Oblast: SECURITY

Tema:

Internet napadi

Aleksandar Mirković

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:

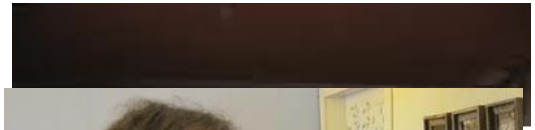
-Access napadi
-Modification napadi
-Denial of service

Access napadi – neovlašćeni pristup

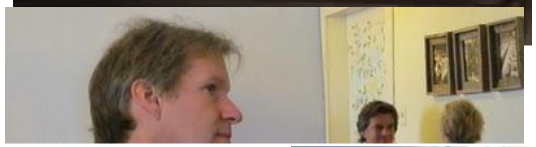
Potraga za informacijama koje će obezbediti pristup nekim podacima ili delovima sistema..

- Interni
- Eksterni

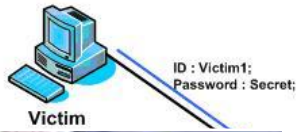
Dumpster diving

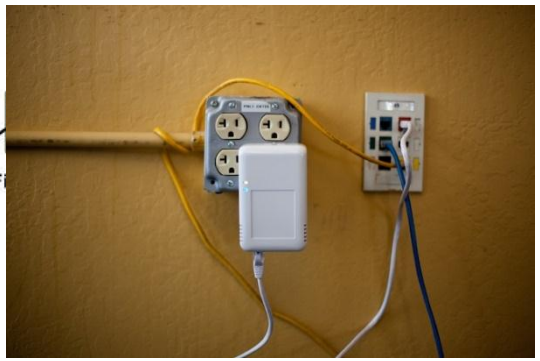


Eavesdropping



Snooping





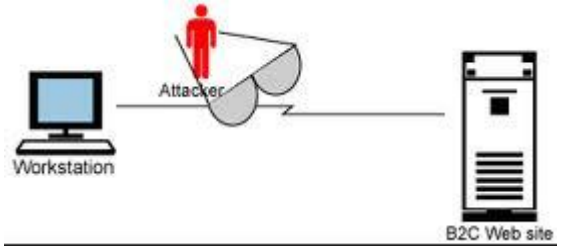
Interception

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

Prikupljanje informacija

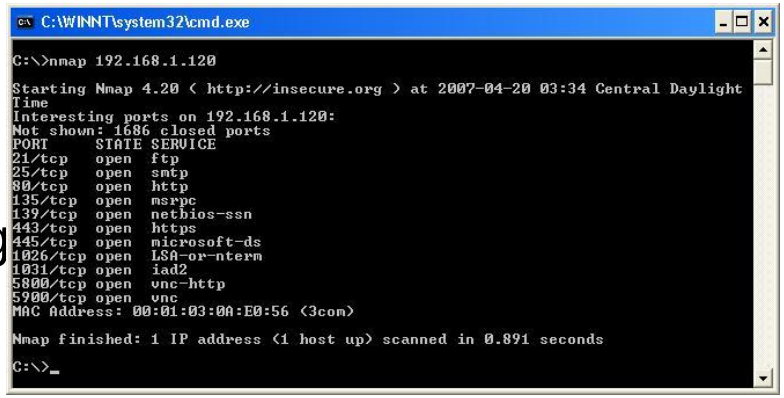
Sniffing –uhvatiti i protumačiti mrežni saobraćaj

- 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 –

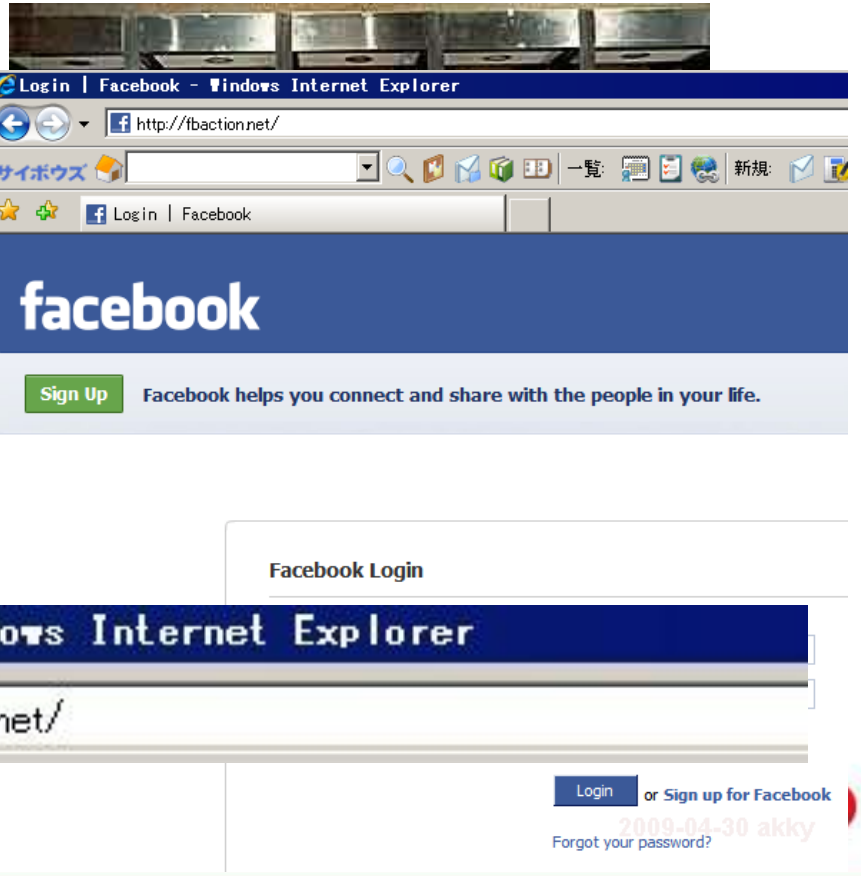
- Većina sistema ostavlja otvorene portove
- Na mnogim sistemima rade aplikacije ovog tipa bez znanja vlasnika



Modification napadi – izmene, dopune

Modification – izmene, dopune, brisanje podataka

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



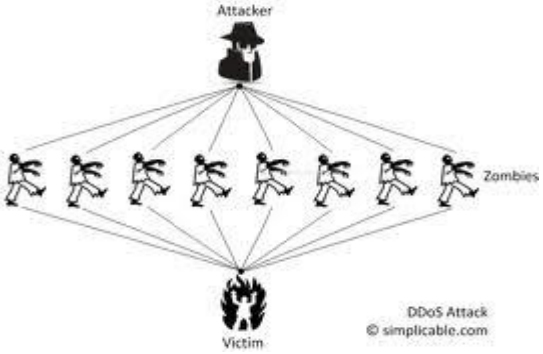
Repudiation – lažno predstavljanje

- 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-komerc kompaniju
- Preko 250k Zombia, preko 15k konekcija u sekundi, preko 45Gb protoka

Koncept napada

Vulnerability – ranjivost – slabost koja omogućava napadaču da upadne i ugrozi sigurnost sistema

Exploit – kod koji omogućava napadaču da iskoristi ranjivost sistema

Payload – kod koji napadač pokreće na sistemu koji je uspešno eksploatisao.

Koncept Napada

Exploit + Payload

Podaci + …

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.

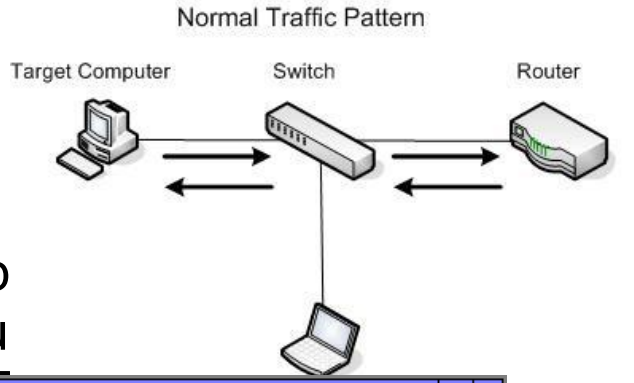
DNS poisoning

- 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

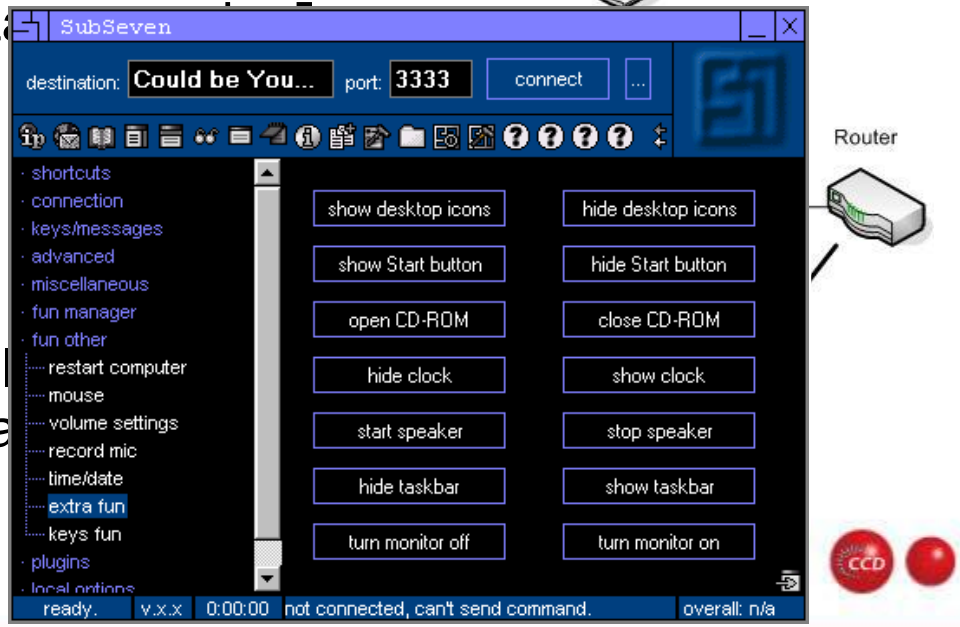
ARP poisoning

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



BackDoor

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



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 !