Firewalls

General Principles

Overview

- Protects machine, LAN or internal network from attackers outside
- Unnecessary if all systems have adequate security and management
- Firewalls enforce security policy
- Examples include
  - protection for corporate networks connected to Internet
  - protection for network management from network users

Protocols used in remote attacks (I)

- TELNET – remote login from network
- RLOGIN – remote login for UNIX – authentication only from IP address
- FTP – file sharing – two connections, one for control, one for data transfer
- X Windows – applications accessed from remote terminals

Protocols used in remote attack (II)

- ICMP – Internet Control Message Protocol – recognise by protocol field (=1) in IP Header – used for
  - *Packet undelivered* because destination unreachable
  - *Redirect* because original router chosen not best path
  - *Ping* to check whether destination is reachable or for measuring round trip delay

Security implications of protocols

- *RLOGIN* – no password required if IP address is on /etc/hosts.equiv list
- *Ping* – may be used to find machines to attack
- *Packet unreachable* - may be used to break communications

Types of Firewall

- Packet filter
- Application level gateway
- Encrypted tunnel (IPSec VPNs)

Packet Filters (I)

- Simple address filter – configure firewall with legal source and destination addresses and drop all other packets
- Traffic filters – e.g. allow email but bar TELNET
  - protocol field in IP Header and layer 4 port (80 for http, 25 for email)

Packet filters (II)

- Initiation direction – e.g. allow connections initiated from inside, disallow from outside
  - examine TCP Header and disallow without ACK flag set
  - For X Windows and FTP examine layer 4 port
- Stateful packet filter
  - dynamic rules based on past events
  - e.g. allow reverse connection for a limited period after allowed initial connection

Application Level Gateway

- Gateway between firewalls at point of entry to internal and external networks
- All communications between external and internal network must pass through gateway
- Gateway examines application (e.g. allow email, disallow remote login)
- Gateways can examine email attachments and disallow executable code or large files

Encrypted Tunnels (IPSec VPNs)

- Allows secure communications between trusted endpoints
- Each endpoint may additionally have access to full internet