CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Malicious Software and Denial of service attacks

Distributed DoS Attacks (DDoS)

Video Summary

- What is Distributed DoS attack?
- Reflector Attack
- Amplification Attack using Broadcast
- Using Compromised Hosts

Distributed Denial of Service (DDoS) Attacks

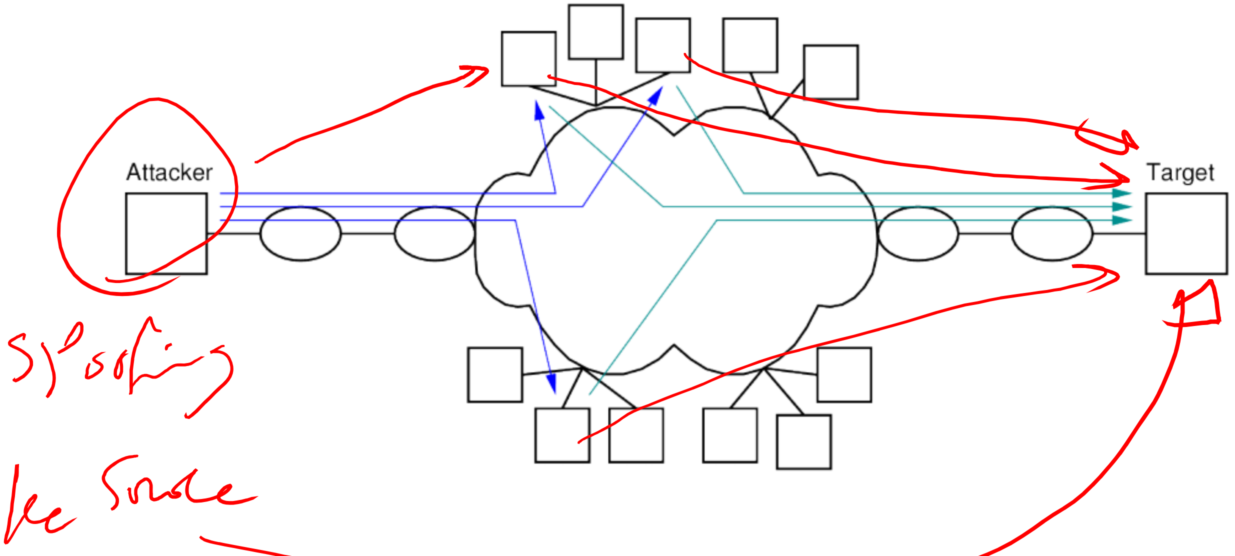
Use of multiple systems to generate attacks

Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)

Large collections of such systems under the control of one attacker’s control can be created, forming a botnet

Flooding and Distributed DoS Attack

- Reflector Attack



spoofing

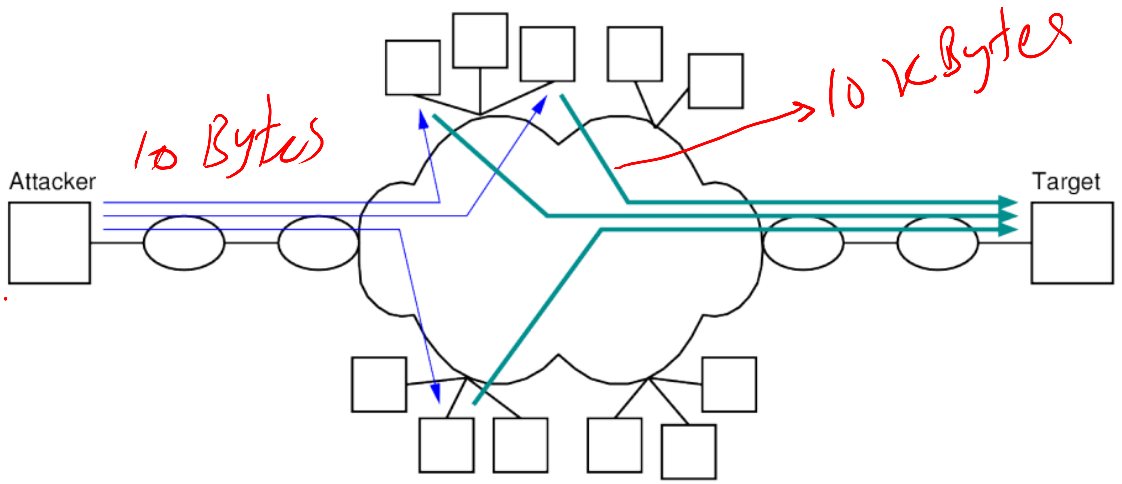
fake Source

Bounce Messages Off Normal Hosts

- Send protocol messages to multiple normal hosts using spoofed source address set to targets
- All hosts respond to target

Flooding and Distributed DoS Attack

- Reflector Attack



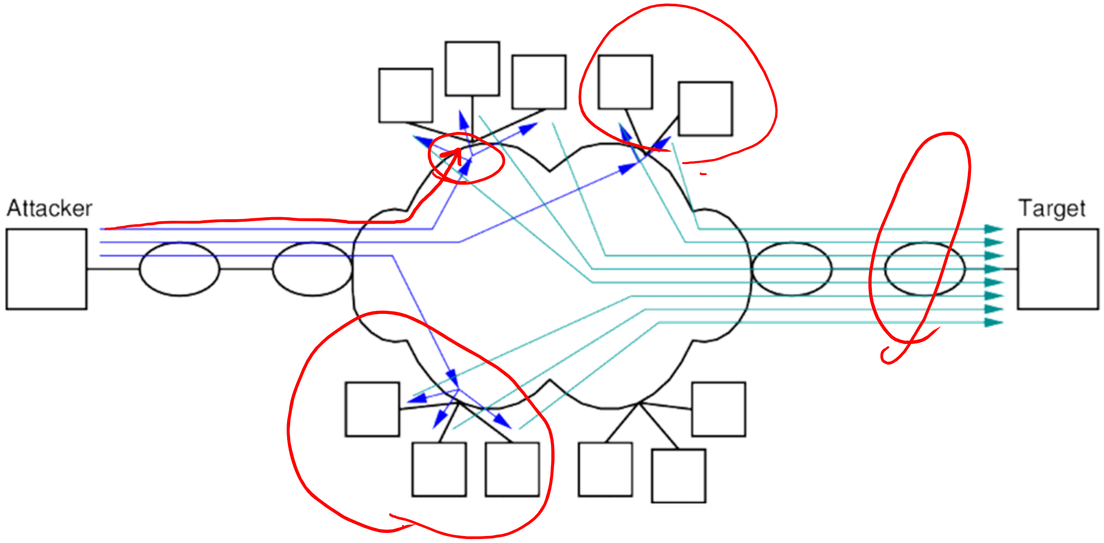
Response Larger than Request

- Use protocol/application where request (sent by attacker) is small, by response (sent to target) is large
- Increases amount of traffic sent to target

Note that ping (request = response) is not used here

Flooding and Distributed DoS Attack

- Amplification Attack using Broadcast

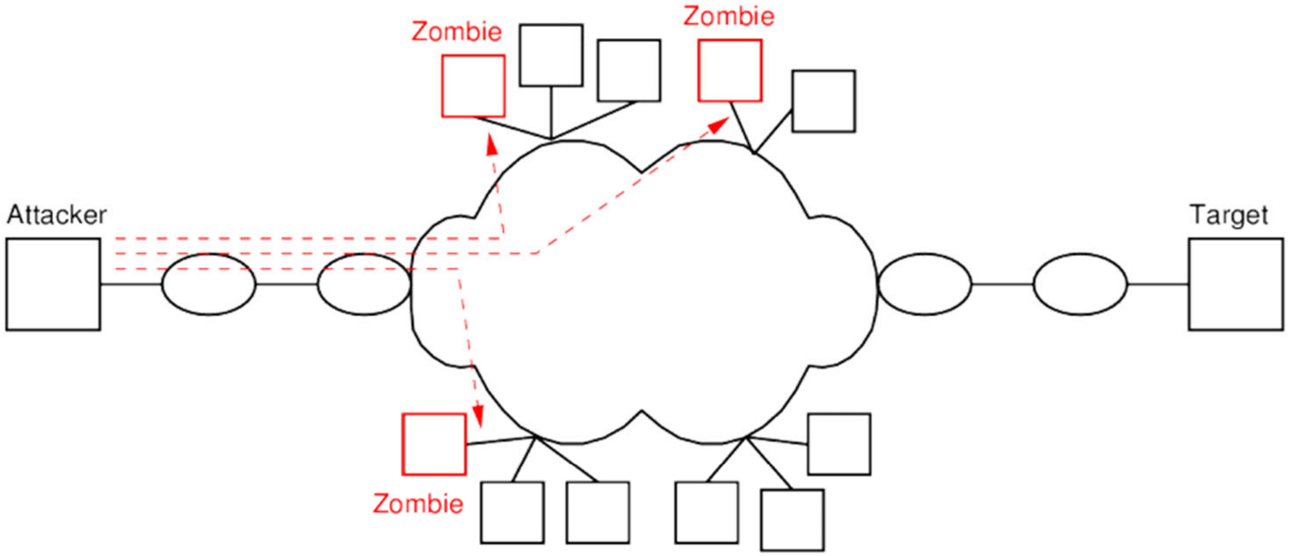


Send Request to Entire LAN

- Packets sent to directed broadcast IP addresses (e.g. 192.168.1.255) are delivered to all hosts on subnet by router
- All hosts respond to target
- Countermeasure: Routers block directed broadcast from outside

Flooding and Distributed DoS Attack

- Using Compromised Hosts

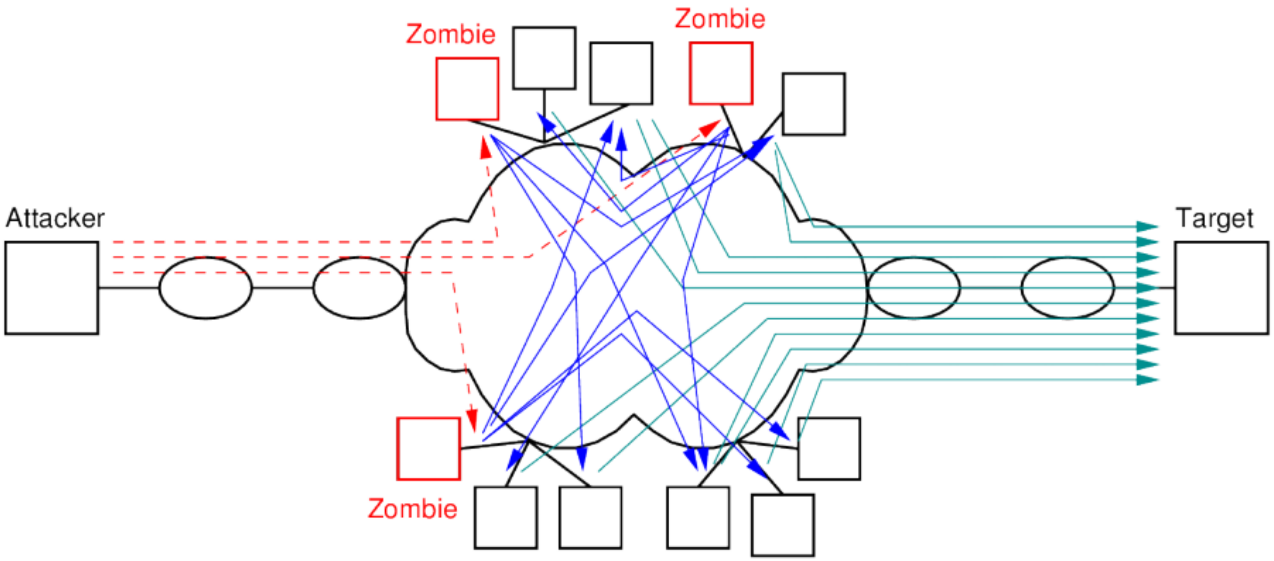


Zombies and Botnets

- Attacker takes control of compromised hosts → zombies
- Attacker triggers zombies to initiate attack
- Collection of zombies called botnet

Flooding and Distributed DoS Attack

- Using Compromised Hosts



Countermeasures

- ?

Antivirus

Patching

updating

Video Summary

- What is Distributed DoS attack?
- Reflector Attack
- Amplification Attack using Broadcast
- Using Compromised Hosts