

# Networking-Based Attacks

# Networking-Based Attacks

- Denial of Service (DoS)
- Interception
- Poisoning
- Attacks on Access Rights

# Denial of Service (DoS)

- A DoS attack is a deliberate attempt to prevent authorized users from accessing a system by overwhelming that system with requests.
- Most DoS attacks today are actually distributed denial of service (DDoS) attacks: instead of using one computer, a DDoS may use hundreds or thousands of zombie computers in a botnet to flood a device with requests.

# Types of DoS attacks

- Ping flood
- Smurf attack
- SYN flood

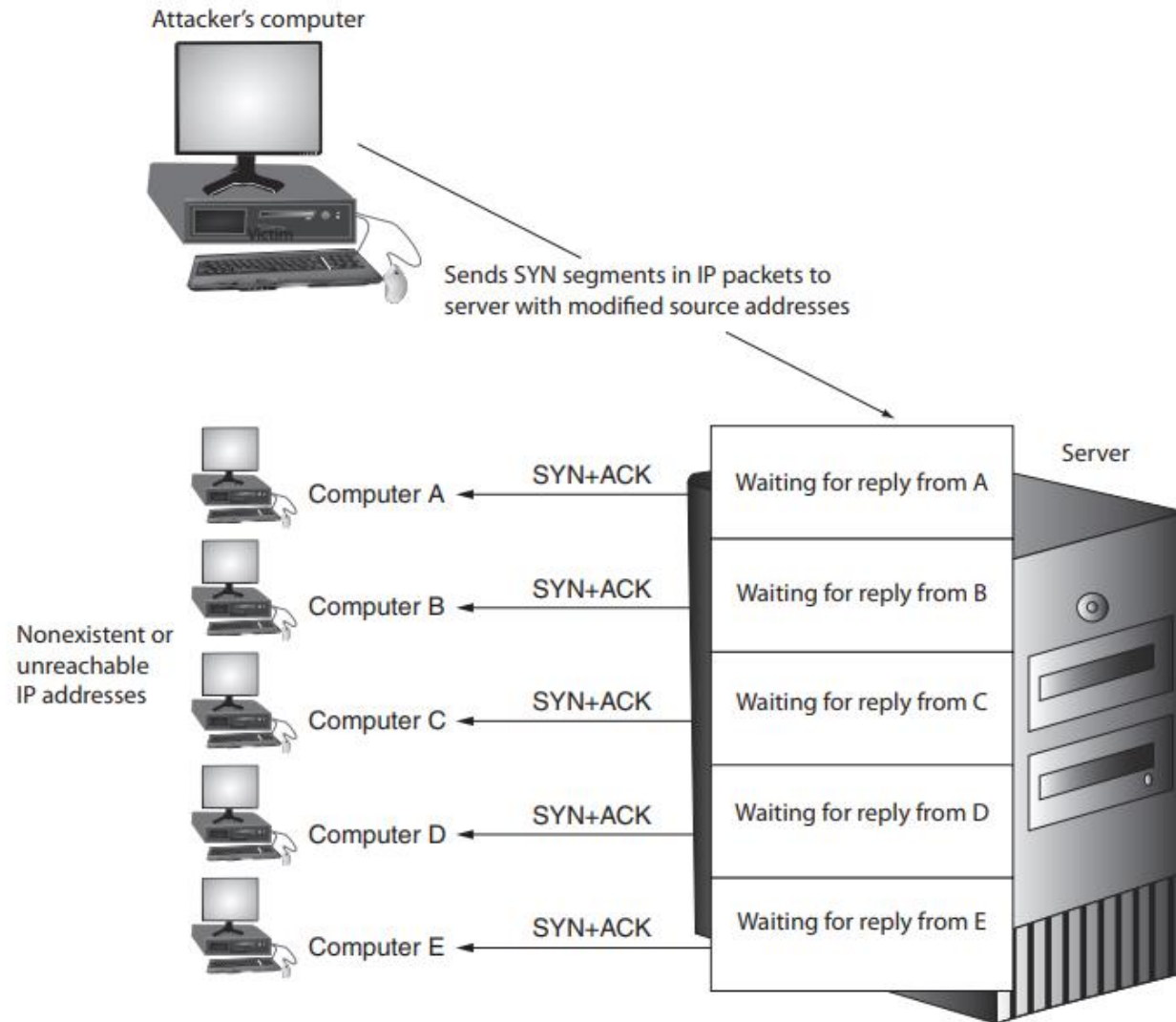
# Ping flood

- Multiple computers rapidly send a large number of ICMP echo requests, overwhelming a server (as well as the network) to the extent that it cannot respond quickly enough and will drop legitimate connections to other clients and refuse any new connections.

# Smurf attack

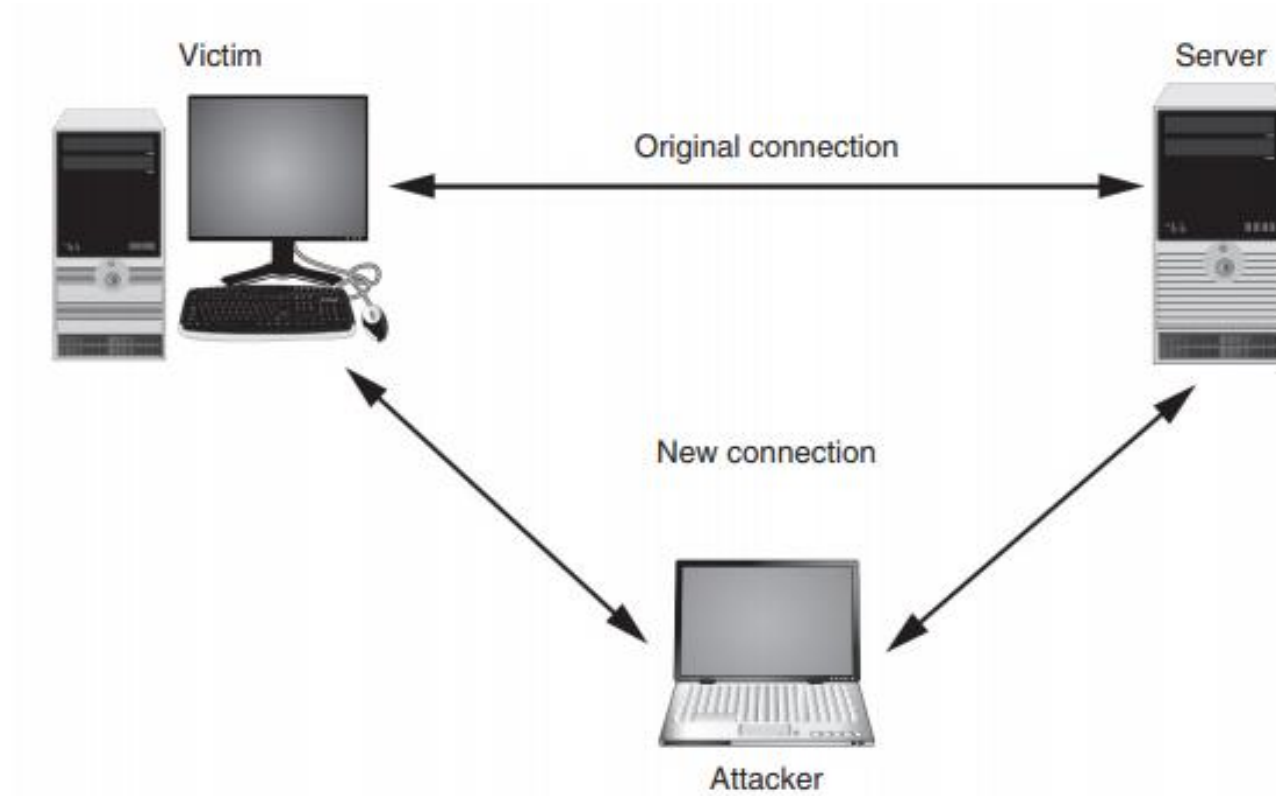
- An attacker broadcasts a ping request to all computers on the network but changes the address from which the request came to the victim's computer.
- Each of the computers then sends a response to the victim's computer so that it is quickly overwhelmed and then crashes or becomes unavailable to legitimate users.

# SYN Flood attack



# Interception

- Man-in-the-Middle attack
- Replay attack





# Interception

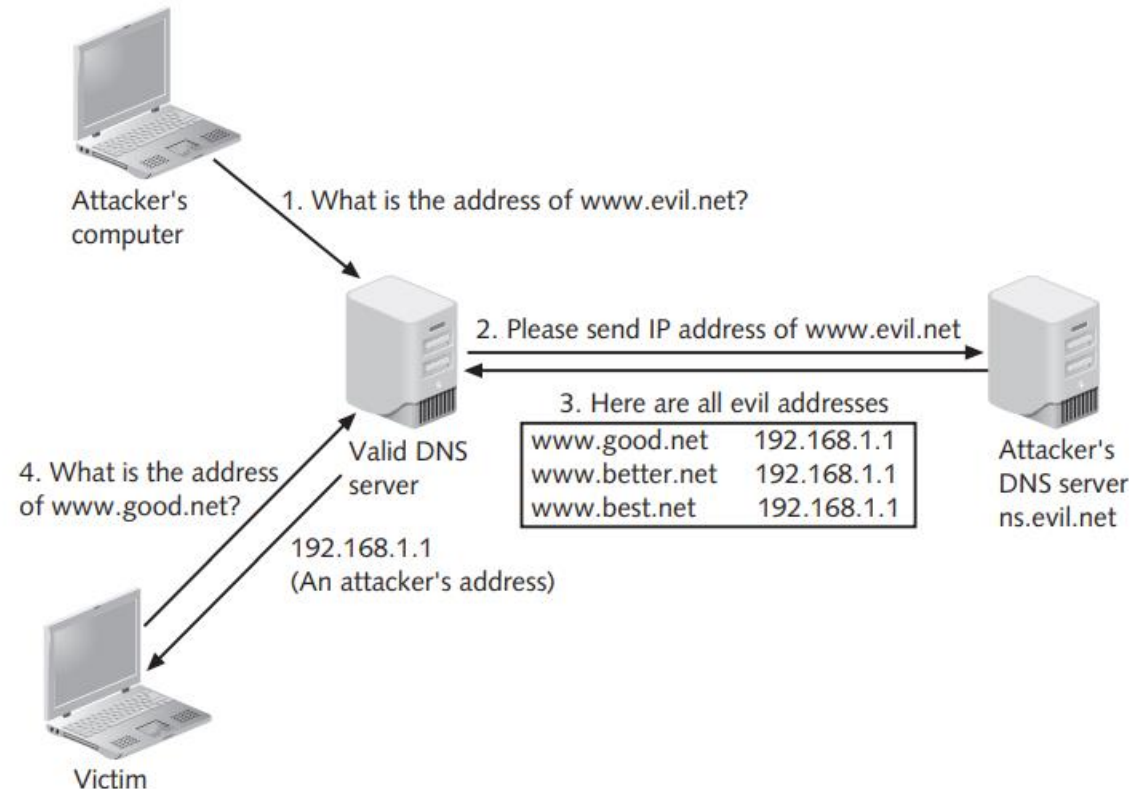
- A replay attack is similar to a passive man-in-the-middle attack.
- Attackers make a copy of the transmission before sending it to the recipient. Later, the attacker can send the original message to the server, and the server may respond. Now a trusted relationship has been established between the attacker and the server.
- The attacker can begin to change the content of the captured message and code. If he eventually makes the correct modification, the server will respond, letting the attacker know he has been successful.

# Poisoning

- ARP Poisoning: An attacker can modify the MAC address in the ARP cache so that the corresponding IP address points to a different computer

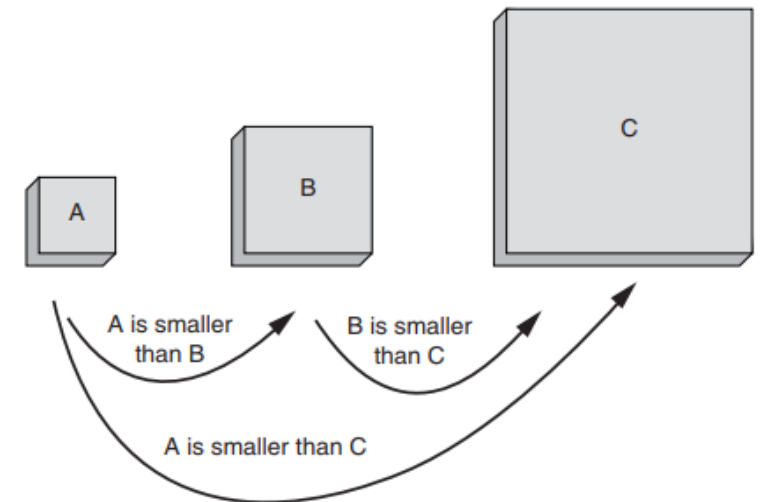
Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.200-AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04
Victim 1	192.146.118.300-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.400-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

- DNS Poisoning is a process of substituting a DNS address so that the computer is automatically redirected to another device



# Attacks on Access Rights

- Privilege Escalation: is exploiting a vulnerability in software to gain access to resources that the user normally would be restricted from accessing.
- Transitive Access: System A can access System B, and because System B can access System C, then System A can access System C.



# Summary

- Networks are a high priority target for attackers. This is because exploiting a single vulnerability may expose hundreds or thousands of devices to an attacker.
- A denial of service (DoS) attack is a deliberate attempt to prevent a system from performing its normal functions in order to prevent authorized users from access to the system.

# Summary

- A man-in-the-middle attack attempts to intercept legitimate communication and forge a fictitious response to the sender.
- A replay attack is similar to a man-in-the-middle attack. Instead of sending the transmission immediately, a replay attack makes a copy of the transmission before sending it to the recipient. This copy is then used at a later time.

# Summary

- Two types of attacks inject “poison” into a normal network process to facilitate an attack: ARP poisoning and DNS poisoning.
- Privilege escalation involves exploiting a vulnerability in software to gain access to resources that the user normally would be restricted from obtaining.
- Transitive access involves using a trust relationship between three elements to gain access rights.