Operational Security

Peter Levinsky, Roskilde, Datamatiker

06.11.2023

Firewall – Survey

- Purpose of a Firewall
  - To allow ‘proper’ traffic and discard all other traffic
- Characteristic of a firewall
  - Allow and blocking traffic
  - The Firewall itself should be immune of attacked

Firewall – possibilities

- 5(6) areas to control:
  - Services (web, ftp, mail …) i.e. Port#
  - Network (hosts) i.e. IP addresses
  - Direction i.e. control inside-out or reverse
  - User i.e. only authorized users allow
  - Behaviour (e.g. attachment to mail)
  - (Denial of Service Inspection)

Firewall – solutions

- Solutions:
  - HW – screening router
  - SW – Computer Based (build in the OS)
  - SW – dedicated Host Firewall

Firewall – limitations

- 3 limitations of Firewalls
  - Cannot protect against traffic not running trough the firewall (obvious!!)
  - Cannot protect against threats from inside
    (e.g. as the school network)
  - Cannot protect against viruses
    (i.e. they come in by legal traffic)

Firewall – Types

- 3 types of Firewalls
  - Packet-filtering
  - Packet-filtering – with state-full inspection
  - Application- gateways

Firewall – Packet-filtering – Layer 3

- Level 3 – network (IP-packets)
  - Filtering on (the access control list):
    - Source/Destination IP-addresses
    - Source/Destination Port-numbers
    - IP-protocol field (e.g. icmp, tcp, egp)
    - TCP-direction (SYN-bit)
    - IN / OUT on each interface
    - ICMP message type

Firewall – Packet-filtering

- Configurations
  - Policies:
    1:optimistic: default set to allow
    2:pessimistic: default set to discard (normal)
  - Setting up rules

Firewall – Packet-filtering

- Weakness
  - Cannot ‘look’ into appl. Level information
  - Limited logging information
  - Do normally not support authentication
  - Can be attack by weakness in IP (e.g. IP-spoofing)

Firewall – Packet-filtering

- Stateful - inspection
  - Normal packet-filtering only look at one packet at a time.
  - Stateful packet-filtering can **remember a sequence** of packets. (can be used to detect spoofing)

Firewall – Application-level – Layer 5

- Level 5 Application gateway
  - Using Proxy Servers
    (e.g. a mail-client and a mail-server)

- Spilt connections into 2
  (one for inbound and one for outbound)

Firewall – Application-level

- More secure
  - Stateful inspection even more developed
  - User authentication are used
- Weakness
  - slow-down performance
  - need to have proxies for all services

Intrusion System

- Deep packet inspection
  - Read and remember history of packets

- Two types
  - Intrusion **Detection** System (IDS)
    - Send alert if behaviour is odd
    - One implementation snort (open source / Linux)
  - Intrusion **Prevention** System (IPS)
    - Filter out suspicious packets