Mrezna sigurnost

Vrste prijetnji
- presretanje, prisluskivanje
- prekidanje, uskracivanje
- promjena (tampering)
- umetanje, ponavljanje
- lazno predstavljanje, maskiranje
- covjek u sredini, MITM

Lokacije ranjivosti
- fizicka
- protokoli
- implementacije
- konfiguracija i koristenje

ARP protokol
- 32-bitni IP -> 48-bitni MAC
- ranjivost
  - moguce poslati arp reply prije pravog racunala sa nekom mac adresom
  - prisluskivanje - preusmjeriti promet
  - dos – preslikavanje u nepostojecu mac adresu
- otkrivanje
  - provjera arp cachea

IPv4 protokol
- ip zavaravanje (ip spoofing)
  - slanje lazne adrese posiljatelja
  - najcesce za (d)dos
  - zastita
    - filtriranje adresa
    - zabrana autorizacije
- ip fragmentacija
  - ping of death
    - prevelik ip paket (> 65535 okteta)
    - buffer overflow, kernel panic ili slicni problemi pri defragmentaciji
    - kriva implementacija
  - teardrop (stari linux kernel)
    - opet svastarije sa fragmentacijom i problemima sa defragmentacijom
    - buffer overflow, kernel panic
    - kriva implementacija
  - tcp overwrite
    - zavaravanje vatrozida
    - prvi fragment ima dozvoljen port u headeru
    - drugi fragment ima zabranjen port u headeru, ali se propusta jer je nastavak prvog
    - datagram ce zavrsiti na zabranjenom portu
    - pogodi tko je ovdje kriv

ICMP protokol

- internet control message protocol
- generalno (d)dos
- icmp redirect sluzi da ruter obavjesti drugo racunalo o boljoj ruti za slanje
  - moze se zlorabiti za dos, preusmjeravanje
- skrivanje payloada u ping porukama (skriveni kanal)
- slanje pinga na broadcast adresu
  - napad smurf
    - ping na broadcast adresu sa laznom izvornisnom adresom
    - zrtva ce dobiti odgovor od svih racunala u mrezi

DHCP protokol

- problemi
  - nema zastite
  - lazni dhcp serveri
  - bilo tko moze slati dhcp poruke
    - iscrpljivanje adresa – dhcp starvation

Ipv6 protokol

- 128-bitne adrese
- fragmentacija se ne provodi u mreznom sloju
- arp se ne koristi
- otezano je skeniranje mreza
- specificne ranjivosti
  - samostalno podesavanje adrese
  - problem velikog adresnog prostora
  - viseodredisne adrese
  - zloupotreba mehanizma DAD (douplicate address detection) za dos
  - nedostatak operativnog iskustva
  - automatsko tuneliranje (komunikacija ipv4 i ipv6)

UPD protokol

- udp spoofing
- udp hijacking
  - odgovaranje na zahtjev prije posluzitelja + udp spoofing
- udp storm/flood
  - napadac posalje zahtjev za neki udp small service sa laznom izvorisnom adresom i portom
  - lazni adresa i port odgovaraju nekom udp small servicu na drugom posluzitelju
  - sada ce ova dva racunala uci u beskonacnu petlju odgovora i zahtjeva
  - radi jer udp ne zahtjeva nikakve potvrde ni rukovanje
  - zagusivanje mreze
- udp aplification
  - slicno kao udp flood, ali ideja je da su odgovori puno veci od zahtjeva
  - primjeri protokola:
    - dns, ntp (network time protokol), snmp
  - zagusivanje mreze

TCP protokol

- tcp syn flood
  - napadac zapocinje otvaranje tcp konekcije i drzi ih tako poluotvorene
  - dopusten samo odreden broj takvih veza
  - zastita
    - syn cookie – stanje se rekonstruira iz zavrsnog odgovora, a ne stvara na prvom slanju

Otkrivanje aktivnih portova

- tcp
  - tcp syn skeniranje
    - syn ack znaci da aplikacija slusa
    - rst znaci da na portu nema aplikacije
  - tcp fin skeniranje
    - segment sa fin zastavicom
    - ako nema nista na portu vraca se rst
  - skeniranje fragmentacijom
    - otezava detekciju skeniranja
- udp
  - slanje praznog udp
    - ako je port zatvoren salje se icmp port unreachable
    - ako je otvoren ne salje se nuzno odgovor
  - problem za napadaca
    - udp nepouzdan
    - OS nekad ogranicava broj icmp poruka u sekundi
- generalni problemi za napadaca
  - velik broj portova po cvoru
  - potencijalno velik broj cvorova
  - moguce da postoji neki filter (firewall)
  - iz porta ne mozemo zakljuciti puno o aplikaciji

Otkrivanje aplikacija

- poznavanjem verzije aplikacije i os-a moze se pripremiti za napad
- problemi za napadaca
  - aplikacija ne javlja svoju verziju

Otkrivanje OS-a

- snimanje ponasanja mreznog stoga

Brute force napadi

- ranjive sve usluge koje omogucavaju prijavu putem mreze
  - telnet, ftp, ssh...
- zastita
  - entropija lozinke, ispravna pohrana
  - ogranicavanje pristupa usluzi
  - ogranicavanje broja pokusaja
  - bolje autentifikacijske metode

Koristenje nesifrirane komunikacije

- snimanje prometa -> bad\

- zastita
  - sifriranje na nizim slojevima
  - tuneliranje kroz ssh ili slicne metode

SSH protokol za udaljeni rad

- teski gas
- ssh transport layer protocol
  - dogovor oko koristenih kriptografskih algoritama
  - prilikom prvog spajanja radi se provjera sazetka posluziteljskog kljuca
  - ~/.ssh/known_hosts
- podrzane autentifikacije
  - username & pass
  - asimetricna kriptografija
  - svasta nesto drugo (kerberos)
- usluge temeljene na ssh
  - scp, sftp
- problemi
  - nezasticen tajni kljuc
  - popis racunala i kljuceva
  - zahtjevna promjena i povlacenje kljuceva

DNS protokol

- svrha napada
  - sprjecavanje pristupa, preusmjeravanje
  - MITM ili podmetanje laznih sjedista
  - preuzimanje domena
- prijetnje
  - presretanje paketa, MITM – odgovor na dns upit je jedan udp paket
  - ne MITM – slicno kao gornji napad, ali napadac pogada podatke koje bi inace znao da je MITM
  - name chaining, cache poisoning
    - iz dns odgovora se cachira adresa napadacevog servera za buduce upite
  - betrayal by trusted server
- zastita
  - mehanizam TSIG
    - djeljeni kljuc, generira se potpis odgovora
  - DNSSEC
    - osigurava kriptografski dokaz ispravnosti primljenih podataka
    - isto ima neki potpis
- raspodjela sigurnosno osjetljivih podataka
  - distribucija javnih ssh kljuceva
- autorizacija i autentifikacija na temelju imena domene

Sustavi za detekciju upada

- pracenjem ponasanja sustava ili prometa moze se detektirati incident
- nacini rada
  - pravila
  - detekcija ponasanja ili anomalije
- mjesta nadzora
  - mrezni (NIDS)
  - racunalni sustavi (HIDS)