INFORMATIKAI BIZTONSÁG

Számítógépes rendszerek biztonsága

Készítette: Lengyel Csaba lengyi84@chello.hu (október 20.-21.-ei előadás alapján)
Forrás: Mátó Péter mato.peter@andrews.hu, Honlap: www.fixme.hu
Tematika: http://www.fixme.hu/nyiregy_compsec_2006.html

Ez csak egy kis segítség a tanuláshoz, ha többet akarsz tudni az adott témáról keress rá a neten, olvass utána, vagy írj Mátó Péternek.
A dokumentumban előforduló esetleges hibákért felelősséget nem vállalok, ha van ilyen jelezd!

Leggyakoribb alkalmazás-protokollok:

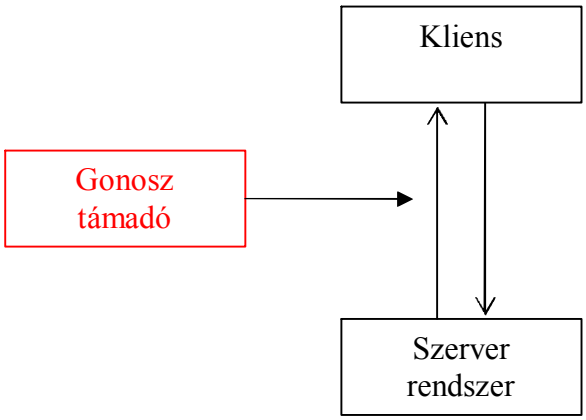
- http, https
- ftp, nfs, smb, nmb
- smip, pop3, imap
- domain
- ntp
- ldap, ocsp

Hálózatok építőelemei:

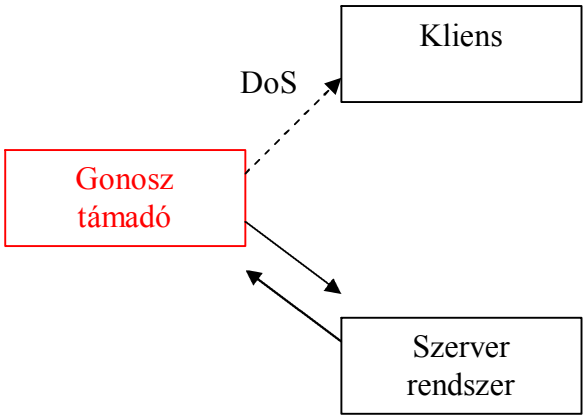
- HUB (repeater-jelismétlő)
- Switch (bridge-híd)
- Router (útvonal-választó)
  Layer.3 – IP cím szerint

Támadási típusok:

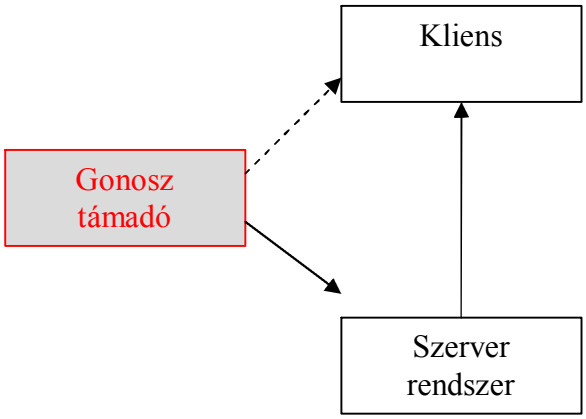
Sniffing:



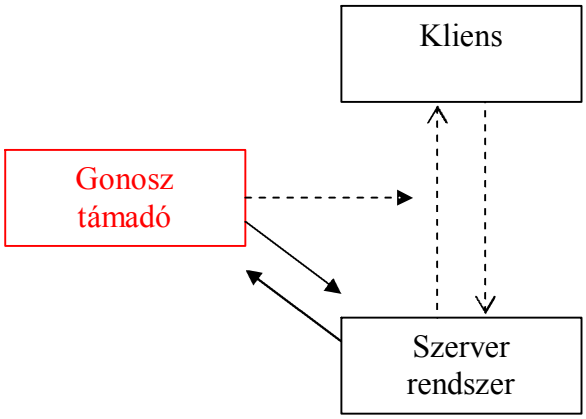
IP spoofing:



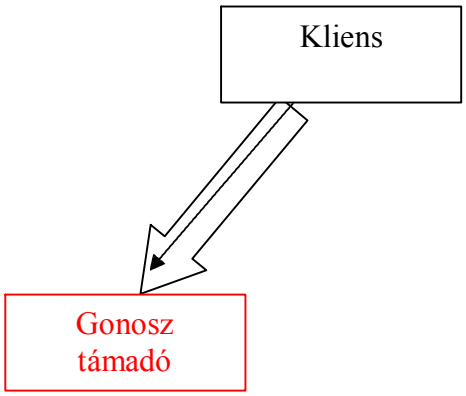
Blind spoofing:



Session hijacking:



Covert channel:
(port forward, socks forward,…)



Smurf attack (ICMP támadás)

Támadások fajtái és eszközei:

- hagyományos megoldások (social engineering)
- hálózati támadások
- erőmegoldások (brute force)
- szoftver támadások (exploit)
- szolgáltatás megbénítása (DoS, DDoS)

Megelőző intézkedések:

- oktatás
- szolgáltatások szűrése
- helyes beállítások
- folyamatos frissítés
- naplóelemzés
- fingerprinting
- erős azonosítás
- titkosítás
- előtétek (wrappers)
- jail-ek
- csomagszűrő
- alkalmazás tűzfalak

NetFilter (Linux beépített csomagszűrő)

- Megfelelő hozzáértéssel nagyon jól használható

Tűzfalak

Tűzfalak típusai:

- csomagszűrő (packet filter)
- állapottartó csomagszűrő 8stateful p.f.)
- protokoll szűrő (application level firewall)
- moduláris protokoll szűrő (modular a. l. f.)

A tűzfalak általános tulajdonságai.

- átlátszó működésre képes (transzparens)
- robosztus legyen (THA)
- a lehető legtöbb hálózattípust támogassa
- tegyen lehetővé erős authentikációt
- finoman hangolható legyen
- költséghatékony legyen
- tegyen lehetővé titkos csatornázást (ssl, ssh, port fw)
- legyen VPN megoldás
- legyen benne IDS
- tudjon riasztást küldeni önállóan
- támadások ellen erősen védett
- legyen hatékonyan menedzselhető

Tűzfalak típusai részletesen

Csomagszűrő tűzfalak

Előnyei:

- nagy sebesség
- egyszerű szabályok
- olcsó (BSD_v_Linux)

Hátrányai:

- nem tud semmit a protokollról
- összetett szabályrendszer (nehezen követhető, javítható)
- megtéveszthető

Állapottartó csomagszűrő:

Előnyei:

- nagy sebesség
- mind a kapcsolatra, mind a protokollra vonatkozó információkat ismeri
- protokoll szinten is be tud avatkozni

Hátrányai:

- nagy állapottér → hibalehetőségek

- megtéveszthető

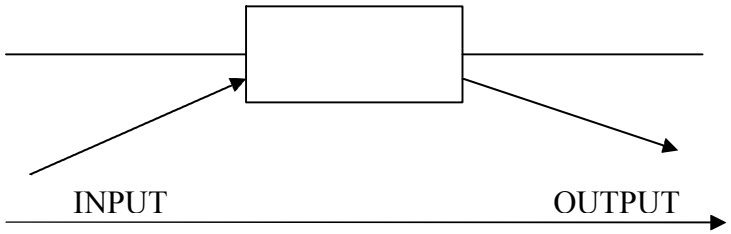
Protokollszűrő tűzfalak:

Előnyei:
- finoman hangolható
- skálázható

Hátrányai:
- nem gyors
- keveset tud a kapcsolatról
- tartalomszűrés nehézkes
- mindent gw-ben implementálni kell bizonyos funkciókat
- szinkronizáció nehézkes
- szinkron miatt csak részleges HA

A NetFilter

Fail-safe



DAC (Discretionary Access Control)
- chroot /mechanizmus/
- naplózásnál az aktuális UID

Posix.1e, 2c
- Access Control List
- Capability

MAN (Mandoatry Access Control)
MLS (Multi Level Security)

LMS rendszer (Linux Security Modul)
- Lehetővé teszi különböző biztonsági rendszerek illesztését a Linux maghoz
- A fontosabb hozzáférési pontokon hook-ok vannak.