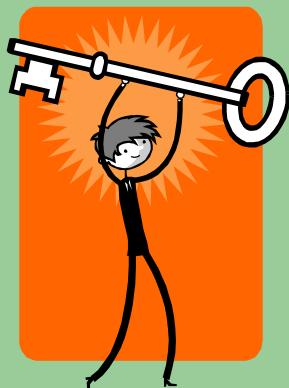


Računalna sigurnost na Internetu i lokalnim mrežama II



Verzija 1.0
Dinko Korunić, 2005.

O predavaču

- višegodišnji vanjski suradnik časopisa Mrež@, kolumna "Digitalna radionica - Linux"
- višegodišnje Unix i Linux iskustvo u dizajnu višekorisničkih mreža, postavljanju i održavanju
- vanjski suradnik SRCE-a: forenzike provaljenih sustava, predavač, itd.
- sigurnosni ekspert pri InfoMAR d.o.o.

Tijekom prezentacije

- **ako što nije jasno - pitajte i tražite objašnjenje!**
- **ako što nije točno - ispravite!**
- **diskusija je poželjna i produktivna - očekuje se vaša suradnja!**
- **podijelimo zajedno vlastita iskustva i mišljenja - predavanje nije statični materijal**

Sadržaj

- Sigurnost
 - uvod i problematika
 - uvijek aktualni problemi
- Sigurnosni pregled i testiranje
 - uvod i problematika
 - postupak pregleda
 - alati i primjeri
 - rješavanje utvrđenih problema

Sadržaj

- Sigurnosni trendovi
 - pharming, phishing
 - spam, spamming
 - problemi bežičnih mreža
 - P2P dijeljenje sadržaja

Sigurnost

uvod i problematika
uvijek aktualni problemi



Što je sigurno?

- računalo zaštićeno lozinkom?
- podaci na disku?

- E-mail (SMTP, POP3, IMAP)
- Web (HTTP)
- Instant Messenger servisi (ICQ, AIM, GoogleTalk, YAIM, MSN, itd)

Što je sigurno?

- **Bili ste na Internetu?**
- **Spojeni ste na Internet?**
- **Jeste li SIGURNI da vaše računalo nije već provaljeno?!**
- bilo koji nezakrpani Windows, Linux, Unix - provaljen u minutama nakon spajanja na Internet: automatizirani crvi, programi za skeniranje mreža, itd.

Što je sigurno?

- problem prisluškivanja, ometanja, modifikacije i ponavljanja:
 - cleartext protokoli: SMTP, IMAP, POP3, HTTP, FTP, TELNET
 - sve prolazi kao čisti test, pa i korisničko ime i lozinka!
 - najčešće postoje alternative, ali ih korisnici nisu svjesni
 - zlonamjerni lokalni korisnici
 - zlonamjerni administratori
 - zlonamjerni udaljeni korisnici - crackeri, hackeri, itd

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

Računalna sigurnost

- **kako:** kroz postojeće nesigurnosti (sigurnosne rupe) koje postoje u skoro svakom softveru bilo kao greška bilo kao zaboravljene postavke
- interdisciplinarna:
 - sistemsko i aplikativno programiranje
 - primijenjena matematika - kriptografija!
 - telekomunikacija, mreže računala, itd.

Računalna sigurnost

- sociološki problem:
 - sigurnosna politika
 - upravljanje korisnicima
 - podjela korisnika na tipove
 - procjena problematičnih korisnika
- suradnja svih sektora dovodi do kvalitetne sigurnosne politike i uspješnog provođenja iste

Uvijek aktualni problemi

- manjak edukacije korisnika:
 - loše lozinke ili odsutnost lozinki: "teško se pamti"
 - neoprezno otvaranje e-mailova: "a mislio sam..."
 - instalacija vlastitih programa: "ali treba mi..."
 - posjećivanje "opasnih" Web stranica: "imali su zanimljive stranice..."
 - posuđivanje računala: "pa samo su ga posudili na minutu"
 - korištenje sigurnosno neprikladnog softvera: "ali meni je u outlooku najlakše..."

Uvijek aktualni problemi

- manjak edukacije administratora:
 - tipovi i zaštita od svježih problema
 - kontinuirano nadograđivanje softvera i hardvera
 - analiza i razumijevanje sistemskih zapisnika
 - učenje novih i dosadašnjih tehnologija
 - ispravna sigurnosna politika - prevencija i rješavanje incidenata, kontrola, backup, definirani programi za korištenje, licence, itd.
 - zamjena nesigurnog softvera onim sigurnijim!

Uvijek aktualni problemi

- manjak ulaganja:
 - stara računala - posuđivanja
 - stari OS - sigurnosne rupe, manjak mogućnosti (kripto, etc)
 - stari hardver, mrežna oprema - nema odgovarajućih zaštita, nema enkripcije, itd.
 - malo programa - korisnici posuđuju ili koriste piratske
 - oprema za spremanje podataka i redovni backup
 - fizička zaštita!

Kako se zaštititi

- nužno koristiti moderne tehnike zaštite:
 - kriptografija u komunikaciji! SSL, IPSec, VPN
 - redovne preslike laptopa, računala, itd.
 - backup!
 - pristupne liste - minimum dozvola da se obavlja posao bez greške
 - kontrola i analiza - promatranje prometa, uočavanje problema na vrijeme, dojava, reakcija
 - zaštita svake pojedine jedinice (računala), grupe računala i naposljetku cijele organizacije

Kako se zaštititi

- minimizacija štete:
 - podjela u organizacijske jedinice/ćelije - dovoljno slične ili iste mrežne dozvole
 - svako računalo ima osobni vatrozid (bez mogućnosti gašenja), recentni i automatski (bez interakcije!) nadograđivani antivirus te sustav nadogradnje Windowsa (SUS ili WSUS)
 - redovni backupovi stanica

Kako se zaštititi

- poslužitelj:
 - minimum prava da funkcioniira ispravno
 - minimum korisnika na poslužitelju, za svakog se zna što radi i zašto je tu
 - bilježenje svih akcija
 - redundantni poslužitelji (twin poslužitelji), redundantni diskovi: LB/HA/storage clusteri
 - IDS sustavi: datotečni sustav, ponašanje korisnika, mrežni IDS, dojava

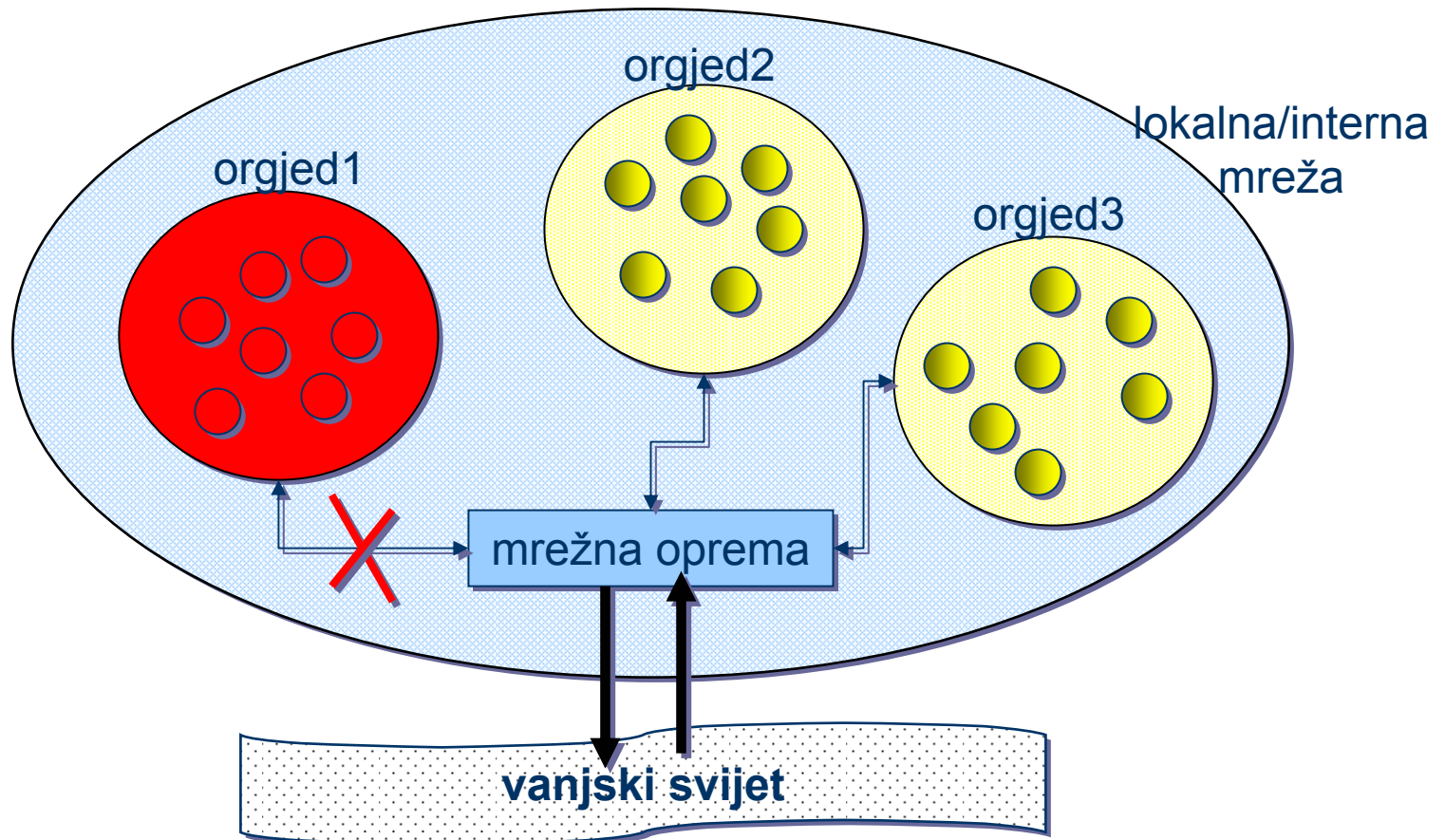
Kako se zaštititi

- mreža:
 - kvalitetna upravljiva aktivna mrežna oprema: Cisco, Juniper, 3Com, HP
 - izbjegavati nesigurne bežične mreže
 - striktna mrežna politika i odgovarajuća pravila
 - ulazni i izlazni vatrozid: port-bazirano blokiranje, filtriranje po stanju, filtriranje po tipovima aplikacije(!), antivirusno filtriranje
 - kvaliteta prometa (QoS), zabrana P2P, dojave
 - HTTP/FTP/HTTPS proxy/filter/gateway

Kako se zaštititi

- korisnici na putu ili udaljene lokacije:
 - kvalitetni VPN softver
 - VPN hardver (Cisco...)
 - X509 certifikati koji vrijede određeni period (pola godine - godinu dana)
- psihološki utjecaj:
 - objasniti i ukazati na nadzor
 - definirati odgovarajuće sankcije
 - sprovoditi iste!

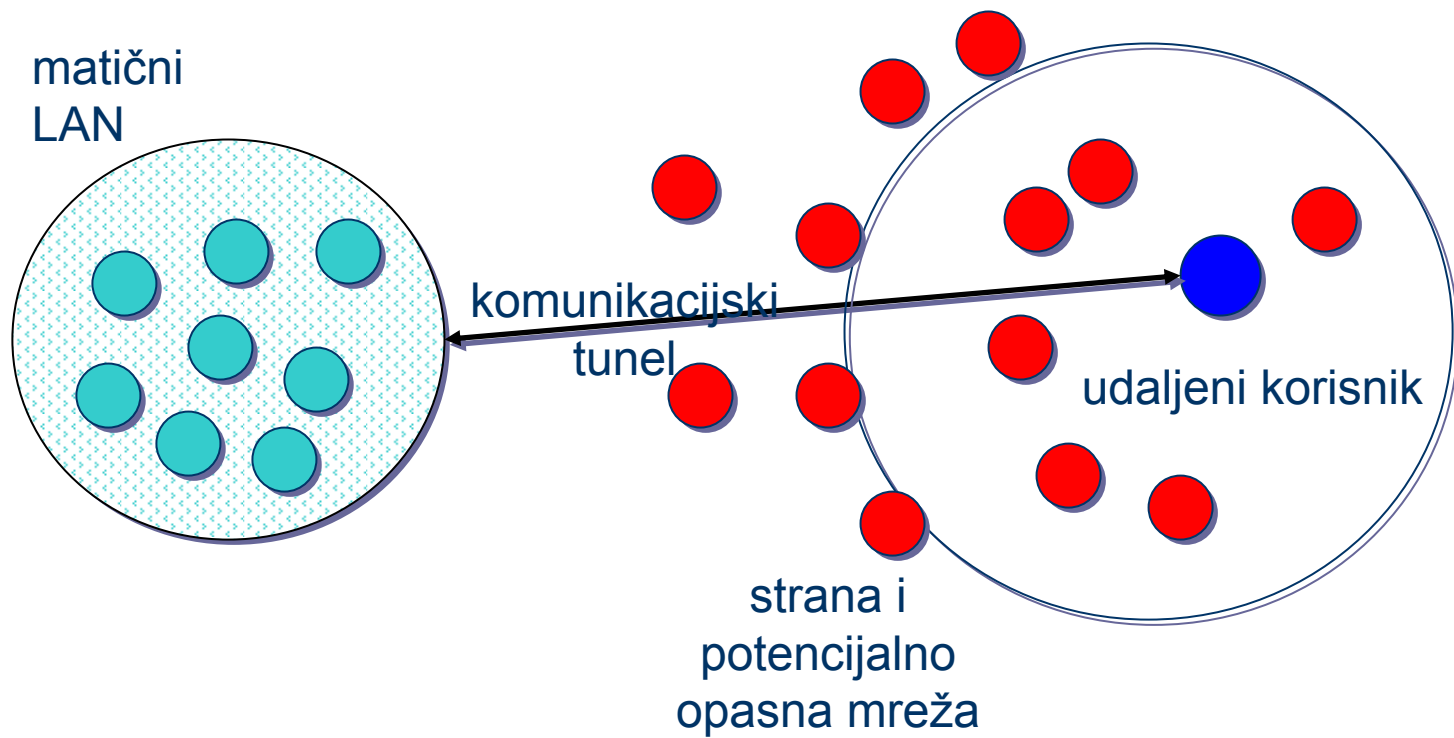
Segmentiranje mreže



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"

VPN model



"Novi" trendovi zaštite

- Microsoft AD:
 - politika zakrpa - automatski
 - antivirusna politika - automatski
 - centralno spremište: datoteke, softver, printanje
 - dvostupanjska autorizacija - potreban USB ključ, biometrija - potreban otisak prsta
- mrežna zaštita:
 - korišćenje 802.1x za autorizaciju računala!
 - alternativno Microsoft ISA klijent po računalima

Internet - raj ili noćna mora

- 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

Internet - raj ili noćna mora

- 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 - raj ili noćna mora

- 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

Exploit

- softver koji iskorištava poznate sigurnosne rupe i propuste
- promjene privilegija ili prekid rada servisa
- lokalni ili udaljeni
- tipovi: buffer overflow, integer overflow, memory corruption, format string attacks, race condition, cross-site scripting, cross site request forgery, SQL injection
- zero day (0-day) - script kiddies

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

- Internet = sjecište različitih grupacija:
 - sistemci - CERT, SANS, itd.
 - sistemci 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!

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
- zombiji, dronovi...

Najčešći problemi radnih stanica

- 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"

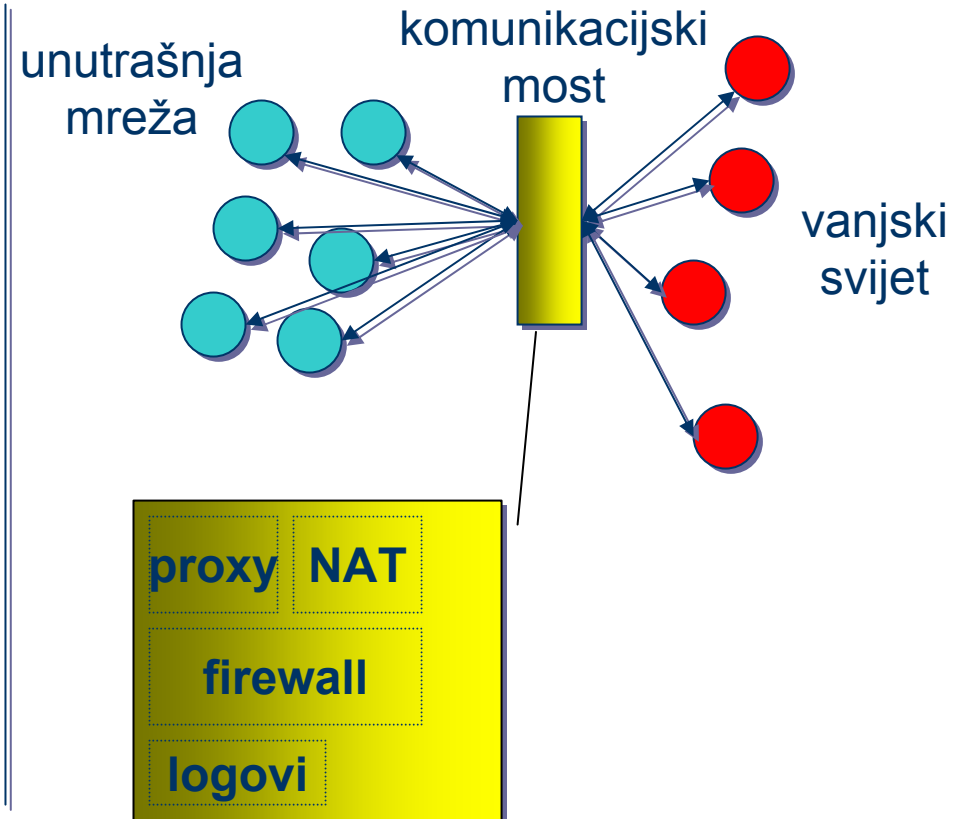
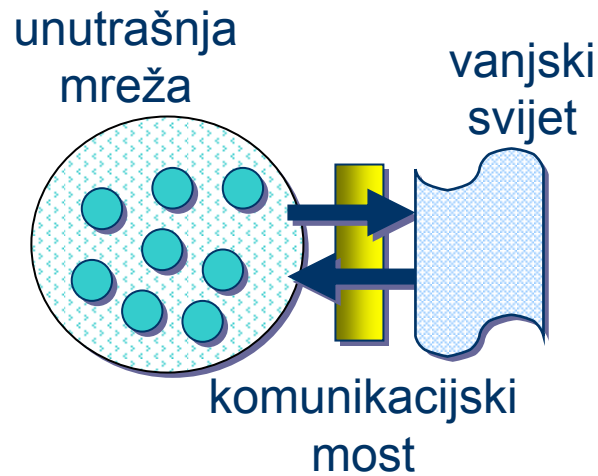
Što napraviti kad je provaljeno

- puna forenzika:
 - svi logovi sa svih relevantnih točaka
 - analiza obrisanih datoteka
 - analiza stanja sustava
 - može trajati tjednima
 - vrlo skup proces - ali obično dovodi do uzroka i saznanja dovoljno detalja o sigurnosnoj rupi

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



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

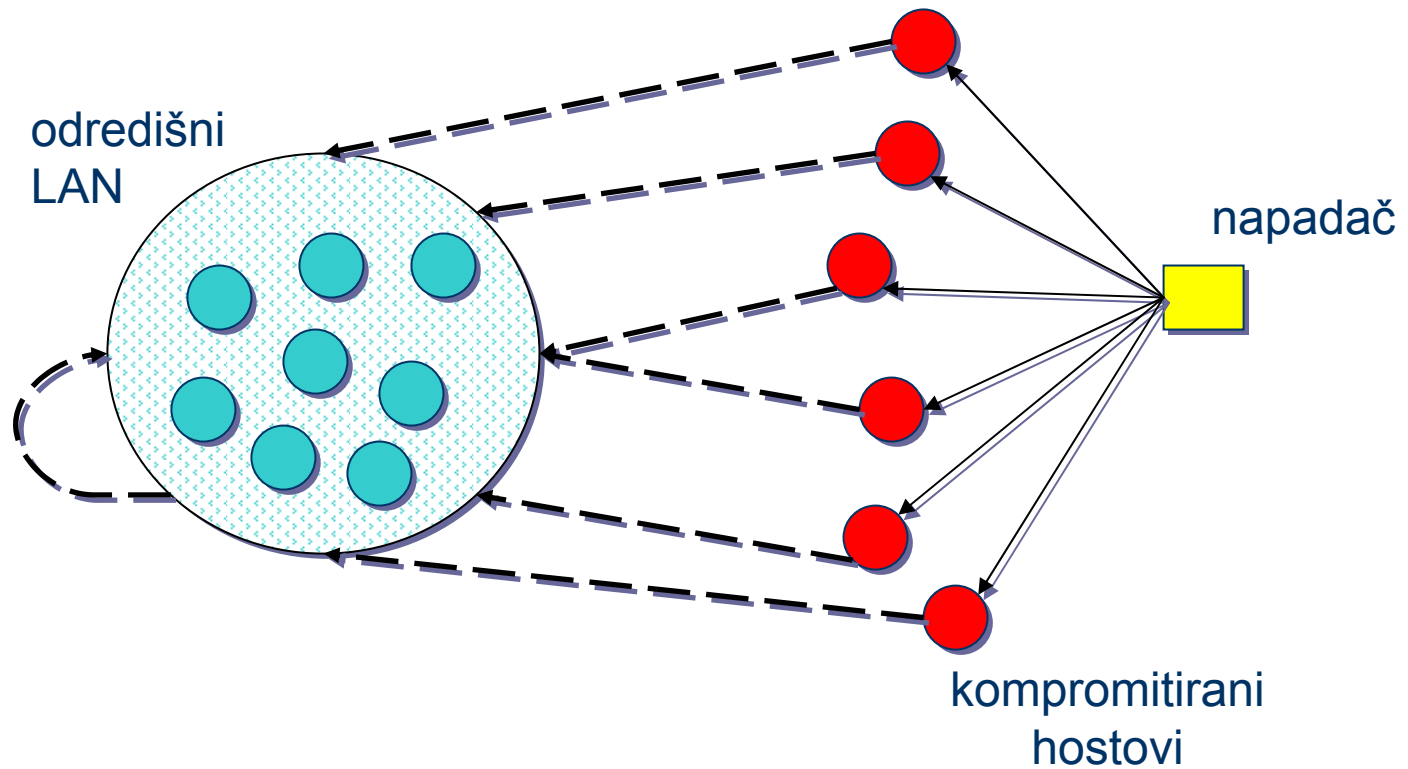
Denial of Service

- 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

- 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



Sigurnosni pregled

uvod

pregled i testiranje

alati i primjeri

rješavanje



Sigurnosni pregled

- temeljita provjera pridržavanja standarda ili nekih kriterija
 - fizička sigurnost i okolina
 - hardver i softver, infrastruktura
 - procesi i baratanje podacima, procedure
 - korisnici i njihovo ponašanje
- gdje treba popraviti, promijeniti, itd.
- automatizirani softver i ljudska ekspertiza
- obično praćena analizom i podukom

Teorija rizika

- nužno je utvrditi...
 - da se bilježe i smanje rizici
 - potencijalne rizike
 - mogućnost pojave pojedinog rizika
 - mogući utjecaj i rezultat
 - oblik mjera za izbjegavanje
 - način izrade i postavke dodatnih mjera za migraciju ako je izbjegavanje neuspješno
 - hitnost i odgovarajuće protumjere

Testovi sigurnosti

- security audit
 - procjena performansi cijelog sustava prema unaprijed definiranoj listi kriterija
- vulnerability assessment
 - pregled cijelog sustava u potrazi za potencijalnim slabostima
- penetration testing
 - niz simuliranih ili stvarnih napada u potrazi za slabostima sustava koje bi iskoristio stvarni napadač

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

- tumačenje najvažniji aspekt!
- nužno raščlaniti i temeljito upoznati:
 - odredišne 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!

Alati

- kvalitetno i komplicirano - Unix alati
- skeniranje:
 - amap, nmap - primjer
 - nessus!
- prislušivanje:
 - sniffit - primjer
 - ethereal, tethereal, tcpdump
 - p0f - primjer
- Auditor Linux distribucija

Procedura

- nužne akcije:
 - priprema = 10%
 - pregled dokumentacije i sigurnosne politike = 10%
 - intervjuji sa zaposlenicima = 10%
 - tehnički pregled = 15%
 - analiza dobivenih podataka = 20%
 - pisanje izvještaja = 20%
 - prezentacija = 5%
 - nužne završne akcije = 10%

Procedura - priprema

- analiza komponenti (računala, poslužitelja, vatrozida, aktivne mrežne opreme)
- razvoj plana skeniranja po topologiji
- minimizacija utjecaja na normalne dnevne aktivnosti
- priprema i pregled vlastitih alata - garantirana netaknutost, PGP potpisi
- koji alati? cijena, kvaliteta, platforma
- potrebno izdvojeno računalo, sigurno i fizički zaštićeno

Procedura - dokumentacija

- sigurnosna politika - važna, rijetke kvalitetno napisane:
 - jasna svima, aktualna, detaljna, kompletna
 - nužno definirati procedure i ponašanja
 - privilegije i administratora i korisnika
 - alati, programi, itd
 - bez politike - teško je znati granice pri vršenju pregleda

Procedura - razgovori

- prikupljanje informacija - svi koji su vezani fizički i virtualno za određenu lokaciju
- svi su relevantni - ne nužno tehničari ili manageri, već i standardno osoblje
- da li je politika razumljiva? čitljiva? itd.
- uzorci, tip, praksa korištenja resursa

Procedura - istraga

- početak - automatizirani alati
- pregled dobivenih logova - od alata i od poslužitelja
- pregled svih aktivnih procesa i servisa
- kritični servisi sa visokim privilegijama
- kritični servisi "viška" - slaba održavanost
- odnosi "povjerenja"
- vlastite aplikacije - nužno provjeriti, sigurno programiranje je posebna vještina!

Procedura - istraga

- aktivni test - mogući upadi, prekidi rada
- nužno isprobati odgovarajuće exploite
- istraga vrlo ovisna o veličini mreže - moguće su nužne redukcije radi dobivanja ikakvog rezultata (ključne jedinice!)
- pregled hardvera (aktivna mrežna oprema, tipovi poslužitelja, itd)
- pregled komunikacijskih protokola

Procedura - izvještaj

- ogromna količina materijala - no uvijek što kraći i razumljiviji izvještaj
- nužna edukacija čitatelja
- problemi razbijeni u individualne, pregled detalja i zaključaka + sistemski zapisnici i sl
- savjeti oko rješenja problema
- prioriteti, ključna računala
- ukupni dojam o sigurnosti, korelacija sa sigurnosnom politikom

Nessus - sigurnosni scanner

- 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)

Kratki pregled



- repetitorij, pregled
renomiranog softvera

Pregled

- pasivni tipovi napada
 - nesigurni mediji (http, smtp, telnet, ...)
 - prislušivanje (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

- 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

- 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

- 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

- 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

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

Pregled

- 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

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

Pregled

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

Pregled

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

Sigurnosni trendovi

pharming, spam
bežične mreže
p2p



Phishing

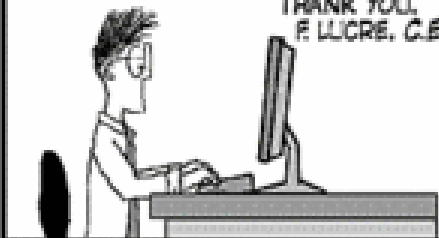
- fishing, carding, spoofing
- socijalni inženjering, krađa osjetljivih informacija:
 - lozinke, informacije kreditnih kartica
 - naizgled službena komunikacija (Email)
- najčešće mete:
 - korisnici banaka, online servisa za plaćanje
- lažni email od npr. banke i lažni link:
 - <http://www.google.com@members.tripod.com/>

Phishing

USER FRIENDLY by J.D. "Illiad" Frazer

DEAR LUCRE INTERNET BANK CLIENT,
DUE TO A MINOR BUG IN OUR BANKING SOFTWARE, WE HAVE RESET YOUR LOGIN AND PASSWORD TO BLANK VALUES. PLEASE VISIT OUR SITE AND ENTER YOUR NAME, NEW LOGIN, AND NEW PASSWORD AND YOU WILL HAVE ACCESS TO YOUR ACCOUNT ONCE MORE.

THANK YOLL,
F. LUCRE, C.E.O.



Copyright © 2001 J.D. "Illiad" Frazer. All rights reserved. www.illiad.com

stef murky ←
smurky ←
butter-parkay ←



YOU DON'T REALLY HAVE MUCH MONEY IN CHECKING, DO YOLL.

WAIT A SECOND
SOMETHING'S NOT
QUITE RIGHT..



Phishing

- danas:
 - koriste se ranjive skripte/programi od same banke/napadnutog servisa - XSS
 - sve izgleda korektno - ali link i dalje vodi na alternativnu lokaciju
- primjeri:
 - PayPal, SouthTrust
- ogroman porast incidenata!
- krađa identiteta...

Phishing



Dear SouthTrust bank customer,

Technical services of the SouthTrust bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

<https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation>

Please do not answer to this email – follow the instructions given above.

We present our apologies and thank you for co-operating.

Phishing

- rješenja:
 - edukacija!
 - dvosmjerna autentifikacija: dodatne fraze (forma lozinke), autogenerirana slika
 - dodaci na Web preglednike - prikaz IP adrese i DNS labele
 - IDN zakrpe, itd.
 - pravna rješenja

Pharming

- korištenje ranjivosti u DNS softveru
 - Bind9, Microsoft DNS
 - moderni softver - uglavnom riješeno
- modifikacija DNS labele i potencijalna redirekcija
- kopija originalnog sadržaja
- snimanje osjetljivih informacija
- primjeri: Panix, eBay.de, Hushmail
- defacement

Spamming

- neželjena pošta - uglavnom komercijalne naravi, reklame
- medij:
 - e-mail, IM, Usenet, Web pretraživači, weblogovi, SMS, itd.
- sadržaj:
 - Viagra, Cialis, pornografija, itd.
 - ugnjetavanje - potpisivanje tuđim imenom i sl.
- lažirane izvorne informacije (zaglavlje)

Spamming

ADVERTISEMENT

Inexpensive Generic Drugs from Canada. Made in state-of-the-art labs, but you don't pay for the American brand name and costly R&D and advertising costs. No doctor prescription necessary, and free shipping!

NEW! We now offer Generic **Viagra**, **Valium**, and **Xanax!**

Viagra 	Xanax 	Phentermine 	Valium 	Ambien 	Paxil 	Cialis 
--	---	---	--	--	---	--

All Categories:
Weight Loss -- **Sexual Aids** -- **Anti-Depressants** -- **Sleeping Aids**
Anti-Anxiety -- **Pain Relief** -- **Muscle Relaxants** -- **Sexual Health**

Order Now

Up to 80% Savings on Xanax, Valium, Phentermine, Viagra [HERE](#)

Spamming

- privremeni Internet korisnici za slanje:
 - lažna imena, adrese, telefoni
 - nelegalno, račun se zatvara, spammer stvara novu adresu, itd.
- SMTP protokol:
 - loše dizajniran! sigurnosni problemi
 - rješenja: autorizacija, SPF
 - detekcija i blokiranje open-relay i proxy računala
 - Greylisting!

Spamming

- sakrivanje sadržaja:
 - V1agra, Via'gra, V I A G R A, Vaigra, Viagra, Vi@graa
- kako su pronašli odredišnu adresu
 - Web pretraživači, forumi, liste
 - provaljena računala - zombiji, kupoprodaja informacija
 - inficirana virusom - posebno dizajnirani virusi
 - automatski generirane liste - rječnički napadi
 - pisani časopisi i sl

Spamming

- tehnike zaštite:
 - sadržajni filteri (Bayesian)
 - testovi na spam - SpamAssassin
 - odlaganje e-maila (Greylisting)
 - autorizacijske liste i autentifikacija
 - dinamičke crne liste (DNSRBL) - SpamCop
 - statičke crne liste - SPFilter
 - DNS zapisi (SPF)
- promjena protokola?!

Bežične mreže

- trivijalno prislušivati:
 - jeftina oprema, mali i mobilni uređaji (iPAQ + WiFi), niz postojećih aplikacija za prislušivanje (20ak poznatih)
- zaštita netrivialna:
 - 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; rotiranje ključeva

Bežične mreže

- Wardriving:
 - vožnja po gradu, provaljivanje
 - WEP128 i 64 - prikupljanje i garantirana provala
 - Connection Point - "besplatan" pristup Internetu po cijelom gradu
- popularizacija/omasovljenje:
 - zagušenje 2.4GHz spektra u narednih par godina
 - neupotrebljivost postojeće infrastrukture
 - budućnost - Motorola Canopy?

P2P servisi

- adhoc tip mreže
- nema poslužitelja, klijenata, centralnog poslužitelja ili centralnog usmjerivača
- jednakovrijedni čvorovi su istovremeno poslužitelji i klijenti
- potrebna CPU snaga i visoka propusnost
- današnji P2P uglavnom hibridi:
 - dijeljenje sadržaja - čisti P2P
 - pretraživanje i sl - klijent/poslužitelj

P2P servisi

- kapacitet/propusnost raste sa čvorovima
- failover - redundancija po mnogim čvorovima
- upotreba:
 - ogromno spremište
 - računski zadaci
 - anonimno dijeljenje sadržaja - obično ilegalnog
- poznati servisi/protokoli:
 - Freenet, BitTorrent, Gnutella, eDonkey2000, FastTrack, WinMX, DirectConnect, Napster

P2P servisi

The screenshot displays the eMule v0.42f interface. The top menu bar includes options like Disconnect, Kad, Servers, Transfers, Search, Shared Files, Messages, IRC, Statistics, Preferences, Tools, and Help. Below the menu, there are search filters for Name (Knoppix), Type (Any), and Method (Global (Server)). The main area shows search results for 'knoppix (300)' and 'open office (72)'. A table lists various files with columns for File Name, Size, Availability, Type, FileID, and Known. A context menu is open over the selected file 'Knoppix v3.3 (14-11-2003) De.iso', showing options like Download, Preview, Copy eD2K Link, and Remove Selected Search. The status bar at the bottom indicates connection details: 'Connection established on: Razorback 2', 'Users: 1.96M(0) | Files: 168.36M', 'Up: 25.0(0.0) | Down: 23.3(0.4)', and 'eD2K:Connected|Kad:Not Connected'.

File Name	Size	Availability...	Type	FileID	Known
Knoppix 3.4 Debian.iso	696.07 MB	1/1 (1)	CD-Images	2E968F7A946F178D7582D75CCF0BD131	
Knoppix 3.4 Kernel 2.6.3.iso	669.83 MB	1 (1)	CD-Images	7E7FFE74E62FA79EBA6F0F5C88264F84	
KNOPPIX auf Festplatte installieren.pdf	294 KB	3/2 (1)	Any	DDA242CBA74488036597B0B4AD363AA	
Knoppix ct-Edition.img	688.48 MB	1 (1)	CD-Images	61F43AF43F168395F8B1E0AD512D41A2	
Knoppix download.txt	130 Bytes	1/1 (1)	Any	B1944937B5A49CFDA0F46548A2DE9AA5	
Knoppix install to hard disk HOWTO.htm	10 KB	1/1 (1)	Any	4835963FCEA8DD7F59E08F4A6445A3C6	
Knoppix Linux Azur Versions.txt	3 KB	1/1	Any	D30D57945F52C2226F5EDE826E81D9E2	
Knoppix Linux POB.iso	699.16 MB	113/37 (1)	CD-Images	8F710B5562DDF788ED46164863643E7D	
Knoppix packages.txt	108 KB	1/1 (1)	Any	3CF57B699A608802E7D2DA5E78526E36	
Knoppix STD_FAQ.pdf	489 KB	1/1 (1)	Any	4A039D08050C017F2FC6005AFEC9116E	
Knoppix STD_How to Customize.pdf	500 KB	5/1 (1)	Any	524FDC55A616414DBF36CFA3F5B352B2	
KNOPPIX Systeme d'exploitation GNU-Linux.url	120 Bytes	1/1	Any	CE07D100DA3448D73141A4316788241A	
Knoppix Tutorial.zip	2.39 MB	67/40 (1)	Archive	EB804F684566036D335C58778FDD588	
Knoppix v3.3 (14-11-2003) De.iso	698.62 MB	14/9 (1)	CD-Images	FA87D5E9CDD25139A812DB18FA9DD8A1	
Knoppix v3.3-2004-02-16-Es-190204.iso	661.50 MB	19/7 (1)	CD-Images	D7F05D37C6869E3C7C29497E84137B2B	
Knoppix v3.3-Fr.iso	699.83 MB	35/10 (1)	CD-Images	19FFCDD79ESAB1F6A5DC4CC2A442F4CB	
Knoppix v3.4-2004-05-10-De.iso	688.11 MB	12/5 (1)	CD-Images	E2AF034667DE14AD9CBA446309BA3F05	
Knoppix-3.2-MB-11b.iso	653.94 MB	14/5 (1)	CD-Images	F0870A131FD4D7AF0BEF3CC16D892D04	
Knoppix-3.2-wallpaper-1024x.jpg	156 KB	2/1 (1)	Pictures	6DB0B34B37D67E2926F0E9A4AEEA78DB	
Knoppix-3.4-cdr-by-iso-top.info.iso	671.45 MB	2 (1)	CD-Images	FF208C96D621884CA153AAA8522E7571	
Knoppix-3.4-cdr.mds	50 Bytes	1 (1)	Any	C4460833ADDDDA48C2E1B15D668F3334	
Knoppix-3.4-ct-edition.iso	685.87 MB	57/27	CD-Images	658F08CB71B760B18BAE86D6011D481C	
Knoppix-34-dvd-by-iso-top.info.iso	2.13 GB	1 (1)	CD-Images	F9304E9A5E13E835796C24CA0668DC45	
Knoppix-als2000-paper.pdf	38 KB	3/2	Any	8B780E83A72381088E8BCDF940530C	

P2P servisi

- očití problemi:
 - nepotrebno trošenje propusnosti
 - opterećivanje aktivne mrežne opreme
 - nelegalni sadržaj
- manje očití, ali opasni:
 - trovanje sadržaja, virusi, malware
 - mogući DoS
 - neželjeno otkrivanje identiteta
 - spamiranje

P2P servisi

- zaštita
 - vrlo teško precizno filtriranje - koriste se proizvoljni ulazni i izlazni portovi
 - koristiti L7 analizu i regularne izraze za opis protokola - Layer7 Netfilter
 - kompletno blokiranje svega osim "dobrog" prometa
 - analiza i nadzor mrežnog prometa po IP adresi ulazno i izlazno: Netflow, Ntop, Snort

Diskusija!

