Network security – session 7-3

Network II – Firewall and ACL

Firewalls & Access Control List

- Mitigation
  - Firewalls are used in computer networks for protection against network attacks
- ACL - The basic form of firewall protection
- Access lists can be configured on:
  - router,
  - true dedicated firewall, or
  - on the host computer

Firewall

- Firewalls allow traffic from inside the network to exit but don't allow general traffic from the outside to enter the network
- Monitors the data traffic and recognizes where packets are coming from
- Allow packets from the outside to enter the network if they match a request from within the network

Technologies

- Packet filtering
- Proxy server
- Stateful packet filtering

Packet filtering

- Packet filtering: Technique used to determine whether a packet is allowed to enter or exit the network based on its Layer 3 IP header information, such as source IP address and destination IP address, or its Layer 4 header information, such as protocol and port number
- A limit is placed on the packets that can enter the network
- Can be used to limit information moving from one segment to another

Packet filtering

- ACLs are used to enable the firewall to accept or deny data packets.

- Disadvantages:
- Packets can still enter the network by spoofing or fragmenting the data packets.
- It is difficult to implement complex ACLs.
- Not all network services can be filtered.

Proxy server

- An agent for handling requests from clients seeking resources
- Client must connect to the proxy server to connect to resources outside the network

- Disadvantages:
- It requires processing power.
- Adding services can be difficult.
- There can be a potential problem with network failure if the proxy server fails or is corrupted

Stateful packet filtering

- Stateful firewall - the state of inbound and outbound data packets are tracked and compared to determine if a connection should be allowed
- Includes tracking the source and destination port numbers and sequence numbers, as well as the source and destination IP addresses
- Technique - used to protect the inside of the network from the outside world but still allow traffic to go from the inside to the outside and back

Example

- PC called ABC is on the inside of a network
- ABC establishes connection to www.net-A.edu
- SYN packet sent
- Firewall allows packet to leave the network
- Firewall creates a state that includes source and destination IP address for the connection
- Packet arrives at port 80 of the server
- SYN-ACK packet from server arrives at the firewall
- Firewall examines packet and IF it matches stores state – packet is allowed

Scenario 1

- What if an attacker tries to spoof the firewall to gain access to the interior of the network?
- Attacker spoofs the net-A.edu domain www server's IP address and port 80 (the web server) and tries to use this to gain access to the network
- But, A connection is already established
- Server recognizes a discrepancy with the sequence number and rejects the hacker's connection

Scenario II

- Campus network has a web server. How are outside users allowed access?
- The firewall must be modified so that anybody can connect to the web server via port 80
- The web server may also need to have its own firewall
- Network administrator must continually upgrade the software so that vulnerabilities are removed
- Is Firewall the ultimate answer to all the problems?