Oblast: SECURITY

Tema:

Internet napadi

Aleksandar Mirković

Koncept

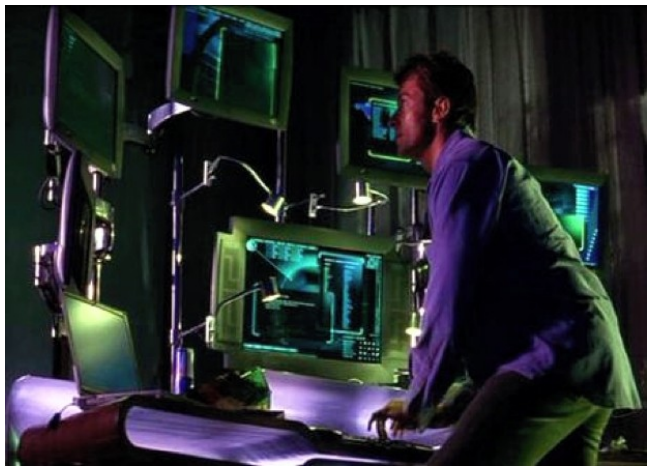
- Osnove
- Strategije napada
    - Access napadi
    - Modification napadi
    - Denial of service napadi
- Rad sa TCP/IP paketima
- Pretnje
    - Propusti (osnovni protokoli, defaultni nalozi, slabe lozinke)
    - Napadi (TCP SYN flood, null session, dns poisoning)
- Maliciozni programi
    - Virusi, crvi, trojanci,..
- Socijalni inžinjering

Napadi.. Sta? Kako? Zašto?

- Česti vojni i policijski termini

Napad nastaje kada neovlašćena individua ili grupa individua pokuša da pristupi, izmeni ili uništi vaš sistem ili strukturu..

Ko su neovlašćene individue? Hackeri..



Napadi.. Sta? Kako? Zašto?

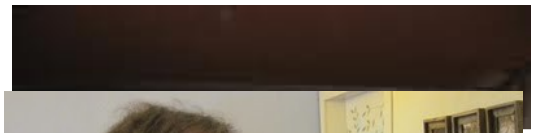
Napadi nastaju iz više razloga i na više načina..
Po izvoru mogu biti:
-Interni
-Eksterni
- Nestruktuirani (script kiddies)
- Struktuirani

Po razlogu nastanka mogu biti:
-Zabava
-Krađa, kriminal
-Politika, terorizam, rasizam
Najbitnija podela je po cilju koji imaju:
-Access napadi
-Modification napadi
-Denial of service

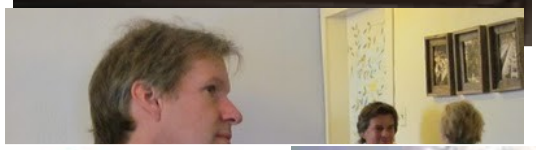
Access napadi – neovlašćeni pristup

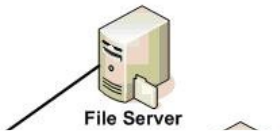
Potraga za informacijama koje će obezbediti pristup nekim podacima ili delovima sistema..
-Interni
-Eksterni

Dumpster diving



Eavesdropping





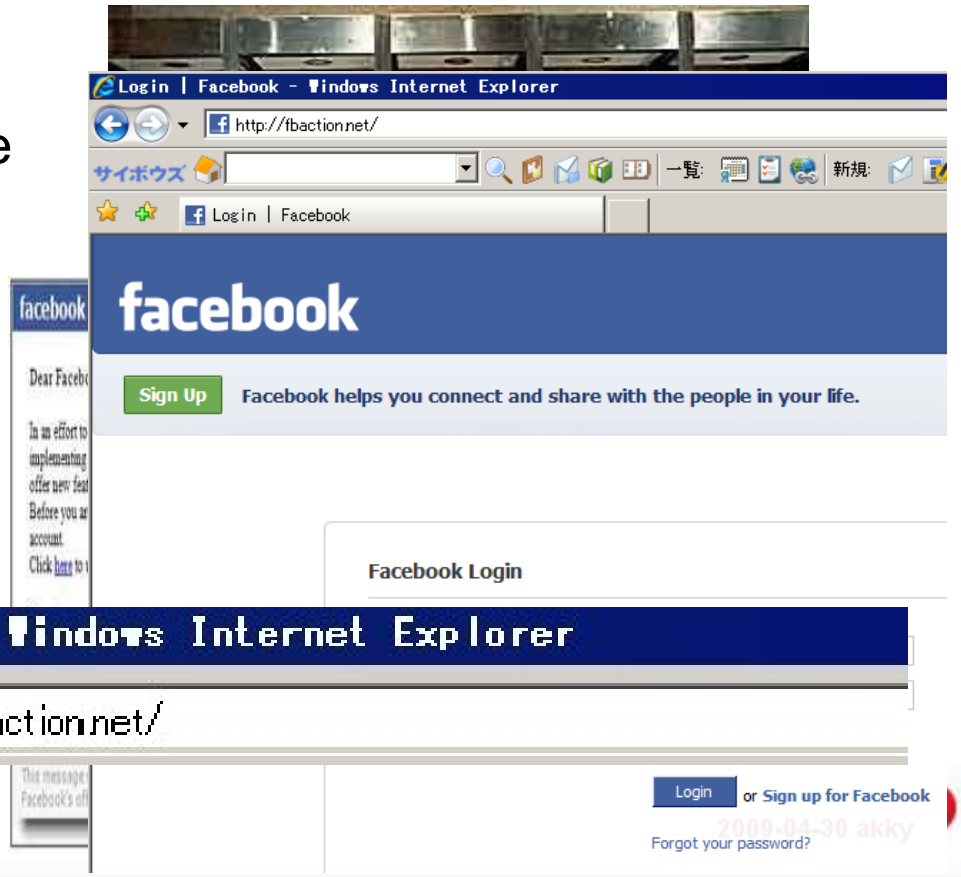
Snooping

Interception
-Pasivno (network monitori)
-Aktivno (Man-in-the-middle, FBI..)

Modification napadi – izmene, dopune

Modification – izmene, dopune, brisanje podataka

-Zero Cool i Acid Burn
-Popravljaje ocena, lažiranje broja kartice



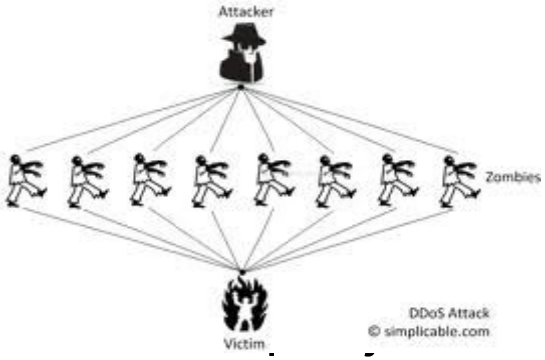
Repudiation – lažno predstavljanje

-Lažni mailovi, lažno predstavljanje
-Lažna logon strana, facebook

Denial of Service

DoS – Denial of Service – onemogućavanje korišćenja resursa
-e-komerca, sajtova (Amazon, Microsoft)

DDoS – Distribuirani Denial of Service
-Napad se pokreće sa više lokacija istovremeno ka jednom ciljanom serveru
-Botnet-i i Zombi-i



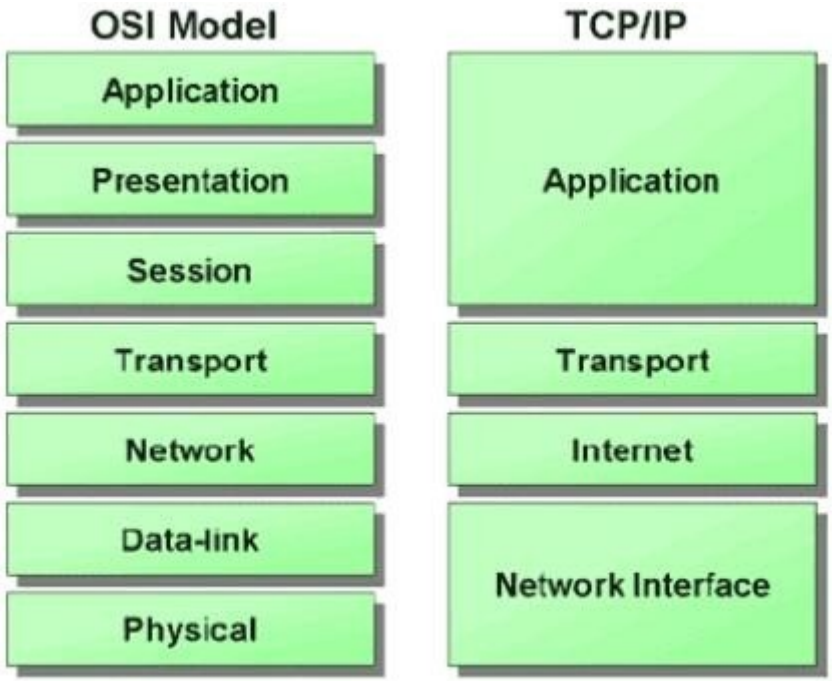
Napadaju se: informacije, aplikacije, sistemi, komunikacija
TCP SYN flood, Pingfo Death, Buffer overflow

Najveći DDoS napad – novembarski napad na Azijsku e-k
- Preko 250k Zombia, preko 15k konekcija u sekundi, preko 45Gb protoka

Rad sa TCP/IP paketima

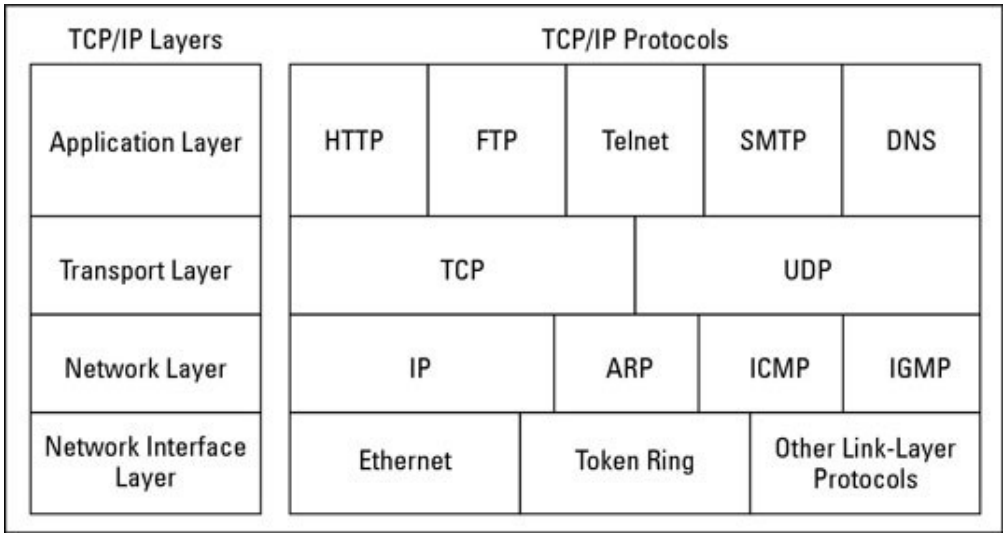
TCP/IP je protokol koji, organizacijama koje imaju potrebu da povežu veliki broj uređaja sa različitim OS-ima i na različitim platformama, pruža mogućnost da to urade relativno lako i budu sigurni u njegovo funkcionisanje dugo..

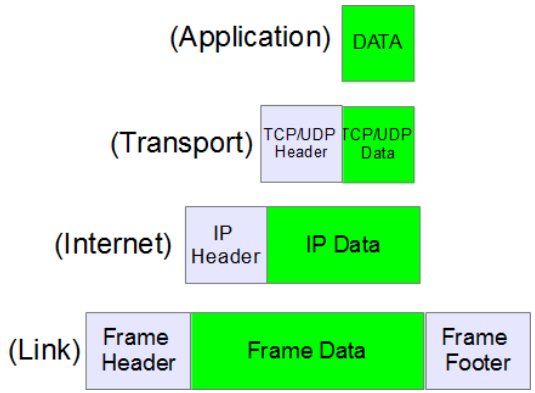
Veliki broj rupa i mogućih propusta vezano za TCP/IP se pojavljuju baš zbog njegove dugovečnosti, ogromne dokumentacije i lake upotrebe.
Dobar deo tih rupa se mogu lako zatvoriti ali je neophodno znati kako TCP/IP funkcioniše i kako paketi putuju.

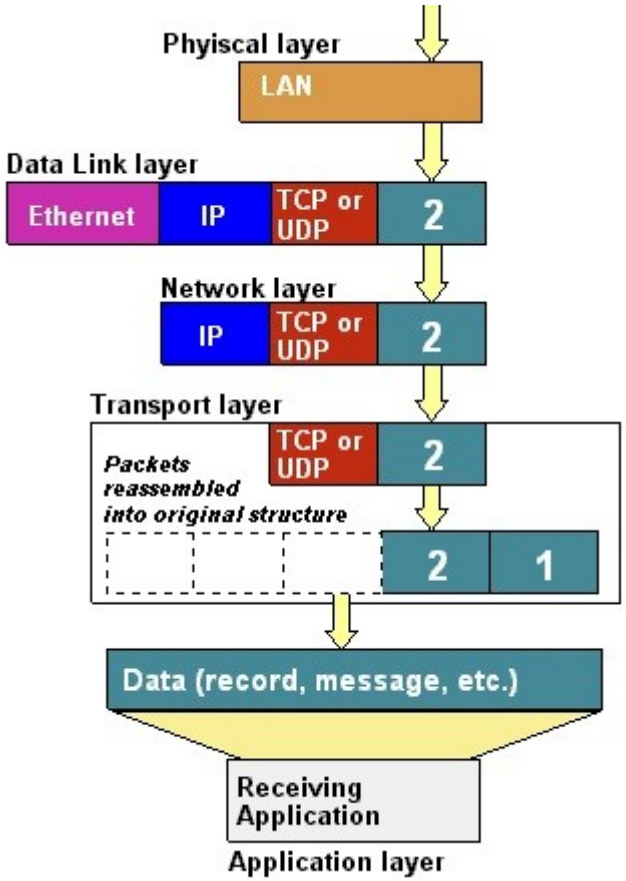


TCP/IP and the OSI model

Rad sa TCP/IP paketima







Rad sa TCP/IP paketima

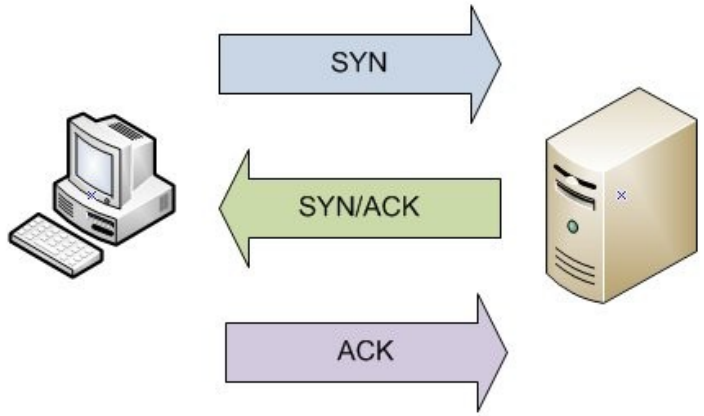
Portovi – softverski zadat kanal kojim komuniciraju aplikacije putem računarskih mreža.

Cilj: razlikovanje, identifikacija, praćenje saobraćaja.

Protocol	Port	Protocol	Port
FTP	20, 21	NNTP	119
SSH, SFTP, SCP	22	IMAP	143
Telnet	23	SNMP	161
SMTP	25	LDAP	389
TACACS	49	ISAMP (VPN)	500
DNS	53	Syslog	514
TFTP	69	LDAP/TLS	636
HTTP	80	L2TP	1701
Kerberos	88	PPTP	1723
POP3	110	Remote access	3389

Three-way handshake

Klijent šalje SYN (TCP segment koji sadrži Initial Sequence Number)
Server odgovara, šalje SYN (koji sadrži ISN i vrednost rezervisanu u bufferu za konekciju)
Klijent šalje ACK (sa podacima buffera servera)



Propusti

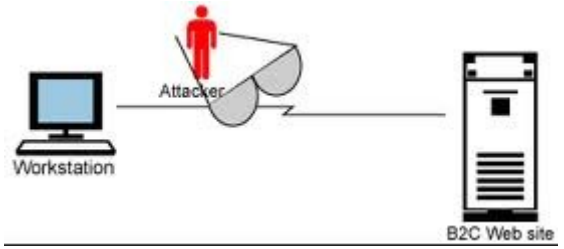
Standardni protokoli (programi, servisi)
•telnet --- SSH (enkripcija, VPN) – Putty
•HTTP --- SSL/TLS (sertifikati)
•NTP --- NTPv3 (autentifikacija)
•SNMP --- SNMPv3 (3DES, AES)
Isključivanje protokola, servisa koji se ne koriste..

Slabe lozinke
•Šta su slabe lozinke
•Šta su i kako je formiraju jake lozinke
•Polise i pravila za formiranje i čuvanje lozinki

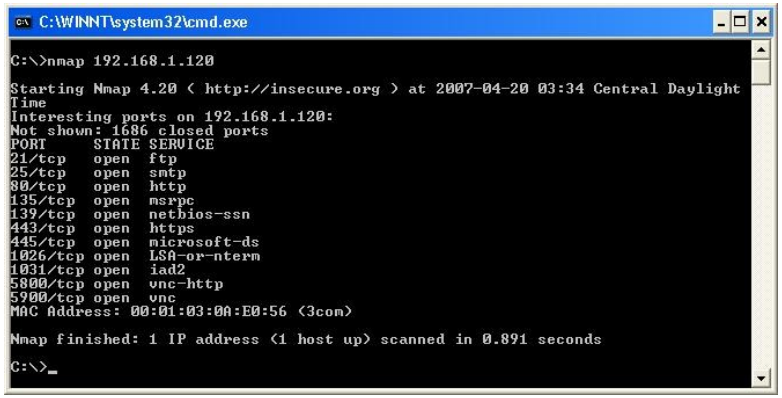
Defaultni nalozi
•Administrator, Root, SA
•SYSTEM

Prikupljanje informacija

Sniffing –uhvatiti i protumačiti mrežni saobraćaj
-Mrežne karte preuzimaju samo pakete namenjene tim računarima
-Dosta mrežnih kartica se mogu prebaciti u tzv. promiscuous mode
-Ruteri mogu da dele mreže u LAN i VLAN
-ARP spoofing (L2) , IP spoofing (L3)
-SystemManagementServer, Wireshark



Port scaning –
-Većina sistema ostavlja otvorene portove
-Na mnogim sistemima rade aplikacije ovog tipa bez znanja vlasnika

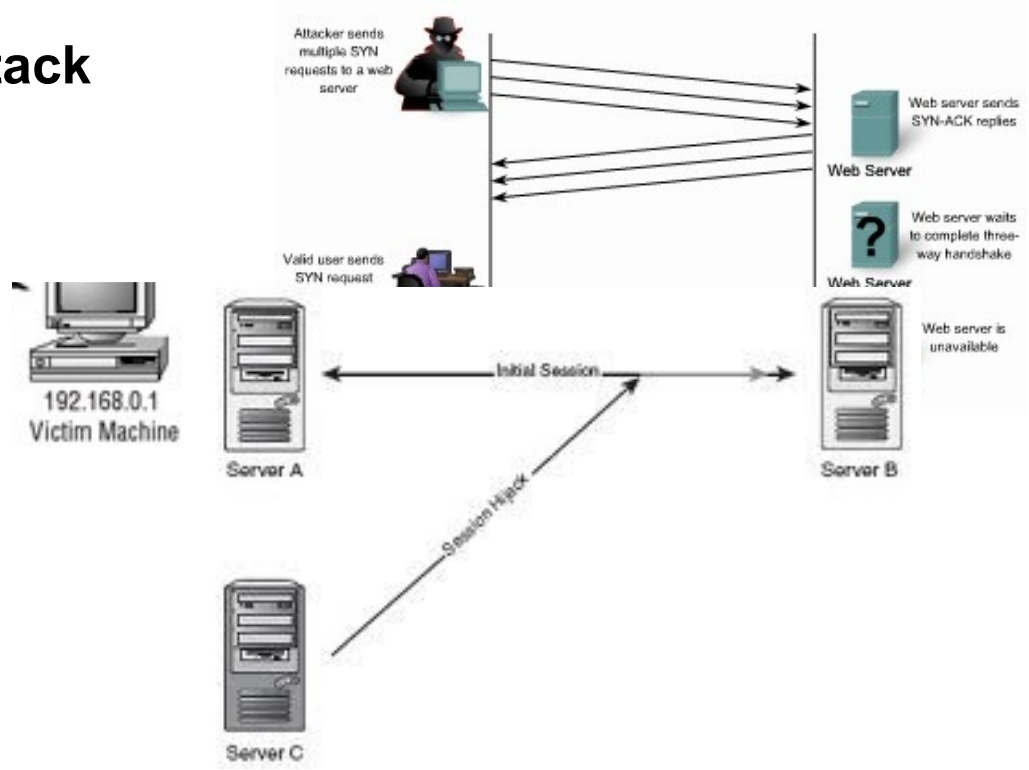


Napadi

TCP SYN ili TCP ACKflood

TCP Sequence number attack

TCP/IP Hijacking
Man in the middle



Napadi

Null Session

```
net use \\IP address_or_host name\ipc$ "" "/user:"
```

- Najveća Windows ranjivost svih vremena
- SMB (server massage block) ranjivost – File and Print shareing
- Povezivanje preko IPC$ share-a
- Odnosi se na NT4 i 2000

Replay

- Uzeti podatke sa mreže pomoću sniffer alata i koristiti ih za lažno predstavljanje i sl.
- Najčešće se traže lozinke, digitalni potpisi..
- Zaštita:
  - korišćenje CHAPv2 (šalje hash + proizvoljni broj)
  - IPSec

Napadi

Domain name kiting

- Više prevara nego pretnja
- Koristi se 5 dana period registracije domena za koji ne treba platiti
- Registruju se na hiljade domena i sajtovi pune reklama
- Uključuje i preotimanje domena većih kompanija.

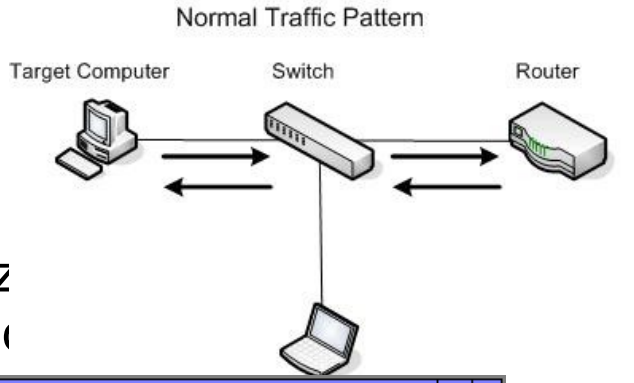
DNS poisoning

- Trovanje se može javiti na raznim aplikacijama i uređajima
    - Ruting tabele, ARP cash, DNS..
- Redirekcija DNS-a na DNS ciljanog domena
- Redirekcija DNS-a na DNS bilo kog domena
- DNS Forgery – vraćanje odgovora na upit pre pravog DNS-a

Napadi

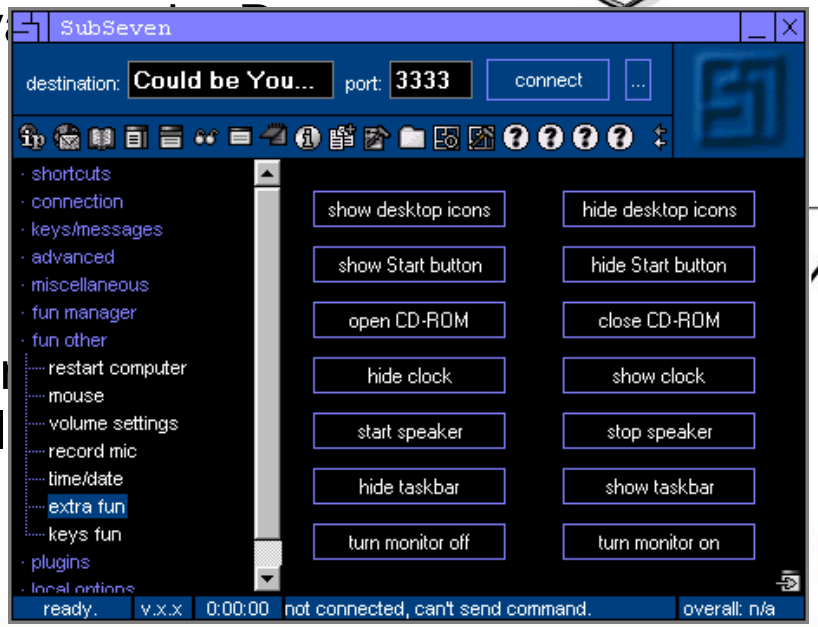
ARP poisoning

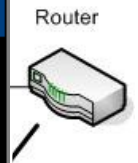
ARP – Adress Resolution Protocol
-IP --- MAC mapiranje
-Veliki broj uređaja može da primi ARP odgovor i bez
-Napad uključuje dodavanje novih zapisa u cash ure
-Cilj može biti, lažno predstavljanje, zav



BackDoor

Zadnja vrata – uvek otvorena ako treba
-Subseven, NetBus, Master Paradise
-Koriste se za krađu, nanošenje štet ili i
-Najčešće ih nose trojanci, freeware apl
-Deo koda neke aplikacije





Maliciozni programi

Virusi

Virus je program, napravljen da napada računarske sisteme..
Može da: ne radi ništa, ošteti podatke, uništi OS, i širi se dalje

-**Armored virus** – zaklonjeni štitom od koda koji zaustavlja debugere
Uglavnom jedan deo koda odvlači skenere u pogrešnom smeru dok se virus krije negde drugde..
-**Companion virus** – lepe se za normalne programe i pretvaraju u program istog imena, a često menjaju pointere u registry-u kako bi upućivali korisnike na sebe
-**Macro virus** – Word, Excel macro-i
Koriste ranjivost mini-Basca ili samog Office-a
-**Multipartite virus** – Napada žrtvu na više nivo..
Napada BOOT sektor, exe fajlove, aplikacije, dokumenta

Maliciozni programi

- **Phage virus** – modifikuje i menja programe i baze
  Jedini način da se ukloni je da se preinstaliraju svi ugroženi programi..
- **Polymorphic virus** – menja oblik u nameri da ostane neopažen
  Uglavnom kriptuje delove koda da bi otežao antivirusima .. Mutira
- **Retro virus** – napada ili zaobilazi antivirus – a
- **Stealth virus** – maskira se u normalnu aplika
  Može da lažira veličinu fajla u kome je, da se

Trojanci

Prenose se koristeći druge programe
Mogu biti u okviru attachment-a, ili deo nel
Može da napravi backdoor, igra ulogu drug i zadatak
Mogu biti prisutni na sistemu dugo, bez zn

Maliciozni programi

Logičke bombe

Programi ili delovi koda koji se izvršavaju u određeno vreme ili nakon neke druge radnje.
Mogu obaveštavati napadača kada je računar ili servis dostupan, kada je korisnik ulogovan.
Mogu izvršiti samouništenje u određenom trenutku ili pod određenim okolnostima..

Crvi

Crv je samostalan.. Nije mu potreban program za koji će se zakačiti, može da sadrži i prenosi viruse, i može se samostalno razmnožavati..
Dobar deo virusa koji su preplavili medie su ustvari crvi..
-Conficker , I love you..
-Nachi

Socijalni inžinjering

Socijalni inžinjering je proces manipulacije kojim se ljudi navode da odaju poverljive informacije o sebi.
Ta tehnika zasniva se na ometanju pažnje određenog lica u cilju prikupljanja informacija koje ono inače ne bi odalo, a kako bi se ti podaci kasnije zloupotrebili..

Primer

KRAJ

Hvala na pažnji !