Denial of Service Attacks

Malicious Software - Lecture (7)

Information Security Department

2nd Class- First Course

5 December . 2023

- **Assist. Lecturer** : **Nuha Kareem Hameed**
- **Email** : **NuhaKareem@uobabylon.edu.iq**

Denial of Service Attacks

- A denial of service (DoS) attack:

  It is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to it customers.

- there are several categories of resources that could be attacked:
  - Network bandwidth
  - System resources
  - Application resources

Denial of Service Attacks

DoS vs. DDoS

DoS stands for Denial of Service. The difference between DoS and DDoS attacks is whether one computer is used in the attack, or the attack is sent from multiple sources. Sources can include traditional computers and also Internet-connected devices that have been taken over as part of a botnet.

Relation between DDoS and Malware

Defines: A DDoS attack is a network attack wherein threat actors force numerous systems (usually infected with malware) to send requests to a specific web server to crash, distract, or disrupt it enough that users cannot connect to it.

DoS Attacks Resources

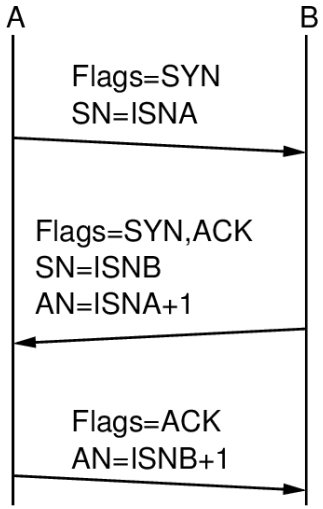
- Network Resources
  - Overload communications link or devices to server
  - Link from organisation to ISP usually lower capacity than links within and between ISP routers
  - As link reaches capacity, router will drop packets
- System Resources
  - Overload or crash its network handling software.
- Application Resources
  - Send packets to applications (e.g. servers) that force them to consume resources

Denial-of-Service Attacks

- Classical Denial-of-Service Attacks
  - TCP SYN Flooding Attack
  - Simple Ping Flooding Attack
- Flooding and Distributed DoS Attacks
  - Source Address Spoofing
  - Reflector Attack
  - Amplification Attack

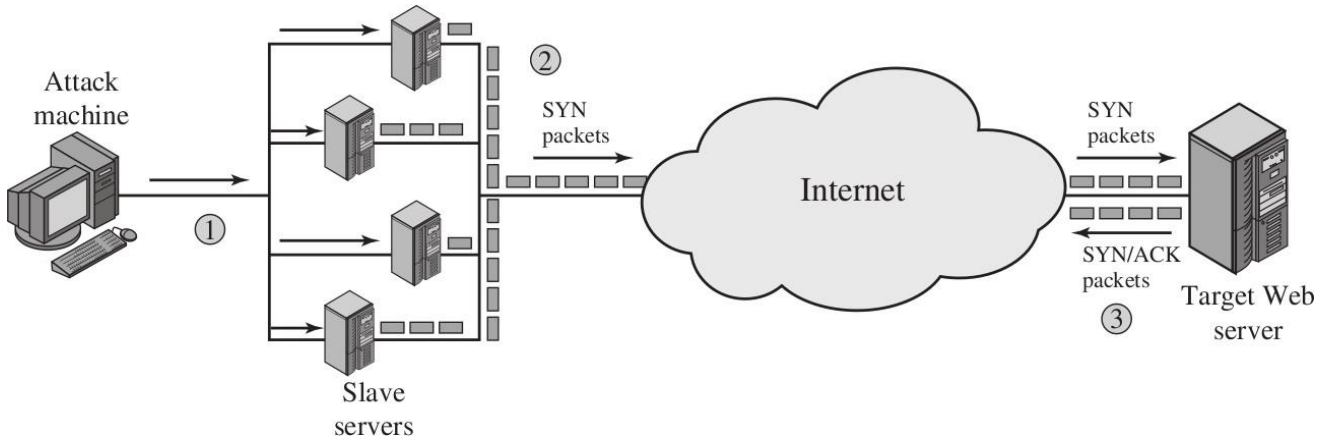
TCP SYN Flooding Attack

- TCP Connection Setup
  - TCP uses 3-way handshake to establish a connection
  - Upon receiving SYN, server stores connection information in memory, and waits for ACK
  - Re-send SYN-ACK if no ACK from client; eventually server deletes connection information if no ACK



TCP SYN Flooding Attack

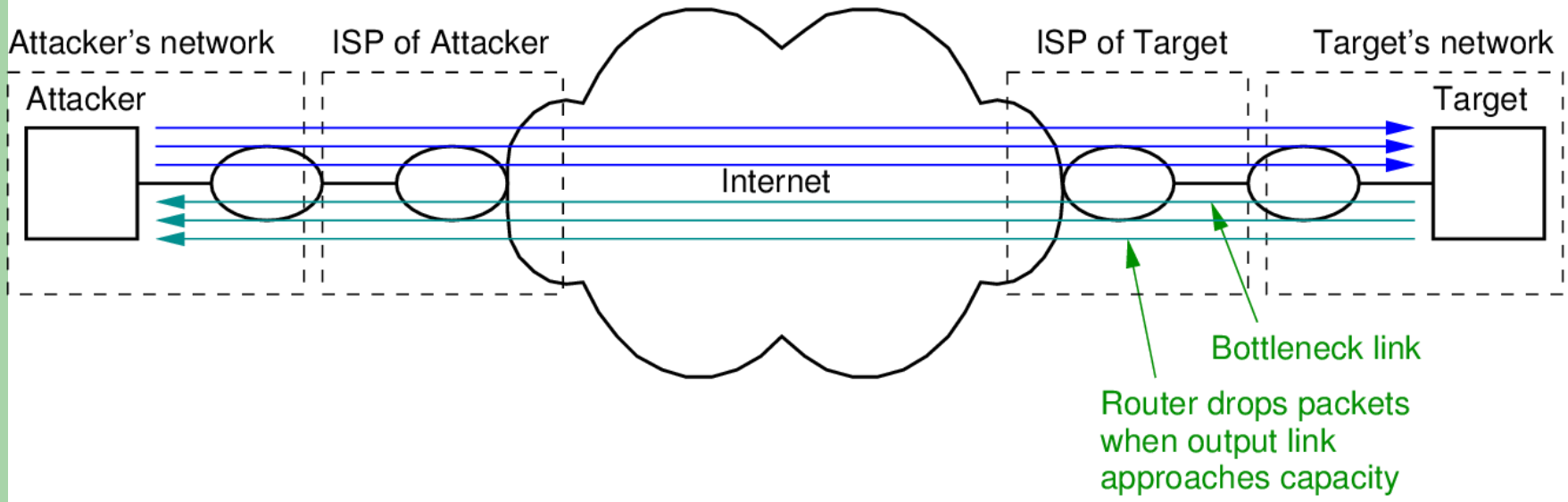
- Attacker sends TCP SYN segments to target
- Source address spoofing is used on TCP SYN segments; no ACKs from client
- Target becomes overloaded processing SYNs and storing connection information in memory
- Countermeasure: filter packets at routers.



Simple Ping Flooding Attack

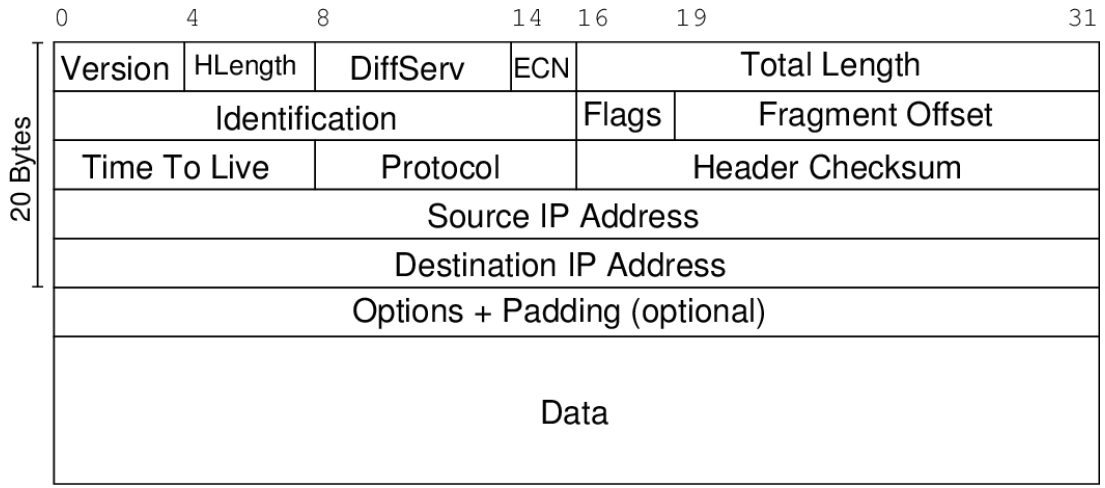
- Assumptions
  - Attacker has access to high capacity link
  - Target's connection to Internet is lower capacity
  - Attack
  - Flood the server: Attacker uses ping to send many ICMP requests to target server
  - Link from ISP to router is overloaded; router drops (valid) packets
  - Countermeasures
  - ISPs block ping (ICMP) packets
  - Target can identify the source: inform ISP, take legal action
  - ICMP responses sent back to attacker, affecting their network performance

Simple Ping Flooding Attack



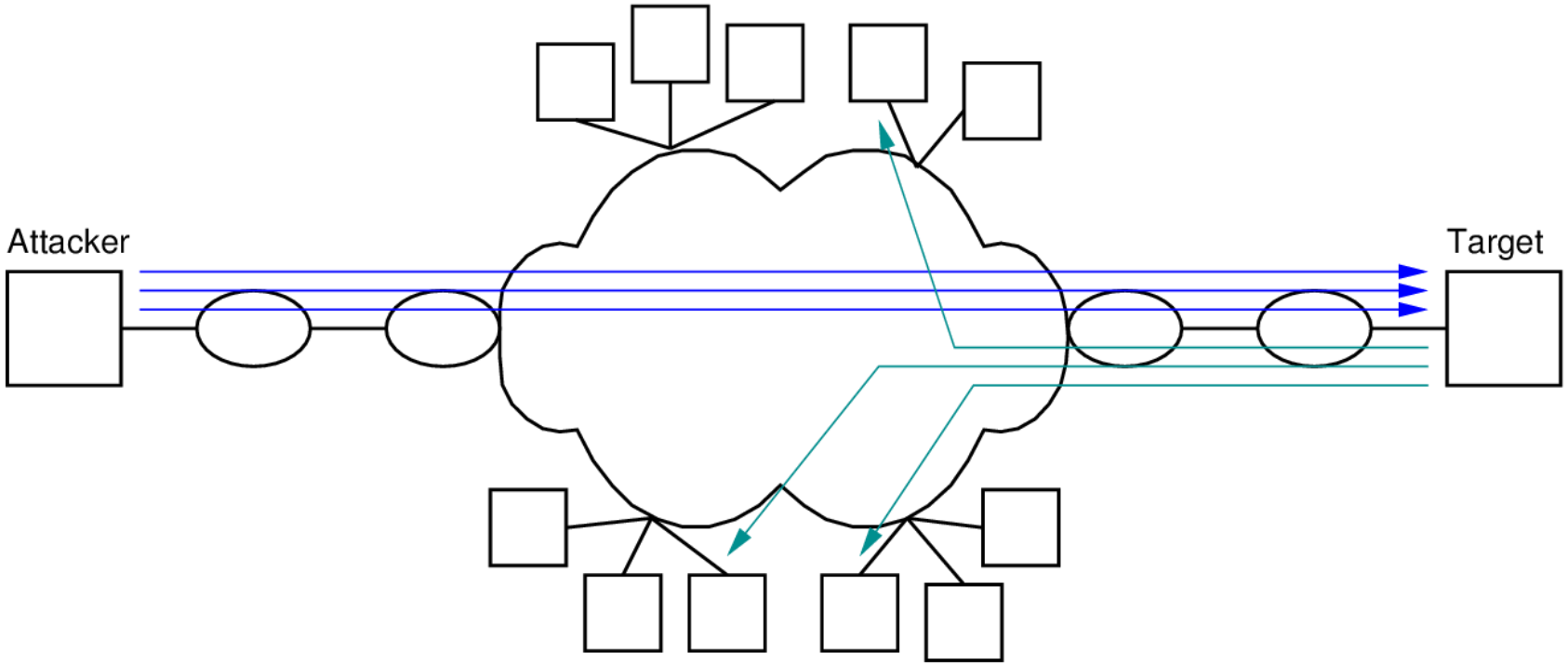
Source Address Spoofing

- Attacker sends packets with fake (or spoofed) source address
  - Target does not (immediately) know who performed attack
  - Responses are not sent to attacker
  - Source address may be of actual host or non-existent



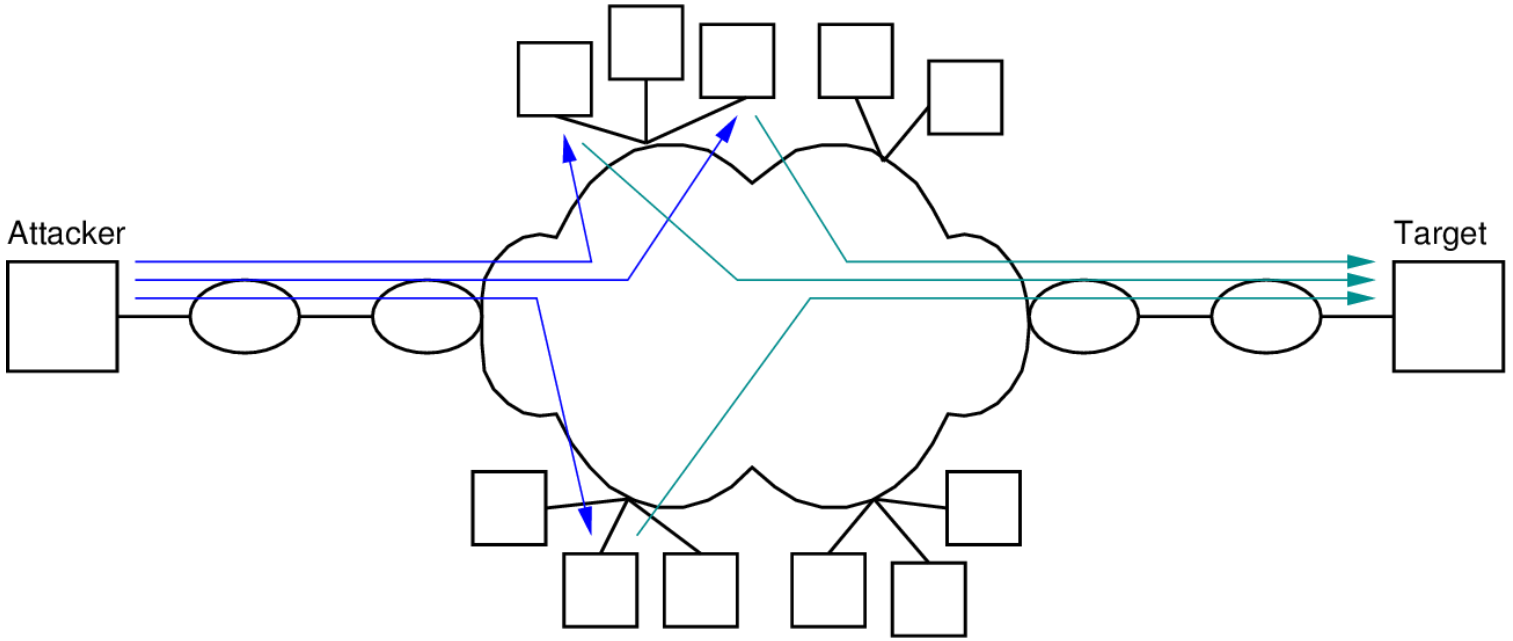
Source Address Spoofing

- Countermeasure
  - ISPs filter (drop) packets that come from invalid source address



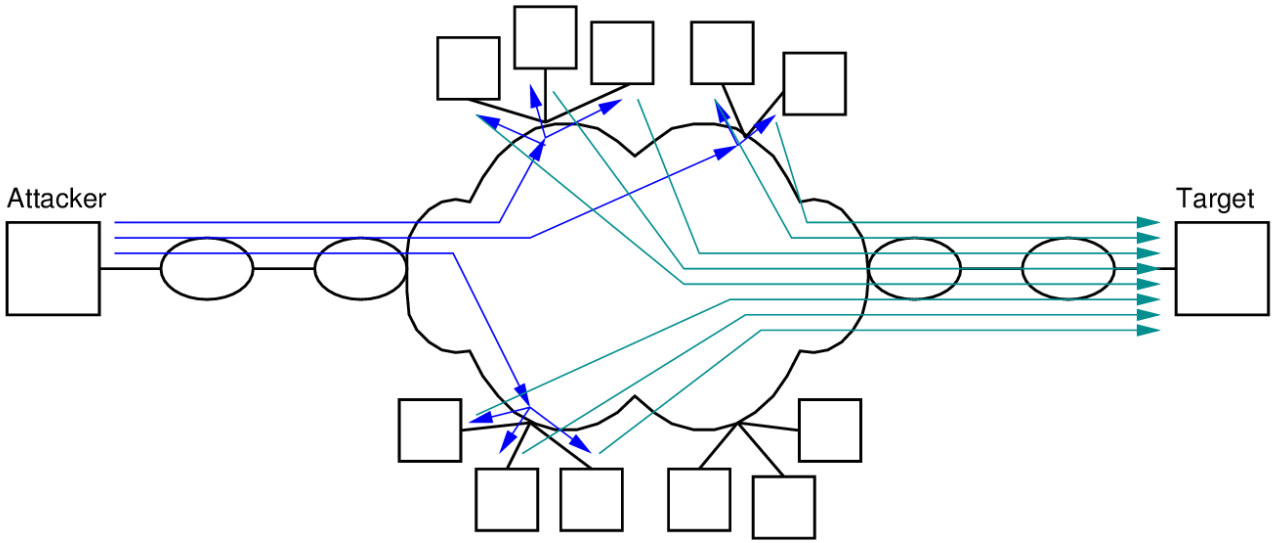
Reflector Attack

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



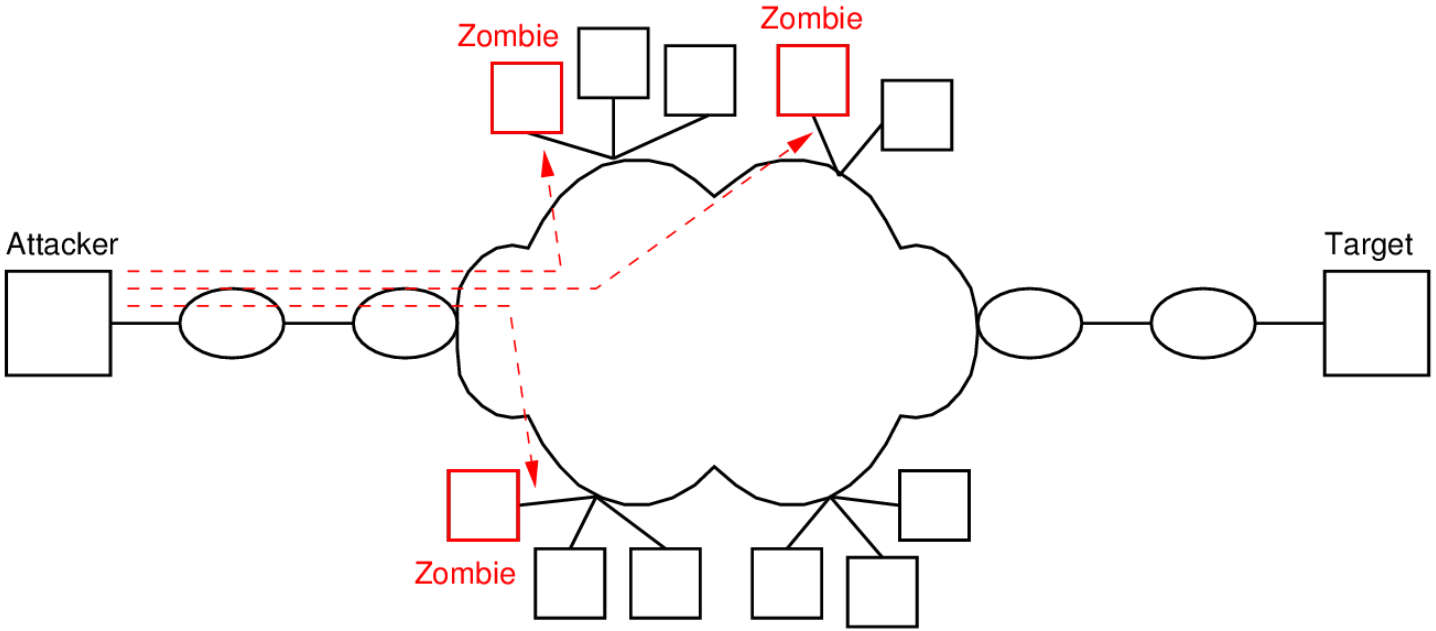
Amplification Attack using Broadcast

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



Amplification 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



Constructing Attack Network

- Attacker must get many slave hosts under its control
  - Infect the hosts with zombie software

1. Create software that will perform the attacks. This should:
   - Be able to run on different hardware architectures and OSes
   - Hide, that is not be noticeable to the normal user of the zombie host
   - Be able to be contacted by attacker to trigger an attack
2. Identify vulnerability (bug) in large number of systems, in order to install the zombie software
3. Locate vulnerable machines, using scanning:
   - Attacker finds vulnerable machines and infects with zombie software
   - Then the zombie software searches for vulnerable machines and infects with zombie software
   - And so on, until a large distributed network of slaves is constructed

Preventing DDoS Attacks

- Prevention
- Allocate backup resources and modify protocols that are less vulnerable to attacks
  - Aim is to still be able to provide some service when under DDoS attack
  - Detection
  - Aim to quickly detect an attack and respond (minimise the impact of the attack)
  - Detection involves looking for suspicious patters of traffic
  - Response
  - Aim to identify attackers so can apply technical or legal measures to prevent
  - Cannot prevent current attack; but may prevent future attacks