Upaya Pengamanan

- Resiko: kemungkinan attacker masuk ke sistem, mengakses/mencuri/merubah/memalsu/merusak
  The Curious: ingin tahu apa saja tentang sistem
- Kerawanan: kemungkinan attacker memanfaatkan kelemahan manusia, prosedur, sistem, aplikasi
- Kegagalan: kebakaran, bencana alam, kerusuhan

Motivasi Penyerang

- The Malicious: ingin menghentikan, merusak
- The High Profile: ingin popularitas, ekspresi
- The Competition: ingin mengambil keuntungan
- The Borrowers: ingin ambil alih, memanfaatkan
- The Leapfrogger: ingin digunakan batu loncatan
- Perubahan trend dari iseng/coba-coba menjadi kriminal dan atau tujuan ekonomi, politik dlsb.

Pengamanan Fisik

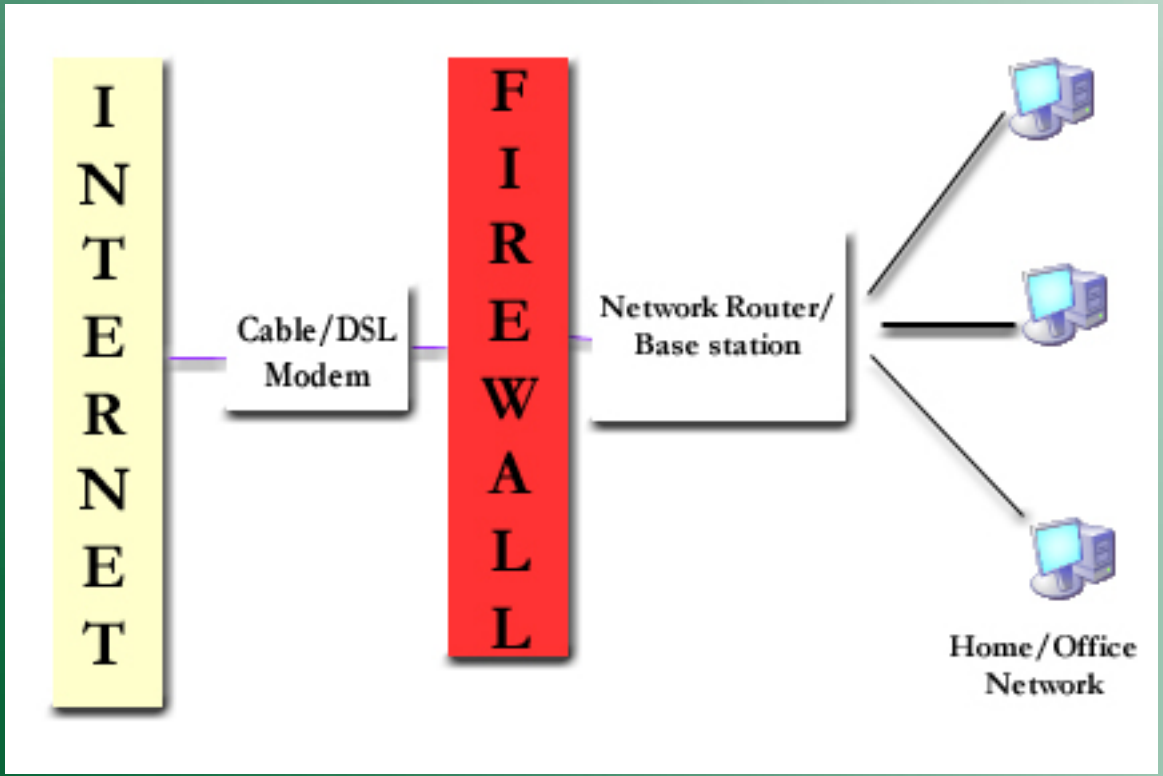
- Mencegah penggunaan oleh orang yg tak berhak
- Mencegah akses dari tempat/jaringan yg tdk sah
- Mencegah akses dari perangkat yg tdk sah
- Computer lock: BIOS, boot loader, local devices
- Pencatatan (logbook), pengawasan (surveillance)
- Manajemen password, one time access (token), encrypted password, perubahan reguler otomatis

Pengamanan Linux?

- Pengamanan IP, port, protocol, service, apps, password, OS/kernel, network vulnerabilities
- Linux system architecture dan file system lebih aman dan lebih sedikit application vulnerability
- Linux Security configuration enabled by default
- Your security is my security, social engineering
- Kita hidup di dunia para attacker, kriminal dan undergorund organized crime

Firewall

- Konfigurasi umum firewall



Bagaimana Firewall Bekerja?

- Memisahkan external/internal networks, DMZ, isolasi internal network dengan IP translations
- Mencegah koneksi masuk yang tidak diinginkan
- Stealth mode: discarding pings (menyembunyikan)
- Port forwarding dan blocking port tidak terpakai
- Packet filtering: allow, drop, reject atau forward
- Membatasi services, application dan run level

Membatasi Services, Apps, Run Level

- Matikan services yg tak digunakan, jangan install apps yg tak digunakan, jalankan run level yg tepat
- 0 Halt runlevel - system shuts down
- 1 Single runlevel - single user mode, hanya root user, tidak menjalankan networking atau X. Ideal untuk system maintenance dan repair
- 2 Boots - multi-user mode, text based console, tak menjalankan network

Run Level (Lanjutan)

- 3 Seperti runlevel 2 tapi network jalan, tanpa X
- 4 Undefined runlevel. Dapat dikonfigurasi untuk custom boot state misalnya untuk server
- 5 Boot system ke dalam lingkungan networked, multi-user dengan X Window System cocok untuk operasi penggunaan desktop atau workstation
- 6 Reboots the system

Pengamanan Lokal

- Mengelompokkan jenis user, level of access dan pembatasan jaringan dengan domain controller
- Root security, root account audit secara berkala
- Files dan file system security: umask settings, file permissions, integrity checking
- Password security dan enkripsi transparan TCFS, akses SSH, VPN, otentikasi (AAA, kerberos), display security, kernel security (compile, device)

Mitigasi Insiden

- Full backup berkala, file dokumen, konfigurasi sistem dan aplikasi, system accounting (logs)
- Update berkala sistem dan aplikasi (zero day)
- Menutup celah keamanan yg diketahui, matikan layanan/aplikasi yg bermasalah, cek kerusakan
- Mencegah attacker masuk kembali, reject IP asal, temukan backdoor, hapus user account tdk sah
- Setelah recovery, laporkan attacker, catat insiden

Linux Sebagai Security Tools

- Packet sniffer: Wireshark, TCPDump
- Firewall: software, distro (Alpine, Vyatta,IPCop, ClarkConnect, DDWRT/Open WRT - embedded)
- Network Audit: Nessus, Netfilter, Netcat, Kismet (wireless), Metasploit, Chkrootkit
- Integrity: Tripwire, IPS/IDS: SNORT, Pentest: BackTrack, Forensic: GIIS