

Računalna sigurnost na Internetu i lokalnim mrežama

Verzija 2.0
Dinko Korunić, 2004.

O predavaču

- višegodišnji vanjski suradnik časopisa Mrež@, vlastita kolumna "Digitalna radionica - Linux", itd.
- vanjski suradnik SRCE-a: forenzike provaljenih sustava, izgradnja sistemskih paketa, helpdesk za sistemce, sigurnost Unix baziranih sustava, predavač, itd.
- sigurnosni ekspert pri InfoMAR d.o.o.

O predavaču (2)

- od 1996. godine dizajnira, stvara i održava višekorisničke sustave temeljene oko Unix, Linux i Windows operacijskih sustava
- programira, razvija pakete i sigurnosne modele za Linux, Solaris, Digital Unix, Ultrix, FreeBSD/OpenBSD/NetBSD, itd.
- razvija sigurne mrežne sustave oko žičnih i bežičnih mreža (AAA, NIDS, vatrozidi, nadgledni sustavi, backup, failover sustavi, itd.)

Tijekom prezentacije

- ako što nije jasno - pitajte i tražite objašnjenje!
- ako što nije točno - **ispravite!**
- **diskusija** je poželjna i produktivna
- ako je prebrzo - tražite da se **uspori!**
- ako je pak presporo i uspavljuje vas - lako se **ubrza** sa sadržajem
- **podijelimo** zajedno vlastita iskustva

Sadržaj

- uvod
 - čemu sigurnost? kako? gdje? čime?
 - osnovni pojmovi, teorija, itd.
- strana **hackera**
 - tko su? zašto to rade? kako to rade? sa čime to rade? kome to rade? gdje se nalaze?
 - tipičan profil, načini i tipovi provala, primjeri

Sadržaj (2)

- strana **system-inženjera**
 - detekcija, zaštita, poboljšanje, poluinteligentna rješenja i samoodržavanje
 - tehnike zaštite, primjeri
- sigurnost mreža
 - bežične mreže, mrežna oprema, ...
 - miskonceptije i lažna sigurnost

Sadržaj (3)

- testiranja
 - testovi sigurnosti, penetracijski testovi, forenzike
 - najčešći programi i aplikacije za testiranje
 - primjeri
- završetak
 - diskusija, pitanja, zaključci, razno

Ciljevi prezentacije

- opći uvod u problematiku
- razumijevanje pojmova
- praktični primjeri
- opis ponašanja crackera i sistemca
- što nam je činiti, a što izbjegavati
- budućnost?

Uvod

- opća problematika
- pojmovi, objašnjenja

Računalna sigurnost

- **što**: prevencija i detekcija nedozvoljenog korištenja računalnih i inih resursa
- **zašto**: nitko ne želi da mu "stranci" kopaju po privatnom sadržaju, a kamoli poslovnim tajnama
- **tko**: napadači (hackeri, crackeri, prolaznici) ne traže nužno vas kao osobu, već vaše računalo ili samo kakvu informaciju
- **kako**: kroz postojeće nesigurnosti (sigurnosne rupe) koje postoje u skoro svakom softveru bilo kao greška bilo kao zaboravljene postavke

Računalna sigurnost (2)

- interdisciplinarna:
 - sistemsko i aplikativno programiranje
 - telekomunikacija, mreže računala, itd.
 - kriptografija
 - sociološki problem:
 - sigurnosna politika
 - upravljanje korisnicima
 - podjela korisnika na tipove
 - procjena problematičnih korisnika

Uvod

- **dijeljenje** "podataka" preko Interneta
- virusi, trojanski konji, DoS napadi, socijalni inženjering = **zlonamjerni sadržaj**
- **milijuni** međusobno umreženih računala
- **"curenje"** informacija:
 - nedostatak obrazovanja
 - nedostatak predostrožnosti
 - nedostatak sigurnosnih mehanizama

Uvod (2)

- linije obrane:
 - **educirani korisnik/pojedinac**
 - **educirani sistem-inženjer** (Bugtraq, Securityfocus, CERT, itd.)
 - **hardver** (hw firewall, VPN, switchevi, VLAN, itd)
 - **softver** (system update, sw firewall, IPSec, IDS, antivirus, kriptografija: PGP, S/MIME, Kerberos, SSL, certifikati, tuneli, digitalni potpisi, CryptoAPI)
 - **security politika! backup!**

Internet danas

- broj računala:
 - **rapidno raste**, ne uvijek **poznat vlasnik** = akademske mreže, lažne adrese, lažni DNS
- opasnost:
 - od znatiželjnih prolaznika do dobro organiziranih, dobro tehnološki potkovanih "**terorista**"
 - razlog = novac, slava(?)
 - **opasnost rapidno raste**: broj napada i sofisticiranost rastu iz godine u godinu

Internet danas (2)

- neodržavani **poslužitelj** = **kompromitirani** poslužitelj
- kompromitirani **poslužitelj** = gubitak novca, moguća tužba, još kompromitiranih računala, mogući izgubljeni ili otuđeni važni podaci!
- isto vrijedi i za **radne stanice**
- nužno definirati sigurnosnu politiku i provoditi je! nužno imati aktivne i stručne sistem-administratore!

Aksiomi

- **operacijski** sustavi imaju ranjivosti
- **mrežni** uređaji imaju "slabe" točke
- većina **protokola** ima "slabe" točke
- **ljudski faktor!**

- svaki poslužitelj ili radna stanica - **provaljiva**
- pitanje je koliko je **vremena** potrebno:
 - predzaštita, detekcija, logovi, zaštitni postupci

Provale

- činjenice:
 - ostvarivanje **nedozvoljenog pristupa** računalu
 - najčešće **repetitivno(!)**
 - služe za daljnje provale, trgovanje, ekstrakciju podataka, ucjenjivanje, poligone za DoS napade
 - **teško "očistiti" zarazu**
- **razlozi** da je došlo do provale:
 - nesavjesnost administratora
 - problem opreme, OS-a ili pripadnih aplikacija
 - nesavjesnost korisnika

Curenje informacija

- **nesigurni** (cleartext) protokoli:
 - http (Web)
 - smtp (e-mail)
 - telnet, itd.
- rješenje? primjena moderne snažne **kriptografije!**
 - asimetrični algoritmi (pola + pola ključa)
 - šifriranje poruka, teksta, podataka, materijala!

Curenje informacija (2)

- **kriptografija** u primjeni:
 - HTTPS = sigurni http protokol (ali ipak postoje SSL propusti)
 - OpenPGP = "sigurna" pošta (digitalni potpisi, enkripcija e-maila, itd)
 - SSH, Kerberos, SSL-telnet = dodatni sigurni načini prijenosa datoteka i sadržaja preko Interneta
 - snažni algoritmi: Blowfish, 3DES, AES, itd.
 - "provaljeni" MD5, MD4, RIPEMD, HAVAL-128

Curenje informacija (3)

- nužno:
 - implementirati kriptografiju **transparentno!**
 - sigurni mehanizmi **autentifikacije**
- svakodnevni život:
 - Windows 2000, Windows XP, Unixodi - kriptografija ugrađena u sustav!
 - https stranice koriste SSL!
 - SecureCards, TLS, 802.1x i oprema, itd.

Zanimljivosti

- što je **cracker/script-kiddie**?
 - koristi tuđe programe
 - slabo razumijevanje rada sistema
 - iskušava tuđe programe dok ne pogodi
- što je **hacker**?
 - piše vlastite programe za provalu i analizu
 - obično ne provaljuju
 - iznimno visok stupanj tehnološke potkovanosti
 - "guru" - specijaliziraju se

Zanimljivosti (2)

- Internet = sjecište različitih **grupacija**:
 - **systemci** - CERT, SANS, itd.
 - **systemci** i **hackeri** zajedno - Bugtraq, SecurityFocus, LinuxSecurity, itd.
 - **crackeri** i **script-kiddies** - EFNet, IRCNet, Undernet (Rumunjska i Poljska - žarišta)
 - obilje informacija i za sistem-inženjere i za provalnike
 - **DefCon**, SANS Institute, CERT, itd.
 - redoviti sastanci i hackera i sistemaca!

Podjela hackera

- **Whitehats**

- hackiranje u dobre svrhe!
- svoja dostignuća javno objavljuju i savjetuju kako se zaštititi
- pomažu poboljšanju softvera/hardvera

- **Grayhats**

- **Blackhats**

- skupine orijentirane prema destrukciji, zlonamjernom provaljivanju
- visoki stupanj organizacije

Najčešći problemi radnih stanica

- **trojanci i backdoorovi:** BackOrifice, Netbus, SubSeven
- **DoS i drone** za DDoS
- nezaštićeni **resursi:** Windows dijeljeni resursi
- **mobilni kod:** Java/JScript/ActiveX i skupljanje informacija
- **cross-site scripting:** zlonamjerne skripte (linkovi, interaktivne forme, dinamički web)
- **e-mail lažiranje** i e-mail **virusi**
- **snifanje** paketa

Ostali sigurnosni problemi

- **virusi** (Klez, Melissa, Michelangelo)
 - pogođene pretežno Windows platforme
 - raširenost, brojnost, automatiziranost
 - izvršavanje on-demand = educirati korisnike!
- **trojanski konji**
 - podmetanje, obično sa nekom namjerom
- **crvi** (Ramen, itd.)
 - visoki stupanj automatizacije i nezavisnosti
 - pogođeni: IIS, SSL, itd.

Što nije sigurnost sustava

- **paranoja**

- zabranjivanje svega - svih mogućih detalja u pristupnim listama
- zaključavanje pristupa "za svaki slučaj"
- "security through obscurity"

- **neugodnost sustava**

- netransparentni rad + forsirana autentifikacija i autorizacija na svim medijima prije rada
- politika "idem zabraniti, pa ću dozvoliti ako će se netko žaliti"

Najčešći sigurnosni problemi

- Intranet **nije podijeljen** od Interneta (a gdje je gw, firewall i NAT?)
- **nema sigurnosne politike** - svatko radi što hoće
- **neidentificirani broj** računala (tko? kada? gdje?)
- **nema filtriranja** sadržaja (firewall, antivirus)
 - Spyware & trojanski konji

Najčešći sigurnosni problemi (2)

- **slaba ažurnost**

- recentni patchevi
- nove verzije programa (servisa, korisničkih aplikacija, itd.)
- popisivanje postojećeg softvera
- dokumentacija!

- **loš mrežni dizajn**

- neprikladna mrežna oprema (hubovi, itd.)

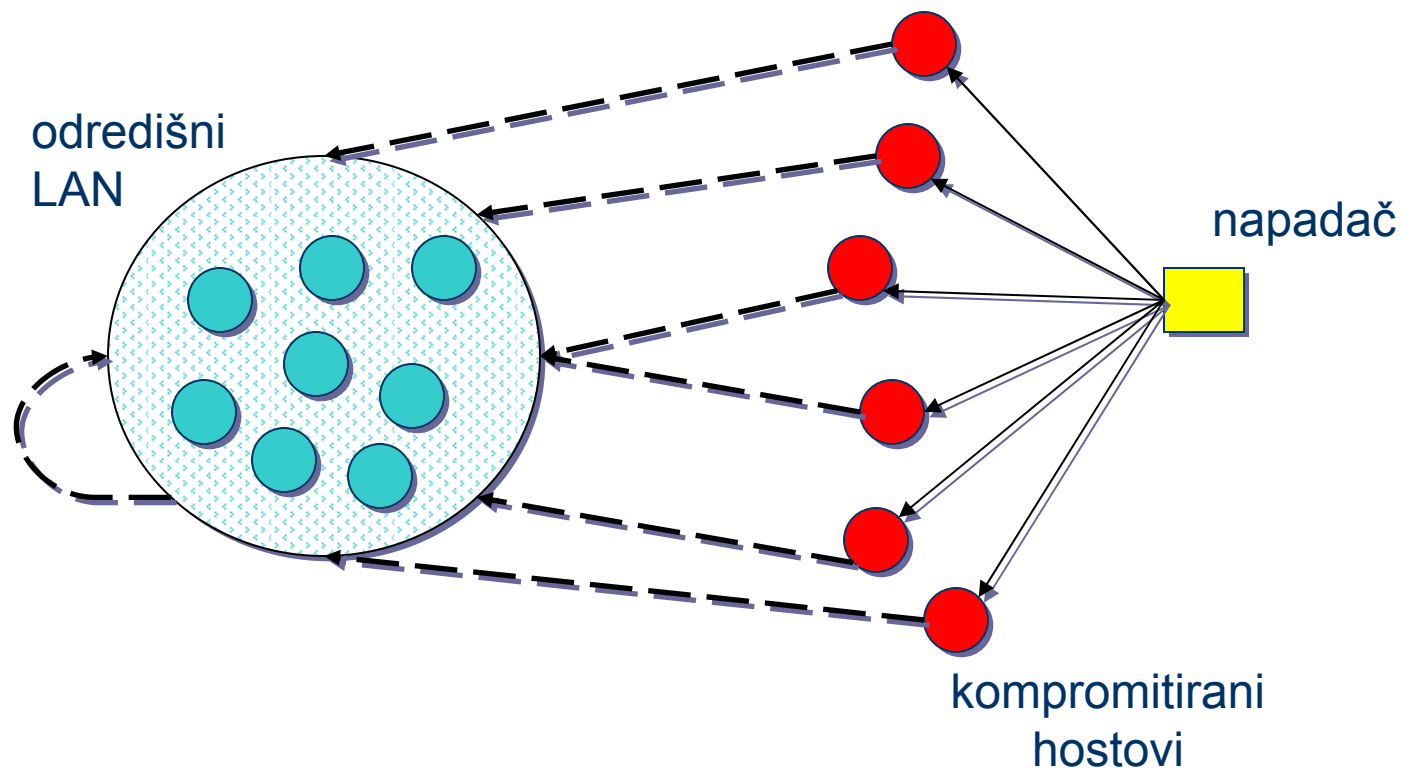
Denial of Service

- napad na servis, servise ili grupe računala s razlogom privremenog ili stalnog prekida rada (DoS, DDoS)
- ping of death, arp storm, udp flood, itd.
- najčešće:
 - velike korporacije (Yahoo, HTHiNet, itd.)
 - "Eldorado" računala (IRC serveri, itd.)
- **lažno predstavljanje**
 - mrežni i softverski problem! (IPv4, TCP)

Denial of Service (2)

- najčešći:
 - trinoo, smurf, mstream, ...
 - postoje alati za detekciju - psad, slice, itd.
- DDoS = Distributed Denial Of Service
- osnovni razlozi uspješnosti:
 - mrežna infrastruktura
 - mrežni protokoli
 - mrežne postavke (uplink filtriranje, itd.)

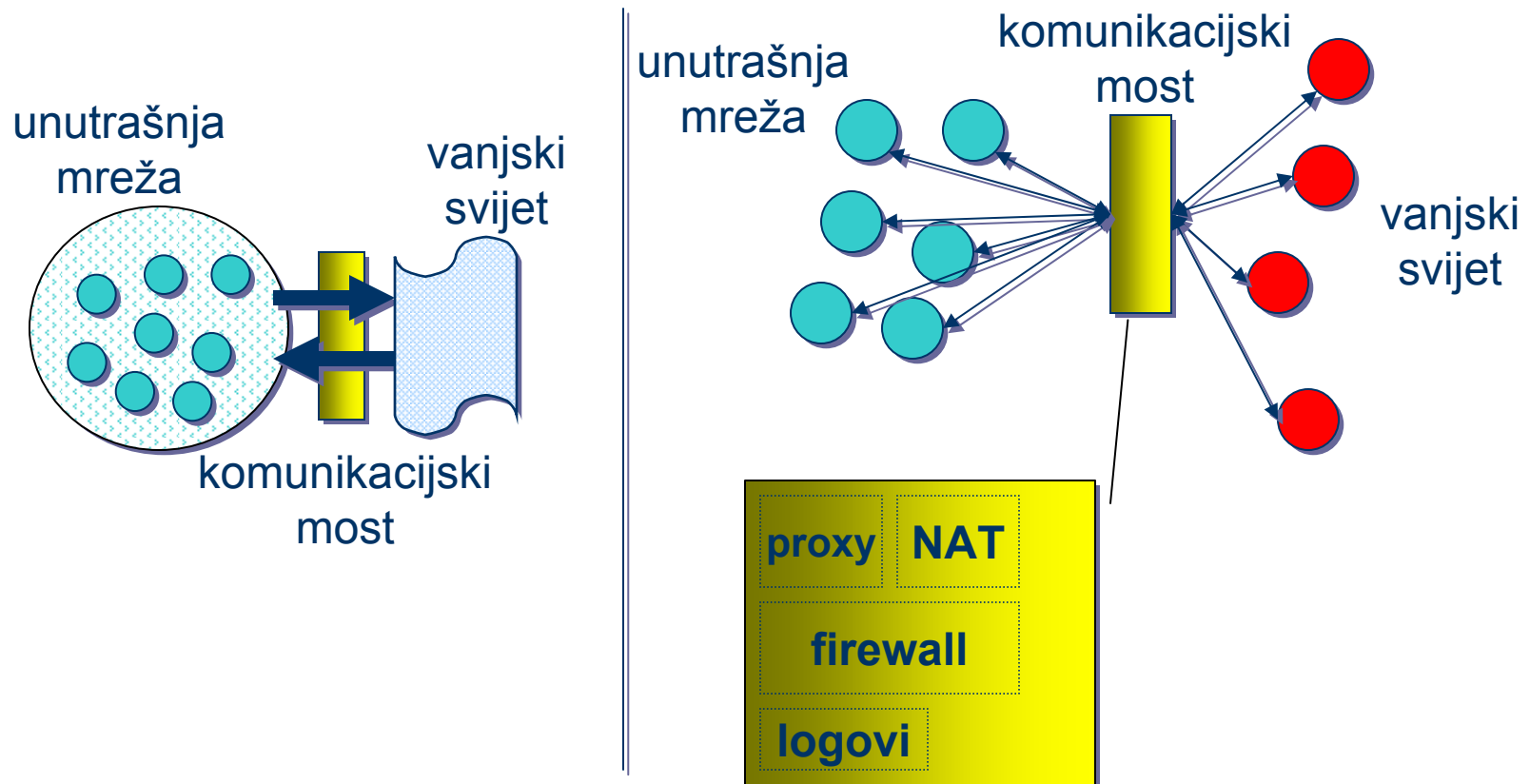
Denial of Service (3)



Najčešće sigurnosne strategije

- **vatrozid**
 - firewall = filtriranje **paketa** prema određenim pravilima (pristupne liste, promet, bitovi u paketu)
 - proaktivni, obični, stateful(!); hardver, softver
- **NAT**
 - Network Address Translation
 - **sakrivanje** grupe računala iza jednog računala
- **proxy**
 - keširanje i filtriranje **sadržaja**

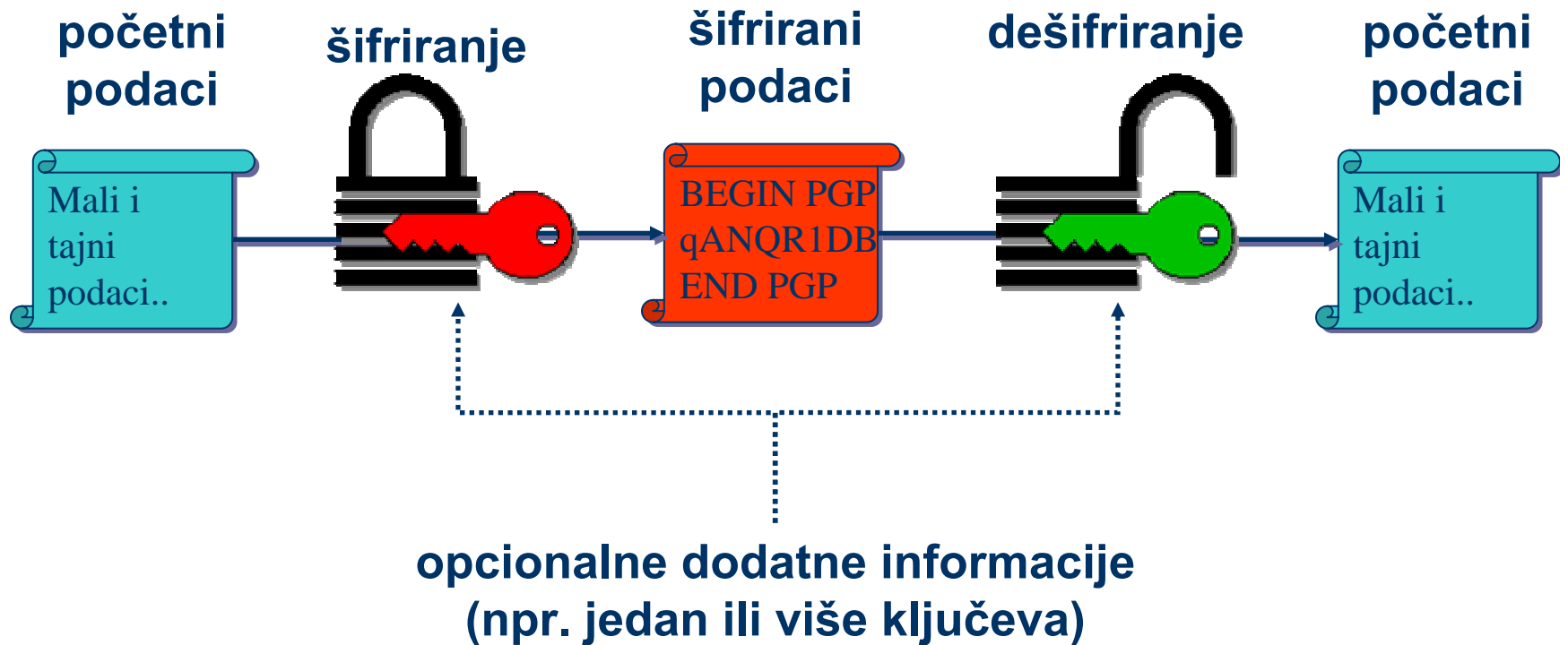
Najčešće sigurnosne strategije (2)



Kriptografija - osnovni pojmovi

- **šifriranje/enkripcija** - skrivanje podataka i transformiranje u obično neprepoznatljiv oblik
- **dešifriranje/dekripcija** - konverzija iz neprepoznatljivog šifriranog oblika u čitljiv oblik
- **ključ** - informacija koji omogućava šifriranje i dešifriranje
 - caesar šifriranje - Julije Cezar radi zaštite tajnosti slao generalima poruke u kojima je svako slobo bilo pomaknuto za 3 slova udesno

Kriptografija u primjeni



Kriptografija - ključevi

- **ključ** - podatak (jedan ili više) koji uz poznati algoritam vodi do početnih podataka i obrnuto
- nekada davno:
 - samo jedan ključ za šifriranje i dešifriranje - u WW2 je to bila crna kutija koja "nešto" radi
 - inicijalno je potrebno "sigurno" prenijeti ključ
 - sigurnost šifriranih podataka = sigurnost inicijalnog ključa!
 - stručan naziv: "standardni kriptosistemi"
 - velika brzina rada naspram "jakog" šifriranja
- **"jako šifriranje"** – nešto što se teško može provaliti u "normalnom" vremenu sa "normalnom" opremom

Kriptografija - ključevi (2)

- prva mogućnost:
 - ključ za šifriranje isti kao i za dešifriranje = **jedinstveni ključ** ⇒ **simetrično šifriranje**
 - jednostavnije, brže, no ako se ključ ukrade - sve pada u vodu
- druga mogućnost:
 - **dva odvojena ključa** - jedan za šifriranje, jedan za dešifriranje ⇒ **asimetrično šifriranje**
 - ključ za šifriranje ne mora biti tajan!
 - vrlo sigurno, kvalitetno, sporo, ali tajno

Kriptografija - ključevi (3)

- treća mogućnost:
 - na poseban način dobije se nekakva suma iz početnog sadržaja
 - takva suma služi **samo** za provjeru autentičnosti i nepromijenjenosti sadržaja
 - jednosmjerno šifriranje \Leftrightarrow nema reverzibilnosti, iz određene sume se ne može dobiti početni sadržaj!
- danas se koriste kombinacije simetričnog i asimetričnog šifriranja u svakodnevnom radu: Windowsi, Unix, GSM, banke, itd.

Kriptografija - kraj

- kriptosistemi oko javnih i tajnih ključeva
- digitalni potpis
- digitalni certifikat
 - FINA ovlašteno tijelo za izdavanje root certifikata
- jednosmjerno šifriranje - kriptosume:
 - CRC16, CRC32, MD4, MD5

Operacijski sustavi

- **server**

- Windows NT 4, Windows 2000, Windows XP?
- Linux? Unixoidi?
 - manja cijena, viša razina moguće(!) sigurnosti
 - veća ulaganja u kontinuiranu edukaciju sistemaca
- PC? Sun Microsystems server? IBM RS6000?
- potrebno odabrati odgovarajući za namjenu!

- **radne stanice**

- Windows! Linux?

10 najčešćih rupa (SANS - <http://www.sans.org/topten.htm>)

- ISC Bind
- Web CGI (Cold Fusion..)
- RPC (ttdbserverd, cmsd, statd)
- IIS (RDS)
- Sendmail (MIME)
- sadmind, mountd
- File Sharing (NetBIOS, NFS, Web sharing, AppleShare)
- standardni accounti i "slabe" lozinke
- POP/IMAP
- SNMP default accounti
- dodatno IE, Office 2k
- postoje automatizirani alati za pretragu:
 - Nessus = Network Security Scanner
 - razni neslužbeni

Pogled crackera na svijet

- što radi, kada radi,
kako radi, sa čime radi

Dan 1

- tko?
 - višak vremena, jeftini spoj na Internet, Linux
 - Vice "hacker" provalio u Pentagon :-)
- **IRC** - središte informacija o potencijalno "provaljivim" računalima
- sklapanje **timova** i interesnih grupa
- gotovi **exploitovi**, itd - Usenet, Bugtraq, specijalizirana skrovida mjesta, itd.
- "mentori"

Dan 2

- odabir odredišne domene ili niza računala:
 - **nasumično**
 - sa određenim ciljem:
 - IRC roboti
 - novac
 - slava
 - daljnje provaljivanje
 - klijenti za DoS mrežu
- odabir **odredišnog** računala

Dan 3

- **prikupljanje** informacija:
 - razne informacije: web, google, whois, irc
 - **pasivna** analiza prometa: sniffit, tcpdump, ethereal (nesigurni promet! lozinke!)
 - **socijalni** inženjering!
 - pronalaženje korisničkih imena (i lozinki!!)
 - **aktivno** pretraživanje:
 - portscanning - nmap, ssh-scan, itd.
 - detekcija OS - nmap, ping, itd.
 - detekcija rupa - nessus, satan, itd.

Dan 4

- analiza dobivenih informacija:
 - odabir **provalničkih programa (exploit ili sl.)** na osnovu dobivenih parametara (OS, vrijeme, korisnici, upotreba)
 - **generiranje lozinki** iz dobivenih podataka:
 - JMBG, broj osobne, ime ljubimca, ime djeteta, prezime muža/žene, ime susjeda/susjede, česti brojevi, omiljena boja, itd.
- **analiza ponašanja** korisnika, sustava i sistemca

Dan 5

- ostvarivanje provale:
 - u odgovarajuće vrijeme (doba dana) i odgovarajući trenutak (mrežni promet)
 - korištenjem jednog ili više dostupnih alata:
 - stvaranje odgovarajuće okoline (tuneli, ARP napad, DoS napad, lažna polazna adresa, lažno predstavljanje, itd.)
 - generatori lozinki (pwgen)
 - gotovi alati za provaljivanje prema danim parametrima
 - vlastiti alati (rijetko!!)
 - brute force ili stealth?
 - man-in-the-middle? lažno predstavljanje?

Dan 5 (nastavak)

- **sakrivanje** tragova:
 - nakon uspješne provale
 - automatizirani alati, ili barbarski (obriši sve)
 - **trojaniziranje** sustava i/ili otvaranje novog **backdoora** (rupe u sistemu)
- **useljenje** vlastite okoline u sustav:
 - vlastiti programi, vlastiti korisnici, vlastiti dio sistema
- cjelokupno **uništenje** sustava(!)

Dan 6

- koristi se novi stroj:
 - za ucjenjivanje
 - daljnje provale
 - ometanje rada (ista domena/niz računala ili drugo) - DoS, lažni e-mail, warez, IRC roboti, itd.
 - itd.
- napomena
 - provaljeni stroj je nužno **odmah** onemogućiti da nastavi sa radom!

Pogled sistemca na svijet

- što radi, kako radi, sa čime radi, itd.

Dan 1

- popisivanje svih računala i opreme u sustavu
- popisivanje željenih servisa (korisnici i cijeli sustav)
- striktno definiranje zadaća računala i servisa na njima
- popis korisnika i standardnog ponašanja (promet i korištenje računala) istih

Dan 2

- izgradnja/poboljšanje mrežne infrastrukture:
 - nabavljanje odgovarajuće opreme: preklopnici, routeri, firewalli
 - segmentiranje i odvajanje prometa i radnih grupa!
 - odvajanje Internet i Intranet mreže
 - dizajniranje mreže prema specifikacijama, očekivanom prometu, itd.
 - eliminiranje SPOF i rad na KISS principu!

Dan 3

- instalacija sustava:
 - optimalni odabir OS i servisa prema zadaćama
 - definiranje pristupa sustavu/servisima prema analizi dobivenih podataka
 - uklanjanje svega suvišnog
 - politika: zabrani sve, dozvoli samo nužno
 - minimizacija "rupa" na sustavu
 - sustav se ne pušta u pogon do kraja definiranja pristupnih listi, sigurnosnih mjera i postavljene zaštite!

Dan 4

- definiranje pristupnih listi za korisnike i sam sustav:
 - mrežu i mrežni promet
 - opći računalni sustav
 - individualne poslužitelje
 - individualne servise
- definiranje administratora
 - zadaće, lozinke, pristup, itd.

Dan 5

- postavljanje zaštite:
 - hardver:
 - firewall, VPN, switch, različita mrežna oprema sa sig. mogućnostima
 - softver:
 - NAT, firewall, antivirus, remote logging, IDS, kriptografija
 - sistemski updateovi, sigurnosna jezgra sustava, samonadgledanje, centrano nadgledanje, automatsko samonadograđivanje
 - analiza ponašanja, SMS alarmi
 - bihevioralni sustavi

Dan 6

- puštanje sistema u pogon:
 - nadgledanje rada
 - burn test
 - analiza ponašanja unaprijed - što će se dešavati sa 24/7 sustavima
 - redovno pregledavanje stanja sustava u inicijalnom periodu
 - podešavanja access listi ovisno o potrebama

Primjeri iz prakse

- provaljena računala,
forenzika, penetracijski
testovi

Provaljena računala

- razlozi:
 - ranjive **aplikacije**, operacijski **sustav** ili kompromitirani **korisnici** - lozinke
- posljedice:
 - **kompromitiranost** aplikacija i cjelokupnog sustava
 - teška identifikacija - rkhunter, chkrootkit, tct, strace, lsof, gdb, fenris
 - zamijenjene aplikacije skrivene, teško detektirati
 - postoje gotovi **rootkitovi**: ShowTee, T0rn, itd.

Forenzika

- postupak - **forenzika**:
 - kako je došlo do provale - **zamrznuta situacija**:
 - logovi (obrisani), datoteke i česte lokacije
 - podatci o korisnicima
 - analizirati kompromitirane datoteke i datotečni sustav:
 - rootkitovi, kernel moduli, radni direktoriji, history datoteke, ostatci logova, swap, itd.
 - pretraživanje ekspertnih baza
 - preporučiti optimalno rješenje:
 - backup, dezinfekcija (rijetko), reinstalacija

Forenzičar

- iskustvo
 - ekspertni sustav
 - što više obavljenih forenzika
- sistemski programer
- mrežni guru
- stručnjak za sigurnost
- nadmudrivanje - na putu da postane hacker

Forenzičar (2)

- nadmudrivanje - provala dobro skrivena:
 - zaražene datoteke enkriptirane - BurnEye projekt, skrivene na sustavu, iste veličine kao originali, istog vremena kao originali, prepoznaju sistemsko praćenje - BurnEye projekt
 - logovi pročišćeni, ali ne obrisani do kraja
 - skrivanje na nivou jezgre - Adore projekt - praktički nemoguće otkriti i teško zaobići
 - lažni tragovi

Zaštita (1)

- individualna računala:
 - Windows: **PF**, centralizirani **WindowsUpdate**, AD i kontrola, user-policy, **minimalne dozvole** korisnicima
 - Linux: sigurnosni **kernel** moduli (Grsecurity, LIDS, SELinux), redovne **nadogradnje** (apt-get, redcarpet) aplikacija i kernela
 - Unixoidi: redovne nadogradnje kernela i aplikacija
 - centralni nadzor, NIDS, segmentiranje mreže

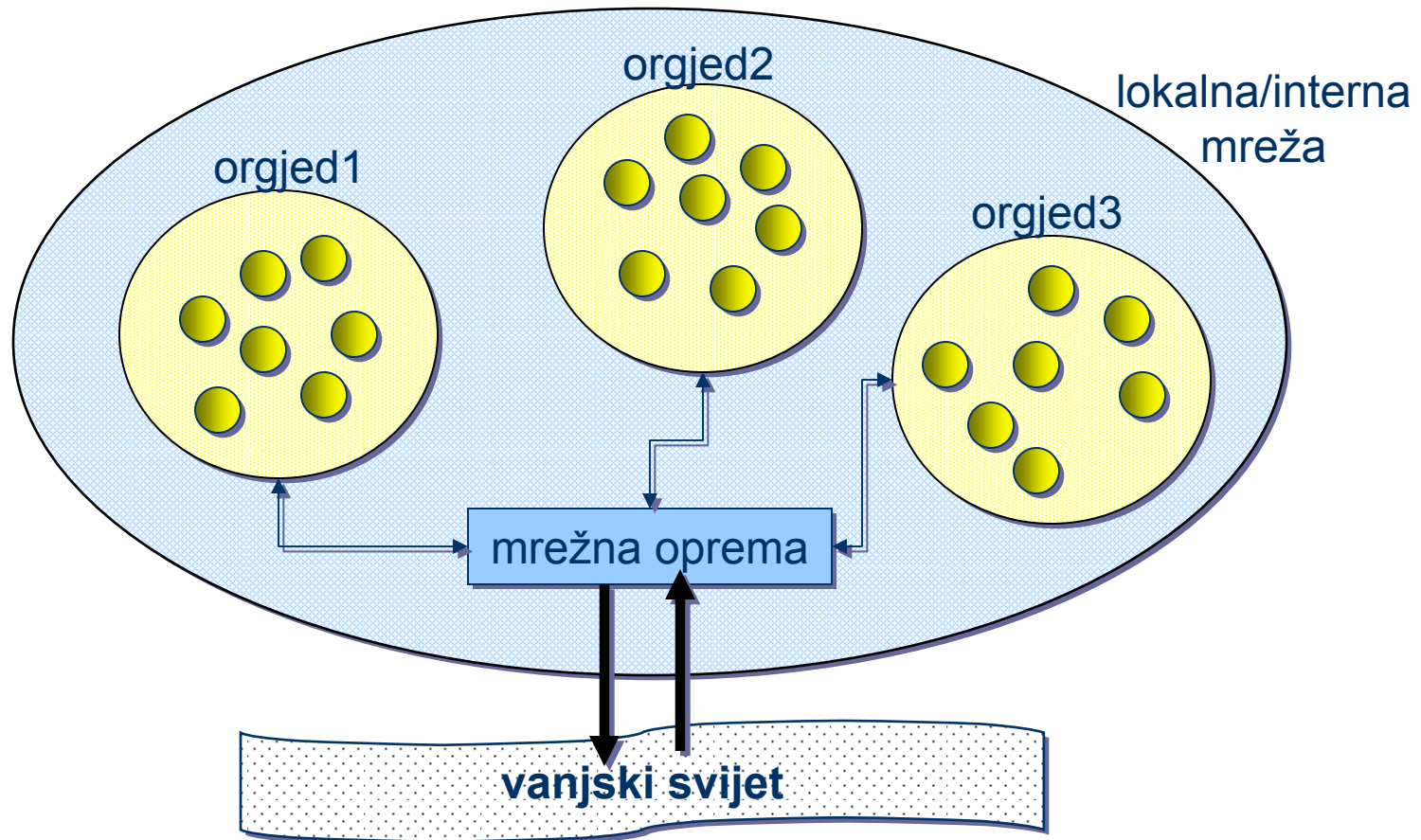
Zaštita (2)

- serveri:
 - **vatrozid** na poslužitelju
 - **liste pristupa** poslužitelju i individualnim aplikacijama
 - **ojačanja** (TCP/IP, nonexec stack, itd)
- mreža:
 - DMZ, NAT, VPN, VLAN, segmentiranje

Segmentiranje mreže

- podjela u logičke cjeline:
 - organizacijske jedinice
 - jedinice sa različitim tipovima/profilima korisnika
- postavljanje segmenata i/ili VLAN-ova
- omogućavanje komunikacije samo gdje je nužna
- minimiziranje rizika:
 - lakše lociranje provale
 - lakše rješavanje potencijalne zaraze/kompromitirane okoline
 - zaštita "nedužnih"

Segmentiranje mreže (2)



Sigurnost mreža

- fiksne mreže:
 - preklopnici - lažna sigurnost, moguće zapuniti ARP tabele
 - VLAN tagovi - moguće zaobići
 - osim kod iznajmljenih linija, moguće presretati komunikaciju
 - nužno korištenje VPN modela:
 - VPN i IPSEC: OpenVPN, CIPE, FreeS/WAN, OpenS/WAN, specijalizirani HW

Sigurnost mreža (2)

- **cleartext** protokoli:
 - moguće prislušivati (sniffit, tcpdump, ethereal)
 - neotporni na man-in-the middle napade (hunt)
 - HTTP, SMTP, SNMP, FTP, Telnet, itd.
- bežične mreže:
 - moguće **prisluškivanje** (kismet, air magnet)
 - enkripcijski WEP64 i WEP128 provaljivi - alternativa dynamic WEP i WPA

Sniffit - prislušivanje

```
01$ zsh 1-$ zsh 2$* zsh
Sniffit 0.3.7 Beta
161.53.71.194 22 -> 161.53.116.16 3004
161.53.116.16 3004 -> 161.53.71.194 22
205.188.7.228 5190
161.53.71.194 42471
193.198.213.8 6667
161.53.71.194 46345
161.53.2.81 8888
161.53.71.194 54501
161.53.71.194 56435
193.198.213.8 6667
195.29.149.42 22
161.53.71.194 22
129.240.242.161 4516
205.188.248.196 9898
161.53.71.194 38876 -> 208.245.212.67 5222

:irc.ffzg.hr PONG irc.ffzg.hr :irc.ffzg.hr..
193.198.213.8 6667 -> 161.53.71.194 54501

Sniffit 0.3.7 Beta
Source IP : All Source PORT : All
Destination IP: All Destination PORT: All

Masks: F1-Source IP F2-Dest. IP F3-Source Port F4-Dest. Port
```

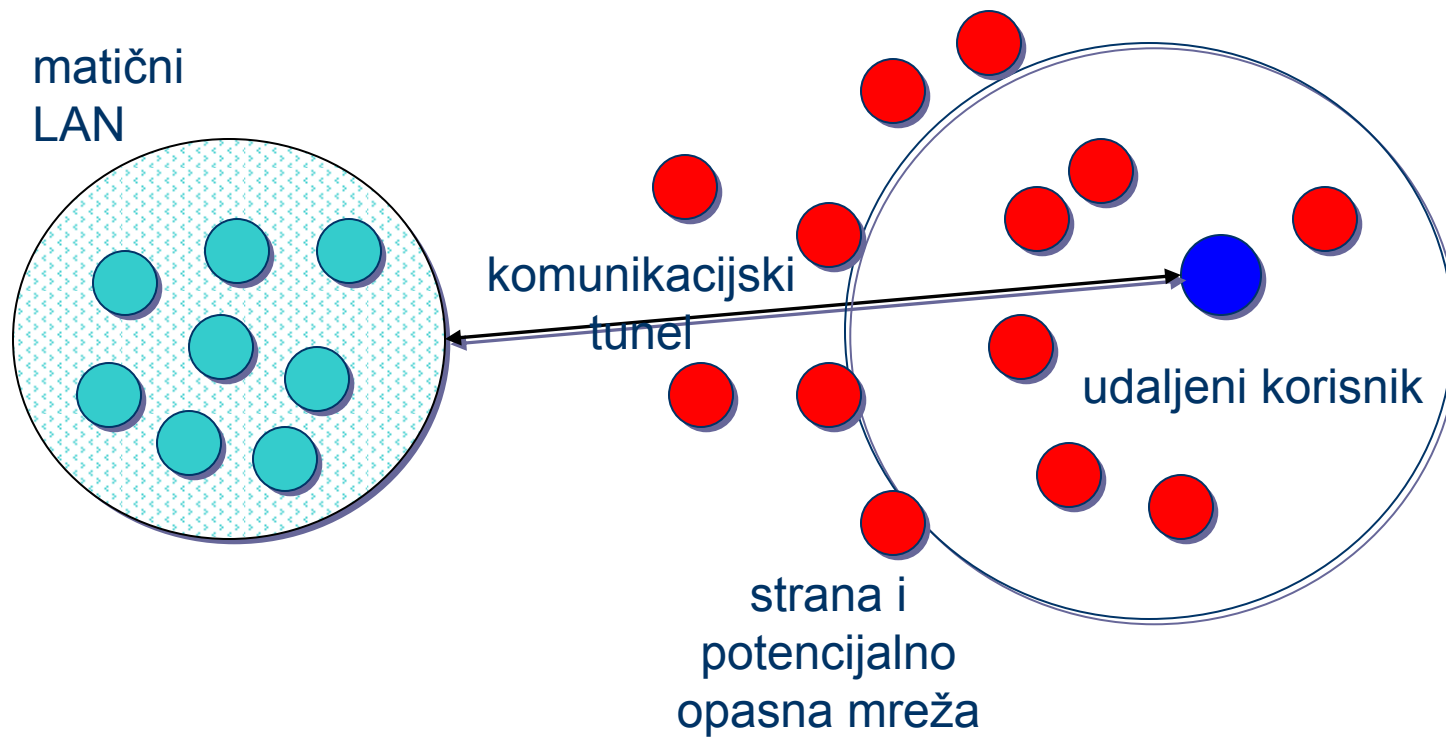
Vatrozid

- točka dodira sa **stranom** mrežom
- **filtriranje** paketa:
 - odredište, izvorište
 - portovi, tip prometa, dužina paketa, itd.
 - analiza stanja
- vrši i dodatne usluge:
 - NAT i/ili **maskerada**, **usmjerivanje** prometa, **redirekcija**, DMZ, NIDS i prepoznavanje uzoraka
 - **QoS** i kontrola toka prometa
 - **uzbunjivanje**, spremanje logova

VPN

- komunikacijski **tunel**
- **kriptografski** siguran
- omogućava povezivanje:
 - **peer-to-peer**: dva računala
 - **multipeer-to-peer**: čvor prema mreži računala
 - **multipeer**: čvorovi se povezuju u mrežu unutar postojeće nesigurne mreže - oportunistička enc.
- tvorba virtualnih i sigurnih mreža

VPN (2)



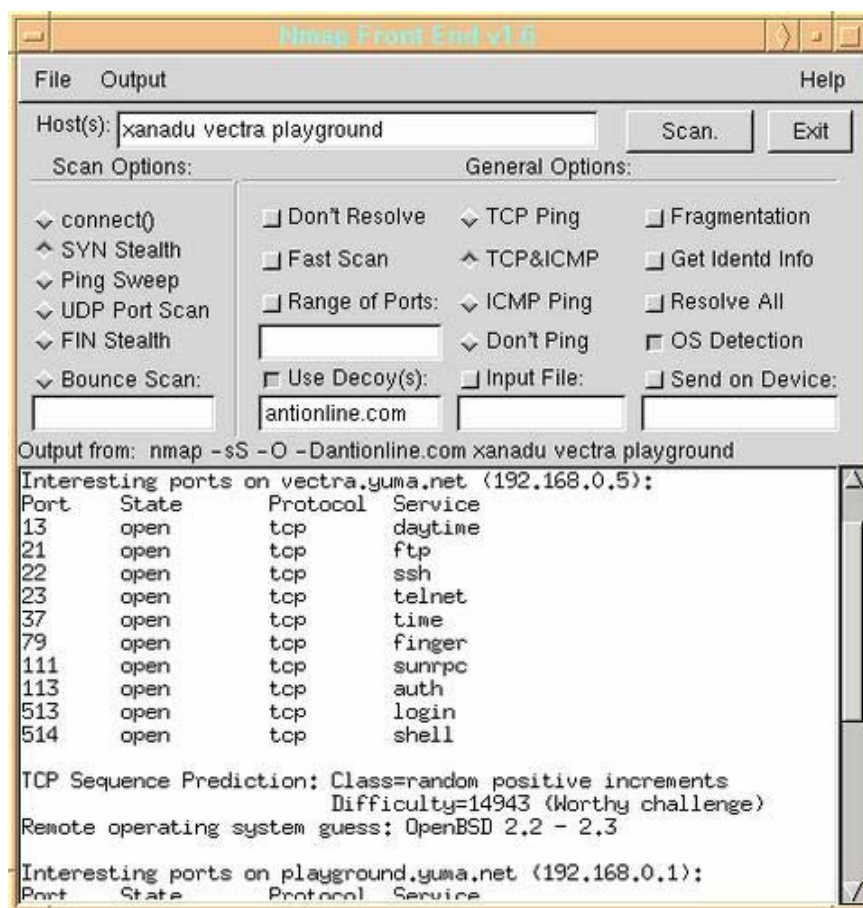
Antivirus

- individualna računala
- server:
 - čišćenje maila i dijeljenih datoteka
 - skeniranje za virusima po mreži
 - content analysis
 - čišćenje mrežnih tokova unutar mreže i tokova u i izvan mreže
 - iznimno složeno, zahtjevno i skupo - ali efikasno
- centralno rješenje

P0f - pasivni fingerprint

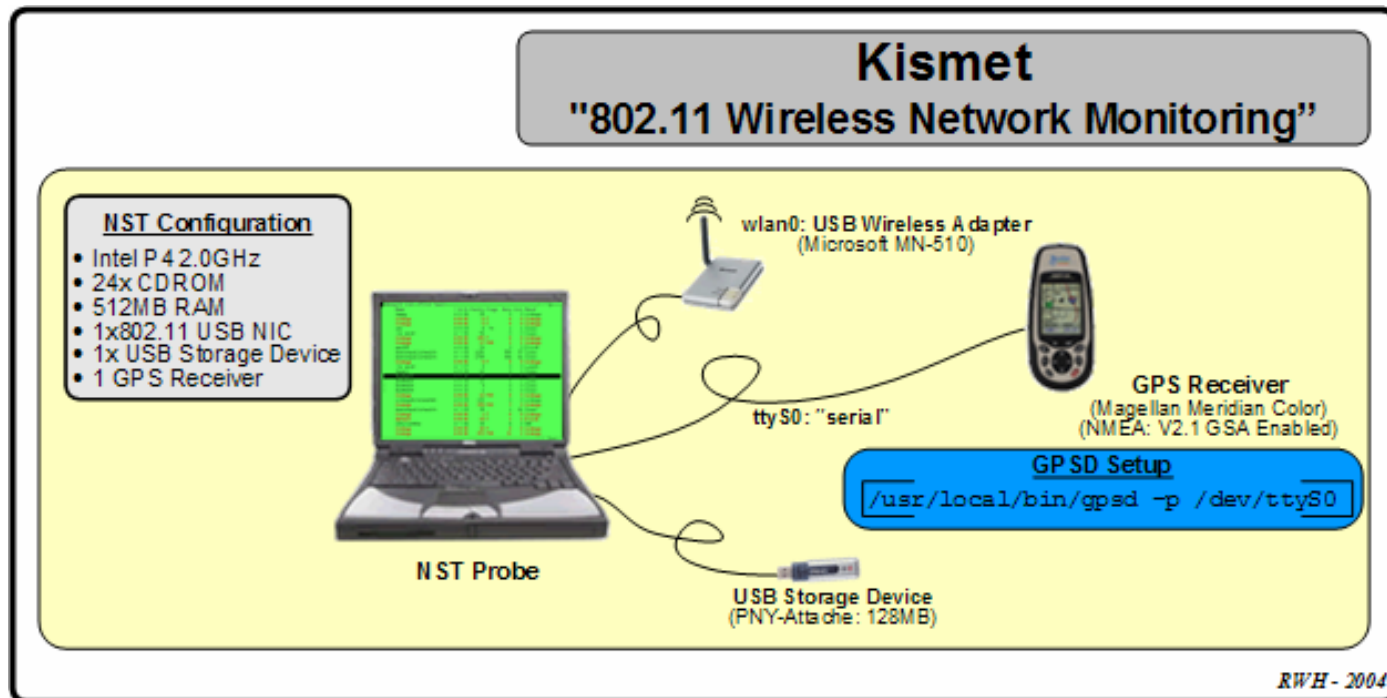
```
0- zsh 1! zsh 2 zsh
p0f: listening (SYN) on 'eth0', 206 sigs (12 generic), rule: 'all'.
82.193.197.104:4447 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 161.53.71.194:110 (distance 7, link: ethernet/modem)
207.46.98.112:3045 - Windows 2000 SP4, XP SP1 [Cable.BG / Teleca.SE]
  -> 161.53.71.180:80 (distance 15, link: ethernet/modem)
161.53.71.10:1109 - Windows XP Pro SP1, 2000 SP3
  -> 161.53.71.194:110 (distance 0, link: ethernet/modem)
66.249.64.173:46976 - Linux 2.4 (Google crawlbrot) [Cable.BG / Teleca.SE] (up: 30
1 hrs)
  -> 161.53.71.180:80 (distance 16, link: (Google/AOL))
66.249.64.169:32986 - Linux 2.4 (Google crawlbrot) [Cable.BG / Teleca.SE] (up: 30
1 hrs)
  -> 161.53.71.180:80 (distance 15, link: (Google/AOL))
193.17.96.40:49040 - OpenBSD 3.0-3.4 [Cable.BG / Teleca.SE] (up: 2016 hrs)
  -> 161.53.71.180:80 (distance 16, link: ethernet/modem)
161.53.71.130:1399 - Windows 2000 SP4, XP SP1
  -> 161.53.71.194:110 (distance 0, link: ethernet/modem)
161.53.71.235:3730 - Linux 2.4/2.6 (up: 1342 hrs)
  -> 161.53.71.194:873 (distance 0, link: ethernet/modem)
193.17.96.40:49381 - OpenBSD 3.0-3.4 [Cable.BG / Teleca.SE] (up: 2016 hrs)
  -> 161.53.71.180:80 (distance 16, link: ethernet/modem)
66.249.64.30:37978 - Linux 2.4 (Google crawlbrot) [Cable.BG / Teleca.SE] (up: 640
9 hrs)
  -> 161.53.71.180:80 (distance 15, link: (Google/AOL))
```

Nmap - aktivno skeniranje



- identifikacija otvorenih "portova"
- identifikacija aplikacija
- identifikacija jezgre sustava
- identifikacija protokola koje podržava
- pronalaženje točnog vremena
- pronalaženje faktične ranjivosti TCP/IP stoga

Wardriving



RWH - 2004

Bežične mreže

- **trivijalno prislušivati:**
 - jeftina oprema, mali i mobilni uređaji (iPAQ + WiFi), niz postojećih aplikacija za prislušivanje (20ak poznatih)
- **zaštita netrivijalna:**
 - MAC pristupne liste, 802.1x i EAP/* za autorizaciju i autentifikaciju
 - nužan WPA za enkripciju podataka, nadolazeći WPA2 - ne podržavaju svi klijentski uređaji, nemaju svi AP-ovi

Kismet

```
dragorn@gir.lan.nerv-un.net: /home/dragorn
```

Network List—(Autofit)								Info
Name	T	W	Ch	Pkts	Flags	Data	Clnt	
p@thf1nd3r	A	Y	06	171		70	35	Ntwrks 105
<no ssid>	A	N	05	1		0	0	Pkts 1258
KrullNet1	A	Y	06	27		0	0	Cryptd 104
linksys	A	N	06	81	FU4	8	2	Weak 0
marley	A	N	06	312		17	1	Noise 289
<no ssid>	D	N	--	20	A2	20	18	Discrd 289
! PARMAS	A	N	07	30		0	0	Pkts/s 50
<no ssid>	A	Y	06	1		0	0	
! GRXWirelessNetwork	A	Y	06	2		0	0	
! SECMAS	A	N	07	13		0	0	
<no ssid>	D	N	--	1	A4	1	66	
! <Lucent Outdoor Router>	O	N	--	267		267	1	

Elapsd
000027

Status

- Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
- Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
- Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
- Found IP 159.139.120.13 for <no ssid>::00:B0:D0:DE:60:E3 via TCP

Battery: AC charging 100% 0h0m0s

Testovi sigurnosti

- neintruzivni:
 - skeniranje računala ili cijele mreže
 - aktivni, pasivni
 - pronalaze **potencijalne** probleme
- intruzivni:
 - **penetracijski** testovi
 - cilj pronaći ranjivosti i **isprobati** ih
 - potencijalno **opasno** i štetno - isključivo na odobrenje naručitelja i potpisivanje ugovora

Testovi sigurnosti (1)

- tumačenje najvažniji aspekt!
- nužno poznavati:
 - određene sustave (mreža, računala, oprema)
 - navedene sigurnosne probleme i njihovu problematiku
 - utjecaj sigurnosnih problema na individualno računalo i lokalnu mrežu
 - optimalan način za rješavanje problema uz minimalne zahvate!

Nessus - sigurnosni scanner

The screenshot displays the Nessus scanner interface with three main panels: Subnet, Port, and Severity. The Subnet panel shows two subnets, 10.163.155 and 10.163.156, with the latter selected. The Port panel lists various services and their ports, with netbios-ssn (139/tcp) selected. The Severity panel shows a Security Warning, Security Note, and Security Hole. The main content area displays a detailed security warning for the host 10.163.156.9, explaining that the host SID can be used to enumerate local users.

Subnet	Port	Severity
10.163.155	unknown (1035/tcp)	Security Warning
10.163.156	unknown (1028/tcp)	Security Note
	snmp (161/udp)	Security Hole
	smtp (25/tcp)	
	qotd (17/udp)	
	qotd (17/tcp)	
	printer (515/tcp)	
	nntps (563/tcp)	
	nntp (119/tcp)	
	netinfo (1033/tcp)	
	netbios-ssn (139/tcp)	
	netbios-ns (137/udp)	
	nameserver (42/tcp)	
	ms-term-serv (3389/tcp)	

Host

- 10.163.156.1
- 10.163.156.9
- 10.163.156.10
- 10.163.156.16
- 10.163.156.205

The host SID could be used to enumerate the names of the local users of this host.
(we only enumerated users name whose ID is between 1000 and 1020 for performance reasons)
This gives extra knowledge to an attacker, which is not a good thing :

- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- NetShowServices (id 1001)
- NetShow Administrators (id 1002)
- IUSR_GABBO (id 1003)
- IWAM_GABBO (id 1004)
- DHCP Users (id 1005)

Nessus - sigurnosni scanner (2)

- vrlo **komplicirano** upravljanje: nužna vrlo dobra edukacija i znanje o problematici
- omogućava **detekciju** većine postojećih i **aktualnih** rupa - postoji i mehanizam nadogradnje uzoraka
- relativno dugo vrijeme testiranja
- omogućava teoretske provjere (**identifikaciju**) ali i dijelove penetration testinga (stvarnu **verifikaciju** problema)

Demonstracije

Opcionalni pokazni dio

- Netstumbler - WiFi sniffer
- Kismet - WiFi sniffer
- Nessus - security scanner
- Nmap - portscanner

Kratki pregled

- repetitorij, pregled
renomiranog softvera

Pregled

- pasivni tipovi napada
 - nesigurni mediji (http, smtp, telnet, ...)
 - prisluškivanje (sniffanje podataka) na različitim medijima (LAN - switchani, neswitchani, wireless, ppp, itd.)
 - analiza prikupljenih podataka (ekstrakcija lozinki, itd.)
 - napredni alati - analiza SSL (https), dekripcija lozinki (md5, des, etc.)

Pregled (2)

- popis najčešće korištenih programa: sniffit, arpwatch, ettercap, ethereal, tcpdump, john, dsniff, airsnort, kismet, itd.
- aktivni tipovi napada
 - scanniranje portova:
 - fragmented, stealth (sin, fin, xmas, nul), vanilla-tcp
 - udaljena detekcija OS (verzija, patchevi, itd.)
 - detekcija i prepoznavanje servisa/aktivnih programa

Pregled (3)

- dizajn zaštite:
 - nivoi zaštite + segmentiranje zaštite
 - vatrozidi, računalni policyji (firma, grupe računala, individualna računala)
 - automatizirani IDS-ovi (firma, grupe, individualna) i sustav dojave
 - antivirusi i sl.
 - kriptografija, više razina autentifikacije, itd.

Pregled (3)

- lažno predstavljanje (scanniranje, lažne adrese - MAC, IP, arpattack, itd.) i man-in-the-middle napadi
- pronalaženje "rupovitog" softvera i korištenje istog za provalu
- tipovi DoS napada i razlozi istog
- popis korištenih programa: nmap, iptraf, nessus, hunt, itd.; razni trojani, virusi, crvi

Pregled (4)

- Firewall:
 - Check Point FireWall-1, Cisco Firewall Services Module
 - Cisco IOS Firewall, Cisco PIX
 - CyberGuard, NetScreen, Nokia IPSO
 - Secure Computing Sidewinder, Stonegate Firewall
 - Symantec Enterprise Firewall, ZoneLabs Integrity
 - ipf, netfilter, itd.

Pregled (5)

- host (filesystem) IDS:
 - Cisco Security Agent
 - Enterasys Dragon
 - Entercept HIDS
 - ISS RealSecure Server Sensor
 - Symantec HIDS
 - Symantec Intruder Alert
 - Tripwire for Server
 - AIDE

Pregled (6)

- NIDS:
 - CATOS, Cisco IDS, Cisco IDSM (Secure IDS switch blade)
 - Cisco IOS IDS, Cisco PIX IDS
 - Enterasys Dragon Sensor, ISS Desktop Protector
 - ISS RealSecure Network Sensor, LANcope Stealth Watch
 - McAfee Intrushield, Netscreen IDP
 - Network Flight Recorder, Snort NIDS
 - Sourcefire, Symantec ManHunt,
 - Tippingpoint, Tripwire NIDS
 - LaBrea

Pregled (7)

- VPN:
 - Check Point VPN-1
 - Cisco VPN Concentrator
 - Cisco VSM (VPN switch blade)
 - Symantec Enterprise VPN
 - FreeS/WAN, OpenS/WAN, CIPE
 - OpenVPN

Pregled (8)

- testovi sigurnosti:
 - eEye Retina Scanner
 - Foundstone Scanner
 - Harris Stat Scanner Professional Edition
 - ISS Internet Scanner
 - nCircle
 - Nessus Scanner
 - Qualys

Pregled (9)

- management i policy:
 - ISS Site Protector
 - McAfee ePolicy Orchestrator
 - Microsoft ActiveDirectory
- ACL i autentifikacija:
 - Cisco ACS, Cisco IOS ACL
 - FreeRadius

Diskusija!