VISOKA POSLOVNA ŠKOLA
STRUKOVNIH STUDIJA
ČAČAK

DIPLOMSKI RAD

Hakeri, gospodari interneta

Mentor:_____
Profesor: _____

Student: _____
Br.Indeksa: _____

SADRŽAJ

1. UVOD

1982. godine William Gibson, pisac znanstvene fantastike, upotrijebio je novu riječ – „cyberspace“. Ali sami termin „cyberspace“ mnogo je stariji. 1871. godine Antonio Meucci, talijanski znanstvenik patentirao je uređaj koji je kasnije prozvan telefon. „Cyberspace“ je „mjesto“ gdje se odvija telefonski razgovor. Ne u samom uređaju, ne u slušalici, ne i u uređaju druge osobe , u drugom gradu. To je „mjesto između telefona“. To je „mjesto između“ gdje se dvoje ljudi uistinu susreću i komuniciraju. Iako, tehnički gledano, to mjesto ne postoji.

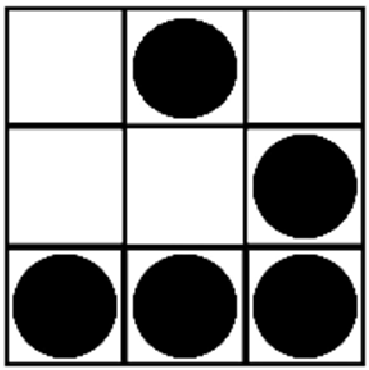
U zadnjih trideset godina to elektronično „mjesto“ što je nekad bilo mračno i jednodimenzionalno, takoreći u kabelu koji se proteže od telefona do telefona razvilo se u nešto epskih, gigantskih razmjera, u Internet. Svjetlost je došla u „cyberspace“, svjetlost u obliku monitora koji nam otvaraju vrata „cyberspace-a“. „Mjesto između“ je postalo jasno vidljivi elektronični prostor. Iako još nema materije, ništa što možete dodirnuti, „cyberspace“ danas ima neku vrstu fizičkog izgleda.

U današnje vrijeme ima smisla pričati o „cyberspace-u“ kao o mjestu koje postoji. Danas ljudi žive „tamo“. Ne samo par ljudi već milijuni ljudi i ne samo na jedan sat ili dan već mjesecima, godinama. „Cyberspace“ danas je mreža (net), matrica (matrix), međunarodnih razmjera koja se razvija, raste, obogaćuje i sve je važnija u svim aspektima života, političkim, vjerskim…

Mnogi ljudi su postali bogati i poznati u „cyberspace-u“, neki su tu usput, radi hobija, ostali ga proučavaju, usavršavaju, pišu o njemu, raspravljaju na forumima ali postoje i oni koji ga zloupotrebljuju, „cyberspace“ kriminalci u široj javnosti poznati po imenom **hakeri**.

U ovom diplomskom radu, kroz povijest, potkulturu, način rada pa i samu etiku hakera, upoznaje se najveća prijetnja sigurnosti računala današnjice, hakeri.

U drugom poglavlju saznaje se samo značenje riječi haker, a u nastavku pogledava prema kratkoj, ali burnoj prošlosti hakera. Kroz hakersku etiku pokušava ih se razumjeti, dok je u trećem poglavlju opisana hakerska potkultura, a u četvrtom poglavlju hakerski alati i tehnika rada. U zadnjem poglavlju opisuju se načini kako ih spriječiti u svom naumu.



Slika 1.1. Logotip hakera

2. DEFINICIJA HAKERA

2.1. Pojam riječi „haker“

Termin „haker“ ima različito značenje među računalnim programerima. U novinama i na vijestima često se čuju priče o hakerima koji su probili u neki računalni sustav i načinili veliku štetu. Objektivno mišljenje u društvu jest da je haker negativna osoba. Mediji pokušavaju hakere opisati kao kriminalce ili bar kao osobe koje obožavaju nanijeti što više štete drugim osobama. Medijska verzija hakera uistinu postoji, ali u većini su hakeri koji nemaju kriminalnih aktivnosti. Među programerima termin „haker“ se više upotrjebljiva kao znak poštovanja prema drugom programeru, a ne kao uvreda. Slavni programerski leksikon poznat kao „The Jargon File“ definira riječ „haker“ kao:

Haker [izvorni prijevod s njemačkog jezika - netko tko radi namještaj sa sjekirom]

1. Osoba koja uživa istraživati detalje računalnih programa i traži način da poveća učinkovitost sistema, za razliku od ostalih korisnika koji uče i koriste samo osnove programa.
2. Osoba koja programira s posebnim entuzijazmom ili osoba koja više uživa u programiranju nego o raspravljanu o istom
3. Osoba koja cijeni vrijednosti pravog „hacka“
4. Osoba koja brzo programira
5. Osoba koja je stručnjak za neki korisnički program ili provodi mnogo vremena koristeći ga (na primjer Unix hacker)

Također postoje dodatni opisi riječi hacker:

1. Stručna osoba bilo koje vrste
2. Osoba koja uživa u intelektualnim izazovima i koja pokušava prijeći postojeće granice kreativnosti
3. Osoba koja špijuniranjem dolazi do povjerljivih informacija
4. Član globalne zajednice definirane internetom

Rječnik engleskog jezika nudi dvije definicije riječi haker:

1. Zanesenjak u programiranju ili korištenje računala radi njih samih
2. Osoba koja koristi svoje vještine za neovlašten pristup računalnim podacima i mrežama

Definicija termina haker veže se za sam odnos prema programiranju i za talent za programiranje. Većina vrsnih programera ne smatraju se hakerima. Najbolji način da se programer definira kao haker jest taj da ga drugi programeri definiraju kao takvog nego on sam. Hakeri smatraju sebe elitom među programerima, postoji neka vrsta osobne satisfakcije, ega, kada su od ostalih programera definirani kao hakeri.
Ako ih sama riječ ne definira, definira ih povijest koju obrađuje sljedeće potpoglavlje.

2.2. Povijest hakera

Hakeri imaju bogatu povijest stvorenu u relativnom kratkom vremenskom periodu.
Kronologija „hakiranja“ nigdje nije čvrsto definirana, ali prema većini stručnjaka kronološki je podijeljena u sljedećih šest razdoblja:

2.2.1. Prapovijest (1878 – 1969)

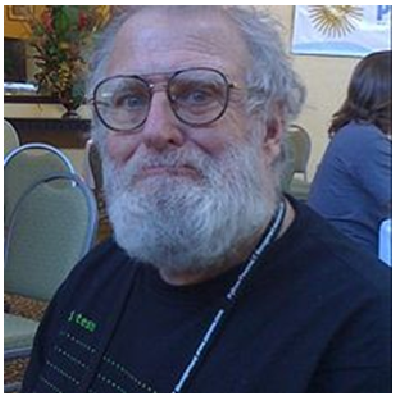
Krajem devetnaestog stoljeća telefonske linije su se pojavile diljem SAD-a, a s njima i prvi hakeri. Termin haker je stvoren mnogo kasnije, ali koristeći termin haker kao netko tko neovlašteno upada u sistem dolazi se do grupe hakera iz pretprošlog stoljeća koji su prisluškivali razgovore, rušili veze i na razne druge načine štetili telefonskim linijama.
Novija povijest hakera počela je 60-tih godina prošlog stoljeća na MIT-u (Massachusetts Institute of Technology) u državi Massachusetts, SAD (slika 2.1.). Prirodno inteligentni i znatiželjni studenti MIT-a istraživali su telefonsku mrežu i kontrole prometa željezničkih mreža te su svojim radom impresionirali profesora Marvina Minskog koji im je dao pristup računalima u MIT laboratoriju (MIT Artificial Intelligence Lab). Ta skupina studenata, koji su sebe prozvali „phranksters“, su bili hakeri u definitivno pozitivnom smislu, poboljšavali su i redizajnirali programe izvan njihovih standardnih okvira i gabarita rada. Ti hakeri su vjerovali u slobodu informacije i tehnologije, bez ikakvog ograničenja.

Slika 2.1. Massachusetts Institute of Technology (MIT)

2.2.2. Phreaker-s (1970 – 1979)

1971. godine mala, ali rastuća, skupina ljudi prevarila je Američke telefonske sisteme s besplatnim pozivima diljem Zemlje. Zvali su se „phreaker-s“.
„Phreaking“ je termin rađen kombinacijom riječi čudak (freak), phone (telefon) i slobodan (free). „Phreaking“ je počeo kada su telefonske kompanije prešle s ljudskih operatera na računalne telefonske sisteme. Novi „direct–dial“ sustavi bili su bazirani na više-frekvencijskim tonovima. Prvi poznati hack u današnjem značenju te riječi ostvaruje 1971. godine stanoviti John Draper (slika 2.2.). On pomoću obične dječje zviždaljke razbija sustav AT&T telekomunikacijske kompanije i ostvaruje besplatne telefonske pozive. Shvativši da

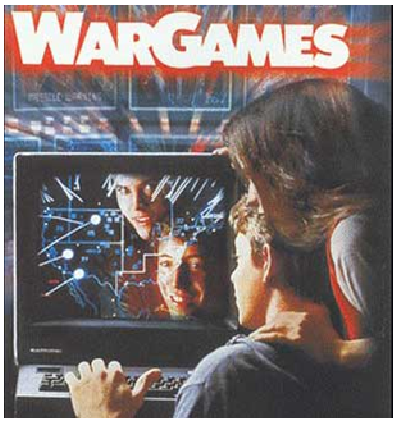
zviždaljka proizvodi ton frekvencije 2.600 herca pokrao je jednu američku telefonsku kompaniju ispuštanjem tona u slušalicu, time je aktivirao operatera, te se služio besplatnim pozivima. Kasnije je bio uhvaćen te je odslužio pet godina zatvora.



Slika 2.2. John T. Draper (Captain Crunch)

2.2.3. Zlatno doba (1980 – 1985)

Do osamdesetih godina prošlog stoljeća hack je bio omogućen samo „phreakerima“ i osobama koje su imale pristup glavnim računalima instituta i fakulteta. Tada se pojavljuju osobna računala (PC – personal computer), a paralelno s tim dolazi do velikog rasta hakera. Među prvim i najpopularnijim osobnim računalima je Commodore 64 .
Godina 1982. bila je u znaku takozvane grupe 414. Radilo se o hakerskom udruženju inteligentnih mladića koji su upali u šezdesetak računalnih sustava, uključujući i laboratorije u Los Alamos-u i memorijalnom centru Sloan – Kettering.
1983. godine pojavljuje se film „War Games“ (slika 2.3) koji širu javnost upoznaje s pojmom hakera i u globalnu svijest donosi svojevrsnu „hakersku paranoju“, što i nije čudno s obzirom da su u filmu hakeri skoro prouzročili treći svjetski rat.



Slika 2.3. War Games (1983. godina)

2.2.4. Kriminalno ponašanje (1985 – 1990)

Sve veći broj hakera sredinom osamdesetih godina prošlog stoljeća nije bio zadovoljan samo s istraživanjem računalnih sistema pa su se okrenuli kriminalnim radnjama. Distribucija piratskih programa i igara je bilo uobičajena stvar. Neki hakeri iz starijeg doba su osjetili da je nova generacija na sceni, generacija koja ne mari za princip slobode tehnologije već su mnogo više zainteresirani za osobni profit. Pravi hakeri su se počeli dijeliti među sobom pa je nastala nova grupa hakera koji su se prozvali krekeri (crackers), vidno orijentirani prema kriminalnim radnjama.
Godinu 1988. neki nazivaju i „godinom Morris-ovog crva“. Te je godine ugledni student s američkog sveučilišta Cornell stvorio opasan računalni virus i njime zarazio preko 6000 Arpanetovih računala (ARPANET – nastao 1961. godine, smatra se pretečom Interneta).
Morris je uhvaćen te je dobio kaznu od tri godine uvjetnog zatvora.

Slika 2.4. Rad na ARPANETU 1961. godine

2.2.5. Crackdown (1990 - 2000)

15 siječnja 1990. AT&T–ova nacionalna mreža je bila ukinuta na punih 9 sati. Govorilo se da je to hakerski napad. Iako danas vjeruju da je uzrok tome pogreška unutar mreže kompanije, tri dana nakon „napada“ krenula je dugogodišnja potjera prema hakerima.
1991. godine računalni virusi nastavljaju harati, pojavljuje se virus Michelangelo koji prijeti da će 6. ožujka 1993. napraviti računalni kaos. Nije se dogodio računalni kaos, ali se virus aktivirao svake slijedeće godine na 6. ožujka ukoliko je još bio u sustavu.
1994. godine skupina Ruskih hakera krade od Citibank-a deset milijuna dolara.
Za krađu je optužen Vladimir Levin te je osuđen na trogodišnju zatvorsku kaznu.
1997. godine petnaestogodišnji hrvatski haker upada u američku bazu u Guam-u. Hrvatski mediji ga slave kao heroja, a mladić je prošao bez većih posljedica.

2.2.6. 2000 +

Novi milenij započinje ljubavnim crvom (worm) koji se širi preko e-mail poruke „Volim te“.
Crv je zarazio milijune računala diljem svijeta te prouzročio paniku (slika 2.5.).

2007. Estonija doživljava najveći hakerski napad u svojoj povijesti. Blokiraju se banke i državne ustanove, a zemljom vlada digitalni kaos. Još nije pronađen krivac za štetu.
Ove godine projekt „Chanology“ napada Internet stranice scijentološke crkve, s poslužiteljskog računala su ukradeni povjerljivi dokumenti te su distribuirani diljem Interneta.

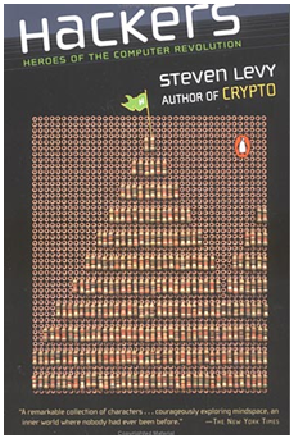
Slika 2.5. Kod virusa “I love you” (2000. godina)

2.3. Hakerska etika i vrste hakera

Prije samog objašnjenja hakerske etike, važno je razumjeti zašto hakeri upadaju u računalne sustave. Za većinu hakera to je izazov, uzbuđenje i zabava. Iako je opće mišljenje da su hakeri osobe koje su asocijalne i izbjegavaju ljude i druženja radi računala, hakeri su u tom svijetu upravo iz razloga jer se žele družiti. Vole da komuniciraju na „chatu“, preko e-mail4-a ili uživo. Dijele priče, mišljenja, glasine i informacije, rade zajedno na projektima, prenose znanje mlađim hakerima, i okupljaju se radi dogovora i druženja. Dijeleći tajne i znanja koje nauče, hakeri dobivaju priznaje za svoja dijela i ulaze u ekskluzivne hakerske grupe.
Nema puno toga neuobičajenog u motivima jednog hakera. Radoznalost, avantura, želja da si cijenjen od grupe ljudi koja ti je slična. Pošto su im djela nelegalna, neki hakeri probijaju sustave upravo zbog uzbuđenja što rade nešto što nije zakonski prihvatljivo. Većina hakera ne probija sustave radi profita ili sabotaže, međutim, ima moćnih motiva iza same atrakcije hakiranja, poput želje da se ima kontrola, da se osjećaš superiorno i da budeš što bliži s elitnim hakerima.
Većim dijelom moralni principi hakera nisu puno drugačiji od većine ostalih koji smatraju hakere lošim osobama. Hakeri se slažu da nije u redu raditi štetu ljudima i nauditi im. Ali hakeri za razliku od ostalih ljudi drugačije interpretiraju riječ „šteta“ i „nauditi“. Hakeri obično ne smatraju čin provaljivanja u sustav štetnim. Za njih, šteta će nastati jedino ako unište podatke medicinske ili neke slične ustanove. Ne smatraju da su oštetili osobe čiji sustav probijaju, ne smatraju da je uzimanje sistemskih datoteka krađa, naprotiv, misle da bi isti ti podaci i datoteke bile neiskorišteni da se ne upotrijebe, što bi bila šteta. Slažu se da pretraživanje tuđeg osobnog računala, njegovih podataka, e-mail-a je povrjeda privatnosti te osobe i zato nije prihvatljivo, ali većina hakera to svejedno rade.
Neki hakeri su ljuti kad ostali hakeri oštete ili izbrišu podatke ili datoteke koje će vidno nedostajati na računalu, naime, među hakerima se smatra da brisanje bilo koje datoteke nije etično, kao što nije ni etično davati zaporke ili ostale sigurnosne podatke osobama koje bi mogli oštetiti računalni sustav.
Hakeri opravdavaju svoja dijela stavom da su učenje i istraživanje dobre osobine, da je sloboda informacija dar od društva, da je korisno otkriti slabe točke računalnog sustava da bi ga poboljšali i da mnoge organizacije što rade programe i sustave koji oni provaljuju se

zasnivaju isključivo na stvaranju profita, a ne na želji za ostvarivanjem neke komunikacije s običnim korisnikom i ispunjavanjem njegovih potreba. Iako se neki hakeri slažu s ovim razlozima, za većinu njih to nije opravdanje za probiti sustav. Neki hakeri tvrde da je odgovornost na sistem operatorima jer nisu sposobni da spriječe napad na njih. Neki od njih kažu da većina sustava treba da bude dostupna svima, jer pravi zločin je skrivanje informacija.
Mnogi ljudi dijele mišljenje da su provaljivanja u sustav pogrešna djela, ali ne toliko pogrešna da bi se kažnjavala tako strogo. Naime, u prošlosti je bilo sasvim normalno uposliti hakera, a većina zaposlenih hakera su postali odgovorni i vjerni zaposlenici. Na fakultetima sasvim je uobičajeno da se studenti, deklarirani od društva kao „hakeri“, smatraju inteligentnim i u načelu dobrim osobama koji višak vremena koriste za programiranje.
Na kraju, etika ima veze s djelima, ne riječima. Ako mi sami ne koristimo dobru etiku, tada ćemo biti licemjeri i loši uzori za hakere koji dolaze, smatraju hakeri. Ipak, najbliži hakerskoj etici u riječima bio je Steven Levy koji u svojoj knjizi iz 1984 godine „Hakeri: Heroji računalne revolucije“ napisao šest osnovnih principa hakerske etike:

- pristup računalima i svemu što može da nas nauči o tome kako svijet funkcionira mora biti neograničen i potpun
- sve informacije moraju biti slobodne
- decentralizacija se postiže kada imamo odbojnost prema autoritetu i vlastima
- hakera treba cijeniti po njegovim djelima („hacku“), a ne prema kriterijima poput diplome, starosti, rase ili položaja u društvu
- pomoću računala kreirajmo ljepotu i umjetnost
- računala mogu da promjene život na bolje



Slika 2.6. Steven Levy – Hakeri: heroji računalne revolucije

Hakeri se prema hakerskoj etici dijele u tri osnove kategorije:

1. White hat hackers (bijeli šeširi)
   Poznati su kao „dobri“ hakeri, uvijek koriste svoje znanje za dobrobit računalnog sustava. Iako „razbijaju“ računalne sustave to rade kako bi oni bili još više optimizirani i bolji. Surađuju s proizvođačima programa te im ukazuju na nedostatke njihovih programa. Također sudjeluju u stvaranju obrambenih mreža i protupiratske zaštite. Obično završe kao vrlo dobro plaćeni mrežni administratori, programeri i sigurnosni savjetnici. U SAD-u ih često zovu „geeks“ (štreberi).

2. Gray hat hackers (sivi šeširi)
   Oni su svojevrsni hibrid white i black hat hakera. Ponekad, iz zabave, probiju se i naprave pomutnju u računalnom sustavu nekom neutralnom korisniku računala. Iako oni misle da je ovakva vrsta aktivnosti bezazlena, posljedice toga što rade ih mogu odvesti i u zatvor.

3. Black hat hackers (crni šeširi)
   Ovi hakeri su glavna prijetnja računalnim sustavima. Neki ih zovu i krekeri (crackers). Oni šalju i izrađuju viruse, uništavaju podatke, napadaju Internet stranice i upadaju u tuđa računala. Pored toga black hats se bore protiv white hats-a (gray hats su u tome, kao i u svemu, neutralni), osnovni cilj im je biti najbolji među „najgorima“.
   Često su povezani s kriminalnim podzemljem, često nelegalnim putem stjecaju novac.

Ako se za kriterij uzme stručnost za određeni program ili operacijski sustav postoje i Windows hakeri, Game hakeri, Unix hakeri…

Detaljnija i preciznija podjela hakera po nivou vještine rada na računalu i po sferi entuzijazma i same etike hakiranja dijeli hakere na sedam osnovnih vrsta hakera.

1. Old school hackers (hakeri stare škole)
   To su „old style“ (staromodni) hakeri s MIT i Stanford instituta. Oni predstavljaju hakere iz šezdesetih godina prošlog stoljeća. Pravo su osvježenje među ostalim hakerima, to su ljudi koji su pokrenuli hakersku revoluciju te ljudi kojima je cilj decentralizacija pristupa komunikacijama, sloboda informacija i najvažnije od svega, koristiti računala za dobrobit čovječanstva.

2. Phreaker-s
   Hakeri su ljudi fascinirani tehnologijom. U toj grupi postoje i ljudi koji su se „specijalizirali“ za telefonske uređaje. Telefon je nevjerojatno jednostavan uređaj, ali opet, telefonski sistem na kraju žice je jedan od kompleksnih sustava ikad napravljeni. Phreakeri imaju dugu povijest, koja datira gotovo od samog izuma telefona, ali s digitalizacijom i uvođenjem računala u široku upotrebu, moć phreakera postala je neograničena. U današnje vrijeme preko računalnih phreaker programa phreakeri naizmjenično mogu pozvati sve moguće kombinacije brojeva dok ne dobije pravu kombinaciju za pristup određenom telefonu.

3. Krekeri
   Krekeri su specijalizirani za provaljivanje u sustav. Mnoštvo hakera posjeduju vještinu upada u drugo računalo, ali većina njih je to „preraslo“. Postoji mišljenje među programerima da je veoma tanka crta između hakera i krekeri, a osnovna razlika između njih je što pravi hakeri grade stvari, a krekeri ih ruše.

4. Warezd00dz
   Ovi hakeri su veoma slični krekerima iz razloga što se, kao i oni, bave provaljivanjem u tuđi sustav. Razlika je što „Warezd00dz“ napada točno određeni program. Sam njihov pomalo neobičan naziv označava program ili aplikaciju u računalu. Specijalizirani su za označavanje programa, pronalaženje njegovog serijskog broja i nelegalnu distribuciju korisnicima. Može ih se staviti u sam vrh računalne piratske industrije.

5. Haktivist
   Haktivisam (riječ je nastala spajanjem riječi „hack“ s riječi „activism“) je pokret nenasilnog korištenja ilegalnih ili legalnih digitalnih uređaja za političke svrhe. Oni rade virtualne sabotaže Internet stranica, „izvan upotrebe“ i „redirect“ napade i sve ostalo što je potrebno da promoviraju svoju političku ideologiju.

Slika 2.7. Sabotaža Internet stranice www.cnn.com za slobodu Tibeta

6. Larval and newbie’s
   Ovo su dvije grupe ograničenog znanja u svijetu računala. Zbog svog neznanja često krše samu hakersku etiku, a da toga nisu ni svjesni. Pokušavaju naučiti što više o računalima i hacku da bi se dobili priznaje i status među ostalim hakerima. Ova vrsta hakera je nastala pojavom filma „War games“ iz 1983, o kojem je bilo riječ u potpoglavlju 2.2.3.

7. Script kiddies lamer
   Kao što nam i samo ime govori, script kiddies lamer su maloljetni „dječji“ hakeri. Njihovo znanje o računalima je minimalno, a njihov motiv je čisto vandalske pobude. Njihova meta su svi korisnici računala, bez osobitog razloga. Zbog nedostatka znanja i nepoštivanja hakerske etike nemaju mjesto u hakerskoj zajednici.

Dakako, podjela hakera po ovim kriterijima nije konačna. Neke vrste hakera teško je staviti u neke određene granice, pa tako i u ove skupine. Neki hakeri po načinu rada pripadaju samo jednoj skupini, a neki se isprepliću s ostalim skupinama. Što se više tehnologija razvija sve je više hakera a s time i vrsta hakera.
O samoj etici za kraj može se reći da nije dovoljno reći mladim ljudima da su upadi u tuđa računala pogrešni, većina njih zna da to nije u redu, oni jednostavno smatraju da su to bezopasni upadi i da ne rade nikome zlo.

3. HAKERSKA POTKULTURA

"Biti haker je zanimljiv način života, ali kad jednom kreneš tim načinom života, teško je izaći iz njega. Cijeli život je nevjerojatno jasan. Samo hakaš i govoriš s ostalim ljudima što hakaju. To je društvo povezano s hakom, to je kultura, to je način života. To je cijeli svijet. Uvijek ima posla da se obavi i nikad nisi sam. Taj način života je izrastao iz hakerskih djela. Ostaju budni cijelu noć, uvijek vidu iste ljude, koji su na istim „otvoreno 24 sata“ mjestima, dijele iste aktivnosti, rastu zajedno, pošto od uvijek žive zajedno…"
Tim je riječima jedan haker opisao svoj svijet. Svoju potkulturu koju slijedi. Za razliku od ostalih potkultura, hakerska potkultura je rođena bez osjećaja da si stranac ili da si drugačiji od ostalih. Centralni predmet hakerske potkulture je računalo. Sve u hakerskoj potkulturi se zasniva na računalu, to je bog njihove religije. „Drugačiji od ostalih“ je priroda hakerske potkulture koja stavlja fokus na računalo, ono oblikuje pravila ponašanja, status, etiku i potkulturu.
Hakerska kultura je mrežna kolekcija potkultura što je jedna velika svijest iskustva, porijekla i vrijednosti koja se prijenosi iz generacije na generaciju. Ima svoje mitove, heroje, zločince, narodne priče, šale, tabue i snove. Pošto su hakeri grupa kreativnih ljudi koji se ograđuju od „normalnih“ vrijednosti i radnih navika, neobično je da dijele tradiciju jedne svjetske kulture koja postoji već 50 godina.

3.1. Elementi hakerske potkulture

Potkultura je skupina ljudi s različitim ponašanjem od kulture kojoj pripadaju. Potkulture se razlikuju po starosti osoba, spolu, rasi, nacionalnoj ili klasnoj pripadnosti. Hakerska potkultura se razvila u okviru hakerske kulture i predstavlja dio koji se povezuje sa računalnim podzemljem (grupe poput crnih hakera, krekera i lamera). Pripadnici ove kulture se ne udaljuju od hakerske kulture već se prepliću s njom pošto imaju zajedničku društvenu ideologiju i ljubav prema učenju o tehnologiji.
Centralni dio hakerske kulture na kojim se ona i razvija su Internet, WWW, GNU projekt, Linux operacijski sustav i svi hakerski alati. U zadnjih dvadeset godina hakerska kultura dobiva dodatne simbole poput Tuxa, the Linux penguin, the BSD Daemon i Pearl Camel. Također je nastao i hakerski logo (kojeg se može vidjeti na slici 1.1.) kojeg je napravio Eric Raymond. Leksikon jargon file (više o njemu opisano je u potpoglavlju 3.2) ima posebnu ulogu u hakerskoj kulturi i jedan je od glavnih zaštitnih znakove ove kulture. Vanjske manifestacije hakerskih aktivnosti lako je uočiti, mnogobrojne su i stvorene u kratko vrijeme. Hakerska kultura se bazira na unutrašnjoj strukturi hakerske zajednice, na običajima, načinu rada, života, komunikacije i samim psihološkim profilima.

3.1.1. Profil hakera

Ljudi gaje razne stereotipe o hakerima, među najčešćima su sljedeća tri:

- mladež koja nije dobro odgojena, oni su omladina kojima netko treba pokazati pravi put, ali ukupno gledajući, bezopasni su. Treba ih poticati da njihovu inteligenciju i kreativnost usmjere prema konstruktivnim ciljevima

- specijalisti za računalnu sigurnost. Hakeri znaju slabosti sigurnosti računala. Treba ih zaposliti kao specijaliste za računalnu sigurnost i iskoristiti njihovo znanje za obranu računala
- hakeri su razbojnici i treba ih tretirati kao i sve ostale razbojnike

Priče o zločestom tinejdžeru koji nema socijalni život je skup ekstremnih osobina koje mogu imati hakeri, te nikako ne predstavlja prosječnog pripadnika hakerske zajednice. Što su stvarno hakeri može se saznati iz leksikona Jargon datoteke (više o njemu opisano je u potpoglavlju 3.2) koji ima dio posvećen načinu života prosječnog hakera.

Fizički profil:

Većinom su bijelci, muškog spola (iako ima i ženskih hakera), imaju ispod trideset godina, svijetle „računalne“ puti, ponekad ekstremno debeli ili ekstremno mršavi.

Psihološki profil:

Visoki kvocijent inteligencije, velika radoznalost i lakoća intelektualne apstrakcije. Nova saznanja ih veoma stimuliraju. Veoma su individualni i komforni. Sposobni su upijati znanje i obraćaju pažnju na svaki detalj. Osoba koja ima prosječnu analitičku inteligenciju i koja ima sposobnost zapažanja detalja može postati odličan haker, dok kreativna osoba koja nema tu sposobnost nikad neće doseći vrhunski nivo hakiranja.

Hakeri nisu jednostrani, zanima ih bilo koja intelektualna tema, i podjednako dobro raspravljaju o mnoštvu različitih tema. Hakeri ne poštuju autoritet i ne žele imati vezu s ni čim što je obvezujuće. Ne vole neodređenost, monotoniju i dosadne stvari koje prate život. Vrlo često su jako dobro sređeni u vlastitom intelektualnom planu, ali su im ostali aspekti života kaotični. Većinu hakera ne motivira novac. Privlače ih izazovi, njihov tip osobnosti je intuitivan, za razliku od tipa osobnosti koji dominira u njihovoj kulturi.

Hakeri nemaju sposobnost emotivne identifikacije s drugim ljudima. Često su arogantni i nestrpljivi. Ne vole kad ih opterećuju stvarima koji oni smatraju gubitkom njihovog vremena. Dobri su u manipulaciji drugim ljudima, pogotovo phreakeri koji dolaze do povjerljivih informacija i zaporki tim putem. Hakeri imaju lošu naviku da stvarima pristupaju iz tehničkog ugla. Pošto su uvjereni da su uvijek u pravu, pogotovo kad je tehnika u pitanju, vrlo su netolerantni, što dolazi do svađa među hakerima (Unix hakeri preziru Windows sustav, old school hakeri preziru Unix i Linux hakere…) što vodi do problema pri uspostavljanu dugotrajnog odnosa i ostvarivanju trajnijih veza. Proizvod toga nastaju klasični“računalni štreberi“ (computer geek), depresivni, seksualno frustrirani i nesposobni za odnos s drugima, koji su u manjini među hakerima.

Obrazovanje:

Većina su studentski obrazovani. Informatika, elektrotehnika, fizika, filozofija, matematika i lingvistika su njihovi omiljeni studiji. Postoje naravno i samouki hakeri koji znaju biti cijenjeni od studentski obrazovanih hakera.

Ostalo:

Poslije 1995 i filma „Hakeri“, hakeri padaju pod utjecaj rave, gothic i punk kulture. To se najviše vidjelo u njihovom stilu odijevanja, a muškarci često imaju brade i dugu kosu, dok žene hakeri nisu sklone šminkanju.

Omiljena hrana hakera je hrana s puno začina (još jedan stereotip je da su veliki ljubitelji takozvane „junk food“ hrane).

Veliki su ljubitelji literature. Najpopularnija je naučna i SF literatura.

Hakeri su u većini ateisti i agnostici ili židovi. Hakeri koji su religiozni trude se da se ne pridržavaju svoje religije.

Politički su liberalno orijentirani, odbijaju ikakvu podjelu na lijevu i desnu stranu, možemo reći da ne poštuju vlast ni autoritet države.

Nisu ljubitelji fizičkih aktivnosti, izbjegavaju kolektivne sportove, među poželjnim sportovima su planinarenje, jedrenje, biciklizam…
Veoma su tolerantni po pitanju seksualnog opredjeljenja u odnosu na ostale kulture. Među hakerima je mnogo homoseksualnih i biseksualnih pripadnika.
Veliki su ljubitelji kave i šećera, većinom ne konzumiraju cigarete i alkohol, skloni su blagim drogama.
Ljubitelji su muzike, intelektualnih igara svih vrste i video igrica.
Izbjegavaju sve proizvode kompanije Microsoft, ne vole laganu muziku, televiziju, programe COBOL i BASIC.

3.1.2. Svijet hakera

Hakeri su pripadnici cyberpunk potkulture. Cyberpunk je žanr znanstvene fantastike fokusiran na računala i tehnologiju. Motivi na kojima se bazira su sukobi među hakerima, umjetna inteligencija i velike korporacije koje kontroliraju svijet u budućnosti. Krajem osamdesetih godina prošlog stoljeća pojavili su se filmovi i video igrice cyberpunk tematike, a početkom devedesetih osobine cyberpunk-a prelaze na modu i glazbu.
Hakeri imaju i niz svojih časopisa među kojima je najpoznatiji časopis „2600“, nastao još 1984 godine. Ime je dobila po 2600 MHz, koliko je proizvodila kultna zviždaljka John Drapera kada je uspio da prevari telefonsku centralu (potpoglavlje 2.2.2.). Postoji naravno i Internet izdanje časopisa koji i dan danas bilježi rekordne posjete.
Vrijedan spomena je i časopis „Phrack“ nastao 1985, a veoma je popularna i Internet verzija hakerske enciklopedije, koja nudi definicije različitih pojmova koji se koriste u hakerskoj zajednici. Od sedme umjetnosti, kultni status među hakerima ima, već spomenuti, „War games“ iz 1983 godine, „Hackers“ iz 1995 godine i „Matrix“ iz 1999 godine.

Slika 3.5. Naslovnica magazina “2600”

3.2. Način komunikacije

Prava moć hakera je u tome koliko dobro razumiju prosječnog korisnika računala. Zato su se pobrinuli da prosječni korisnik njih ne razumije, kreirajući svoj stil pisanja, svoj žargon. Kako i u drugim žargonima, specijalni vokabular hakera pomaže im da sačuvaju svoje mjesto u društvu, da djelu vrijednosti i iskustvo. Isto tako, nepoznavanje žargona, ili krivo korištenje istog, definira hakera kao stranca, ili gore, u žargonu hakera kao „suit“ (haker koji nosi neudobnu odjeću, odijela, haker koji to nije). Sve ljudske kulture koriste žargon kao predmet komunikacije za uključenje ili isključenje iz društva.
Dokument koji je prepoznatljiv na Internetu i koji se može slobodno uzeti, nadopuniti i dijeliti je, za hakere kultni, „Jargon file“, takozvana „Hakerska biblija“. „Jargon file“ je glavno nasljeđe hakerske kulture. Ne postoje legalni smjerovi što da se radi s njim, ali postoji tradicija kako se pravilno koristi i mnogi hakeri to poštuju. Originalna datoteka nastala je 70 tih godina prošlog stoljeća kada su tehničari s američkih instituta počeli zapisivati izraze koje su koristili, a svoju premijeru u knjizi je imala 1981. godine, dok 1983. godine izlazi pod imenom „Hacker`s Dictionary“. S godinama hakeri ga prihvaćaju i nadopunjuju, polako prelazi u urbanu legendu.
Sam „Jargon file“ dijeli se u tri cjeline:

- sleng - jezik uzet od engleskog uobičajenog govora i potkultura koje nemaju tehničku pozadinu, kao što su rokeri, surferi…
- žargon – glavi predmet ovog leksikona, jezik hakera
- tehnički jezik – vokabular programiranja, računalnih znanosti, elektronike i ostalih polja bliskih hakeru

Zadnja verzija „Jargon file“ iz 2003 godine sastoji se od 236406 riječi i 638454 simbola. Na Internet adresi http://www.catb.org/jargon može ga se pogledati, također se može dati savjet, primjedba, pohvala ili zahtjev za dopunjivanje leksikona novim izrazima.

Slika 3.1. Jargon file na stranici http://www.catb.org/jargon

Hakeri su otišli korak dalje od samog žargona. Kreirali su vlastito pismo imena Leetspeak.
Kulturni fenomen zbio se 2007 godine kada je Merriam-Webster proglasila „w00t“ za riječ godine. To je bilo formalno prihvaćenje riječi sastavljene od dva slova i dva broja, znak da je Internet jezik došao u teen kulturu. „W00t“ se izgovara kao „woot“, znači veselje, a to je samo jedna od mnogih riječi novog „cyber“ jezika naziva „Leetspeak“.

Slika 3.2. Tastatura prilagođena „Leet“ jeziku

Godinama računalni hakeri i igrači video igrica koristili su ovaj jezik za komunikaciju u mreži, to je doslovno elitni („leet“) vokabular često korišten da zaobiđe cenzuru. U današnje vrijeme postaje važan čimbenik generacije koja je rasla uz Internet.
Leet može imati više formi, slova su zamijenjena brojevima ili simbolima, kao na primjer „3“ za „e“, i „1“ za „i“. Sama riječ „Leet“ može se napisati kao „l33t“, „1337“ ili „31337“, ovisno o razini težine pisanja. Vokabular igrača video igrica je također našao prostor u ovom jeziku. Jedna od čestih riječi je „pwn“, izgovara se kao „own“ što znači dominirati nad protivnikom. „N00b“ je „newbie“ što znači „novi tip“. Leet je još „underground“, ali sve je više „N00b“ (novih) koji ga pokušavaju naučiti i prihvatiti, pa se jezik sve manje koristi za tajne i cenzuru, a sve više za izražavanje. Cijeli virtualni svijet je prenesen u stvarnost, a polako, generacije koje dolaze, formiraju cijelu novu civilizaciju na leet jeziku.

A	4 /\ @ /-\ ^ ä ª
B	8 6 |3 ß P> |:
C	[¢ < (
D	|) o| [) I> |> ?
E	3 & £ ë € ê |=-
F	|= ph |#
G	6 & (_+ 9 C- (,
H	# /-/ [-] {=} <~> |-|]~[}{ ? }-{
I	1 ! | & eye 3y3 ï][
J	,| _| ;
K	X |< |{]{ }< |(
L	1 7 1_ | |_ # l
M	//. ^^ |v| [V] {V} |\/| /\/\ (u) []V[] (V)
N	// ^/ || /\/ [\], <\> {\} []\[] n /V ₪
O	0 () ?p ö
P	ph |^ |* |o |^ (o) |> |" 9 []D ‽, |7
Q	9 (,) <| ^(o)| ¶ O_
R	| 2 P\ |? |^ lz [z ? Я
S	5 $ z §
T	7 + -|- 1 ']['

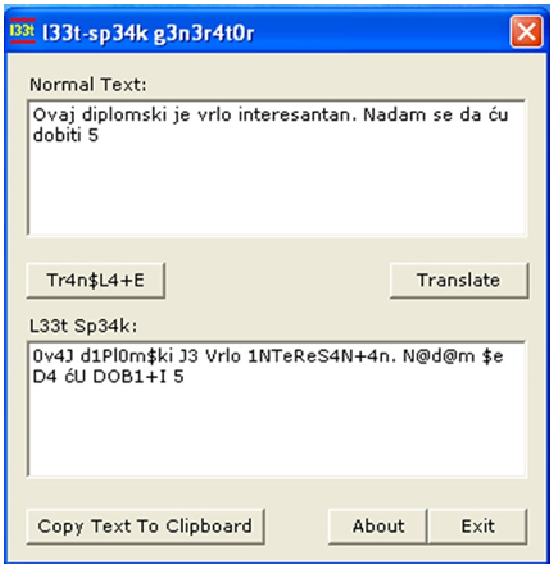
U	(_) |_| v ü
V	\/
W	\/\/ '// \^/ (n) \V/ \// \X/
X	>< ? +)(
Y	Y '/, `/ V/ \-/ j ¥ %
Z	2 z ~_ ~/_

Slika 3.3. Leet abeceda

Hakeri, u pravilu, vole igru riječima i veoma su uporni i inovativni u upotrebi svojih jezika. Specijalna varijanta leeta koristi obrnute riječi u jezicima kao HTLM koji ne dopuštaju rotaciju teksta. Koristeći „Unicode“ simbole može se dobiti dojam obrnutog teksta (flip text). Slova s, x, z su rotacijski simetrična, za razliku od slova b/q, d/p i n/u. Ostatak slova su kodirani u Unicode simbolima, tako da je kreirana cijela obrnuta abeceda. Velika slova u obrnutom leet-u se izbjegavaju kao i brojevi (osim 0,8 i 6/9) a sama interpunkcija riječi je vrlo dobro pokrivena. Ovaj leet je višenamjenski. Može se koristiti za umjetničke svrhe (na utakmicama lige prvaka ime momčadi na računalnoj simulaciji „hajduk split - ʇılds ʞnpɾɐɥ“), može se koristiti kao zagonetka ili šala.
Primjer obrnutog leet-a:

- predmet: sigurnost računala i podatka, diplomski rad: hakeri
- ɹɐʞǝɥ :pǝɹ ɹʞsɯoldıp 'ɐʞʇɐpod ı ɐlɐunčɐɹ ʇsouɹnbıs :ʇǝɯpǝɹd

Leet se može izgovoriti kao jedan slog, /`li:t/, što se rimuje s „eat“, gdje se opet dolazi do „elite“. Kao ostali sleng jezici, leet voli pogrešnu gramatiku standardnog jezika. Izgubiti gramatiku, kao izgubiti slova daje neku vrstu značaja, ironičnu ili običnu. Čitatelj mora više obratiti pozornost na sam izraz, a ne na strukturu rečenice, da bi shvatio značenje rečenice. Leet ima neke svoje potpuno nove riječi, stvorene od tipičnih grešaka pri pisanju, što je običaj novim korisnicima računala. Leet nije isključivo vezan samo za jedan jezik. Grčki, ruski, kineski i ostali jezici imaju također leet forme, a leet jednog jezika može koristiti znakove dugog leet jezika. Veoma su česti simboli kod leet jezika, kao na primjer uskličnik, pošto znak „!“ dijeli mjesto s znakom „1“ na QWERTY tastaturi. U svakom slučaju, kombinacija je puno, ostaje samo da se upotrijebi mašta i da se počne pisati na leet-u.
Postoje i programi koji prevode standardne riječi u leet jezik. Internet pretraživač „Google“ prepoznaje leet jezik, te se može vršiti pretraga pomoću njega.



Slika 3.4. Leet prevoditelj

Ukratko, u pismu hakera leet-u nema pravila. Svakodnevno nastaju novi simboli, načini pisanja i riječi, koji su u toku s medijima današnjice. Govorni leet također postoji, ali u veoma maloj mjeri, najčešće se upotrebljava u igraonicama video igara. Govorni leet je nepraktičan, težak za izgovor, nimalo zvučan i sama komunikacija teče mnogo sporije nego uobičajeno.

Leet ima važnu ulogu u hakerskoj kulturi, to je njihov jezik, on izražava njihova djela i iskustva, on omogućava slobodu govora, bez cenzura i zabrana što autoriteti postavljaju.

4. HAKERSKI NAPADI I ALATI

4.1. Napad i metode napada hakera

Hakeri koriste trikove da pronađu prečac za nedopušteni ulaz u računalni sustav. Mogu koristiti ovaj ulaz za ilegalne ili destruktivne svrhe, ili jednostavno mogu testirati vlastitu vještinu da vide jesu li sposobni za takav ulaz u sustav. Većini hakera je glavni motiv napada znatiželja i višak slobodnog vremena, pa je velika vjerojatnost da će haker u jednom trenutku, nakon bezbrojnih pokušaja, pronaći naprednu metodu napada i ući i u najbolje čuvani sustav. Ostali motivi su psihološka potreba, želja za učenjem, znatiželja, osveta, eksperimentiranje, nepovjerenje u druge osobe, samo-priznanje, želja da nekoga pobjede ili zabava.

Da bi se efikasno procijenile sigurnosne potrebe neke organizacije i da bi se odabrali različiti sigurnosni proizvodi, pravila, procedure i rješenja, rukovodiocu u tvrtki koji je zadužen za sigurnost potreban je sistematičan način definiranja zahtjeva u pogledu sigurnosti i kategorizacije pristupa koji omogućavaju da se ti zahtjevi zadovolje.

Jedan pristup je da se razmotre tri aspekta sigurnosti informacija:

- napad na sigurnost (security attack) - bilo koja akcija koja ugrožava sigurnost informacija
- sigurnosni mehanizam (security service) – mehanizam koji treba da otkrije i preduhitri napad ili da sustav oporavi od napada
- sigurnosna usluga (security service) – usluga koja povećava sigurnost sistema za obradu i prijenos podataka. Sigurnosna usluga podrazumijeva upotrjebu jednog ili više sigurnosnih mehanizama.

4.1.1. Vrste napada

U osnovi, napadi su hakerske akcije koje su usmjerene na ugrožavanje sigurnosti informacija, računalnih sustava i mreža. Postoje različite vrste napada, ali se oni generalno mogu podijeliti u četiri osnovne kategorije:

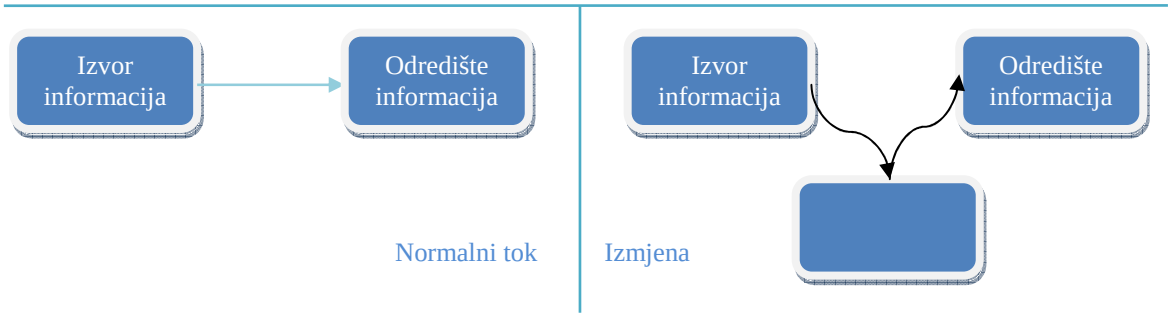
1. Presijecanje ili prekidanje (interruption) predstavlja napad na raspoloživost (availability). Presijecanjem se prekida tok informacija, tj. onemogućava se pružanje neke usluge ili funkcioniranje nekog sustava. Ovakav napad je aktivan.

Slika 4.1. Napad presijecanjem

2. Presretanje (interception) predstavlja napad na povjerljivost (confidentiality). Presretanje može biti u praksi provedeno kao prisluškivanje prometa, nadziranje njegovog intenziteta, uvid u osjetljive informacije ili slično. Kao pasivni napad, teško se otkriva jer ne mijenja podatke, ne utječe na unutrašnje funkcioniranje sustava. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.

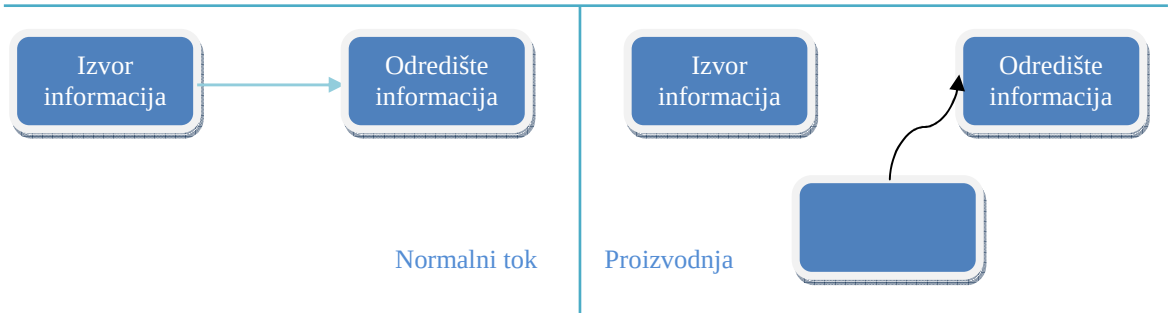
Slika 4.2. Napad presretanjem

3. Izmjena (modification) predstavlja napad na integritet (integrity). Po svojoj prirodi, to je aktivan napad. Ukoliko djeluje na prijenosnom putu, može se, na primjer, dogoditi napad „čovjek u sredini“ (man in the middle). Napad se može obaviti i unutar nekog računalnog sustava. U tom slučaju radi se o izmjeni podataka, pristupnih prava, načina funkcioniranja programa ili sustava i slično. Iako mijenja podatke i sustav, često ostaje neprimijećen izvjesno vrijeme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.



Slika 4.3. Napad izmjenom

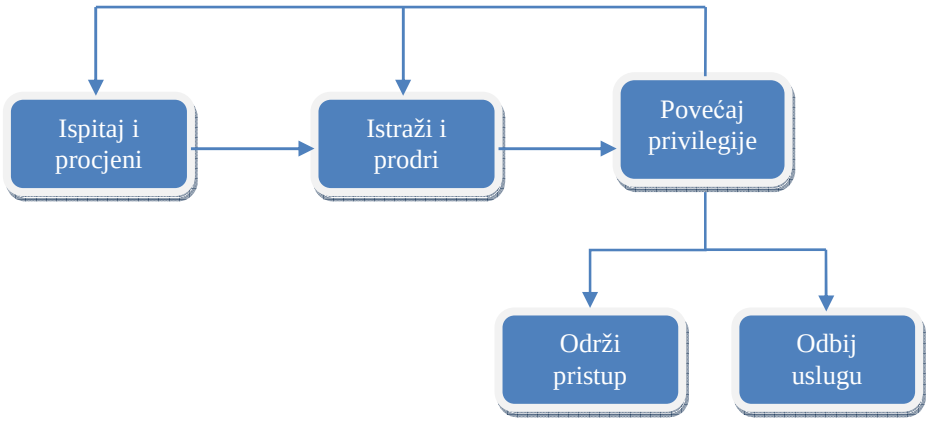
4. Proizvodnja (fabrication), predstavlja napad na autentičnost (authenticity). Napadač izvodi ovakav aktivni napad tako što generira lažne podatke, lažni promet ili izdaje neovlaštene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, poslužiteljskog računala, Web strane ili nekog drugog dijela sustava.



Slika 4.4. Napad proizvodnjom

4.1.2. Građenje napada

Ako se razumije osnovni pristup koji hakeri/napadači koriste da „osvoje“ neki sustav ili mrežu, lakše se mogu preuzeti obrambene mjere, zna se što je primijenjeno i protiv čega. Osnovni koraci napadačeve metodologije opisani su na slici 4.5.



Slika 4.5. Osnovni koraci napada

1. Ispitaj i procijeni (survey and assess). Prvi korak koji haker/napadač obično preuzima je istraživanje potencijalne mete i identificiranje i procjena njenih karakteristika. Te karakteristike mogu biti podržani servisi, protokoli s mogućim ranjivostima i ulaznim točkama. Napadač koristi informacije prikupljene na ovaj način kako bi napravio plan za početni napad. Na primjer, napadač može primijetiti ranjivost tipa cross-site scripting (XSS - tip računalne sigurnosti tipičan za web aplikacije koje dopušta računalni virus u Internet stranice koje drugi korisnici pregledavaju), tako da će ispitati vraća li neki upravljački element Web strane jeku (echo) na izlaz.

2. Istraži i prodri (exploit and penetrate). Nakon što je istražio potencijalnu metu, haker/napadač pokušava da istraži ranjivost i da prodre u mrežu ili sustav. Ako su mreža ili umreženo računalo (najčešće poslužiteljsko računalo) potpuno osigurani, aplikacija postaje sljedeća ulazna točka za napadača – napadač će najlakše upasti u sustav kroz isti ulaz koji koriste legitimni korisnici. Na primjer, može se upotrijebiti stranica za prijavljivanje ili stranica koja ne zahtijeva provjeru identiteta (authentication).

3. Povećaj privilegije (escalate privileges). Nakon što napadač uspije da ugrozi aplikaciju ili mrežu – na primjer, ubacivanjem (injecting) koda u aplikaciju ili uspostavljanjem legitimne sesije na operacijskom sustavu – odmah će pokušati povećati svoja prava. Posebno će pokušati preuzeti administratorske privilegije tj. da uđe u grupu korisnika koji imaju sva prava nad sustavom. Definiranje najmanjeg nužnog skupa prava i usluga koji je neophodno omogućiti korisnicima aplikacije, primarna je obrana od napada povećanjem privilegija.

4. Održi pristup (maintain access). Kada prvi put uspije da pristupi sustavu, haker/napadač preuzima korake da olakša buduće napade i da prekrije tragove. Čest način olakšavanja budućih pristupa je postavljanje programa sa „zadnjim vratima“ (back-door) ili korištenje postojećih naloga koji nisu strogo zaštićeni. U prikrivanje tragova često spada brisanje dnevničkih datoteka (log files) i skrivanje hakerskih alata.

Uzevši u obzir da su dnevničke datoteke jedan od objekata koje napadač želi da modificira kako bi prekrio tragove, one treba da budu osigurane i da se redovno analiziraju. Analiza dnevničkih datoteka često može otkriti razne znakove pokušaja upada u sustav, i to prije nego što nastane šteta.

5. Odbij uslugu (deny service). Hakeri/napadači koji ne mogu da pristupe sustavu ili računalnoj mreži i da ostvare svoj cilj, često preuzimaju napad koji prouzrokuje odbijanje usluge (denial of service attack, DoS), kako bi spriječili druge da koriste aplikaciju (primjer ovakvog napada je SYN flood attack; haker/napadač koristi program koji šalje veliki broj TCP SYN zahtjeva da bi se zagušio red dolazećih konekcija na poslužiteljskom računalu, onemogućavajući tako druge korisnike da se povežu na poslužitelj i iskoriste njegove usluge). Za druge hakere/napadače, DoS napad je cilj od samog početka.

4.1.3. Rizik i prijetnje

Rizik je, u kontekstu sigurnosti računalnih sustava i mreža, mjera opasnosti, mogućnost da nastane oštećenje ili gubitak neke informacije, prestiža ili ugleda. Rizik treba definirati eksplicitno, na primjer, „rizik od narušavanja integriteta baze klijenata“ ili „rizik odbijanja usluga od strane on-line portala banke“. Rizik se obično izražava u obliku jedinice rizika, gdje je:

Rizik = Prijetnja × Ranjivost × Vrijednost imovine

Prijetnja (threat) je haker, situacija ili splet okolnosti s mogućnošću ili namjerama da istraži ranjivost sustava. Ova definicija prijetnje stara je nekoliko desetljeća i jednaka je opisu terorista.
Prijetnja može biti strukturirana ili nestrukturirana. Strukturirane prijetnje su protivnici s formalnom metodologijom, financijskim sponzorom i jasno definiranim ciljem. Takve prijetnje su karakteristične za ekonomsku špijunažu, organizirani kriminal, strane obavještajne službe i takozvane „informatičke ratnike“ (cyber-warriors). Prijetnje se dijele na pasivne i aktivne.

- pasivne prijetnje ne utječu neposredno na ponašanje sustava i njegovo funkcioniranje. U pasivne prijetnje spadaju otkrivanje sadržaja poruka (na primjer, prisluškivanje) i analiza prometa
- aktivne prijetnje mogu utjecati na ponašanje i funkcioniranje sustava ili na sadržaj podataka. U aktivne prijetnje spadaju: maskiranje, tj. pretvaranje, lažiranje (masquerade), reprodukcija, tj. ponavljanje mrežnog prometa (replay), izmjena sadržaja poruke i odbijanje usluge.

Ranjivost (vulnerability) predstavlja slabost u nekoj vrijednosti, resursu ili imovini koja može biti iskorištena, tj. objavljena. Ranjivost su posljedica lošeg projektiranja, implementacije ili „zagađenja“.

- Loše projektiranje je greška projektanta sustava. Proizvođač koji piše loš kod – kod koji sadrži greške (bugs), kao što je prekoračenje međuspremnika (buffer) na dinamičkoj memoriji (heap memory) – pravi osjetljiv proizvod koji se može lakše „razbiti“. Pametni hakeri/napadači će iskoristiti slabosti u arhitekturi programa.
- Implementacija je odgovornost klijenta koji instalira proizvod. Iako proizvođači trebaju pripremiti dokumentaciju o sigurnom korištenju svojih proizvoda, korisnik mora biti vrlo oprezan.

- „Zagađenje“ se odnosi na mogućnost da se dostigne stepenica „iza“ predviđene upotrebe proizvoda. Dobro projektiran programski proizvod treba obavljati predviđenu funkciju i ništa više od toga. Odluke koje ponekad donesu proizvođači i korisnici, mogu da prouzrokuju „zagađenje“, tj. da stvore mogućnost za prekoračenje predviđene upotrijebe proizvoda.

Vrijednost imovine je mjera vremena i resursa potrebnih da se neka imovina zamjeni ili vrati u prethodno stanje. Zato se kao ekvivalentan termin može koristiti i „cijena zamjene“. poslužitelj baze podataka na kome se čuvaju informacije o kreditnim karticama klijenata, podrazumijevano je vrijedni, tj. ima veću cijenu zamjene nego radna stanica za ispitivanje programskih proizvoda.

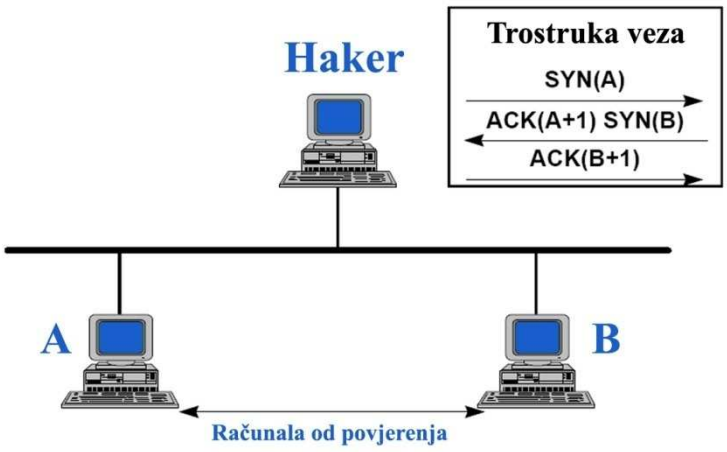
4.1.4. Metode napada

Računali sustav i računalna mreža mogu se napasti na mnogo načina. Najčešće korištene metode eksploatacije slabosti su DoS, lažiranje IP adresa i njuškanje.

1. **Odbijanje usluga** (Denial of Service, DoS). DoS izaziva prestanak rada servisa ili programa, čime se drugima onemogućava rad s tim servisima ili programima. DoS napad se najlakše izvršava na transportnom sloju – slanjem velikog broja SYN paketa (TCP CONNECTION REQUEST), a zaštita se postiže kontroliranjem broja SYN paketa u jedinici vremena.

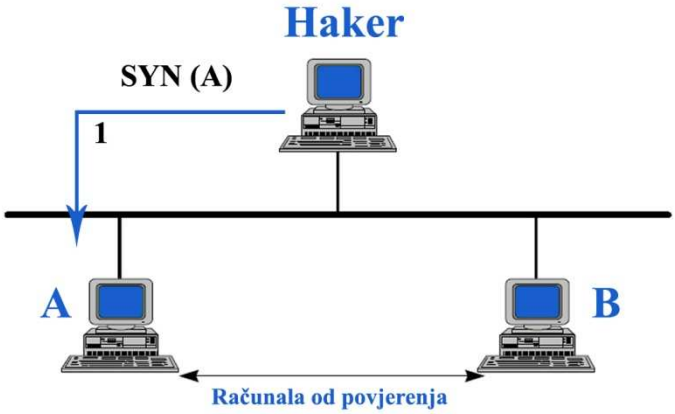
2. **Lažiranje IP adresa** (spoofing). Haker prati IP adrese u IP paketima i predstavlja se kao drugo računalo (slika 4.6 do 4.9). Kako DNS ne provjerava odakle dolaze informacije, haker može da izvrši napad lažiranjem tako što DNS servisu daje pogrešnu informaciju (ime računala od povjerenja). Najbolja zaštita od ovog napada je sprječavanje usmjeravanja paketa na adresama izvora (source address) za koje sigurno znamo da su neispravne – na primjer, odbacivanje paketa koji stižu na javno sučelje rutera, a imaju adresu lokalne mreže.
   Primjer lažiranja IP adresa u četiri koraka:

   a) Slika 4.6. prikazuje normalan računalni sustav i tri korisnika, dva korisnika koji se poznaju (A i B) i uljeza (Haker).



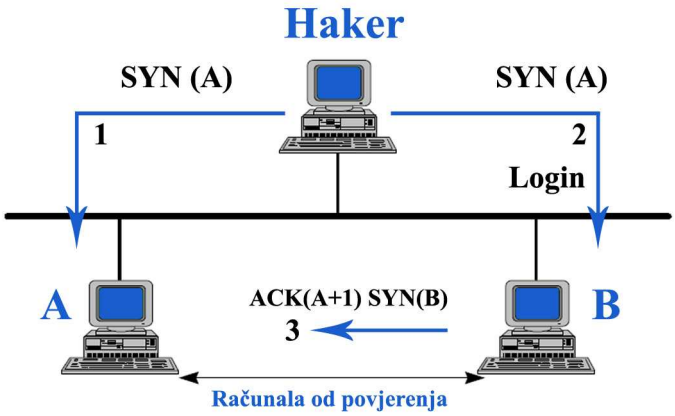
Slika 4.6. Lažiranje IP adresa – prvi korak

b) Haker prvo ometa i „zatrpava“ vezu s računalom A tako da mu šalje višestruke SYN pakete (Slika 4.7).



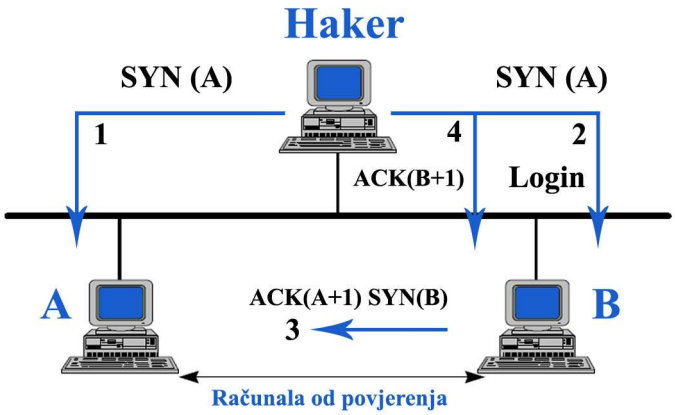
Slika 4.7. Lažiranje IP adresa – drugi korak

c) Haker tada šalje zahtjev za prijavu računalu B, a zahtjev izgleda da stiže s računala A. Računalo B odgovara računalu A, ali računalo A je još „zatrpano“ SYN paketima pa ne može da odgovori (Slika 4.8).



Slika 4.8. Lažiranje IP adresa – treći korak

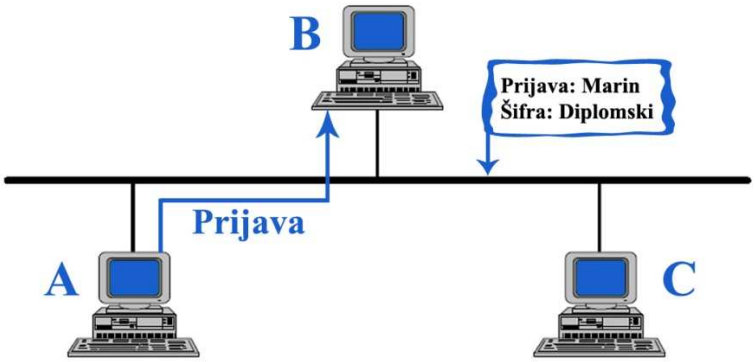
d) Haker tada „naslijepo“ završava prijavu kao da prima upit od računala B. Tada dodaje ++ na .rhosts datoteku i prekida vezu. Haker se od tog trenutka može spojiti na računalo B kad poželi (Slika 4.9).



Slika 4.9. Lažiranje IP adresa – četvrti korak

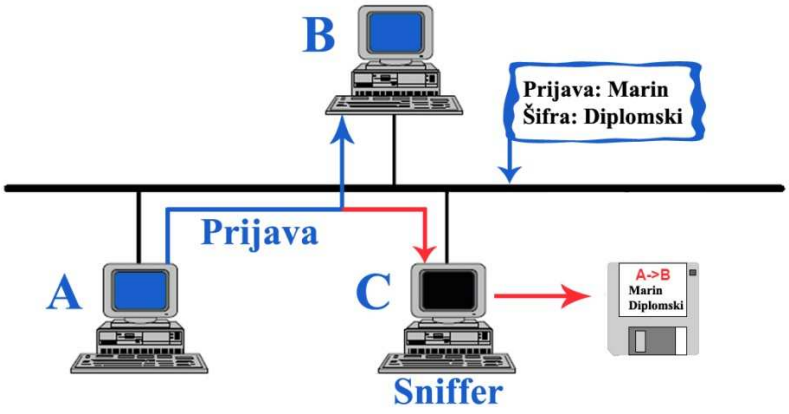
3. **Njuškanje** (sniffing). Haker/napadač specijalnim programima (više o njima u nastavku poglavlja) presreće TCP/IP pakete koji prolaze kroz određeno računalo i po potrebu pregleda njihov sadržaj (slika 4.10 i 4.11). Kao se kroz mrežu obično kreću nešifrirani podaci, program za njuškanje (sniffer) lako može doći do povjerljivih informacija.

   Primjer njuškanja u tri koraka:

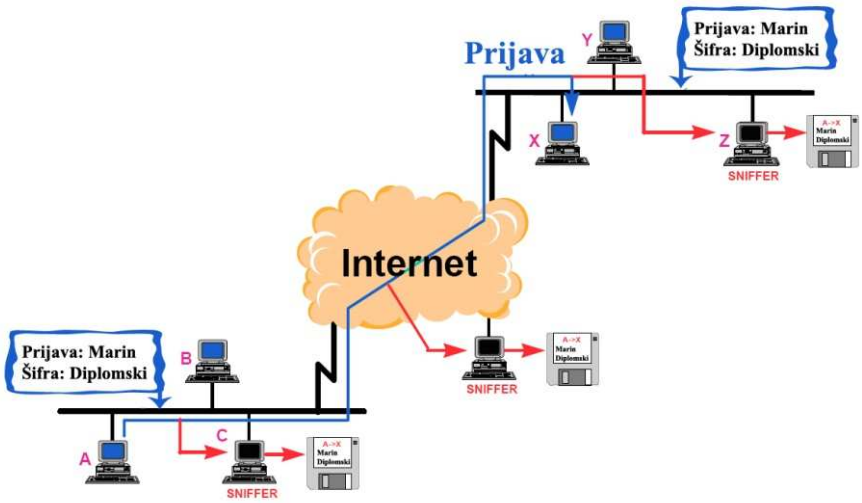


Slika 4.10. Njuškanje – prvi korak

   a) Sniffer stavlja sučelje u slučajni mod gdje prihvaća sve pakete smještene u pod-mreži. Prvih 128 bitova Telnet (mrežni protokol unutar IP grupe protokola koji se koristi na Internetu ili u lokalnim mrežama) konekcije je prijavljeno (logged) (slika 4.11).



Slika 4.11. Njuškanje – drugi korak



Slika 4.12. Snifferi na Internetu

Osim „njuškanja“ i ostalih metoda, program koji je napisao jedan korisnik (programer), a kojim se služe drugi korisnici, može predstavljati prijetnju i dovesti do uspješnog napada na sustav. Prijetnje ovakvog tipa zovu se programske prijetnje; u njih se ubrajaju trojanski konji, klopke i prekoračenje, tj. prelijevanje međuspremnika (buffer).

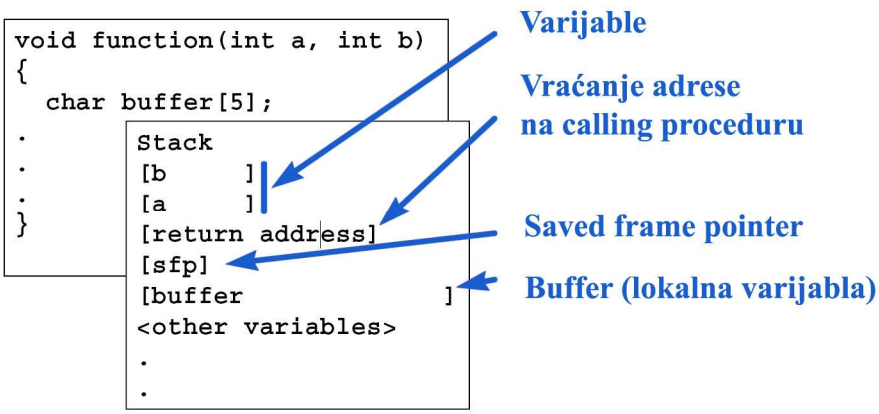
- **Trojanski konj** (trojan horse) ilegalan je segment koda, podmetnut u kod nekog programa, a cilj mu je da promijeni funkciju ili ponašanje originalnog programa. Na primjer, u editor teksta može biti podmetnut potprogram koji pretražuje otvorenu datoteku i – u slučaju da pronađe željenu sekvencu – kopira datoteku na mjesto dostupno programeru koji je napisao taj editor. Specijalna varijanta trojanskog konja je program koji oponaša proceduru prijavljivanja na sustav ili mrežu; haker/napadač koristi programe ovog tipa – a i neznanje korisnika – kako bi omogućio pristup računalnom sustavu ili mreži s tuđim akreditivima.
  Programi takvog tipa presreću legitimnu proceduru prijavljivanja na sustav i prikazuju odzivnik za prijavljivanje, identičan onom pravom, koji čeka da korisnik unese korisničko ime i lozinku. Korisnik unosu korisničko ime i lozinku koje trojanski konj smješta u neku datoteku dostupnu hakeru/napadaču, a potom obavještava korisnika da je pogrešno unio lozinku. Trojanki konj, zatim, predaje kontrolu pravoj proceduri prijavljivanja na sustav. Korisnik smatra da je unio pogrešnu lozinku, unosi je ponovo i prijavljuje se na sustav. Haker/napadač provjerava datoteku i prijavljuje se na sustav pod tuđim imenom. Korisnik najčešće nije i svjestan što se dogodilo.

- **Zamka** (trap door). Autor programa može slučajno ili namjerno ostaviti prazna mjesta u svom kodu (zamka) – uljez koji zna za ta mjesta može da podmetne svoj kod i time ostvari neku dobit. Osim toga, autor programa može izmijeniti dio koda tako da se izmjena ne može jednostavno primijetiti. Na primjer, zaokruživanje iznosa transakcije na neku cjelobrojnu vrijednost u određenim trenucima, predstavlja zamku ukoliko se ostatak zaokruživanja prenosi na račun programera. Zamke se teško otkrivaju, jer treba analizirati cjelokupan kod sumnjivog programa.

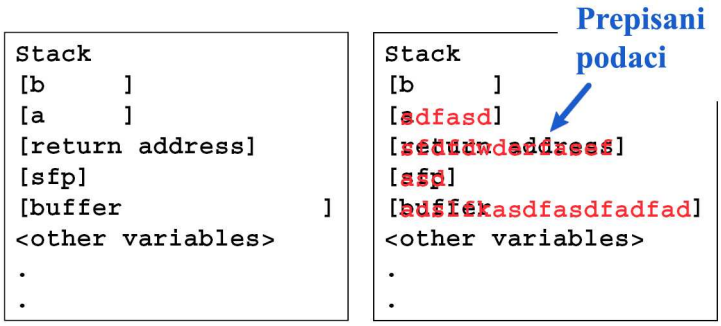
- **Prekoračenje**, tj. prelijevanje međuspremnika (buffer overrun, buffer overflow) na stogu ili dinamičkom dijelu memorije. Prekoračenje međuspremnika je najčešći napad s mreže pri pokušaju neovlaštenog pristupa sustavu. Ovlašteni korisnici također mogu odabrati ovu vrstu napada kako bi prevarili računalni sustav i ostvarili veća prava od

onih koja imaju. Po pravilu, haker/napadač koristi grešku u programu, tj. neodgovarajuću kontrolu razdvajanja stoga, podataka i koda. Tada haker/napadač šalje više ulaznih podataka nego što program očekuje, prepuni ulazno polje, argumente komandne linije ili ulazni međuspremnik – sve dok ne dođe do stoga. Potom preko važeće adrese u stogu upisuje adresu svog koda, puni dio niza znakova svojim kodom, koji – na primjer – izvršava neku komandu (kopira neke podatke ili pokreće komandni prevoditelj). U slučaju uspješnog napada, umjesto nedovoljno zaštićenog programa izvršit će se ilegalni kod, ubačen zahvaljujući prekoračenju međuspremnika.
Primjer rada prekoračenja:

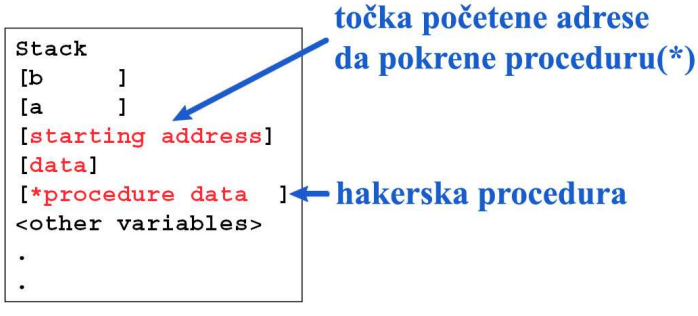
a) Kad se funkcija pozove, povratna adresa i lokalne varijable su gurnute na stog. Stog to zapiše u memoriju:



b) Ako se kopira previše informacija u međuspremnik bez provjeravanja limita informacije se prepišu preko povratne adrese:



c) Birajući koje podatke će se staviti u međuspremnik, mogu se staviti procedure u međuspremnik i njegove adrese u polje povratne adrese. Kad se funkcija vrati, pokreće tu proceduru.



Mnogi operacijski sustavi imaju mehanizam pomoću kojeg procesi mogu generirati druge procese. U takvom okruženju moguće je zlonamjerno korištenje datoteka i sustavnih resursa. Prijetnje ovog tipa nazivaju se sistemske prijetnje. Dvije metode kojima se one mogu postići jesu crvi i virusi.

- **Crvi** (worms) su samostalni zlonamjerni programi koji se šire s računala na računalo. Uobičajene metode prenošenja na žrtvu je upotreba elektronske pošte i Internet usluge. Crv istražuje ranjivost žrtve (na primjer, prekoračenja međuspremnika neke mrežne usluge) ili koristi metode prijevare i obmane, poznate kao društveni inženjering (social engineering), kako bi natjerao korisnika da ga pokrene. Crv degradira performanse računala, a ponekad nanosi i dodatnu štetu.
- Za razliku od crva, koji su samostalni programi, **virusi** su fragmenti koda koji se ubacuju u druge legitimne programe. Dakle, virus zahtijeva nosioca u vidu izvršne datoteke. Poslije pokretanja, virus obično inficira i druge izvršne datoteke na sustavu. Virusi su, najčešće, vrlo destruktivni i teško se uklanjaju ukoliko administrator zaraženog sustava nema zdrave kopije izvršnih datoteka. Zbog svega navedenog, virusi su jedan od glavnih problema pri korištenju osobnih računala.

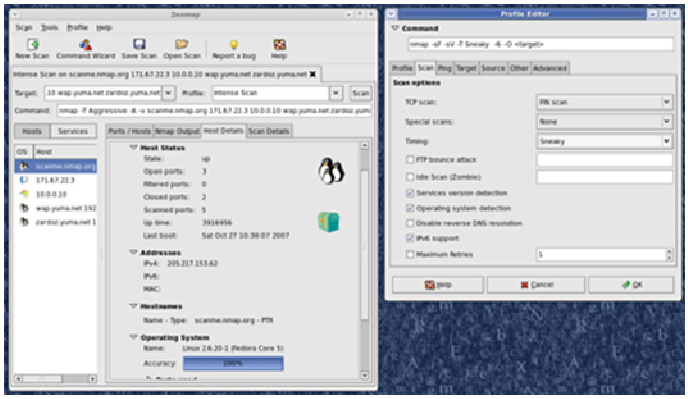
4.2 Hakerski alati

Hakeri koriste razne alate za napad na računalni sustav. Svaki od opisanih alata ima različite sposobnosti. Izrada i testiranje (dijelova) source kodova koji su korišteni u ovom poglavlju rađena je u Solaris okruženju i zasnovana na istraživanjima tvrtke Sun Microsystems (Solaris 2.6 OS - operacijski sustav tvrtke Sun Microsystems kompatibilan s POSIX-om. Zasnovan je na ranim inačicama Unix-a, BSD i AT&T). Sama teorija ovog teksta može se primijeniti u bilo kom okruženju i programskom jeziku, a primjeri i biblioteke koje su ovdje upotrijebljeni mogu se koristiti samo u Solaris okruženju. Opisani su najpopularniji alati za svaku od slijedećih kategorija:

4.2.1. Pretraživači pristupnih točaka (port scanners)

Pretraživači pristupnih točaka su vjerojatno najčešće upotrjebljivani alat za pretraživanje (scanning tool) na Internetu. Ovi alati pretražuju velike IP prostore i izvještavaju o sustavu koji je napadnut, priključnim točkama koje su slobodne i ostalim informacijama, kao što je tip operacijskog sustava. Najpopularniji pretraživač pristupnih točaka je Network Mapper (NMap).

Network Mapper (NMap) je open source alat za pretraživanje Interneta tj. sigurnosno istraživanje. Rađen je da ubrzano pretražuje velike mreže. Nmap koristi IP pakete na nove načine da predvidi koja se računala slobodna na mreži, koje priključne točke nude, koji operacijski sustav (i verziju OS-a) koriste, koji tip filtra paketa / vatrozida je u uporabi i mnoštvo drugih karakteristika. Nmap se može pokrenuti na većini tipova računala, postoji verzija za konzole i grafičke verzije programa. Nmap je besplatan program, dostupan s punim izvornim kodom (uz uvjete upotrebe).



Slika 4.13. Prikaz programa Network Mapper (NMap)

Nmap je izvrsni sigurnosni alat jer omogućava da predviđanje koje su priključne točke ponuđene od sustava. Pošto je Nmap napravljen da skenira veliku količinu IP adresa, može se koristiti za sve IP adrese korištene od organizacije, ili od svih IP adresa kabelskih modema koje koristi organizacija. Nakon korištenja Nmapa da se pronađu sva računala i identificira njihova djelatnost, može se pokrenuti Nessusov pretraživač (Nessus vulnerability scanner - više o njemu u idućem poglavlju) koji traži slabosti na računalnim sustavima.
Nmap podržava impresivan niz vrsta skeniranja koji dopuštaju sve od TCP SYN do Null pretrage (kada nema zastavica u zaglavlju paketa). Dodatne opcije uključuju OS fingerprinting (operacijski sustav udaljenog računala kojem je moguće utvrditi usporedbom njegova mrežnog prometa sa svojstvenim "mrežnim otiscima" operacijskih sustava iz prethodno stvorene baze podataka), paralelno skeniranje (više skeniranja odjednom) i decoy skeniranje (poznato kao skeniranje s mamcem).

Da bi se pokazale mogućnosti Nmap-a, treba pokrenuti skeniranje na računalu. Ispis skeniranja prikazuje djelatnosti na računalu. Nmapova sposobnost da identificira operacijski sustav je korisna jer može značajno skratiti vrijeme napada na određeno računalo.
Ispis Nmap-ovog skeniranja:

```
# /user/local/nmap -O ganassi
Starting nmap V. 2.53 (www.insecure.org/nmap/)
Interesting ports on ganassi (10.8.10.231):
(The 1515 ports scanned but not shown below are in state: closed)
Port        State            Service
7/tcp       open        echo
9/tcp       open        discard
13/tcp      open        daytime
19/tcp      open        chargen
21/tcp      open        ftp
23/tcp      open        telnet
25/tcp      open        smtp
37/tcp      open        time
79/tcp      open        finger
111/tcp     open        sunrpc
512/tcp     open        exec
513/tcp     open        login
514/tcp     open        shell
515/tcp     open        printer
540/tcp     open        uucp
1103/tcp    open        xaudio
```

```
4045/tcp    open        lockd
6112/tcp    open        dtspc
7100/tcp    open        font-service
32771/tcp   open        sometimes-rpc5
32772/tcp   open        sometimes-rpc7
32773/tcp   open        sometimes-rpc9
32774/tcp   open        sometimes-rpc11
32775/tcp   open        sometimes-rpc13
32776/tcp   open        sometimes-rpc15
32777/tcp   open        sometimes-rpc17
32778/tcp   open        sometimes-rpc19
Remote operating system guess: Solaris 2.6 -2.7
Uptime 0.054 days (since Wed Sep 10 09:41:59 2008)
Nmap run completed -- 1 IP address (1 host up) scanned in 37 seconds
```

4.2.2. Skeneri koji traže slabosti

Skeneri koji traže slabosti (vulnerability scanner) traži specifičnu slabu točku ili skenira računalni sustav tragajući za potencijalnom slabošću u sustavu. Postoje također besplatani programi. U radu je opisan trenutno najbolji skener, Nessus.
Nessus projekt cilja da omogući Internet zajednici slobodni, moćni i praktični sigurnosni skener za korištenje. Sigurnosni skener je program koji daljinski provjerava mrežu i predviđa loši mogu li napadači probiti u nju ili je zloupotrijebiti u nekom pogledu.
Za razliku od mnogih ostalih sigurnosnih skenera, Nessus ništa ne zaobilazi pri skeniranju.
Ako se pokrene mrežni poslužitelj na priključnoj 1234, program će ga otkriti i testirati njegovu sigurnost.
Neće pokrenuti sigurnosni test s obzirom na verziju broja na prijenosnim uslugama, ali će pokušati istražiti slabost sustava.
Ovaj alat omogućava administratorima i hakerima skeniranje računalnih sustava i procjenu slabosti u njima, ali je mnogo praktičniju u njegovoj GUI (vizualna verzija programa) verziji.

Da bi se pokazale mogućnosti Nessusa, kao i u slučaju Nmap-a, treba pokrenuti skeniranje na računalu.

Naredba u primjeru pokreće Nessus skeniranje računala upisanih u „targetfile“ datoteku, te rezultate pohranjuje u „outfile“datoteku.

```
# nessus  - T text localhost 1241 noorder targetfile outfile
```

Nessus tada pokreće sažetak rezultata skeniranja

```
Nessus Scan Report
------------------
SUMMARY
- Number of hosts which were alive during the test : 1
- Number of security holes found : 2
- Number of security warnings found : 15
- Number of security notes found : 1
TESTED HOSTS
192.168.0.90 (Security holes found)
```

Program nastavlja s detaljima za svako sigurnosno upozorenje. Ovo je odlomak iz izlazne liste detalja:

```
DETAILS
+ 192.168.0.90 :
. List of open ports :
o unknown (161/udp) (Security hole found)
o unknown (32779/udp) (Security warnings found)
o unknown (32775/tcp) (Security warnings found)
o unknown (32776/udp) (Security warnings found)
o unknown (32778/udp) (Security warnings found)
o unknown (32774/udp) (Security hole found)
o unknown (32777/udp) (Security warnings found)
o unknown (32780/udp) (Security warnings found)
o unknown (32775/udp) (Security warnings found)
o lockd (4045/udp) (Security warnings found)
o unknown (32781/udp) (Security hole found)
. Vulnerability found on port unknown (32774/udp) :
The sadmin RPC service is running.
There is a bug in Solaris versions of
this service that allow an intruder to
execute arbitrary commands on your system.
Solution : disable this service
Risk factor : High
```

Pomoću ove izlazne liste hakeri dobivaju mogućnost upada u računalni sustav.
U dodatku za ostale slabosti u sustavu, sljedeća, DoS slabost pojavljuje se na ispisu:

```
DETAILS
. List of open ports :
o general/tcp (Security hole found)
. Vulnerability found on port general/tcp :
It was possible
to make the remote server crash
using the 'teardrop' attack.
A cracker may use this attack to
shut down this server, thus
preventing your network from
working properly.
Solution : contact your operating
system vendor for a patch.
Risk factor : High
CVE : CAN-1999-0015
```

Na osnovu rezultata otkriva dvije „rupe“ u sigurnosti mreže i petnaest upozorenja na Solaris 2.6 sustavu.

4.2.3. Alati za dobivanje administratorskih ovlasti na sustavu (rootkit)

Termin „rootkit“ opisuje grupu ispisa i izvršnih paketa zajedno, koji dozvoljavaju hakerima da sakriju bilo kakav dokaz ili trag da su uspjeli uči u sustav. Ovo su neke od radnji što takvi alati obavljaju:

- modificiraju sustav dnevničkih datoteka da bi izbrisali dokaze o hakerskim aktivnostima

- modificiraju alate sustava da bi se teže otkrile hakerske radnje
- kreiraju skrivene ulazne točke sustava
- koriste sustav kao početnu točku napada na ostale umrežene sustave

Za demonstraciju programa, Alex Noordergraaf iz Sun Microsystems istraživačkog odijela upotrijebio je „HoneyNet rootkit" projekt na Solaris 2.6 sustavu.
Alat ima nekoliko vrsta programa koji spadaju u sljedeće kategorije:

- program za praćenje prometa na mreži (network sniffers)
- program za brisanje zapisa u dnevničkim datotekama (log file cleanup)
- Internet relay chat (IRC) proxy

Zajedno s alatom dobije se i instalacijska skripta za automatsku instalaciju alata, postavljanje programskih dopuštenja i brisanje dokaza iz dnevničkih datoteka.

Instalacija alata na računalni sustav:

```
ganassi# ./setup.sh
hax0r w1th gforce
Ok This thing is complete :-)
cp: cannot access l0gin
cp: cannot create /korisnik/local/bin/find: No such file or
directory
mv: cannot access /etc/.ts
mv: cannot access /etc/.tp
- WTMP:
/var/adm/wtmp is Thu Sep 16 13:21:36 2008
/usr/adm/wtmp cannot open
/etc/wtmp is Thu Sep 16 13:21:36 2008
/var/log/wtmp cannot open
WTMP = /var/adm/wtmp
No user re found in /var/adm/wtmp
[...]
./setup.sh: ./zap: not found
./secure.sh: rpc.ttdb=: not found
#: securing.
#: 1) changing modes on local files.
#: will add more local security later.
#: 2) remote crap like rpc.status , nlockmgr etc..
./secure.sh: usage: kill [ [ -sig ] id ... | -l ]
./secure.sh: usage: kill [ [ -sig ] id ... | -l ]
#: 3) killed statd , rpcbind , nlockmgr
#: 4) removing them so they ever start again!
5) secured.
193 ? 0:00 inetd
cp: cannot access /dev/.. /sun/bot2
kill these processes@!#!@#!
cp: cannot access lpq
./setup.sh: /dev/ttyt/idrun: cannot execute
Irc Proxy v2.6.4 GNU project (C) 1998-99
Coded by James Seter :bugs-> (Pharos@refract.com) or IRC pharos
on efnet
--Using conf file ./sys222.conf
--Configuration:
Daemon port......:9879
Maxusers.........:0
Default conn port:6667
Pid File.........:./pid.sys222
Vhost Default....:-SYSTEM DEFAULTProcess
```

```
Id.......:759
Exit ./sys222{7} :Successfully went into the background.
```

Instalacijska skripta nije elegantan ili precizna, ali obavlja posao. Zamijenila je sljedeće sistemske datoteke:

```
/bin/ls
/usr/bin/ls
/bin/ps
/bin/netstat
/usr/bin/netstat
/usr/sbin/rpcbind
```

Sada haker ima izvorni ulaz u sustav na kojemu je:

- teško za administratora detektirati uljeza/hakera s standardnim Solaris 2.6 komandama, kao što su ls, find ili ps, jer su binarne brojke zamijenjene s trojanom koji je skriven na sigurnom mjestu u sustavu
- hakeru/napadaču vrlo lako dobiti ulaz u sustav u više navrata jer novi binarni sustav (pod trojanom) za „login“ i „rpcbind“ dopušta hakeru da dobije ulaz i daljinski izvrši naredbe na sustavu.

Program instalira četiri aplikacije za praćenje mrežnog prometa na napadnuti sustav: le, sniff, sniff – 10mb i sniff – 100mb.
Samo „sniff – 100mb“ se može koristiti na „ganassi-u“ (sučelju na kojom su Sun Microsystems radili istraživanja); ostali sniffer-i su kodirani za specijalna sučelja. „Sniff – 100mb“ izvršna datoteka se postavlja na hme0 sučelje na „ganassi“ sustavu. Kad se datoteka pokrene formira se lijepo oblikovan sažetak mrežnih aktivnosti u sustavu.

```
ganassi # ./sniff-100mb
Using logical device /dev/hme [/dev/hme]
Output to stdout.
Log started at => Thu Sep 16 15:31:10 [pid 856]
-- TCP/IP LOG -- TM: Thu Sep 16 15:31:19 --
PATH: 10.8.10.200(34398) => ganassi (telnet)
STAT: Thu Sep 16 15:31:48, 111 pkts, 128 bytes [DATA LIMIT]
DATA: (255)(253)^C(255)(251)^X(255)(251)^_(255)(251)
(255)(251)!(255)(251)"(255)(251)’(255)(253)^E(255)(250)^_
: P
: ^X(255)(240)(255)(252)#(255)(252)$(255)(250)^X
: DTTERM(255)(240)(255)(250)’
: (255)(240)(255)(253)^A(255)(252)^Anoorder
: t00lk1t
: ls
: who
: cd /var/tmp
: ls -al
```

Izlaz uključuje korisnički ID i zaporku za ulazak u sustav. Alat uključuje program za brisanje zapisa u dnevničkim datotekama i IRC (Internet Relay Chat – komunikacija među korisnicima na mreži) proxy.
Više grupa dnevničkim datoteka premješteno je preko sljedećih alata: utmp, utmpx, wtmp, wtmpx, lastlog. Program koji premješta dnevničke datoteke zove se „zap“ (traži i premješta datoteke u određeni direktorij).

IRC proxy u programu uključuje bot (program). Proxy preskače IRC poruke kroz privatni IRC kanal. Bot omogućava da je kanal otvoren i da odgovara na određene naredbe.

4.2.4. Alati za „njuškanje“ (sniffer)

„Njuškalo“ (sniffer) je detaljnije opisan u potpoglavlju 4.1.4. Solarisov operacijski sustav posjeduje alat koji se zove „snoop“, a služi za hvatanje i prikazivanje svog mrežnog prometa kojeg trenutno vidi mrežno sučelje u računalnom sustavu. Iako je relativno primitivan, ovaj alat može učinkovito prikupiti ID adrese i zaporke na mreži. Mnogi popularni protokoli koji se danas koriste kao Telnet (mrežni protokol unutar IP grupe protokola koji se koristi na Internetu ili u lokalnim mrežama), FTP(File Transfer Protocol - protokol za prijenos datoteka, uobičajen je naziv za najstariju i vrlo važnu uslugu na Internetu koja služi za prijenos podataka između računala), IMAP (The Internet Message Access Protocol ili IMAP je jedan od dva najrasprostranjenija Internet standard protokola za e-mail usluge, drugi je POP-3) i POP-3 ne šifriraju svoju korisničku ovjeru i identifikacijsku informaciju.
Jednom kad uđe u sustav, haker instalira program za praćenje prometa na mreži da dobije dodatni korisnički ID i informacije o zaporkama, pomoću kojih dolazi do informacije kako je mreža građena i u koje svrhe se koristi.
U idućem primjeru Sun Microsystems-a korišten je snoop alat, da se pokaže sposobnost sniffer-a da „izvuče“ korisnički ID i zaporku od Telnet i IMAP razdjele podataka. Skupljanje informacija za primjere je potrajalo samo par sekundi.
Sljedeći primjer su slabosti Telnet-a:

```
# snoop -d qfe0 port telnet ganassi
ganassi -> nomex-lab TELNET R port=32835
\377\373\1\377\375\1login:
nomex-lab -> ganassi TELNET C port=32835 r
ganassi -> nomex-lab TELNET R port=32835 r
nomex-lab -> ganassi TELNET C port=32835 o
ganassi -> nomex-lab TELNET R port=32835 o
nomex-lab -> ganassi TELNET C port=32835
nomex-lab -> ganassi TELNET C port=32835 o
ganassi -> nomex-lab TELNET R port=32835 o
nomex-lab -> ganassi TELNET C port=32835
nomex-lab -> ganassi TELNET C port=32835 t
ganassi -> nomex-lab TELNET R port=32835 t
nomex-lab -> ganassi TELNET C port=32835
ganassi -> nomex-lab TELNET R port=32835 Password:
nomex-lab -> ganassi TELNET C port=32835
nomex-lab -> ganassi TELNET C port=32835 t
ganassi -> nomex-lab TELNET R port=32835
nomex-lab -> ganassi TELNET C port=32835 0
ganassi -> nomex-lab TELNET R port=32835
nomex-lab -> ganassi TELNET C port=32835 0
ganassi -> nomex-lab TELNET R port=32835
nomex-lab -> ganassi TELNET C port=32835 l
ganassi -> nomex-lab TELNET R port=32835
nomex-lab -> ganassi TELNET C port=32835 k
ganassi -> nomex-lab TELNET R port=32835
nomex-lab -> ganassi TELNET C port=32835 1
ganassi -> nomex-lab TELNET R port=32835
nomex-lab -> ganassi TELNET C port=32835 t
nomex-lab -> ganassi TELNET C port=32835
ganassi -> nomex-lab TELNET R port=32835 Last login: Thu Mar
nomex-lab -> ganassi TELNET C port=32835
ganassi -> nomex-lab TELNET R port=32835 #
```

Sljedeći primjer su slabosti IMAP-a:

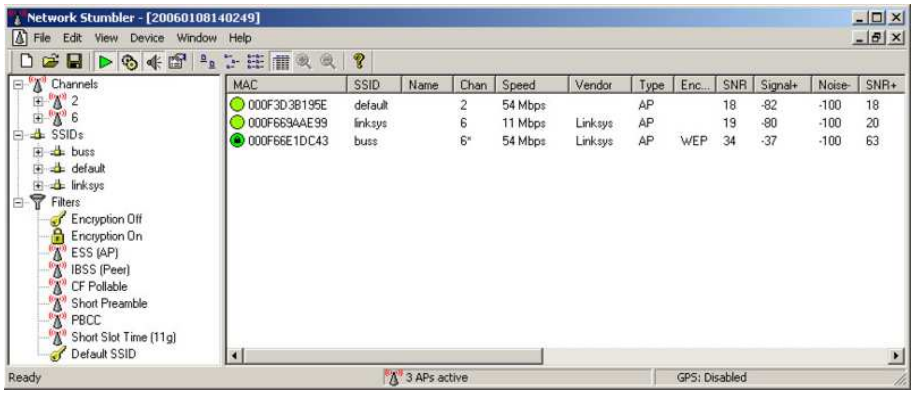
```
# snoop -d qfe0 port imap2 ganassi
jordan -> ganassi IMAP C port=46600
ganassi -> jordan IMAP R port=46600
jordan -> ganassi IMAP C port=46600
ganassi -> jordan IMAP R port=46600 * OK ganassi SIMS (tm)
2.0p12
IMAP
jordan -> ganassi IMAP C port=46600
jordan -> ganassi IMAP C port=46600 1 capability\r\n
ganassi -> jordan IMAP R port=46600
ganassi -> jordan IMAP R port=46600 * CAPABILITY IMAP4 STATUS
SCAN
IMAP4
jordan -> ganassi IMAP C port=46600
jordan -> ganassi IMAP C port=46600 2 login "hacked"
"t00lk1t”\r\n
ganassi -> jordan IMAP R port=46600 2 OK LOGIN completed
```

Korištenje snoop alata je vrlo jednostavno. Ako radi vrlo dugo prikuplja veliku količinu podataka, ali može ga se primijetiti. Idealna solucija za napadača/hakera je automatski alat koji samo sprema korisničke ID-ove i informacije o zaporkama za specifičnu listu protokola. Nekoliko alata je dostupno da obave ovaj zadatak: relativno jednostavan sniffit (to je paket sniffer za TCP/UDP/ICMP paket) i mnogo više fleksibilniji i veći dsniff (alat koji omogućuje automatski mehanizam za napadnute mreže s prospajanjem paketa). Bilo koja od ovih alata može da radi tjednima ili mjesecima, te može skupiti stotine, možda i tisuće zaporki.

4.2.5. Ostali alati

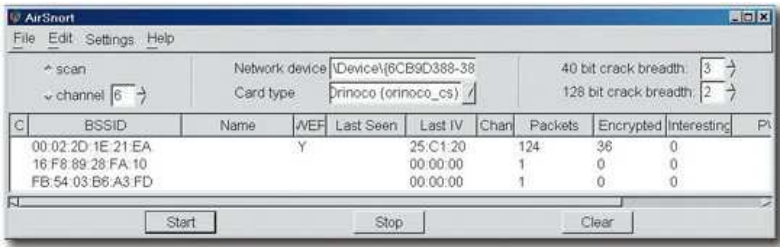
Haker koji je zainteresiran za veće znanje o računalnoj sigurnosti i istraživanje slabosti treba dobar set osnovnih hakerskih alata. Na njihovu sreću, Internet je pun besplatnih alata, a ovo su najpopularniji od njih:

- Jedan od popularnih alata, neophodan za svakog hakera je Network Stumbler poznat još kao **NetStumbler** (slika 4.14). To je program koji radi u Windows okruženju, hvata bežične mreže i bežične signale koristeći 802.11b, 802.11a i 802.11g WLAN standarde. Također ima mogućnost hvatanja šumova i smetnji na signalima.



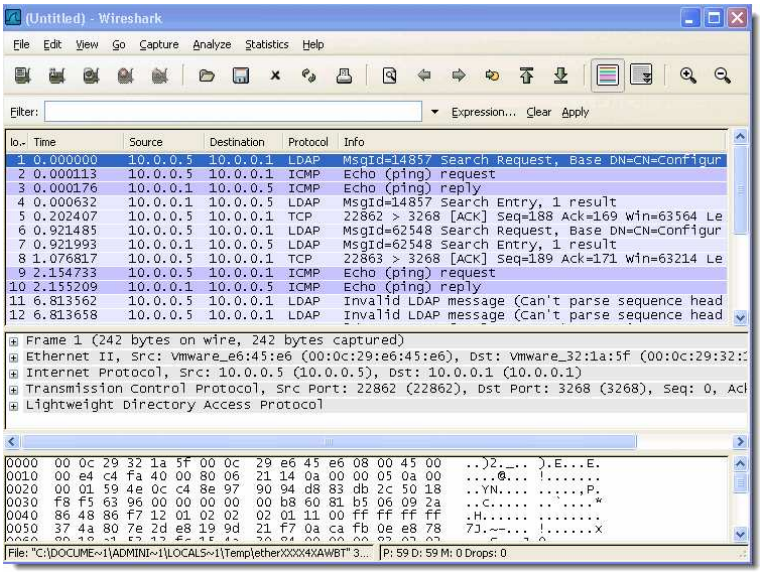
Slika 4.14. Prikaz programa NetSumbler

- Kad se pomoću programa kao što je NetSumbler nađe bežična mreža, idući korak je pokušati se spojiti na nju. Ako mreža koristi nikakav tip provjere autentičnosti i šifrirane sigurnosti, može se upotrijebiti program **Airsnort** (slika 4.15). Program je vrlo lagan za korištenje i služi za „njuškanje“ (sniff) i „razbijanje“ (crack) WEP ključa (Wired Equivalent Privacy je protokol ugrađen u 802.11 standard (taj standard definira arhitekturu bežičnih mreža), koji služi za zaštitu podataka u podatkovnom sloju). Iako mnogi ljudi izbjegavaju koristiti WEP, bolje je nego ne koristiti nikakvu zaštitu. Ponekad pomoću ovog alata treba poslati mnogo uhvaćenih paketa da bi se probio WEP ključ.



Slika 4.15. Prikaz programa AirSnort

- Pokušali se direktno spojiti na bežičnu mrežu ili ne, ako je ta mreža u dometu, tamo su i podaci i datoteke koje „lete zrakom“ u svakom trenutku. Za skupljanje tih podataka potreban je program **Wireshark** (nekad poznat pod imenom Ethereal) (slika 4.16). Ovaj alat može skenirati bežične i Ethernet podatke, a ima i filtar za odvajanje podataka.



Slika 4.16. Prikaz programa Wireshark

Od ostalih hakerskih alata ističu se: **Ettercap** („čovjek u sredini“ napad na LAN), **Kismet** (detektor bežičnih mreža), **Cain & Abel** (alat za obnavljanje zaporki), **NetCat** (Unix alat, čita i ispisuje podatke koristeći TCP protokol), **PsTools** (skup alata za daljinsko upravljane drugim sustavom) kao mnogi drugi alati, od kojih je većina besplatna i lako dostupna, pa se ne treba čuditi rastućem broju hakera.

5. ZAŠTITA OD HAKERA

Potreba za zaštitom od hakera veća je nego ikad prije. Hakiranje je postalo jedna od najdražih aktivnosti novih generacija. U današnje vrijeme ostaviti računalo bez ikakve zaštite je kao da ostavite auto na ulici s otvorenim vratima, s ključem u njemu i upaljenog motora.

5.1. Pojam sigurnosti

Da bi se što bolje zaštitili od hakera treba razumjeti pojam sigurnosti. Sigurnost je proces održavanja prihvatljivog nivoa rizika. Sigurnost je proces, a ne završno stanje ili konačan proizvod. Organizacija ili institucija ne može se smatrati „sigurnom“ ni u jednom trenutku poslije izvršene posljednje provjere usklađenosti s vlastitim sigurnosnim pravilima. Često se čuje kako velike svjetske kompanije, uključujući i tržišne vođe, reklamiraju u raznim medijima svoje proizvode kao svemoguća rješenja. Oni koji vjeruju da sigurnost može biti jednom „dostignuta“ i da će poslije toga sustav ostati siguran, voljni su da kupe proizvode i usluge koji se na taj način reklamiraju. Treba vrlo oprezno razmotriti tako oglašenu ponudu.
Dakle, kada se govori o sigurnosti i zaštiti informacijskih sistema i mreža, nekoliko principa danas vrijede kao osnovne smjernice:

- sigurnost je proces. Sigurnost nije proizvod, usluga ili procedura, već skup koji ih sadrži – uz još ,mnogo elemenata i mjera koje se stalno sprovode
- ne postoji apsolutna sigurnost
- uz različite metode zaštite, treba imati u vidu i ljudski faktor, sa svim slabostima

5.1.1 Sigurnosne metode

Za sigurnosne metode također postoji nekoliko pristupa i podjela. S vremenom ove klasifikacije evoluiraju i mijenjaju se kako se razvijaju tehnologije i primjene računalnih sustava i mreža. Prema nekim autorima, postoje četiri grupe metode zaštite:

- kriptografske metode
- programske metode
- organizacijske metode
- fizičke metode

Mnogi autori ovu podjelu smatraju starom i sve češće se koristi shema zasnovana na deset domena sigurnosti koje je definirala organizacija (ISC)2. Neki autori, također, definiraju takozvane metode obrane, klasificirajući ih na slijedeći način:

- šifriranje
- programska kontrola pristupa (pristupna ograničenja u bazi podataka ili operacijskom sustavu
- kontrola pristupa sklopovlja (pametne kartice – smartcards, biometrijske metode)
- zaštitne police, tj. pravila zaštite (poput inzistiranja da se često mijenjaju šifre)
- fizička kontrola pristupa

Kao što je već rečeno, kontrola pristupa je sigurnosna usluga kojom se dozvoljava objektu provjerenog identiteta da koristi određene usluge sustava, tj. određuje tko ima pravo da pristupi resursima i na kakav način. Za kontrolu pristupa u općem smislu, najčešće važi sljedeće:

- kontrola pristupa je obavezna i neizostavna
- svi korisnici moraju biti ovlašteni da bi mogli da pristupe nekom objektu

- svi korisnici mogu prava nad objektima koji njima pripadaju dodijeliti drugim korisnicima
- korisnici sustava ne smiju neovlašteno upotrebljavati tuđa prava niti mijenjati tuđa prava nad entitetima koji im ne pripadaju.

Aspekti zaštite se vrlo često definiraju u odnosu na položaj mehanizma zaštite u računalnom i informacijskom sustavu ili računalnoj mreži. Pod ovim se često podrazumijevaju sljedeći nivoi:

- Zaštita na nivou aplikacije: Zaštita na nivou aplikacije može obuhvaćati, na primjer, sljedeće elemente: programsku zaštitu aplikacije (recimo, zaštitu od prekoračenja međuspremnika), izoliranje bitnih aplikacija na namjenskim poslužiteljima i umreženim računalima, primjenu specifičnih protokola (za primjer, kriptografski zaštićenog protokola SSH umjesto nezaštićenog protokola Telnet).

- Zaštita na nivou operacijskog sustava. Kad se govori o zaštiti na nivou operacijskog sustava, ulazi se u veoma složeno i obimno područje koje na neki način dotiče sve slojeve operacijskog sustava. Zaštita na nivou operacijskog sustava obuhvaća i vezu operacijskog sustava – aplikacije, kao i odnos prema mrežnoj arhitekturi tj. vezama s drugim sustavima. Prema nekim preporukama minimalna zaštita obuhvaća: blokiranje nepotrebnih usluga (finger, FTP, telnet), omogućavanjem sveobuhvatne i obavezne kontrole pristupa na nivou korisnika, omogućavanje integriteta programa koji čini operacijski sustav (većina sigurnosnih napada usmjerena je na operacijske sustave bez primljenih zakrpa, pa je zato potrebno redovito ažurirati sve elemente sustava novim „zakrpama“).

- Zaštita na nivou mrežne infrastrukture. Kada se govori o zaštiti na nivou mrežne infrastrukture, obično se misli na sljedeće osnovne elemente: primjenu mrežnih barijera, tj. vatrozida (firewall) (slika 5.3), blokiranje nepotrebnih priključnih točaka (port), šifriranje putanje, izoliranje putanje pomoću usmjernika i komutatora ili pomoću posebne infrastrukture.

Slika 5.1. Vatrozid u windows XP okruženju

- Proceduralna i operacijska zaštita. Ovaj nivo zaštite obuhvaća sljedeće elemente: definiranje i provođenje pravila zaštite, politike i procedure, detekciju napada, aktivno djelovanje, tj. provođenje preventivnih mjera u cilju zaštite i smanjivanja ranjivosti

sustava, upravljane konfiguracijom sustava, podizanje svijesti o sigurnosnim problemima i obrazovanje korisnika.

Posebne segmente u metodama zaštite čine zaštita o elementarnih nepogoda (požara, poplava, zemljotresa) i zaštita od terorizma ili drugih destruktivnih i rušilačkih akcija. Treba voditi računa i o pravnim, etičkim, društvenim i psihološkim aspektima.

5.1.2 Sigurnosni alati

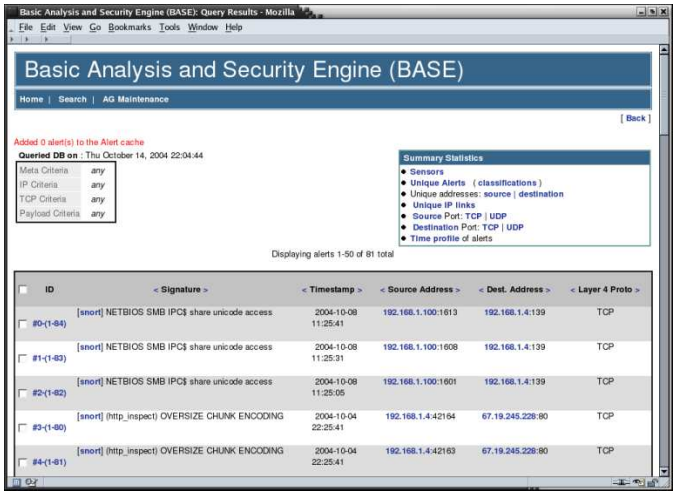
Paralelno s hakerskim alatima što služe za ugrožavanje sigurnosti računala i mreže, postoje i alati za sigurnost istih. Većina tih alata nije besplatna, za razliku od hakerskih alata, što je gledajući s etičke strane veoma interesantno.

- **Antivirusni programi** su programi koji skeniraju računalo i provjeravaju dali je računalni sustav „zaražen“ s virusom ili crvom. Najpoznatiji antivirusni programi su Norton (slika 5.2.), Mcafee, AVG i Kaspersky. Antivirus pretražuje sustav na temelju baze virusa. Naime, kada se pojavi novi virus, stručnjaci prouče neke njegove jedinstvene karakteristike i na osnovu njih naprave virusni potpis (signature). Radi toga je veoma važno da se što češće „osvježava“ (up-to-date) antivirusni program s novim zakrpama. Zbog sve učestalijeg broja virusa koji se šalju elektroničnom poštom potrebno je postaviti antivirus na MTA poslužitelj (Mail Transfer Agent, poznat kao mail poslužitelj).

Slika 5.2. Norton AntiVirus

- **Sustav za detekciju napada** (IDS)
  IDS (Intrusion detection system) je program ili sklopovlje dizajnirano da otkrije neželjene pokušaje ulaska, manipulacije i oštećenja računalnog sustava, većinom putem Interneta. Postoje dvije vrste IDS-a, korisnički (host) i mrežno (network) bazirani IDS.
  Mrežni IDS (to je u biti sniffer) traži određene potpise (signature), ili neke statističke anomalije, te kad ih nađe, poduzme neku akciju. Detekcija potpisima slična je detekciji virusa kod antivirusnog programa. Traži se poznati potpis (usporedba s podacima iz baze) u mrežnom prometu. Kod detektiranja statističkim anomalijama uspoređuje se "trenutno stanje" (korištenje procesora, aktivnost diska, broj korisnika...) s nekim "idealnim stanjem".

Korisnički IDS se instalira na poslužitelju i gleda da li su sistemski pozivi dozvoljeni, da li su sistemske datoteke nepromijenjene, da li netko pokušava nekakvo prekoračenje (buffer overflow) ili slično. Kod korisničkog IDS-a gledaju se prvenstveno promjene na poslužitelju, tj. on proučava poslužiteljeve zapise, dok mrežni IDS pregledava jedan mrežni segment kao izvor za svoje informacije.
Akcije koje IDS poduzima nakon što otkrije uljeza mogu biti raznolike i ovise o prioritetima pojedinih upada. Mogu biti vrlo jednostavne od slanja mail-a administratoru, običnog dokumentiranja upada, pa sve do promjene postavki vatrozida te prekida veze.
Bitna razlika između vatrozida i IDS-a je u tome sto IDS prepoznaje napad. Na primjer zamislimo da je kuća poslužitelj. Oko nje postoji zid koji brani uljezima ulazak. Taj zid predstavlja vatrozid. Ako netko pokušava preskočiti zid motkom, ili prokopati tunel ispred njega, on to može učiniti tako da mi nećemo ni saznati. Tu uskače IDS, koji može vidjeti onog koji pokušava ući u sustav.
Idealno bi bilo postaviti dva IDS-a i vatrozid, jedan IDS ispred, a jedan iza vatrozida.
Kao primjer alat sustava za detekciju napada izdvaja se program Snort (slika 5.3.).



Slika 5.3. Prikaz programa Snort

Snort je mrežni IDS. To je „otvoreni kod” (open source) program, i postoji za više različitih operacijskih sustava, čak i za Windowse. U zadnje vrijeme vrlo je popularan među korisnicima Linux sustava.
Tri su osnovna načina rada ovog alata: „njuškanje“ (sniffer), zapisnik paketa (packet logger) i mrežni IDS. U sniffer modu alat jednostavno čita pakete s mreže i prikazuje ih na ekranu, zapisnik paketa čini isto, samo sprema podatke na disk, dok je mrežni IDS najbolji način rada za ovaj alat, najkompleksniji i s najviše mogućnosti za konfiguriranje.

- Ostali popularni programi za zaštitu računala su **Ad-aware** (pronalazi i briše oglase i kolačiće (cookies)), **SpyBot** (skenira računalo i traži spyware i ostale opasnosti za računalo), **CW Shredder** (sprječava da se izmjeni početna stranica (cool web site problem) u pretraživaču), **PopUp Blocker** (blokira „skočne“ (pop-up) prozore) i **MailWasher** (filtrira dolaznu elektroničnu poštu).

5.1.3 Zaštita sigurnosti: primjeri

U ovom dijelu navedeni su neki praktični primjeri i situacije u kojima se koriste različite metode i tehnike zaštite od hakera i ostalih prijetnji računala.

- Formiranje demilitizirane zone (DMZ). DMZ je neutralna zona između privatne i javne mreže, formirana pomoću računalnog sklopovlja i programa. Koristi se kombinacija usmjernika, vatrozida, posredničkih poslužitelja (proxy servers) i programskih sustava za detekciju i sprječavanje napada.
- Ispitivanje programa. Prije instaliranje bilo kojeg programa u bilo kojem proizvodnom ili operacijskom okruženju, potrebno je detaljno ispitati taj program u razvojnom okruženju. U ispitivanje programa spada i instaliranje, na primjer Web poslužitelja, FTP poslužitelja, poslužitelja za elektroničku poštu i sustava za upravljanje bazama podataka (obavezno uključiti sve potrebne zakrpe, koje se vrlo često odnose na sigurnost rada).
- Zaštita vitalnih kompanijskih podataka. Posebno osjetljive datoteke (podaci o klijentima, podaci o uplatama i isplatama, podaci o plaćama, podaci o dokumentima) čuvaju se u bazama podataka koje imaju ograničenu mogućnost povezivanja s vanjskim mrežama. Čuvanje pojedinih vitalnih podataka na odvojenom mjestu ili mediju, s ograničenim pristupom, izuzetno je važno, na primjer, pri skladištenju podataka o kreditnim karticama.
- FTP i Telnet. Blokirati FTP i Telnet kako bi se spriječilo da hakeri/neovlašteni korisnici preko ovih usluga pristupe štićenom sustavu. Ove usluge se lako konfiguriraju da budu dostupne onda kada su stvarno potrebni.
- Korištenje zaporki. Obavezno upotrebljavati korisničke zaporke i često ih mijenjati. Ne koristiti „očigledne“ zaporke kao što su imena članova porodice, datumi rođenja, telefonski brojevi, imena kućnih ljubimaca i slično. Paradoks: korištenje složenih zaporki može ponekad u praksi povećati opasnost, jer ih treba zapisivati, a to povećava sigurnosni rizik.
- Ažuriranje programa. Pravovremeno ažurirati verzije programa. Starije verzije programa često sadrže sigurnosne propuste koje napadači mogu da iskoriste. Postoje timovi koji prate sigurnosne probleme i izdaju odgovarajuće savjetodavne izvještaje (advisory reports) o primijećenim problemima.
- Politika zaštite informacija. Organizacija mora da procijeni rizike. Potrebno je da razvije jasnu politiku pristupanja informacijama i njihove zaštite.

Ljudi su, uglavnom, najosjetljivije mjesto u svakoj sigurnosnoj shemi. Ljudski faktor (na primjer, zlonamjeran ili nepažljiv radnik, ili radnik koji nije svjestan važnosti zaštite informacija) može da poništi i najbolju zaštitu.

6. ZAKLJUČAK

Cilj ovog diplomskog rada nije bio da čitatelja navede da se opredijeli za neko mišljenje o hakerima. Skupljao sam tekstove i informacije iz različitih izvora koje su imali drugačije stavove i razmišljanja o svijetu hakera, s ciljem da ih obuhvatno predstavim kroz njihov rad, a na samom čitatelju se ostavlja mogućnost da na osnovu svojih zapažanja formira mišljenje.

U radu su dane definicije same riječi haker kao i pregled povijesti hakera. U trećem poglavlju opisana je kultura hakera, njihovi načini komunikacije i profil. Četvrto poglavlje opisuje najčešće hakerske napade i alate, a peto daje osnove zaštite od napada hakera.

Moje subjektivno mišljenje je da haker, bio dobar ili loš, produktivan ili destruktivan, od samog početka ubrzano gura tehnologiju ka napretku. Nekada na pozitivan način, pisanjem besplatnih programa, eksperimentirajući s mogućnostima računala ne ugrožavajući nikoga, a nekad se taj napredak ostvaruje i kroz destruktivne aktivnosti, kao što je „obaranje“ sustava, mreža…navodeći one koji su zaduženi za njihov nastanak i sigurnost da rade još napornije.

„Cilj opravdava sredstvo“ rekao je Machiavelli. Ako je pri tom cilj napredovanje tehnologije, hakeri su najbolje sredstvo za ostvarivanje tog cilja. Oni se svakodnevno nadmeću i igraju s tehnologijom, pomičući joj granice iz dana u dan.

Unatoč svemu, tijekom pisanja ovog diplomskog rada i posjećivanja hakerskih stranica pokupio sam par trojana (Trojan horse) što mi je znatno smanjilo brzinu računala, a i natjeralo me da osim pisanja diplomskog poradim i na sigurnosti svog računala, pa sam i ja u osobnoj dvojbi: haker, moderni ratnik ili običan kriminalac?

Za kraj izdvajam interesantnu rečenicu iz hakerskog miljea: Kad si dobar haker, svi te znaju. Kad si najbolji haker, nitko te ne zna.

7. LITERATURA

1. Alex Noordergraaf: „How Hackers Do It: Tricks, Tools, and Techniques, Sun Blueprints, Santa Clara, 2002.
2. Eric Cole: „Hackers Beware: The Ultimate Guide to Network Security (NRG - Voices)“, Sams, 2001.
3. Kevin D. Mitnick: „The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers“, Wiley, 2005.
4. M. Carić, D. Pleskonjić, B. Đorđević, N. Maček: „Sigurnost računarskih mreža-priručnik za labaratorijske vežbe“, VIŠ, Beograd, 2006.
5. Robert W. Taylor: „Digital Crime And Digital Terrorism“, Prentice Hall, Austin, 2005.
6. Slobodan Lazarević: „Hakeri“, Knjiga Komerc, Beograd, 2000.
7. Steven Levy: „Hackers: Heroes of the Computer Revolution“, Penguin, updated edition (2001)
8. www.2600.com
9. www.artofhacking.com
10. www.catb.org/jargon.html
11. www.cs.berkeley.edu
12. hackingworld.bloger.hr/
13. www.mit.edu/hacker/hacker.html
14. www.paulgraham.com/gh.html
15. www.phrack.ogr
16. www.ryanross.net/leet
17. www.slashdoc.com/tag/hacking.html
18. www.tehnopedija.net
19. www.Thehacktivist.com
20. www.Wikipedia.org