Network security – session 7-2

Network II

Network Security

- Denial of Service (DoS)
- SYN attack
- Smurf attack
- Distributed Denial of Service (DDoS) attack
- Firewall
- Access lists

Denial of Service

- No service to a computer
- No service to a network
- No service to network servers

DoS attack

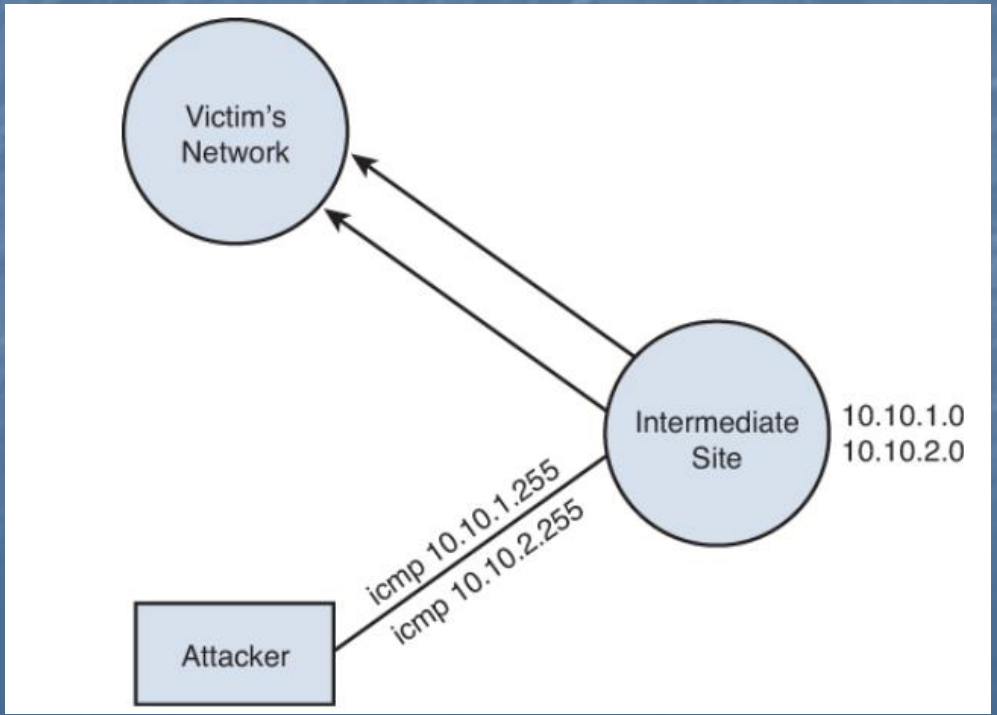
- How is it done?
- Initiated by exploiting Software vulnerability
  - SW vulnerability can permit buffer overflow – Machine crashes
    - Database of SW vulnerability - https://nvd.nist.gov/
- Vulnerable software DoS attack – The system reboots repeatedly
- DoS attack on routers via the software options available for connecting to routers
  - Fx SNMP management software – similar core code that can contain the same vulnerability

DoS attack

- SYN attack – TCP SYN (synchronizing) packet
- Attacker opens many TCP sessions by sending TCP SYN packets
- Host machines has limited memory for open connections
- Other users kept form accessing services from the computer due lack of TCP connection –full connection buffer
- Modern OS have counter measures on this issue
  - SYN cookies
  - RST cookies

DoS attack

- SMURF Attack
  - A way of generating a large amount of data traffic
  - Attacker sends a small packet and receives many in return
  - Attacker inserts an IP address from the victims network –Spoofing
  - Attacker sends a packet to all in the network using the networks broadcast address
  - All the machines on the network sends a reply to source address – within the visctims network



- Network should not be allowed to become an intermediate site
  - No ip direct-broadcast – (Routers allow broadcast to be sent to specific subnet
- Use Access list – to prevent network being attacked!!

Distributed Denial of Service Attacks

- Attacker does a port scan and look for an open port or a software application that is vulnerable to an attack
- The machine is ***hacked*** (attacked) and distributes the malicious software – by using worm
- Once the software is on the victim machines, the attacker can issue a command or instruction that starts the attack on a specific site

Mitigation

- PREVENT INTRUSIONS