Smurf Attack

Smurf Attack

Smurf is a network layer distributed denial of service (DDoS) attack. Smurf attacks are somewhat similar to ping floods attack, as both the attacked flood the target machine with ICMP Echo request packets. Smurf attack is some what different than the regular ping flood attack. Smurf is an amplification attack vector that boosts its damage potential by exploiting characteristics of broadcast networks.

A spoofed ICMP Echo request is send over the network broadcast address targeting the victim machine as a source. As a result a ICMP Echo response is send back resulting a flood of incoming ICMP packets to the target machine. Which slows down or crash the targeted machine resulting a Denial of service.

Attacks

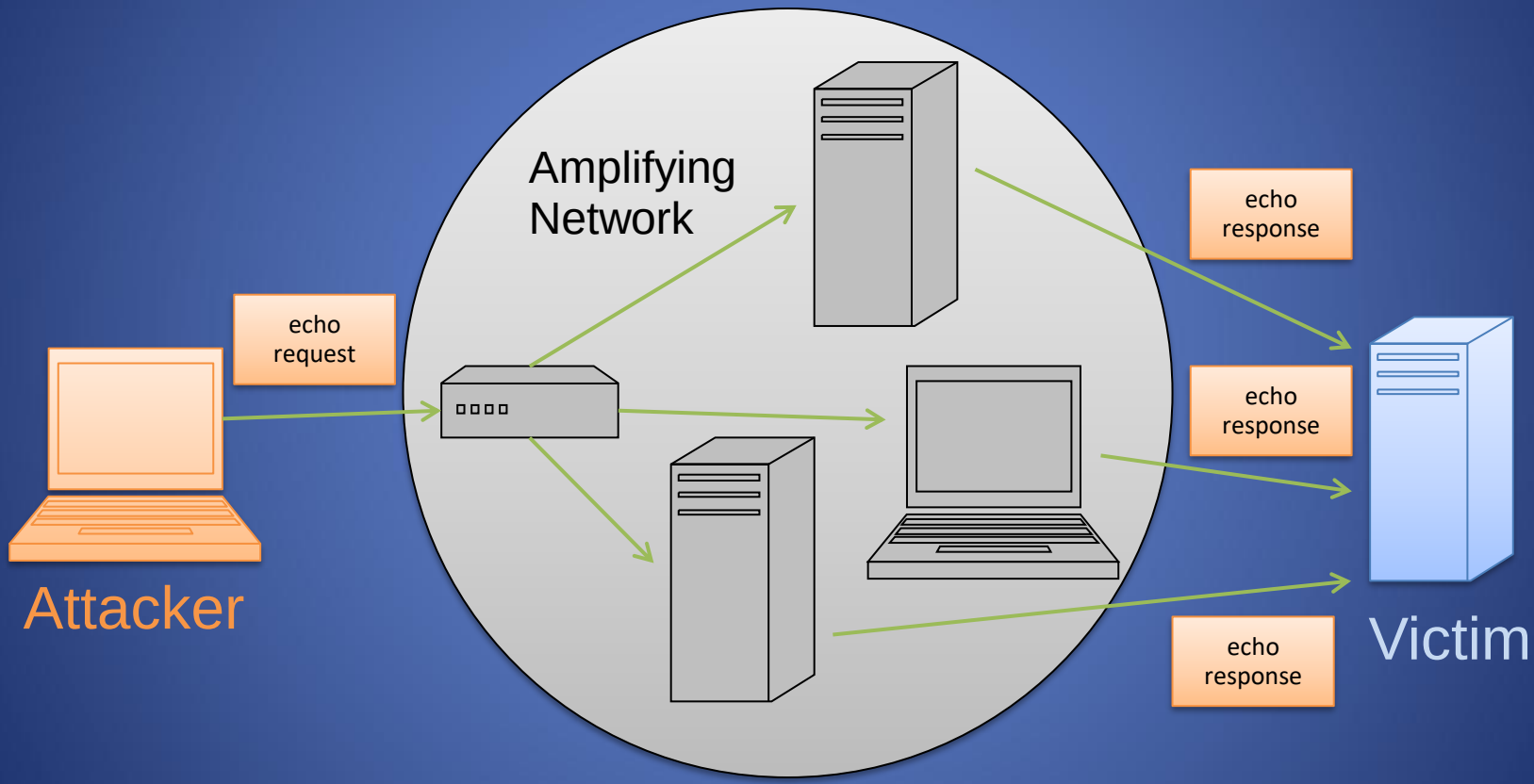
- Distributed Denial-of-service attacks: DDoS attack is often target the compromised computer system to attack the target victim machine. Where the target system is forced to slow down or even crash and shutdown with large number of malformed packets or connection requests from various spoofed source IP address or compromised computer to the targeted machine .

Example

An attacker make use of network scanning software like Nmap and monitor the network activity over the network. The attacker target the victim computer system most the one with high value target like servers.

The attacker craft a spoofed ICMP echo request packets with victim computer system as a source and send the request to the network broadcast IP address. The ICMP Echo request is flooded over the network and the ICMP response is send back to the victim machine lead to a Distributed Denial-of-Service DDOS attack.

Example


Amplifying
Network
echo
request
echo
response
echo
response
echo
response
Attacker
Victim