Poslovno-Komercialna šola Celje

HEKERSKI VDORI

SEMINARSKA NALOGA

PREDMET: INFORMATIKA

Hekerski vdori

Uvod....2
Hekerski vdori....2
Heker....3
Hekerska etika....4
Vrste hekerskih vdorov....4
IP Spoofing....4
Spyware....5
Napad za zavrnitev storitve....5
Zaščita pred hekerskimi vdori....6
Požarni zidovi (Firewall)....6
Kriptografske metode....7
Zaščita pred oddajanjem elektromagnetnih pulzov (shielding)....8
Hekerski vdori v Sloveniji....8
Neupravičen vstop v zaščiteno zbirko ginekološke klinike....8
Klik NLB!....9
Zaključek....9
Viri....9
Uvod....2
Hekerski vdori....2
Heker....3
Hekerska etika....4
Vrste hekerskih vdorov....4
IP Spoofing....4
Spyware....5
Napad za zavrnitev storitve....5
Zaščita pred hekerskimi vdori....6
Požarni zidovi (Firewall)....6
Kriptografske metode....7
Zaščita pred oddajanjem elektromagnetnih pulzov (shielding)....8
Hekerski vdori v Sloveniji....8
Neupravičen vstop v zaščiteno zbirko ginekološke klinike....8
Klik NLB!....9
Zaključek....9
Viri....10

Uvod

Če bi nekoga pred 20 leti vprašali kaj je hekerski vdor, verjetno ne bi vedel. Sedaj leta 2007 pa večina ljudi že ve kaj je hekerski vdor, heker in kako se pred tem zaščititi. V tej seminarski nalogi pa vam bi rad predstavil nekaj načinov kako hekerji sploh lahko vdrejo v računalnik, strežnik ali celo omrežje. Predstavil vam bom tudi kako se pred tem obraniti in tudi nekaj hekerskih vdorov, ki so se zgodilo v Sloveniji.

Hekerski vdori

Vdor je posledica napak v programski opremi: operacijskem sistemu, aktivnih strežniških programih, napak pri nastavitvah (konfiguracij) programske opreme ali napačnega ravnanja uporabnikov. Verjetno že veste, da je v zadnjem času najpogostejši način vdora klik na datoteko, ki je pripeta elektronski pošti. Tako je zagotovo mogoče vdreti v mnogo računalnikov, vendar če hoče kdo vdreti v točno določen sistem, to verjetno ni prava metoda. Za vdor v sistem določene organizacije mora heker najprej zbrati čim več podatkov o cilju. Takšno zbiranje splošnih informacij imenujemo sledenje (footprinting) in to je prva stopnja napada na določen cilj

Medmrežje je bogat rudnik informacij tudi za nepridiprave. Spletna stran podjetja, odkrita z iskalnikom ali kako drugače, jim običajno služi kot dobra izhodiščna točka. Hekerji si ogledajo vizitko, natančno ime, lokacijo sedeža in podružnic, kontaktne osebe, telefonske številke, naslove elektronske pošte (vse za morebitno lažno predstavljanje), pregledajo izvorno kodo spletne strani, v kateri vidijo uporabljeno tehnologijo, tehnično raven avtorjev, mnogo informacij pa razkrivajo tudi komentarji na spletnih straneh. Nato preiščejo spletne registre, kot je www.ripe.net, kjer so podatki o organizacijah in njihovih domenah. Pridobiti skušajo naslove imenskih strežnikov in iz njih imena ter naslove računalnikov v omrežju. Imenski strežniki (DNS – domain name server) upravljajo predvsem preslikavo med številčno ter opisno obliko IP naslovov, vendar lahko vsebujejo še nekatere druge informacije.

Zdaj to ni več tako preprosto, vseeno pa je še vedno mnogo slabo nastavljenih imenskih strežnikov, ki omogočajo prenos cone nepooblaščenim osebam. Prenos cone je postopek, s katerim nadomestni (sekundarni) imenski strežniki uskladijo svoje stanje s stanjem glavnega imenskega strežnika. Nadomestni DNS strežniki so potrebni za primer nerazpoložljivosti glavnega oziroma primarnega strežnika.

Potem ko pridobijo IP naslove, nadaljujejo z odkrivanjem topologije omrežja (običajno s programi, kot sta Traceroute v Linuxu ali Tracert v Windowsih. Priprava vdora lahko zahteva kar nekaj časa, posebno če gre za veliko organizacijo.

Statistika kaže, da največ vdorov v sisteme podjetij izvedejo (nekdanji) zaposleni. Razširjeno je tudi industrijsko vohunstvo; dogaja se, da se v podjetju za nekaj časa zaposli delavec konkurenčnega podjetja in se po opravljeni nalogi vrne v matično podjetje. Zaposleni mnogo lažje pridobijo dostop do zaupnih podatkov, saj mnogi delavci radi razglašajo svoja gesla, hekersko izobraženi mnogo lažje vdirajo, ker poznajo lokalni sistem (in njegove pomanjkljivosti) pa tudi varnostna infrastruktura (požarni zid) jih ne ovira.

Hekerski vdori

Ko napadalec spozna topologijo omrežja, preide na naslednjo stopnjo, ki ji pravimo skeniranje (scanning) oziroma pregledovanje in v kateri preverja posamezne računalnike. Tako izve, kateri računalniki delujejo in so priključeni v omrežje. Z orodji, kot je nmap, lahko poleg tega ugotovi operacijski sistem in aktivne strežniške programe. Nekateri programi poleg različice operacijskega sistema ciljanega računalnika ugotovijo tudi različice strežniških programov v njem. Če se pokaže, da te niso najnovejše (torej niso naloženi vsi popravki), je to, če gre za varnostne popravke, očitna priložnost za vdor.

Tudi če so nameščeni vsi popravki, to ne jamči varnosti. Hekerji se namreč takšnih sistemov lotevajo s programi za ugibanje gesel, s prisluškovanjem geslom in lažnim predstavljanjem. Velik problem so strežniški programi (posebno spletni strežniki), ki so nameščeni v operacijski sistem ter vsebujejo ranljivosti, kot je npr. prekoračitev vmesnika. Če imamo v računalniku mnogo takšnih programov, obstaja velika verjetnost, da bo heker našel kakšnega, ki nima nameščenih vseh popravkov. Prek takšnega nezakrpanega programa, lahko nato heker pridobi tudi skrbništvo, administratorsko geslo, kar je njegov glavni cilj.

Po uspelem vdoru napadalec najprej odstrani (ali vsaj skrije) sledi, ki so nastale pri tem (na primer v dnevniku aktivnosti), nato namesti (in skrije) več stranskih vrat, nekatere programe zamenja s trojanskimi inačicami in v vdrt računalnik shrani tudi komplet orodij za vdiranje – za napadanje še drugih sistemov. Računalnik, v katerega so strokovno vdrli, je zelo težko očistiti, če sploh. Zato moramo dosledno upoštevati varnostne napotke, tako da bodo (manj spretni) hekerji obupali in se lotili bolj ranljivega plena.

Z nastopom brezžičnih tehnologij, so se tudi hekerjem odprle nove priložnosti, posebno še zato, ker na tem področju varnost še ni dovolj dodelana. Največji problem brezžičnih tehnologij je, da podatki potujejo po zraku, predvsem v obliki radijskih valov, zato jim lahko prisluškuje vsak, ki ima primeren sprejemnik in je v njihovem dosegu.

Požarni zid je najpomembnejši element zaščite lokalnega omrežja pred nevarnostmi iz medmrežja, obenem pa otežuje delo tudi legalnim uporabnikom, programerjem in skrbnikom oziroma administratorjem. Sam požarni zid za varnost omrežja pogosto ne zadostuje, zato vseh pogosteje dodajamo detektorje vdorov. Posebno v zadnjem času je vse več izdelkov, ki združujejo lastnosti požarnih zidov in detektorjev vdorov.

Heker

Héker (angleško Hacker) je računalniški zanesenjak, ki uživa v raziskovanju programov, sam navdušeno (celo obsedeno) programira in spoštuje lastna etična pravila, ki pravijo, da mora biti dostop do računalnikov mogoč vsakomur, informacije svobodno dostopne, da nam računalniki izboljšujejo življenje, oblasti (politiki, vojski in pravosodju) pa ne gre zaupati.

Hekerji se ločijo na dve skupini, ki so sekači in lomači. Sekači spoštujejo nekatera etična pravila, ki jih ločijo od lomačev, ki svoje znanje in sposobnosti uporabljajo za krajo podatkov, in povzročanje škode. Brez sekačev pa na primer ne bi bilo Interneta - Vsi računalniški sistemi, ki jih danes uporabljamo so rezultat zgodnjega sekaškega raziskovanja, v glavnem zaradi ljubezni do računalništva in morebitne slave - brez kakršnekoli denarne motivacije.

Hekerski vdori

Hekerji uporabljajo svoje znanje za vdore v informacijske sisteme in omrežja. Pri hekerjih govorimo o ljudeh, ki vdirajo v informacijske sisteme iz različnih vzrokov. Eden glavnih razlogov za to dejanje predstavlja intelektualni izziv oziroma primerjanje z vrstniki. Veliko kaznivih dejanj, povzročenih s strani hekerjev, pa je posledica njihovega dolgočasja in s tem povezanega preizkušanja raznih možnosti v zvezi z novimi podvigi (vdori). Kriminalizacija vdora v sistem je predmet mnogih debat, saj sam vdor ne predstavlja škode, temveč, če je zaznan, poveča varnost sistema. Poleg tega bo pravi sekač npr. poslal elektronsko sporočilo nadzorniku sistema z naduporabniškega računa in mu opisal slabosti. Nekateri sekači vdirajo v sisteme tudi po naročilu, za denar - samuraji.

Hekerska etika

V današnji moderni dobi, je hekerska etika lahko:

a) Prepričanje, da je širjenje informacij pozitivno oz. dobro, ter da je dolžnost hekerjev, da te informacije delijo z drugimi in da z njihovimi brezplačnimi orodji lahko vsi dostopajo do računalniških podatkov.
b) Prepričanje, da je hekanje za zabavo in raziskovanje etično spremenljivo, dokler heker ne zagreši nobene tatvine, vandalizma ali kršitve zaupnosti.

Vrste hekerskih vdorov

IP Spoofing

Enostavno bi spoofing lahko opredelili kot domišljeno tehniko predstavljanja napadalčevega sistema, ki se napadenemu sistemu s ponarejanjem komunikacijskih paketov predstavi kot zaupanja vreden.
V medsebojni identifikaciji imata velik pomen dva dejavnika: zaupanje in sam overitveni proces.
Zaupanje je odnos med sistemi, ki so avtorizirani za medsebojno povezavo, overitev pa je proces, ki ga ti sistemi uporabljajo za identifikacijo. Velja pravilo, da med sistemoma, med katerima je visoka ravne zaupanja, za vzpostavitev povezave ni potrebna stroga overitev.
Ponavadi se postopkov overitve niti ne zavedamo, kljub temu pa smo neprestano podvrženi njenih procesom, ne glede na to, ali uporabljamo:

- klicni dostop do interneta,
- FTP,
- telnet.

Sistemi pa medsebojno overitev zagotavljajo na druge načine, kot je npr. ime strežnika ali njegov IP naslov. Prav v ta namen obstaja sistem RHOST, ki zagotavlja odnose med zaupanja vrednimi sistemi. Z manipulacijo datoteke RHOST in podobnih, lahko sistem prepričamo, da smo zaupanja vreden sistem, s čimer se preprosto izognemo vnašanju uporabniškega imena in gesla; če smo seveda ustrezno prilagodili datoteko v svojem sistemu, iz katerega izvajamo napad.
IP spoofing je v hekerskem svetu dosegel kultni sloves, saj velika večina napadov še vedno temelji na podobnih tehnikah in pristopih.

Spyware

Je kategorija programske opreme, ki zbira podatke o posameznikovih spletnih navadah ter jih posreduje avtorju. Spyware napadalcem omogoča:

- odpiranje nezaželenih reklamnih oken,
- beleženje pritiskov tipk oziroma gesel,
- spreminjanje telefonskih številk klicnega internetnega dostopa v plačljive številke,
- tatvino osebnih podatkov,
- nameščanje zadnih vrat v sistem.

Ponavadi okuži računalnik s pomočjo oglasnih pasic, kjer oglaševalci uporabnika prepričajo v namestitev katerega od brezplačnih programov. Preostali načini so predvsem sistemi za trenutno sporočanje (IM – instant messaging), p2p-aplikacije za deljenje datotek, spletne igre n tudi pornografske spletne strani. Večina tovrstnih škodljivcev je usmerjenih na Internet Explorer. Uporabniki modernih brskalnikov, kot sta Mozilla Firefox in Applov Safari, pa se lahko veliko bolj brezskrbno sprehajajo po spletu.

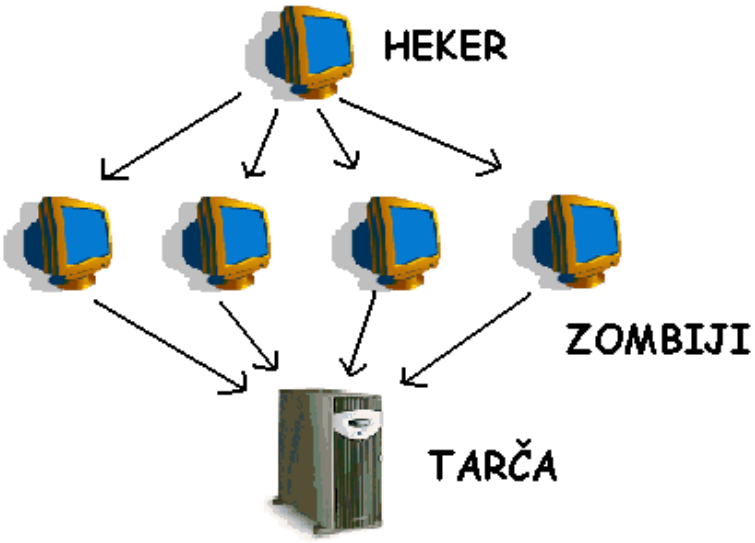
Najnovejše dogajanje v svetu spywara je razvoj tako imenovanih škodljivcev drive-by-download, ki za okužbo sistema ne potrebuje interakcije z uporabnikom. Za okužbo s tovrstnimi škodljivci je dovolj že obisk spletne strani ali klik na povezavo, v kateri v ozadju kraljujejo ActiveX, Java in podobno. Znani so tudi primeri, ko je bil spyware skrit v slikah ali pa so ga žrtvam dostavili v obliki gonilnikov za njihovo strojno opremo.

Napad za zavrnitev storitve

DoS (angleško *Denial Of Service*) ali zavrnitev storitve je proces, ki so go odkrili hekerji okoli leta 2000, svoj razcvet pa je doživel leta 2002, ko so hekerji onesposobili strežnike kot so Amazon.com in Download.com za nekaj ur. DoS se izvaja tako, da heker pošlje tarči veliko količino podatkov določenega protokola (včasih samo na določena vrata). Heker uporablja ponavadi protokole UDP, TCP, ICMP, SYN ipd. UDP in TCP sta protokola, ki potekata preko vsakih vrat v našem računalniku, ICMP protokol je za odmev, pošiljanje samo SYN del TCP paketkov pa zelo primeren za Server DoS. Torej zavrnitev storitve poteka takrat, kadar 1 računalnik pošlje določeno kapaciteto podatkov, določenega protokola v vrata ali na celotno povezavo določenega računalnika. Ponavadi so prvi znaki DoS napada upočasnjena miška in delovanje interneta, rezultati pa so odklop (disconnect) in včasih tudi samodejen ponoven zagon računalnika.

Podoben napad je tudi **DDoS** (*Distributed Denial of Service*) ali porazdeljana zavrnitev storitve. Pri tem napadu se zelo podobno dogoja kot pri DoSu, samo da je pri DDoSu različno sledeče. Heker ima podračunalnike imenovane "DoS boxe" ali "zombije", ki sledijo hekerskim ukazom. Ponavadi si je heker te računalnike pridobil z vdorom ali pa ima legalen dostop do njih. Heker sporoči svojim DoS računalikom z določenimi ukazi, ali pa kar z programom (TFN - Tribe flood Network) naj napadejo z določeno kapaciteto podatkov tarčo. Pri tem napadu je podatkov bistveno več kot pri DoSu saj več računalnikov pošlje več podatkov kot eden.

Skica DDoS napada na tarčo:



Zaščita pred hekerskimi vdori

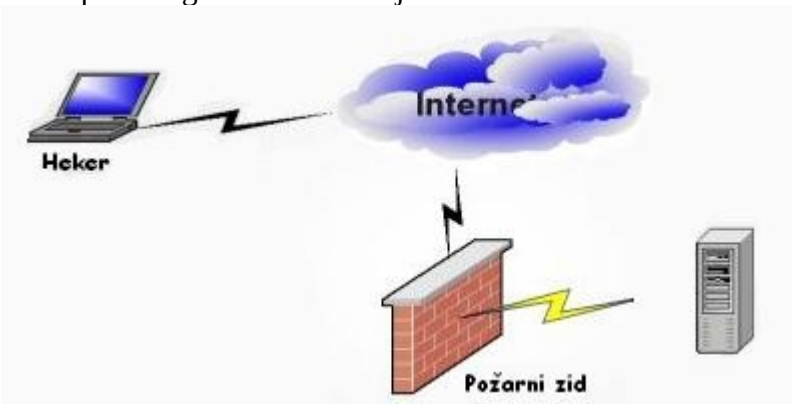
Požarni zidovi (Firewall)

Postavitev požarnega zidu je zelo učinkovita metoda, s katero napadalcem občutno omejimo možnosti za vdor v sistem, hkrati pa uporabnikom dovoljuje varno uporabo interneta. Za čim večjo učinkovitost in zaščito pa moramo požarni zid konfigurirati, namestiti in vzdrževati z veliko natančnostjo.

Razvoj požarnih zidov nam je prinesel zares veliko različnih izdelkov, ki so med seboj v veliki meri razlikujejo. Na tržišču so dobro znani izdelovalci, kot so Microsoft, Cisco, Checkpoint, Symantec, Nortel, SonicWall, NAI ter še nekateri drugi, ki so v zadnjih letih začeli z uvajanjem nove tehnologije, imenovane DPI (deep packet inspection). Ta tehnologija je nekaj posebnega zato, ker paketke mrežnega prometa tako rekoč sleče do golega, pri čemer pregleduje tudi podatkovno vsebino paketov. DPI – vsebino prometa analizira na podlagi skupine pravil, ki jih je predhodno nastavil skrbnik. Tovrstni inšpekcijski DPI pregledi vsebujejo podpise znanih napadov in sovražne kode, hevristiko, statistiko napadov in detekcijo neobičajnih omrežnih nepravilnosti.
DPI tehnologija obljublja višjo varnost s tem, da analizira in pregleduje XML-sporočila, dinamično odpira in zapira komunikacijska vrata za VoIP-komunikacijo, opravi protovirusni in antispammski nadzor, spremlja in pregleduje IM (instant messaging) promet, preprečuje napade na servise NetBIOS, omogoča nadzor p2p-promet in SSL-komunikacije.

Hekerski vdori

Skica požarnega zidu in omrežja:



Nekaj najbolj znanih osebnih požarnih zidov:

Požarni zid	Njihove lasnosti
Zonelabs ZoneAlarms	Varuje pred vdori, omogoča nadzor piškotkov in blokira nezaželeno oglaševanje. Ponuja tudi analizo prometa in spletni filter.
F-Secure Distributed Firewall	Temelji na uporabi značilnosti in varuje pred namernimi in naključnimi napadi.
Norton Personal Firewall	Primeren je predvsem za varovanje enega računalnika. Vsebuje nadzor aplikacij, zaščito zasebnosti in zaznavanje vdorov.

Kriptografske metode

Izvirajo iz kriptografije, ki je veda o tajnosti, šifriranju, zakrivanju sporočil in o razkrivanju šifriranih podatkov. Poznamo še pojma enkripcija (šifriranje) in dekripcija (dešifriranje).

Sporočilo pri nekem postopku spremenimo v kriptirano sporočilo, pri tem pa za določene vrednosti uporabimo paramente v algoritmu, ki jim rečemo ključ. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila.

V prvih letih svetovnega spleta so uporabljali postopek ROT-13[1] za šifriranje neprimernih šal in podobnega. Seveda ni predstavljal nobene resne zaščite.

Klasični algoritmi spadajo med simetrične algoritme ali algoritme z zasebnim ključem. Problem predstavlja tudi število ključev – vsak uporabnik mora imeti za vsakega dopisovalca poseben ključ.

Odkar uporabljamo računalnike, so se ravno zaradi teh problemov razvile asimetrične metode ali algoritmi z javnim ključem. Uporabnik pri uporabi asimetrične metode ustvari dva med seboj povezana ključa in enega javno objavi. Vsi, ki mu hočejo poslati sporočilo, bodo lahko uporabili njegov javni ključ za šifriranje sporočila. Dešifriral pa ga bo lahko le on sam z uporabo svojega skritega ključa. Te metode so računsko bolj zahtevne in zato počasnejše kot simetrične.

[1] Zamenjava črkl a -> a+13 po modulu 26 – angleška abeceda

Nikakor pa ne smemo misliti, da šifriranje podatkov samodejno zaščiti naše podatke pred vsemi zlorabami. V računalniku, kjer se dešifrira, so podatki nezaščiteni – če nismo poskrbeli za njihovo zaščito, nam šifriranje ne pomaga kaj dosti. Velik problem so namreč trojanski konji, ki hekerjem omogočajo, da upravljajo z računalnikom žrtve, ne da bi se tega zavedala.

Zaščita pred oddajanjem elektromagnetnih pulzov (shielding)

Vsa elektronska oprema, od sušilcev las in navadnih TV sprejemnikov do računalnikov oddaja elektromagnetno valovanje. Z dokaj poceni opremo lahko storilec prestreže signale vsakokrat, ko uporabnik pritisne tipko na tipkovnici. Da bi se zaščitili pred oddajanjem elektromagnetnega valovanja, lahko uporabimo radiofrekvenčno zaščito (RF). Takšen ščit razredči elektromagnetne signale in jih ozemlji, še preden se lahko razširijo po prostoru. Takšna zaščita lahko varuje računalnike, omrežne povezave ali vso poslopje.

Poleg obveščevalno varnostnih služb omenjene metode poznajo tudi hekerji, saj dobro vedo, da katodna cev računalniškega monitorja oddaja elektromagnetno valovanje. To valovanje se da zajeti že z uporabo navadne usmerjene televizijske antene, pri čemer se slika z monitorja prikaže na navadnem televizijskem zaslonu. Z nekaterimi izboljšavami lahko povečamo domet antene (prek sto metrov), pa tudi zapisovanje podatkov na računalniški disk in poznejše pregledovanje.
Vedno bolj se pa uporabljajo tudi LCD-monitorji, ki tovrstnih pomanjkljivosti zaenkrat nimajo.

Hekerski vdori v Sloveniji

Neupravičen vstop v zaščiteno zbirko ginekološke klinike

Ginekološka klinika Ljubljana je leta 2000 podala prijavo vdora v zaščiteno računalniško zbirko podatkov oziroma spletni strežnik klinike.

Kmalu so razkrili , da je neznani storilec vdrl v spletni strežnik klinike, zato je odgovorna oseba o vdoru najprej obvestila SI-CERT[2]. Storilec naj bi prenesel vse podatke, ki so bili v spletnem strežniku ginekološke klinike. Ti podatki so vsebovali uradno spletno stran klinike, telefonski in elektronski imenik zaposlenih n kliniki, podatkovne zbirke s podatkih o zdravnikih in pacientkah, knjige v elektronski obliki in različno testno programsko opremo.

Po vdoru naj bi storilec v strežniku spreminjal gesla in sistemske nastavitve ter namestil prisluškovalno programsko opremo za pridobitev gesel (sniffer) . Oškodovana klinika je prijavi priložila tudi del izpisov, ki jih je zabeležil varnostni dnevnik strežnika (datoteke log). Iz teh zapisov je bil razviden IP-naslov računalnika, iz katerega je bil opravljen vdor. Na podlagi lP so ugotovili, da gre za dinamičen naslov računalnika, ki je pripadal organizaciji Arnes. Na podlagi pridobljene odredbe so pri akademski in raziskovalni mreži Slovenije (ARNES), na oddelku SI-CERT, pridobili podatke dinamičnega lP oziroma podatke o tem, na katero telefonsko številko je bil v trenutku vdora vezan lP. Ugotovili so, kdo je bil lastnik telefonskega priključka, nato pa opravili hišno preiskavo (v nadaljevanju bomo osebo imenovali Xanez123).

[2] Organizacija, ki deluje v okviru Arnesa ter skrbi za posredovanje obvestil o zlorabah in vdorih v računalniške sisteme.

Po hišni preiskavi Xanez123 so zasegli osebni računalnik, diskete in CD-je. Pozneje so kriminalisti ob prisotnosti lastnika opravili pregled zasežene računalniške opreme, pri čemer so našli računalniške programe, ki omogočajo nadzor oddaljenih računalnikov. V programu SecureCRT 3.0 je bil seznam strežnikov, za katere naj bi skrbel Xanez123. Iz nastavitev strežnikov je bilo razvidno geslo, ki je bilo tudi v mapi, v kateri so zbrani zapisi o dostopih na internetne strani, in pa tako imenovali cookies (piškotki), ki jih nekatere spletne strani samodejno pošljejo obiskovalcu. Iz piškotkov je bilo razbrati, da je Xanezl23 uporabljal svoje uporabniško ime. Konkretnejših dokazov, da naj bi Xanezl23 vdrl v strežnik klinike, niso našli. Ugotovili so, da je bil trdi disk pred kratkim formatiran, programi pa na novo nameščeni. Xanezl23 je med preiskavo povedal, da je bil računalnik nekaj časa pred tem sesut.

V dokaznem postopku so uporabili IP-naslov, ki ga je Xanezu 123 s priklopom prek klasičnega modema dodelil Arnes. Pri priklopu je Xanez 123 uporabljal ukradeno uporabniško ime, kar pa ni moglo prikriti identitete dejanskega uporabnika. Neizpodbitni dokaz so tudi dnevniški izpisi strežnika klinike, ki je beležil početje napadalca.

Kot je razvidno iz opisa vdora, je napadalec dobro poznal hekerske metode in načine vdorov. Zgodba je dobila tudi sodni epilog, v katerem je sodišče Xaneza123 obsodilo na nekajmesečno zaporno kazen – pogojno.

Klik NLB!

Eden najodmevnejših dogodkov pri nas je bil prav gotovo primer Klik NLB.

Slovenski heker je razvil program, natančneje trojanskega konja, s katerim je obšel varnostno zaščito Klika NLB in vstopil v sistem. Tam se je igral s prenosom na svojih dveh računih in torej ni naredil nobene škode.

Trojanski konj uporablja lastnost Internet Explorerja, ki ponudi svoje zmogljivosti drugim programom. Trojanski konj se torej infiltrira v brskalnikovo okolje, zato je na strani banke videti kot običajen uporabnik internetnega brskalnika. Za trojanskega konja je heker razvil tudi zdravilo, ki ga je ponudil banki in ji hkrati zagrozil, da bo sicer zadevo predal medijem. Hekerja so odgovorni v NLB prijavili policiji, ki ga je aretirala zaradi izseljevanja in mu zasegla obe različici programa skupaj z izvirno kodo. Za svoj program naj bi heker vložil predlog za pridobitev patenta.

Zaključek

Sedaj po koncu, te naloge sem prepričan, da ste izvedeli kaj novega in da boste vedeli kako se ubraniti pred hekerji in njihovimi zamislicami.

Viri

- http://sl.wikipedia.org/wiki/Napad_za_zavrnitev_storitve [19.4.2007]

Hekerski vdori

- http://sl.wikipedia.org/wiki/Heker [5.4.2007]
- http://en.wikipedia.org/wiki/Hacker_ethic [27.5.2007]
- http://en.wikipedia.org/wiki/Software_cracking [19.4.2007]
- Verdonik, Ivan.Bratuša, Tomaž.(2005).Hekerski vdori in zaščita.Ljubljana:Pasadena