správ, ako len ECHO a ECHO REPLY. Preto je potrebné zvážiť, ktoré zprávy potrebujeme a ktoré nie.

2.3 Trasovanie

Pomocou programu traceroute môžeme odhaliť hlavné smerovače medzi nami a cieľovým počítačom. To je dobrý základný kameň v odhaľovaní sieťovej infraštruktúry smerovačov v sieti. Traceroute odošle smerom k cieľu niekoľko sieťových paketov(v Unixe typu UDP vo Windows typu ICMP). Prvý paket bude mať hodnotu TTL(Time To Live, zostavajúca životnosť paketu) nastavenú na 1 a každý nasledujúci bude mať TTL o 1 väčší. Keď smerovač posiela paket ďalej, zníži TTL o 1. Pokiaľ je hodnota TTL nulová, paket je zahodený a odosielateľovi sa odošle správa „TTL EXPIRED“. Vo výpise programu potom vidíme každé zariadenie, ktoré po ceste k cieľu odpovedalo paketom „TTL EXPIRED“

```
C:\>tracert www.fri.utc.sk

Výpis trasy k kinfo.fri.utc.sk [158.193.138.7]
s nejvýše 30 směrováními:

  1     1 ms    < 1 ms    < 1 ms  my.router [192.168.1.1]
  2    17 ms    17 ms    16 ms  adsl-d239.213-81-234.telecom.sk
[213.81.234.239]
  3    18 ms    18 ms    16 ms  babo141.213-81-254.telecom.sk
[213.81.254.141]
  4    18 ms    16 ms    16 ms  babo78.213-81-254.telecom.sk
[213.81.254.78]
  5    17 ms    18 ms    17 ms  Sanet-gw.six.sk [192.108.148.10]
  6    20 ms    20 ms    19 ms  ZU-Zilina.sanet2.sk [194.160.8.197]
  7    20 ms    20 ms    20 ms  sw-vd-a.net.utc.sk [158.193.7.241]
  8    20 ms    19 ms    20 ms  kinfo.fri.utc.sk [158.193.138.7]

Trasování bylo dokončeno.
```

Vidíme, že 158.193.7. 241 je posledným zariadením pred cieľovým počítačom. Je veľmi pravdepodobné, že sa jedná o smerovač, ktorý spracováva pakety pre celú sieť a bude teda prvým miestom útoku, ktoré si útočník vyberie. Ale znalosť IP adresy nestačí k prieniku do smerovača.
Musíme preto získať viacej informácií pomocou skenovania portov, identifikácie operačného systému a prieskumu verejne dostupných databáz, aby sme mohli využiť chyby, špecifické pre daného výrobcu.

2.4 Ochrana proti trasovaniu

Najjednoduchšou ochranou je zakázať routeru odpovedať na pakety typu ICMP EXCEEDED. Táto konfigurácia však nemusí byť vždy žiadúca a preto je lepšie zakázať routeru odpovedať len na ICMP pakety z neznámej destinácie.

2.5 Skenovanie portov

Skenovanie portov je proces, keď sa útočník pripája k TCP a UDP portom systému s cieľom identifikovať bežiace služby. Niekedy sa tiež používa termín počúvajúcich alebo otvorených portov. Identifikácia otvorených portov na cieľovom počítači nám pomôže zistiť typ operačného systému počítača a typ prevádzkovaných aplikácií. Ak sú bežiace aplikácie chybne nakonfigurované alebo obsahujú programové chyby, je možné ich využiť k prieniku do siete. Pretože je skenovanie portov veľmi rozšírenou technikou, popíšeme niekoľko najčastejšie používaných metód.

Je niekoľko cieľov, ktoré chceme skenovaním portov dosiahnuť. Toto sú najdôležitejšie z nich:

- Identifikácia TCP a UDP služiab na cieľovom systéme
- Identifikácia typu operačného systému na cieľovom zariadení
- Identifikácia konkrétnych aplikácií a ich verzií

Typy skenov

- TCP spojenie – pri tomto type skenovania dochádza ku kompletnému

trojcestnému (SYN, SYN/ACK, ACK) napojeniu na cieľový port, cieľovým systémom je tento postup jednoducho identifikovateľný.

- TCP SYN scan – táto technika je tiež nazývaná scan pomocou napoly naviazaného spojenia (halfopen scanning), pretože nedochádza k plnému naviazaniu spojenia, tak ako v predošlom prípade. Miesto toho sa odošle SYN paket, pokiaľ je späť prijatý SYN/ACK paket, môžeme s veľkou pravdepodobnosťou povedať, že je port otvorený. Pokiaľ je prijatý paket RST/ACK, väčšinou to znamená, že port je zatvorený. Pretože to je všetko, čo sme chceli zistiť, je k cieľovému portu odoslaný paket RST/ACK. Spojenie teda nikdy nie je úplne nadviazané. Výhoda techniky spočíva v tom, že nemusí byť logovaná cieľovým systémom.
- TCP FIN scan – v tomto prípade je na cieľový port zaslaný FIN paket. Podľa RFC 793 by mal cieľový systém odpovedať RST paketom pre všetky uzavreté porty. Táto technika však väčšinou funguje len v prípade unixových serverov.
- TCP Xmas Tree (vianočný stromček) scan – na cieľový port je odoslaný paket FIN, URG a PUSH. Podľa RFC 793 by systém mal odpovedať RST paketom pre všetky uzavreté porty.
- TCP Null scan – je odoslaný paket s vynulovanými príznakmi (flags). Cieľový systém by mal na základe RFC 793 znova odpovedať RST paketom pre všetky uzavreté porty.
- TCP ACK scan – táto technika sa používa k mapovaniu filtrov na firewalle, umožňuje zistiť, či sa jedná o jednoduchý paketový filter, ktorý identifikuje len nadviazané spojenia (spojenia s nastaveným ACK bitom), alebo či ide o stavový firewall s dokonalejšími možnosťami filtrovania.
- TCP Windows scan – táto technika môže detekovať otvorené alebo filtrované porty na niektorých systémoch. Využíva anomálie v spôsobe, akým je oznamovaná veľkosť TCP okna.
- TCP RPC scan – technika je špecifická pre unixové systémy. Používa sa k detekcii otvorených RPC portov a im asociovaných čísel verzie a programu.
- UDP scan – v tomto prípade je na cieľový port odoslaný paket UDP. Pokiaľ cieľový port odpovie ICMP správou PORT UNREACHABLE (nedostupný port), je port uzatvorený. Ak túto správu späť nedostaneme, môžeme predpokladať, že je otvorený. Pretože ale protokol UDP nereaguje na doručenie paketu, presnosť tejto techniky veľmi závisí na mnohých faktoroch, ktoré majú

súvislosť so zaťažením siete a systémových zdrojov.

```
[root@bakalarka root]# nmap -sS 158.193.138.40
Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2006-
05-16 15:58 CEST
Interesting ports on frix.fri.utc.sk (158.193.138.40):
(The 1623 ports scanned but not shown below are in state:
closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
25/tcp     open        smtp
80/tcp     open        http
   .   .   .
5432/tcp   open        postgres
9999/tcp   open        abyss
Nmap run completed -- 1 IP address (1 host up) scanned in
6.065 seconds
```

2.6 Ochrana proti skenovaniu portov

Detekovanie skenu nám umožní urobiť si predstavu o tom, kedy môže prebehnúť útok na náš systém a kto tento útok podnikne. Hlavnou metódou detekcie tohoto útoku je použitie IDS, ako je napríklad snort.

Tiež väčšina firewallov dokáže detekovať pokusy o sken portu. Niektoré z nich vedia popísať aj vyššie uvedené „neviditeľné“ skeny. Mnohé napríklad dokážu rozpoznať SYN skeny, ale úplne ignorujú FIN skeny.

Je sice ťažké zabrániť niekomu skenovať náš systém, môžeme ale dopady takejto činnosti výrazne znížiť tým, že vypneme všetky nepotrebné služby. V prostredí Unixu sa to dá dosiahnuť zakomentovaním nepotrebných služieb v súbore /etc/inetd.conf a reštartom démona inetd. V prostredí Windows môžeme tiež zakázať všetky služby, ktoré nepotrebujeme. Je to o niečo zložitejšie kvôli princípu fungovania Windows a ich využívania portov 139 a 445.

2.7 Identifikácia operačného systému

Pre útočníka je životne dôležité určiť typ operačného systému, ktorý je prevádzkovaný na cieľovom počítači. S touto informáciou môže podniknúť omnoho cielenejší útok a môže využiť obrovské množstvo údajov o chybách v konkrétnom operačnom systéme. Aktívna identifikácia operačného systému je metóda, založená na získaní TCP/IP implementácie (stack fingerprinting).

Implementáciou protokolu TCP/IP sa operačné systémy od seba navzájom líšia v mnohých detailoch. Architekti operačných systémov často interpretujú doporučenia uvedené v RFC značne rozdielne. Pokiaľ sa teda zameriame na tieto rozdiely, budeme s vysokou mierou pravdepodobnosti schopní rozlíšiť jednotlivé implementácie a tým i jednotlivé operačné systémy. Aby bola zaručená maximálna spoľahlivosť, vyžaduje táto metóda na cieľovom počítači aspoň jeden otvorený port. Nmap sa sice pokúsi odhadnúť typ operačného systému i v prípade, že na cieľovom počítači nie je otvorený žiadny port, avšak presnosť takéhoto odhadu je veľmi nízka.

Typy testov používaných k rozlíšeniu operačných systémov:

- FIN test – na otvorený port je odoslaný FIN paket. Ako bolo uvedené vyššie, systém by podľa RFC 793 na takýto paket vôbec nemal reagovať. Existujú však systémy, napr. Windows NT, ktoré odpovedia paketom FIN/ACK.
- Test neexistujúcim príznakom – je odoslaný SYN paket s vyplneným neexistujúcim príznakom v hlavičke TCP. Niektoré operačné systémy, ako napr. Linux, odpovedia paketom, ktorý má tento príznak tiež nastavený.
- Vzorkovania ISN (initial sequence number) – cieľom je nájsť jednoznačnú vzorku v inicializačných sekvenčných číslach spojenia TCP.
- Monitorovanie bitov „nefragmentovať“(don´t fragment bit) – niektoré operačné systémy nastavujú z dôvodu výkonnosti bit nefragmentovať. Tento bit môže byť monitorovaný a podľa toho je možné určiť, aký operačný systém túto metódu používa.
- Počiatočná veľkosť TCP okna – niektoré operačné systémy vracajú unikátnu veľkosť TCP okna. Túto informáciu môže útočník použiť k výraznému spresneniu odhadu.

- Hodnota ACK – implementácia sa líši v hodnote vráteného sekvenčného čísla ACK. Niektoré operačné systémy vracajú hodnotu zhodnú s hodnotou, ktorú sme im odoslali a niektoré túto hodnotu zväčšia o 1.
- Analýza ICMP správ – niektoré operačné systémy sa líšia v množstve informácií zasielaných ICMP správami.
- Integrita ICMP správ – niektoré systémy menia hlavičky IP paketov, keď vracajú späť chybové hlásenia. Skúmaním spravených zmien môžeme odhadnúť typ operačného systému.
- Typ služby (TOS - type of service) – je kontrolovanýTOS v prípade ICMP správy PORT UNREACHABLE. Väčšina implementácií nastavuje TOS na nulu, ale v niektorých prípadoch sa stretávame s hodnotou rôznou od nuly.
- Spôsob spracovania fragmentu – rôzne systémy rôznym spôsobom spracovávajú fragmentované pakety. Niektoré prepisujú behom skladania fragmentu pôvodné dáta v hlavičkách inými dátami, atď. Spôsob, akým sú skladané fragmenty môže veľa napovedať o cieľovom systéme.
- Rozšírené položky TCP záhlavia označované tiež ako TCP voľby sú definované v RFC 793 a RFC 1323. Väčšina nových volieb popísaných v RFC 1323 doposiaľ nie je v niektorých implementáciách TCP/IP realizovaná. Odoslanie paketu s nastavenými voľbami umožňuje získať ďalšie informácie o cieľovom systéme.

Nmap má v sebe zaimplementované všetky spomínamé metódy detekcie operačného systému.

```
[root@bakalarka /]# nmap -O 158.193.138.40

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2006-
05-16 16:21 CEST
Interesting ports on frix.fri.utc.sk (158.193.138.40):
(The 1623 ports scanned but not shown below are in state:
closed)
Port       State       Service
21/tcp     open        ftp
   .   .   .
9999/tcp   open        abyss
```

```
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20, Linux Kernel 2.4.18 -
2.5.70 (X86)
Nmap run completed -- 1 IP address (1 host up) scanned in
10.733 seconds
```

Je vidieť, že identifikácia operačného systéme na cieľovom počítači nerobí programu nmap žiadny problém. Dokonca aj v prípade, že cieľový systém nemá otvorené žiadne porty, môže sa nmap pokúsiť odhaliť typ operačného systému.

2.8 Ochrana proti identifikácií operačného systému

Na detekciu môžeme použiť niektorý z IDS systémov, ktoré síce nie sú schopné útoku zabrániť, ale zato vedia presne identifikovať, o ktorý typ skenu ide. Riešenie problému prevencie však nie je jednoduché. Ale sťažiť detekciu operačného systému možné je, a to tak, že všetky nepotrebné porty zatvoríme a tým pádom budú odhady detekčných programov oveľa nespoľahlivejšie.

2.9 ARP presmerovanie

Address resolution protocol (ARP) dynamicky mapuje 32-bitové IP adresy na 48-bitové fyzické adresy (MAC). Keď chce systém komunikovať s iným užívateľom v sieti, odošle ARP broadcast s otázkou na MAC adresu cieľového zariadenia. Cieľové zariadenie odpovie svojou MAC adresou a komunikácia môže začať. Bohužiaľ môže byť ARP ľahko oklamaný tak, že systém, ktorý pakety odosiela, ich bude zasielať na systém útočníka namiesto toho, aby ich posielal na cieľový systém, a to aj v prepínanej sieti. Presmerovaný tok dát môže byť zistený sieťovým analyzátorom a potom odoslaný cieľovému systému.

V tomto príklade sú pripojené do prepínača 3 systémy. Prvý systém bude smerovač s IP adresou 10.1.1.1., druhý systém bude odosielateľom s IP adresou 10.1.1.2. a tretí bude útočníkov systém s IP adresou 10.1.1.3. Hacker spustí na svojom systéme program ARPredirect, ktorý je súčasťou balíka dsniff. Hacker je pripojený k prepínaču, takže za normálnych okolností by mal vidieť len pakety určené priamo jemu a broadcast pakety. Pomocou programu ARPredirect je však možné

všetku komunikáciu zo systému odosielateľa a smerovača presmerovať na hackerov systém. Hacker zadá na svojom systéme nasledujúce príkazy:

```
[hacker] arpredirect -t  10.1.1.2  10.1.1.1
intercepting traffic from 10.1.1.2 to 10.1.1.1
```

Tento príkaz spustí ARPredirect a celý tok dát zo systému odosielateľa, určený pre smerovač na útočníkov systém hacker. Systém hacker musí byť schopný preposielať už analyzované pakety ďalej na smerovač, takže musí mať zapnuté preposielanie IP paketov (IP forwarding). Preposielanie je možné zaistiť na úrovni jadra operačného systému, ale to nie je príliš vhodné, pretože to vo väčšine prípadov spôsobí generovanie ICMP redirectu, ktoré celý proces preruší. Namiesto toho môže útočník použiť program fragrouter, ktorý zaistí bezproblémové preposielanie IP paketov použitím prepínača -B1.

```
[hacker] fragrouter -B1
```

Nakoniec stačí, aby útočník na systéme spustil analyzátor paketov. Systém po týchto úpravách funguje nasledovne: Hneď, ako útočník spustil arpredirect, jeho systém hacker začal s odosielaním falošných ARP odpovedí systému odosielateľa, v ktorých tvrdil, že je smerovač. Odosielateľ si opravil ARP tabuľku novou MAC adresou, potom začal užívateľ systému odosielateľa FTP a POP relácií s FTP a POP serverom, avšak namiesto toho, aby zasielal dáta na smerovač, zasiela ich na systém hackera. Pretože má v ARP tabuľke MAC adresu systému hacker, ktorý po analýze pakety preposiela na smerovač vďaka programu fragrouter.

2.10 Ochrana proti ARP presmerovaniu

Ako sme uvádzali, presmerovanie funguje na základe zmeny MAC adresy v ARP tabuľke cieľových systémov. Preto je vhodné nastaviť tam, kde je to možné, v ARP tabuľke statický záznam. Bežne sa napríklad nastavujú statické záznamy medzi firewallom a hraničnými smerovačmi. Nastavenie permanentných záznamov na všetkých zariadeniach vo vnútornej sieti však nie je príliš praktické. Elegantnejšie je preto použiť program arpwatch, ktorý oznamuje všetky zmeny vo vzťahu MAC a IP adries v ARP tabuľke.

2.11 Útoky na protokol STP

STP (Spanning Tree Protocol) – tento protokol predchádza záplavám všestranne šírených správ (broadcastov) a ďalším nechceným vedľajším efektom, ktoré sa vyskytujú pri slučkách v smerovaní. Ide o protokol, IEEE 802.1D. Používa algoritmus STA (Spanning Tree Algorithm), ktorý rozpozná viacnásobné cesty pri komunikácii s iným uzlom, nájde tú najlepšiu, a všetky ostatné zablokuje. Každý prepínač si tak pre každý segment siete vyberie jedinú sieťovú cestu. Tieto informácie potom prepínače zdieľajú s pomocou rámcov BPDU (Bridge Protocol Data Units). Útočník so systémom s viacej sieťovými rozhraniami v jednej oblasti STP má možnosť podvrhnúť prioritu STP bridge a vybrať nižšiu, než akú má aktuálny koreňový bridge. Pokiaľ to vykoná, prevezme funkciu koreňového bridgu a zmení topológiu STP, potom všetka komunikácia bude prechádzať systémom útočníka. Útočník tiež môže spôsobiť jednoduchý útok typu DoS (Denial of Service) a to tým, že bude neustále prepočítavať STP a následne odstráni z cesty iné STP zariadenia použitím nízkych priorít.

2.12 Ochrana proti útokom na protokol STP

Obrana proti útokom na protokol STP je veľmi jednoduchá. Aby sme sa ubránili, je potrebné povoliť na koncových zariadeniach funkciu portfast. Zariadenia umiestnené na takto označených portoch nemôžu ovplyvniť topológiu STP.

2.13 Útoky na protokol VTP

VTP (VLAN Trunking Protocol) je ústredný protokol zaisťujúci konzistenciu VLAN (Virtual LAN) konfigurácie tým, že riadi pridávanie, rušenie a presmerovávanie sietí VLAN v rámci jednej domény VTP. Takáto doména sa skladá z jedného alebo viacej sieťových zariadení, ktoré zdieľajú rovnaké meno domény VTP. Všetky takéto zariadenia musia byť prepojené kmeňovými (trunk) spojeniami, pretože jedine cez ne môžeme komunikovať protokolom VTP. Útočník, ktorý získa k takémuto portu prístup, má možnosť posielať správy VTP jako server, ktorý nemá nakonfigurované žiadne VTP domény. Pokiaľ sa to stane, všetky siete VLAN sú v doméne zrušené.

2.14 Ochrana proti útokom na protokol VTP

VTP môže niekedy priniesť viacej škody jako úžitku. Preto sa doporučuje nastaviť na VTP heslo a režim VTP na transparentný.

2.15 Zhrnutie

Najskôr sme popísali, ako je možné identifikovať funkčné systémy LAN. Následne sme ukázali, ako je pomocou trasovania možné odhaliť topológiu siete a tým identifikovať dôležité zariadenia a ako je možné pomocou skenovania portov identifikovaťotvorené porty na jednotlivých zariadeniach. Popísali sme tiež jednotlivé typy skenov. Ďalej sme uviedli, ako je možné identifikovať typ operačného systému daného zariadenia a tiež typy testov používaných k rozlíšeniu operačných systémov. Popísali sme zároveň postup útočníka pri ARP presmerovaní a pri útoku na protokoly STP a VTP. Vo všetkých uvedených prípadoch samozrejme nepopisujeme len priebeh daných útokov, ale zameriavame sa aj na popis obrany proti nim a snažíme sa uvádzať konkrétne príklady, ako pri nej postupovať.

3. Zabezpečenie hostiteľských počítačov

V tejto časti budeme definovať tri úrovne zabezpečovacích techník, ktorými môžeme chrániť hostiteľské počítače pred miestnymi, sieťovými a aplikačnými útokmi. Vďaka rozdeleniu zabezpečovacích krokov do troch kategórií budeme môcť ohraničiť správanie riadených systémov a presne určiť rozsah zabezpečenia, ktoré je pre jednotlivé hostiteľské systémy najvýhodnejšie.

3.1 Úroveň 1: Zabezpečenie proti miestnym útokom

Zabezpečenie konfigurácie hostiteľa proti miestnym útokom je pomerne priamočiare. Na tejto úrovni sa zameriame na obmedzenie používania vplyvných utilít, ako sú napríklad spravovanie diskov a správu užívateľov. Tiež nastavíme opatrenia pre systém súborov, aby sme pomocou prístupu „najmenšieho možného oprávnenia“ zaistili, že užívatelia budú mať len také malé množstvo práv, aké je pre nich nevyhnutné. Správne plánovanie užívateľských účtov a skupín pomáha pri riadení obmedzení prístupu a uľahčuje úlohy systémového administrátora.

Administrátori často používajú mnoho silných nástrojov pre vytváranie užívateľských účtov a skupín, alebo pre nastavenie systémových služieb. Niektoré nástroje poskytujú užívateľsky príjemné rozhranie, ktoré umožňuje robiť množstvo funkcií pre správu systému. Príkadom takéhoto programu, ktorý je súčasťou systému Windows 2000 je nástroj správa počítača.

Aby sme ochránili nástroje pre systémovú správu, rovnako ako ďalšie aplikácie a dáta, musíme aplikovať opatrenia pre prístup k súborovému systému. Ako prvé je potrebné sa uistiť, že hostiteľský systém používa súborový systém, ktorý umožňuje nastaviť oprávnenia k súborom. V moderných súborových systémoch, ako je napríklad NTFS (NT file system) a systém súborov pre Unix (UFS) môžu administrátori obmedziť prístup k súborom na základe identity užívateľa.

Keď útočník zvolí za cieľ hostiteľský systém, bude chcieť zistiť, aký užívateľský účet môže použiť pre získanie prístupu. Útočník sa bude opakovane pokúšať o prístup k privilegovaným účtom, ako je napríklad užívateľ root alebo administrátor, pretože cez tieto účty môžu získať najväčšie oprávnenie k prístupu do systému.

Ďalej je potrebné umiestniť užívateľské účty do špecifických skupín a priradiť týmto skupinám oprávnenie prístupu k internetu. Skupinám by sme mali zabezpečiť len takú malú mieru oprávnení, aká je nevyhnutná na to, aby mohli jednotliví členovia skupín robiť požadované úlohy.

Bezpečnostné logy (záznamové súbory) sú neoceniteľnými pomocníkmi pri preverovaní správnej funkčnosti ochranných prvkov hostiteľského počítača. Ďalším dôvodom pre uchovávanie záznamových súborov je skutočnosť, že sa tak zaistí dôkazový materiál, keď je potrebné zistiť, čo sa stalo.

Súčasťou systému Microsoft Windows NT 2000 sú všestranné nástroje, ktoré nám uľahčia robenie zaznamenávania a auditov. Pokiaľ nenastavíme inak, systém Windows implicitne zaznamenáva len typické systémové udalosti s cieľom vyriešiť možné chyby systému a aplikácií.

3.2 Úroveň 2: Zabezpečenie proti sieťovým útokom

Na tejto úrovni sieťového zabezpečenia sa zameriame na praktiky, ktoré pomáhajú ochrániť systémy pred útokmi vedenými proti celej sieti. Medzi kroky pri zabezpečovaní systému na tejto úrovni patrí napríklad eliminácia nepoužívaných užívateľských účtov, ku ktorým sa môžeme vzdialene pripojiť. Táto úroveň zabezpečenia je kľúčová pre zaistenie celkovej bezpečnosti hostiteľského počítača, pretože hlavné systémové narušenia sa vyskytujú nad sieťou.

Jednou z najefektívnejších metód, ako môžeme zabrániť neautorizovanému prístupu cez sieť, je odstránenie nepotrebných užívateľských účtov z hostiteľského počítača.

Pokiaľ niekto získa heslo niektorého z užívateľov, môže spúšťať ďalšie útoky proti hostiteľskému počítaču, rovnako ako môže získavať informácie, ktoré sú pre uvedený užívateľský účet dostupné. Užívateľské účty so slabými heslami patria medzi najčastejšie zneužívané bezpečnostné slabiny.

Väčšina operačných systémov má štandardne nainštalované služby, ktoré nie sú požadované pre obchodnú činnosť hostiteľského počítača. Správca systému by mal vypnúť všetky služby, ktoré nie sú potrebné, obzvlášť pokiaľ sú prístupné zo siete. Útočníci často skenujú sieť a pátrajú po systémoch načúvajúcich na bežne používaných portoch. Obzvlášť hľadajú systémy spojené so službami, ktoré majú zneužiteľné slabiny. Teda ak necháme v systéme bežať nepotrebné služby, zvýši sa tým riziko nabúrania do systému.

Medzi omyly mnohých správcov systému patrí aj to, že nevymažú hodnoty zdieľaných reťazcov protokolu Simple Network Management Protokol (SNMP), ktoré majú veľmi často implicitné hodnoty public a private. Tieto reťazce sú podobné heslám. Používajú sa k jednoduchému prevereniu užívateľa, keď má získať systémové informácie pomocou nástrojov SNMP. SNMP všeobecne podporuje použitie verejného zdieľaného reťazca pri overovaní užívateľov, ktorí chcú prístup „len na čítanie“ štatistických informácií a nastavení z hostiteľského počítača. Pre pridelenie prístupu pre čítanie a zápis informácií z a do hostiteľského počítača sa používa súkromný reťazec (community string).

Nezabezpečené systémy Windows majú tendenciu ponúkať informácie komukoľvek, kto ich hľadá. Jedna z najväčších slabín tohto typu systému je známa ako spojenie pomocou null sessions (anonymná relácia), kde sa hostiteľský počítač pokúša nadviazať anonymné spojenie s iným systémom Windows. Pokiaľ nie sú anonymné relácie zakázané, Windows nevyžaduje, aby bola u spojenia tohto typu preverovaná identita.

3.3 Úroveň 3: Zabezpečenie proti útokom na aplikácie

Po zvýšení bezpečnosti lokálnej a sieťovej vrstvy hostiteľského počítača sa môžeme zamerať na aplikácie, ako na koncovú vrstvu zvýšenia odolnosti hostiteľského počítača. Najbežnejšie slabiny aplikácie sa dajú rozpoznať celkom jednoducho. Aplikácia by napríklad mala používať najnovšie bezpečnostné záplaty, a mala by komunikovať na čo najmenej portoch. Slabé miesta spôsobené zlými implicitnými nastaveniami umožňujú, aby osoba i s malými znalosťami spôsobila veľké problémy. Takéto slabiny práve útočníci hľadajú. Medzi najčastejšie používané chyby aplikácie patria slabé defaultné nastavenia a pretečenie pamätí (buffer overflow).

Pri inštalácii aplikácie je dôležité najskôr preveriť predajcom dodaný doporučený postup. Výrobcovia sú si stále viac vedomí nevyhnutnosti zabezpečenia a často pre svoje aplikácie poskytujú cennú dokumentáciu, ktorá nám môže pomôcť prispôsobiť defaultné nastavenie aplikácie podľa našich potrieb a požiadaviek na zabezpečenie. Mnoho administrátorov inštaluje aplikácie, ktoré by mali mať práva ako užívateľ a majú viac práv, než potrebujú. Napríklad aplikácia môže využívať účet správcu systému, namiesto toho, aby mala vlastný účet len s tými prístupovými právami k operačnému systému, ktoré sú nevyhnutné pre jej funkčnosť.

Aplikácie, ktoré majú svoje vlastné heslá, by mali mať tiež podporu zabezpečenia hesiel, zložitosť hesiel, a najmä zaznamenávanie pokusu o prístup. Databázy sú pre útočníkov veľmi lákavým cieľom, najmä pokiaľ ide o centrálne ukladané dáta, akoje kontakt na zákazníka, alebo informácie o kreditnej karte. Mnoho útočníkov vie o existencii východzích hesiel pre aplikačné a databázové systémové účty. Tieto účty sa často vytvárajú automaticky počas inštalácie a mohli by byť správcom prehliadnuté. Po tom, čo je aplikácia nainštalovaná, je určite potrebné zmeniť heslá všetkých účtov.

Výrobcovia pravidelne zverejňujú záplaty operačných systémov. Inštalácia týchto záplat je rozhodujúca pre zvýšenie odolnosti hostiteľského počítača voči známym slabinám. Mať nainštalované najnovšie záplaty od výrobcu môže byť časovo náročné, ale je to nevyhnutné, aby správcovia systému poznali a odstránili slabé miesta skôr, ako ich útočník zneužije.

3.4 Zhrnutie

Aby sme sa uistili, že navrhujeme a vytvárame správne a spoľahlivé procedúry zabezpečenia, definovali sme tri úrovne zabezpečenia systému: lokálnu, sieťovú a aplikačnú. Pri obrane proti lokálnym útokom sme sa sústredili na obmedzenie užívania správcovských nástrojov, obmedzenia práv prístupu k súborom, obmedzenia členstva v skupinách a na aktiváciu zaznamenávania udalostí, súvisiacich so zabezpečením. Aby sme hostiteľský počítač ochránili pred útokmi zo siete, odstránili sme nepotrebné účty a zablokovali sme nebezpečné služby, prístupné po sieti. Tiež sme sa zamerali na riešenia bezpečnostných problémov aplikácií. Obmedzili sme prístup ku komponentom aplikácie a uistili sa, že sú pravidelne inštalované bezpečnostné záplaty.

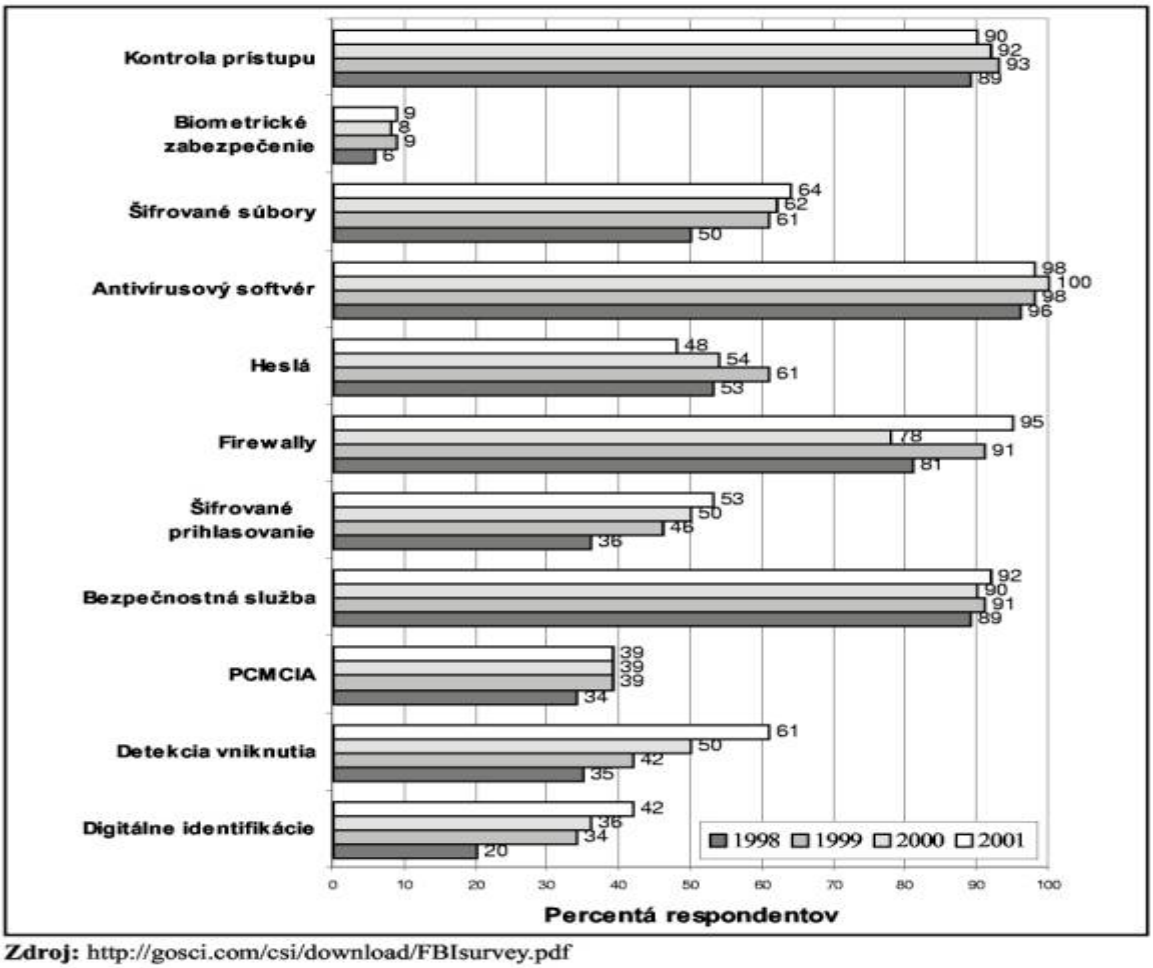
Zabezpečenie nastavenia hostiteľských počítačov nám umožňuje posilniť bezpečnosť celej siete, pretože sa riadime princípmi obrany systému do hĺbky. Rovnako, ako všetky zložky ochrannej infraštruktúry sa pri ochrane zdrojov proti útokom spoliehame na viacnásobné obranné vrstvy. V akom rozsahu by mal byť systém posilnený, závisí na jeho úlohe v sieti a na miere jeho zodpovednosti za zdroje, ktoré poskytujeme na údržbu chráneného nastavenia.

4. Dopad útokov na počítačové siete

V predchádzajúcich kapitolách našej práce sme prezentovali niektoré spôsoby, akými môžu hackeri uskutočniť útok a ako sa proti týmto útokom môžeme chrániť. Skutočnosť, že hackerstvo predstavuje celosvetový a veľmi naliehavý problém, dokazujú aj výskumy prevádzané v USA, ktoré patria medzi najvyspelejšie krajiny v oblasti počítačovej bezpečnosti. Výskumy sú realizovan0 Americkým inštitútom počítačovej bezpečnosti *(Computer Security Inštitúte - CSI)* v spolupráci s FBI *(Federal Bureau of Investigation)* na území USA s cieľom získavať a vyhodnocovať informácie súvisiace s počítačovou kriminalitou. Výskum prebieha niekoľko rokov.

Výskum prebieha anonymne v spoločnostiach, ktoré praktizujú počítačovú bezpečnosť a každý rok sa ho zúčastní približne 550 respondentov zastupujúcich súkromný aj štátny sektor.

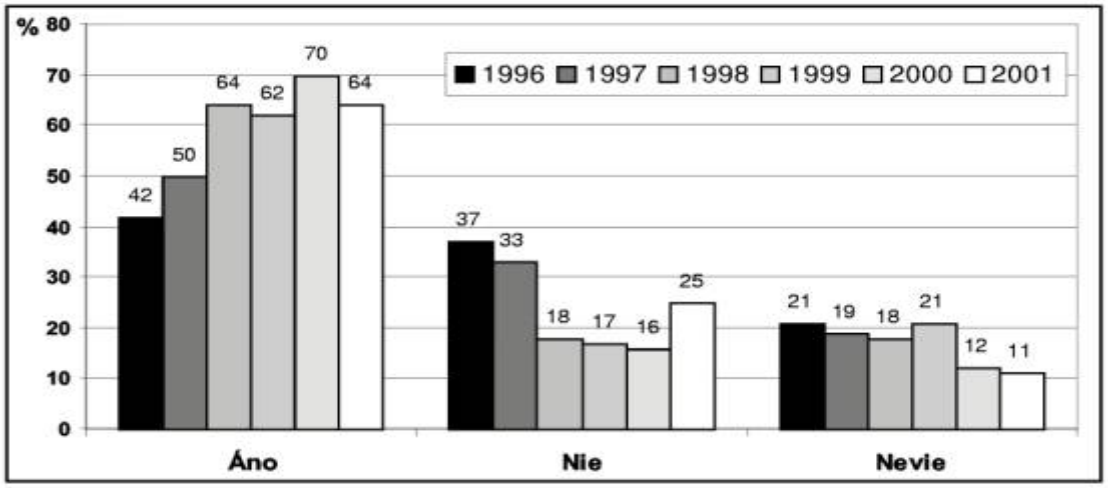
Graf č. 1: Používané bezpečnostné technológie.



Zdroj: http://gosci.com/csi/download/FBIsurvey.pdf

Na grafe č. 1 vidíme vývoj v používaní bezpečnostných technológií za posledné štyri roky. Hodnoty uvádzajú percentuálny podiel respondentov využívajúcich uvedený spôsob zabezpečenia pred počítačovými útokmi. Z uvedených informácií je najvýraznejš rastúci trend v používaní firewallov a detekcie vniknutia v roku 2001 oproti ostatným rokom.

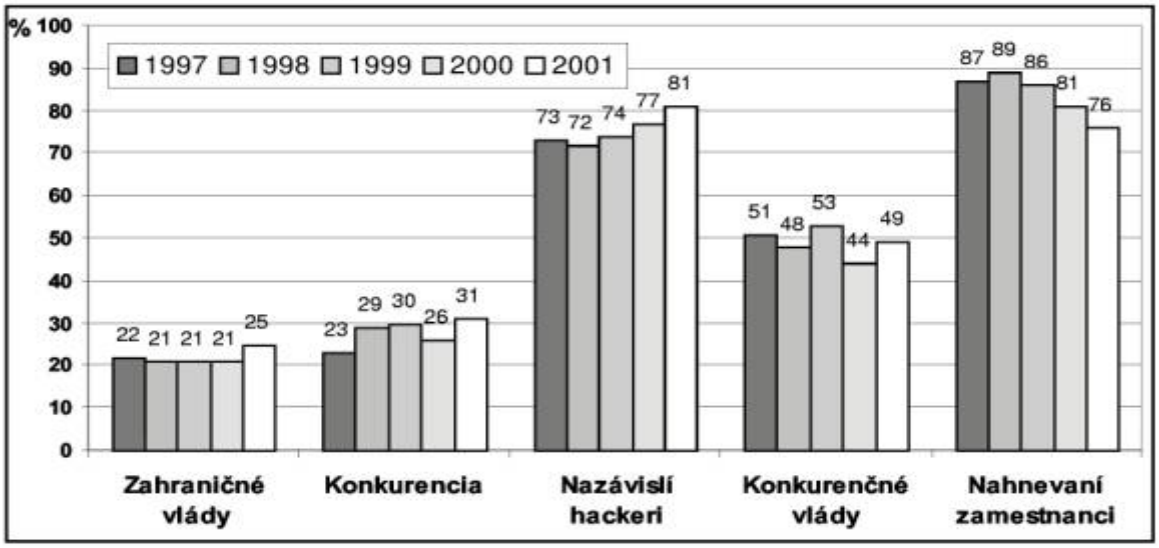
Graf č. 2: Stali ste sa obeťami počítačového útoku?



Zdroj: http://gosci.com/csi/download/FBIsurvey.pdf

V grafe č. 2 znázorňujeme, koľko percent respondentov sa stalo obeťami počítačového útoku v rokoch 1996 až 2001.

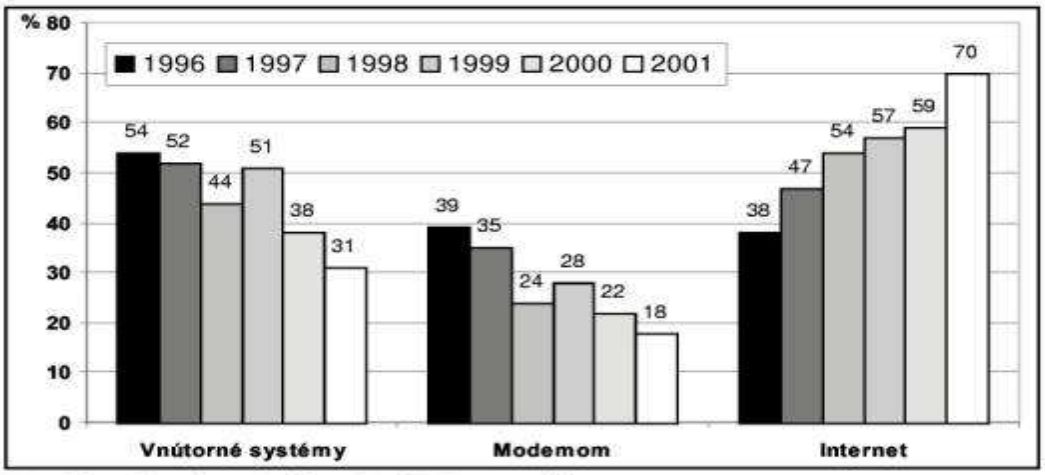
Graf č. 3: Pravdepodobné zdroje útokov.



Zdroj: http://gosci.com/csi/download/FBIsurvey.pdf

V grafe č. 3 znázorňujeme porovnanie pravdepodobných zdrojov útokov uvádzaných respondentmi v období rokov 1997 až 2001.

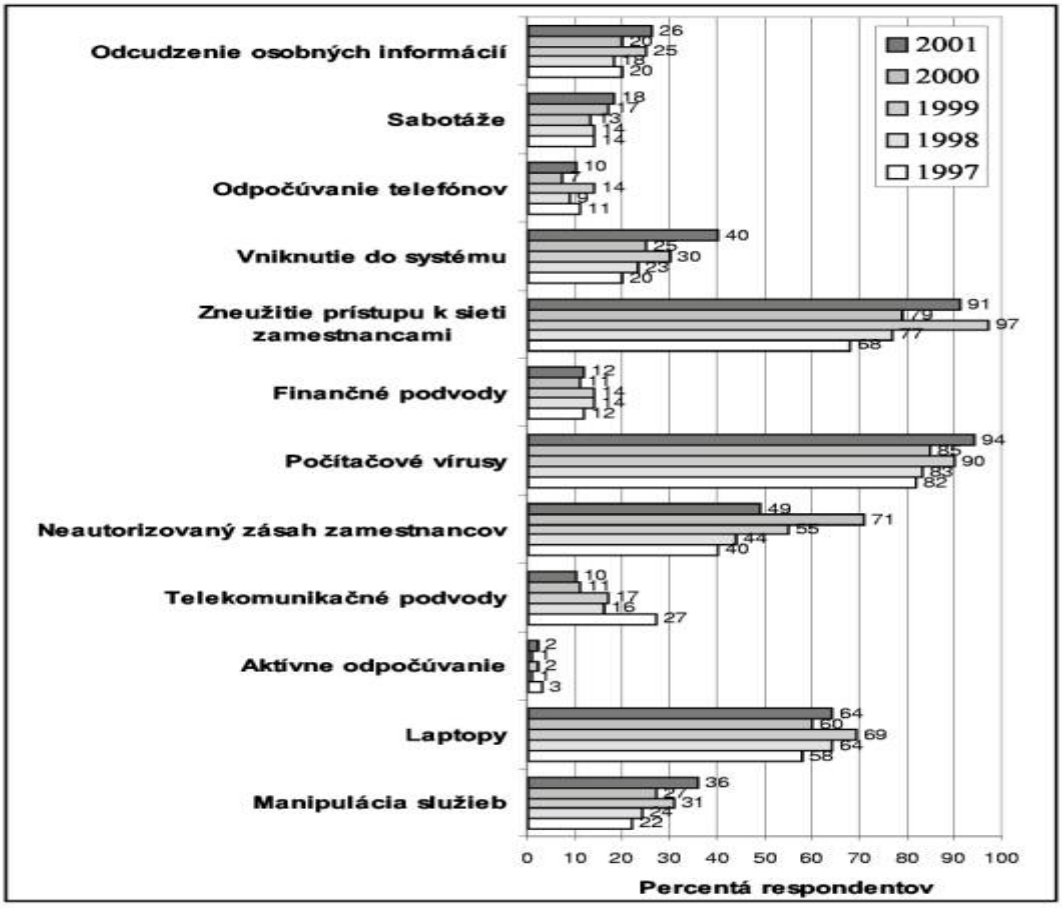
Graf č. 4: Spôsob pripojenia útočníka pri útoku.



Zdroj: http://gosci.com/csi/download/FBIsurvey.pdf

Z grafu č. 4 vidieť stúpajúcu tendenciu počtu útokov z Internetu v rozpätí rokov 1996 až 2001.

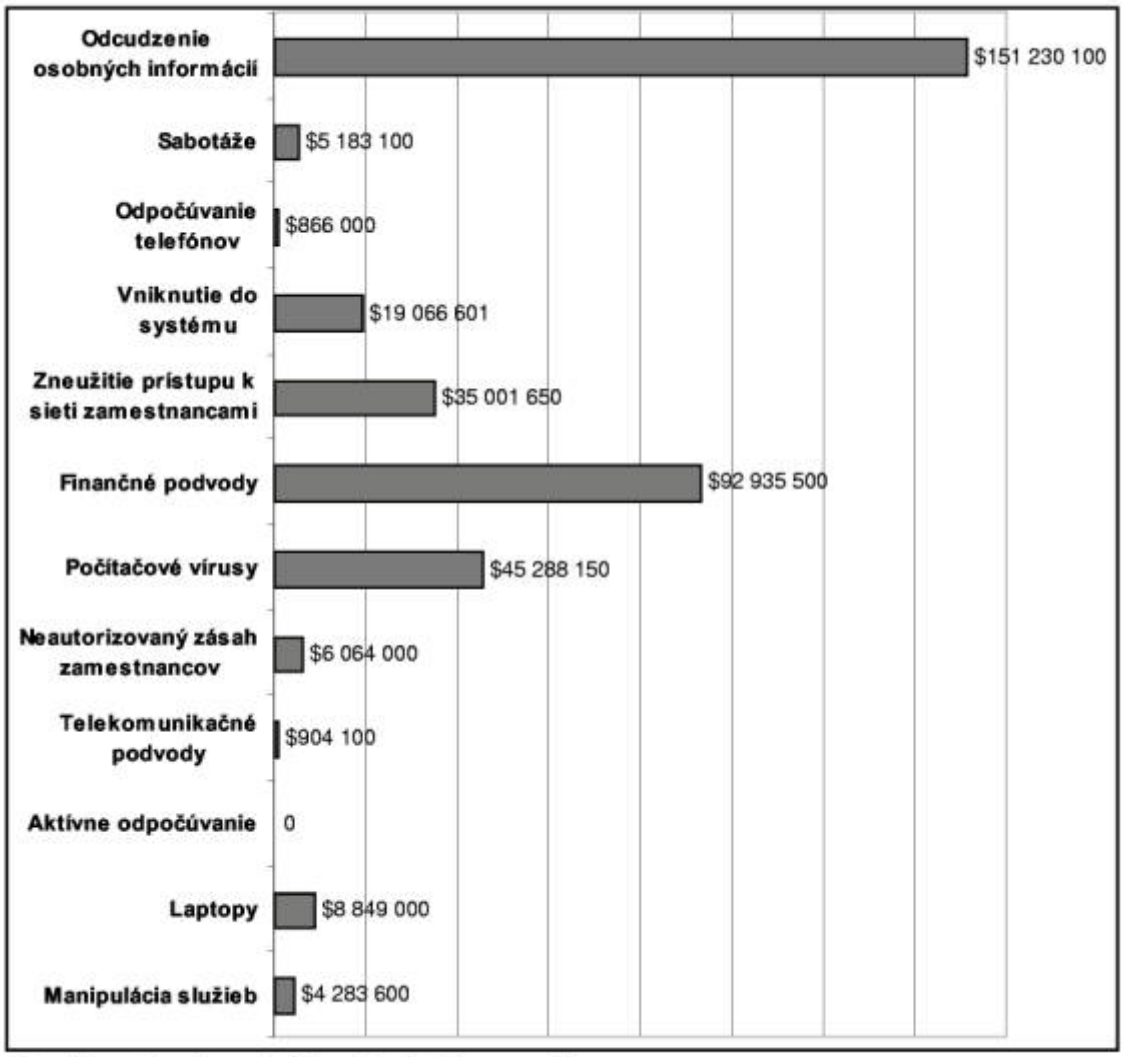
Graf č. 5: Najčastejšie druhy počítačových zločinov.



Zdroj: http://gosci.com/csi/download/FBIsurvey.pdf

V grafe č. 5 sú uvedené druhy útokov a spôsoby zneužitia, ktoré spoločnosti zaznamenali v rozpätí posledných piatich rokov

Graf č. 6: Finančné straty spôsobené jednotlivými druhmy počítačových zločínov.



Zdroj: http://gosci.com/csi/download/FBIsurvey.pdf

V grafe č. 6 sú vyjadrené straty v amerických dolároch spôsobené rôznymy druhmi útokov, ktoré spoločnosti zazanamenali v rozpetí rokov 1996 až 2001

4.1 Zhrnutie

Výskum v oblasti počítačovej bezpečnosti z roku 2001 potvrdil trendy posledných rokov, ktoré môžeme zhrnúť v štyroch bodoch:

- spoločnosti sú pod útokom z vonkajšej, ale aj vnútornej strany počítačového obvodu, jestvuje veľmi široká škála počítačových útokov,

- počítačové útoky môžu spôsobiť veľké finančné straty,
- úspešná ochrana pred počítačovými útokmi si vyžaduje použitie viac ako jednej bezpečnostnej technológie.

5. Záver

V súčasnej modernej spoločnosti sú počítačové útoky vnímané s ešte väčšou intenzitou ako účinný a lacný spôsob ochromenia ekonomiky v rozvinutom svete. Internetoví červi nám znovu a znovu dokazujú, že krátky úsek kódu, ktorého napísanie nevyžaduje takmer žiadne náklady, môže mať veľmi vážne následky.

Informačná bezpečnosť má aj svoj spoločenský rozmer. Vláda vydáva oprávnenia a licencie výrobcom automobilov za to, že predchádzajú zabíjaniu ľudí neschopnými vodičmi. Nanešťastie sa v oblasti bezpečnosti IT podobné licencie nevydávajú, ale následky môžu byť obdobné. Zanedbané opravy bezpečnostných dier boli hlavným faktorom, ktorý umožnil červom spôsobiť také rozsiahle škody a kolaps Internetu. Jediný moderný počítač s červom je ekvivalentný rýchlemu autu rútiacemu sa do davu.

Zo všetkého najskôr musíme pochopiť, že žiadna jednotlivá vec (napríklad firewall) nedokáže sama o sebe zaistiť obranu siete. Niekoľko komponent dohromady to už ale zaistiť môže. Je potrebné použiť taký typ obrany, ktorý je zároveň flexibilný, pretože v ňom môžeme vybrať rôzne komponenty podľa konkrétnych technických, finančných či politických možností a obmedzení a skombinovať ich tak, aby nedošlo k narušeniu celkovej bezpečnosti ani použiteľnosti siete.

Obrana pred útočníkmi spočíva v rukách tých, ktorí navrhujú, zostavujú a spravujú informačnú infraštruktúru. Základné mechanizmy sa skladajú zo sledovania verejných bezpečnostných postupov a dobrých návykov. Okrem toho je nutná technicky vzdelaná sila, schopná analyzovať situácie a robiť zodpovedné bezpečnostné rozhodnutia na základe dobrého porozumenia rizikám. Znalosť hackovacích techník je kľúčom k adaptívnej bezpečnostnej stratégii.

Je veľmi dôležité rizikám porozumieť. Riziko je fukciou hrozieb, zraniteľných miest a príležitostí – na druhej strane stojí adekvátne protiopatrenie. Je zrejmé, že bez porozumenia hrozbám a zraniteľným miestam, nie je možné riziká správne odhadnúť a teda ani sa účinne brániť. V našej práci sme sa preto snažili poskytnúť informácie dôležité pre hlbšie porozumenie hrozbám, zraniteľným miestam a príležitostiam, ktorým čelia moderné informačné technológie. Čím viac sú tieto informácie rozšírené, tým je pravdepodnejšie, že útočník natrafí na šikovného

obrancu a kvalitné protiopatrenie.

Existuje mnoho spôsobov ochrany a zabezpečenia informácií pred neoprávneným prístupom a ich následným zneužitím, no zatiaľ sa nepodarilo objaviť dokonalý spôsob ochrany údajov, ktorý by zabezpečil ich spoľahlivú ochranu. S miernym náznakom paranoje a humoru stále platia dve hlavné zásady sieťovej bezpečnosti, jediným slušne zabezpečeným počítačom, je počítač nepripojený k sieti, a jediný skutočne bezpečný počítač je „mŕtvy" počítač.

Sme si plne vedomí skutočnosti, že rozsah tejto práce ani spracovanie nosnej témy nám neumožnili plne vyčerpať problematiku počítačových útokov na LAN siete a už vôbec nie bezpečnosti IT ako takú. Napriek tomu ju však považujeme za prínosnú pre stručný a výstižný prehľad o tejto problematike, ktorý môže byť základom pre jej ďalšie hlbšie naštudovanie v odbornej literatúre.