Module 5.2

DOS Attacks

WHAT IS “DOS ATTACK”

- DOS Attack 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.
- legitimate users of a service from using that service.
- Too many requests for a particular web site “clog the pipe” so that no one else can access the site
- DoS = when a single host attacks
- DDoS = when multiple hosts attack simultaneously

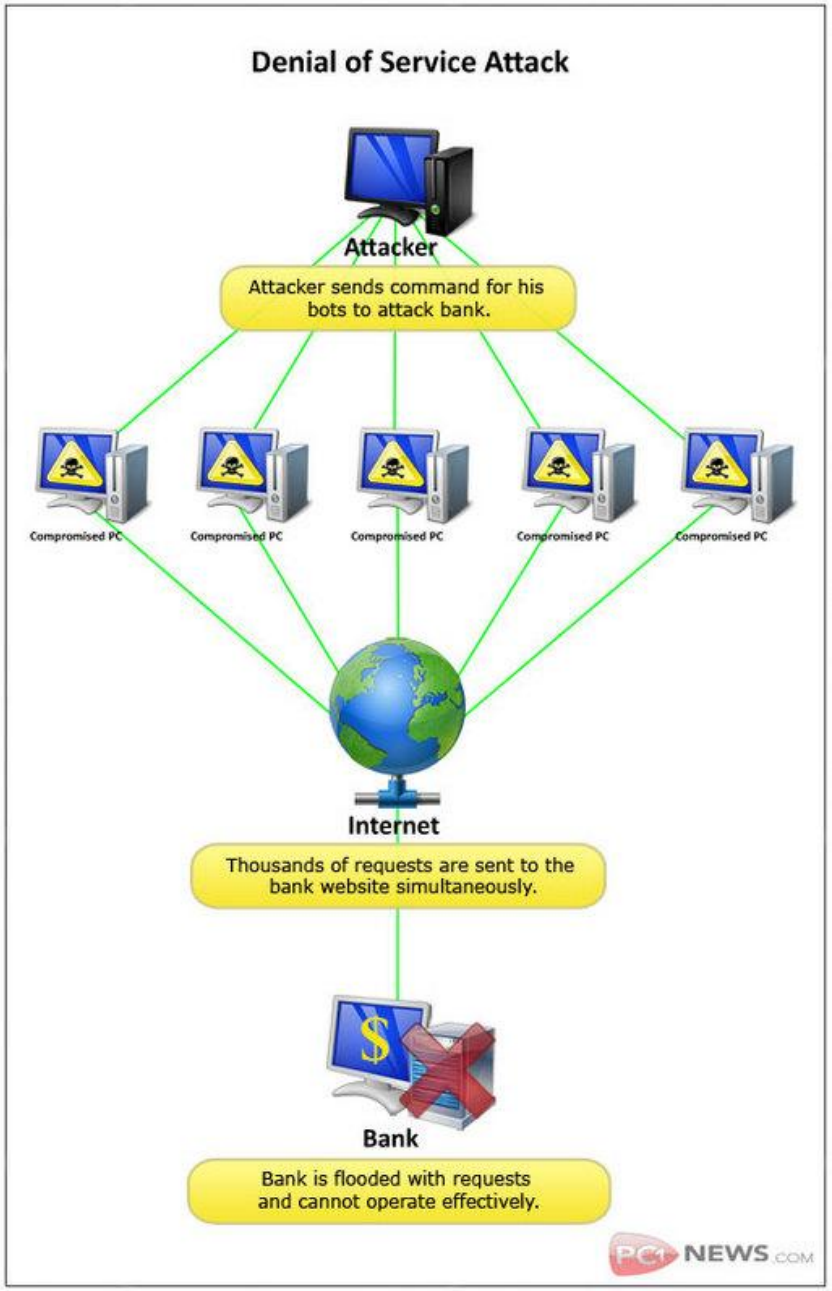
IDEA OF “DOS ATTACKS”

- Purpose is to shut down a site, not penetrate it.
- Purpose may be vandalism, extortion or social action (including terrorism) (Sports betting sites often extorted)
- Modification of internal data, change of programs (Includes defacement of web sites)

Possible impacts

- Possible impacts:
  -May reboot your computer
  -Slows down computers-Certain sites
  -applications become inaccessible
  **you are off.

TYPES OF DOS ATTACKS



TYPES OF DOS ATTACKS

- Penetration
- Eavesdropping
- Man-In-The-Middle
- Flooding
- Bandwidth attacks
- Protocol exceptions
- Logic attacks

.

TYPES OF DOS ATTACKS

Penetration

- Attacker gets inside your machine
- Can take over machine and do whatever he wants
- Achieves entry via software flaw(s), stolen passwords or insider access

TYPES OF DOS ATTACKS

Eavesdropping

- Attacker gains access to same network
- Listens to traffic going in and out of your machine

TYPES OF DOS ATTACKS

Man-in-the-Middle

- Attacker listens to output and controls output
- Can substitute messages in both directions

TYPES OF DOS ATTACKS

Flooding/Bandwidth attack

- Attacker sends an overwhelming number of messages at your machine; great congestion
- The congestion may occur in the path before your machine
- Messages from legitimate users are crowded out
- Usually called a Denial of Service (DoS) attack, because that's the effect.
- Usually involves a large number of machines, hence Distributed Denial of Service (DDoS) attack
- A bandwidth attack is the oldest and most common DoS attack. In this approach, the malicious hacker saturates a network with data traffic. A vulnerable system or network is unable to handle the amount of traffic sent to it and subsequently crashes or slows down, preventing legitimate access to users.

TYPES OF DOS ATTACKS

Protocol Attack

- A protocol attack is a trickier approach, but it is becoming quite popular. Here, the malicious attacker sends traffic in a way that the target system never expected, such as when an attacker sends a flood of SYN packets.

HOW TO DEFEND

- Firewalls - can effectively prevent users from launching simple flooding type attacks from machines behind the firewall.
- Switches - Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding to detect and remediate denial of service attacks
- Routers - If you add rules to take flow statistics out of the router during the DoS attacks, they further slow down and complicate the matter
- DDS based defense
- Clean pipes

Internet Control Message Protocol

- Provides feedback about network operation
  - Error reporting
  - Reachability testing
  - Congestion Control
- Example message types
  - Destination unreachable
  - Time-to-live exceeded
  - Parameter problem
  - Redirect to better gateway
  - Echo/echo reply - reachability test

ICMP attacks

- ICMP Tunneling
- ICMP Router Discovery
- Smurf attack
- Fraggle Attack
- ICMP flood attack
- Ping of death attack
- Information Gathering
- Trace Route
- Port Scan
- OS fingerprinting
- Teardrop

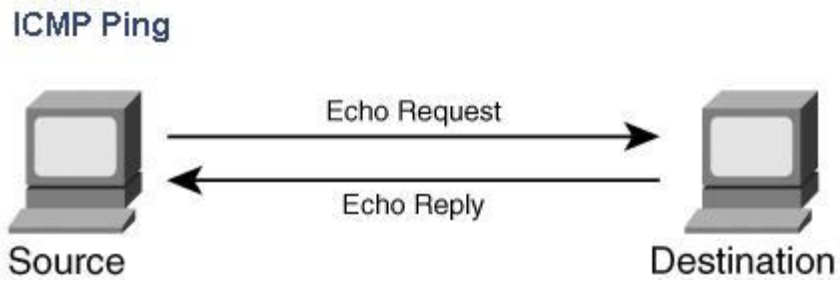
- https://www.socinvestigation.com/icmp-attacks-types-codes-for-log-analysis-detection-defense/

ICMP flood Attack

- An Internet Control Message Protocol (ICMP) flood DDoS attack, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings)
- ICMP echo-request and echo-reply messages are used to ping a network device in order to diagnose the health and connectivity of the device and the connection between the sender and the device.
- By flooding the target with request packets, the network is forced to respond with an equal number of reply packets. This causes the target to become inaccessible to normal traffic.

PING OF DEATH

A Ping of Death attack uses Internet Control Message Protocol (ICMP) ping messages. Ping is used to see if a host is active on a network. It also is a valuable tool for troubleshooting and diagnosing problems on a network. As the following picture, a normal ping has two messages:



PING OF DEATH

- BUT
- With a Ping of Death attack, an echo packet is sent that is larger than the maximum allowed size of 65,536 bytes. The packet is broken down into smaller segments, but when it is reassembled, it is discovered to be too large for the receiving buffer. Subsequently, systems that are unable to handle such abnormalities either crash or reboot.
- You can perform a Ping of Death from within Linux by typing ping –f –s 65537. Note the use of the –f switch. This switch causes the packets to be sent as quickly as possible. Often the cause of a DoS attack is not just the size or amount of traffic, but the rapid rate at which packets are being sent to a target.

Tools:-

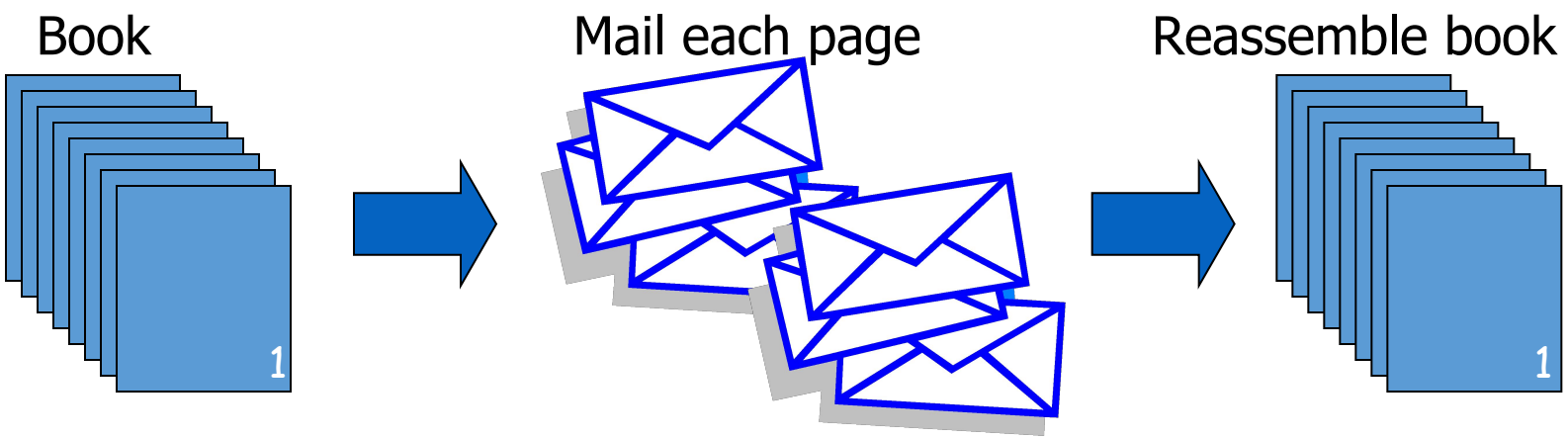
-Jolt -SPing-ICMP Bug -IceNewk

ICMP Attack

- More info….refer this site
- https://www.netscout.com/what-is-ddos/icmp-flood#:~:text=An%20Internet%20Control%20Message%20Protocol,echo%2Drequests%20(pings).

Transmission Control Protocol

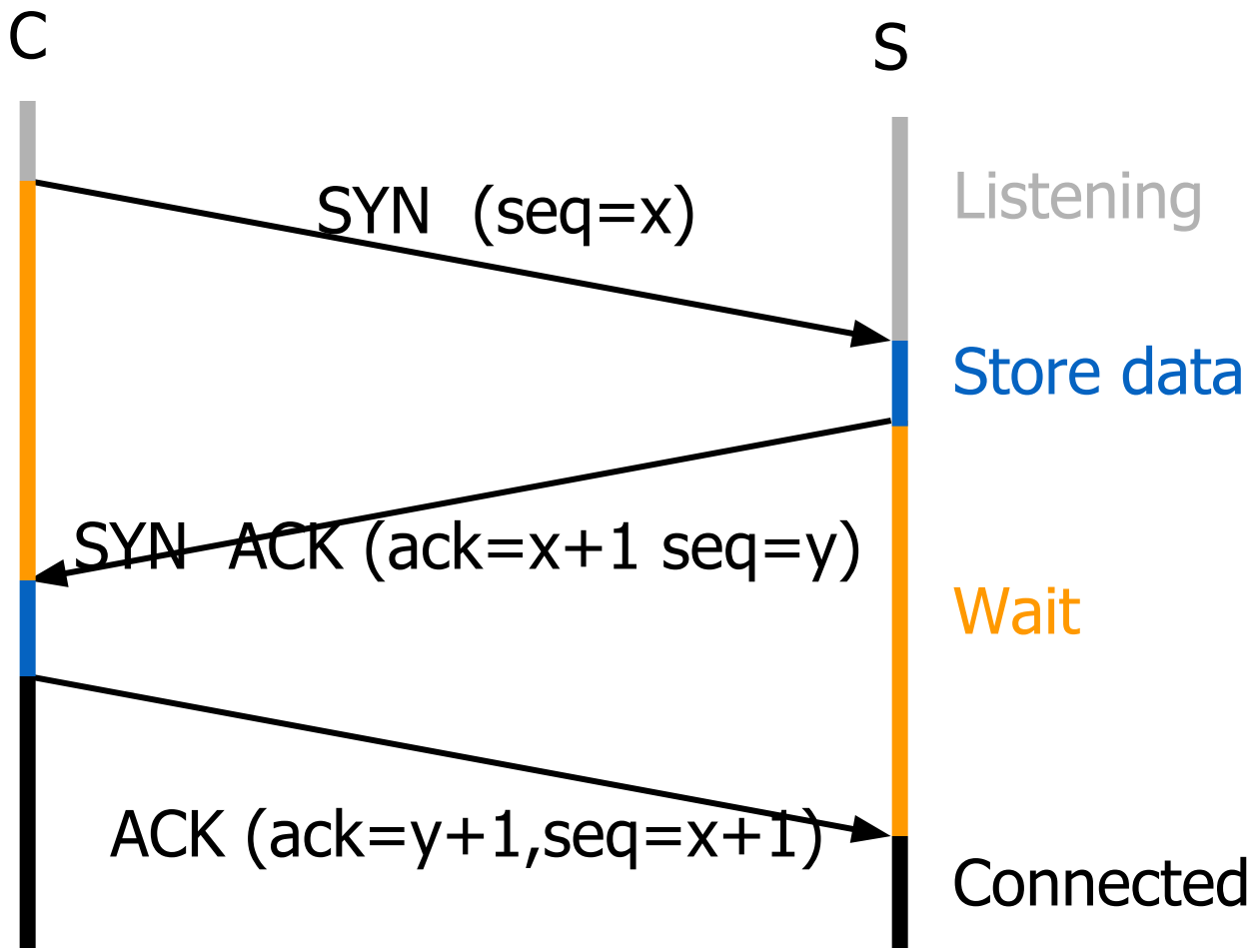
- Connection-oriented, preserves order
  - Sender
    - Break data into packets
    - Attach sequence numbers
  - Receiver
    - Acknowledge receipt; lost packets are resent
    - Reassemble packets in correct order



TCP Sequence Numbers

- Sequence number (32 bits) – has a dual role:
  - If the SYN flag is set, then this is the initial sequence number. The sequence number of the actual first data byte is this sequence number plus 1.
  - If the SYN flag is clear, then this is the accumulated sequence number of the first data byte of this packet for the current session.
- Acknowledgment number (32 bits) –
  - If the ACK flag is set then this the next sequence number that the receiver is expecting.
  - This acknowledges receipt of all prior bytes (if any).

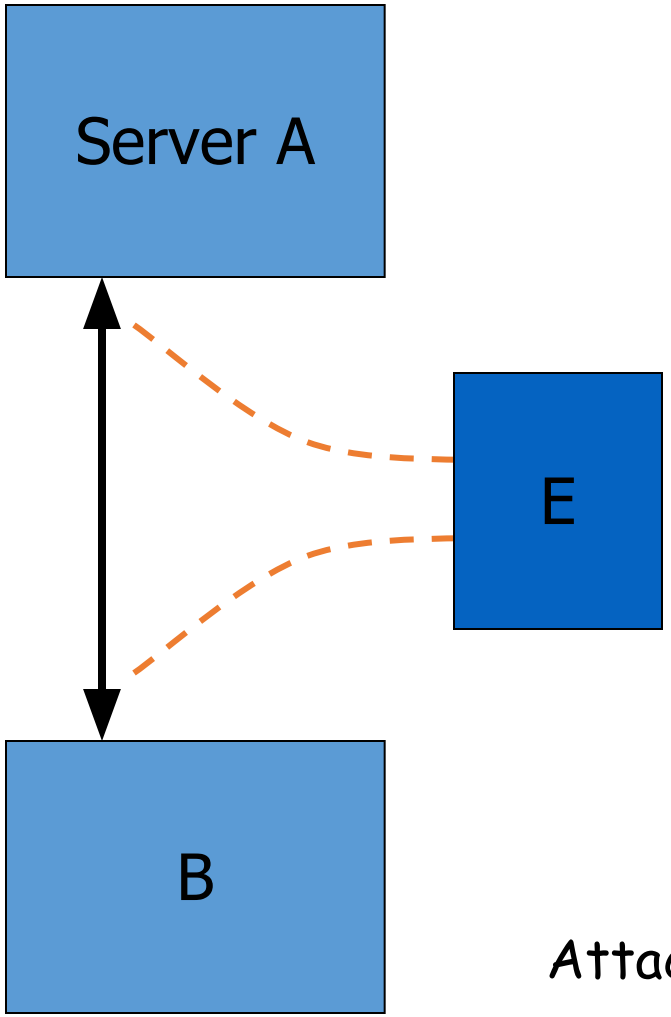
TCP Handshake



TCP sequence prediction attack

- Predict the sequence number used to identify the packets in a TCP connection, and then counterfeit packets.
- Adversary: do not have full control over the network, but can inject packets with fake source IP addresses
  - E.g., control a computer on the local network
- TCP sequence numbers are used for authenticating packets
- Initial seq# needs high degree of unpredictability
  - If attacker knows initial seq # and amount of traffic sent, can estimate likely current values
  - Some implementations are vulnerable

Blind TCP Session Hijacking



- A, B trusted connection
  - Send packets with predictable seq numbers
- E impersonates B to A
  - Opens connection to A to get initial seq number
  - DoS B's queue
  - Sends packets to A that resemble B's transmission
  - E cannot receive, but may execute commands on A

Attack can be blocked if E is outside firewall.

Risks from Session Hijacking

- Inject data into an unencrypted server-to-server traffic, such as an e-mail exchange, DNS zone transfers, etc.
- Inject data into an unencrypted client-to-server traffic, such as ftp file downloads, http responses.
- Spoof IP addresses, which are often used for preliminary checks on firewalls or at the service level.
- Carry out MITM attacks on weak cryptographic protocols.
  - often result in warnings to users that get ignored
- Denial of service attacks, such as resetting the connection.

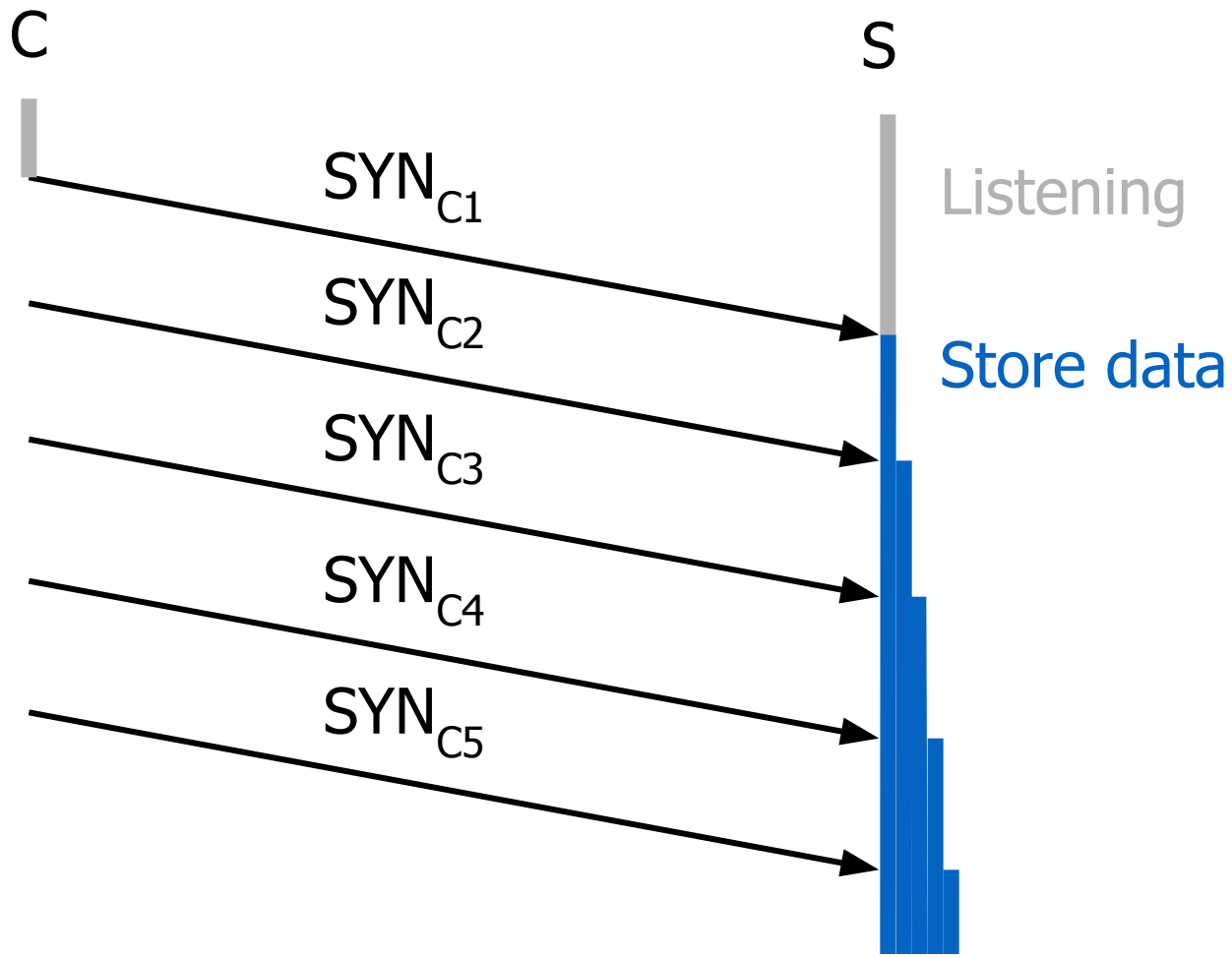
DoS vulnerability caused by session hijacking

- Suppose attacker can guess seq. number for an existing connection:
  - Attacker can send Reset packet to close connection. Results in DoS.
  - Naively, success prob. is $1/2^{32}$ (32-bit seq. #'s).
  - Most systems allow for a large window of acceptable seq. #'s
    - Much higher success probability.
- Attack is most effective against long lived connections, e.g. BGP.

Categories of Denial-of-service Attacks

	Stopping services	Exhausting resources
Locally	• Process killing • Process crashing • System reconfiguration	• Spawning processes to fill the process table • Filling up the whole file system • Saturate comm bandwidth
Remotely	• Malformed packets to crash buggy services	• Packet floods (Smurf, SYN flood, DDoS, etc)

SYN Flooding



SYN Flooding

- Attacker sends many connection requests
  - Spoofed source addresses
- Victim allocates resources for each request
  - Connection requests exist until timeout
  - Old implementations have a small and fixed bound on half-open connections
- Resources exhausted ⇒ requests rejected

- No more effective than other channel capacity-based attack today

TCP Syn Flood Attack

- TCP SYN flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.
- Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

Attack description

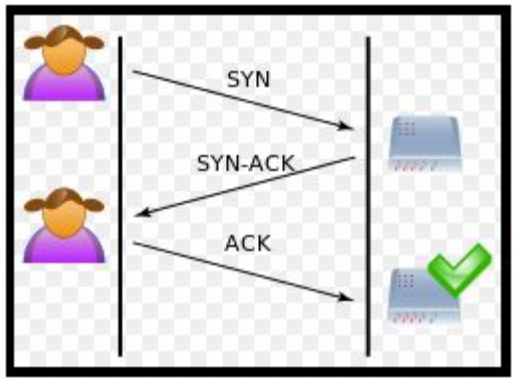
- When a client and server establish a normal TCP “three-way handshake,” the exchange looks like this:

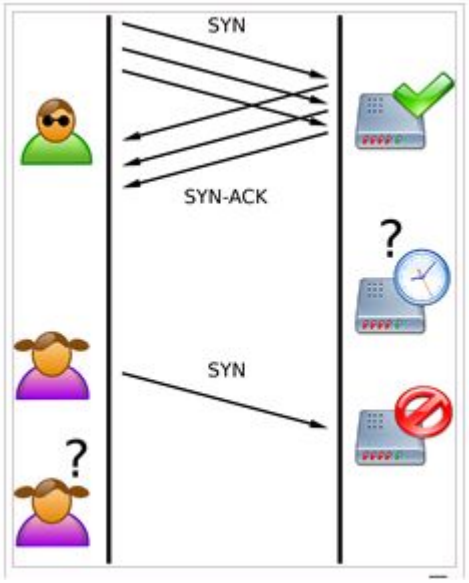
1. Client requests connection by sending SYN (synchronize) message to the server.
2. Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.
3. Client responds with an ACK (acknowledge) message, and the connection is established.

TCP Syn Flood Attack

- In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address.
- The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.
- The malicious client either does not send the expected ACK, or—if the IP address is spoofed—never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet for some time.
- During this time, the server cannot close down the connection by sending an RST packet, and the connection stays open.
- Before the connection can time out, another SYN packet will arrive. This leaves an increasingly large number of connections half-open – and indeed SYN Food attacks are also referred to as “half-open” attacks.
- Eventually, as the server’s connection overflow tables fill, service to legitimate clients will be denied, and the server may even malfunction or crash

normal\Syn flood attack





User Datagram Protocol

- IP provides routing
  - IP address gets datagram to a specific machine
- UDP separates traffic by port (16-bit number)
  - Destination port number gets UDP datagram to particular application process, e.g., 128.3.23.3:53
  - Source port number provides return address
- Minimal guarantees
  - No acknowledgment
  - No flow control
  - No message continuation

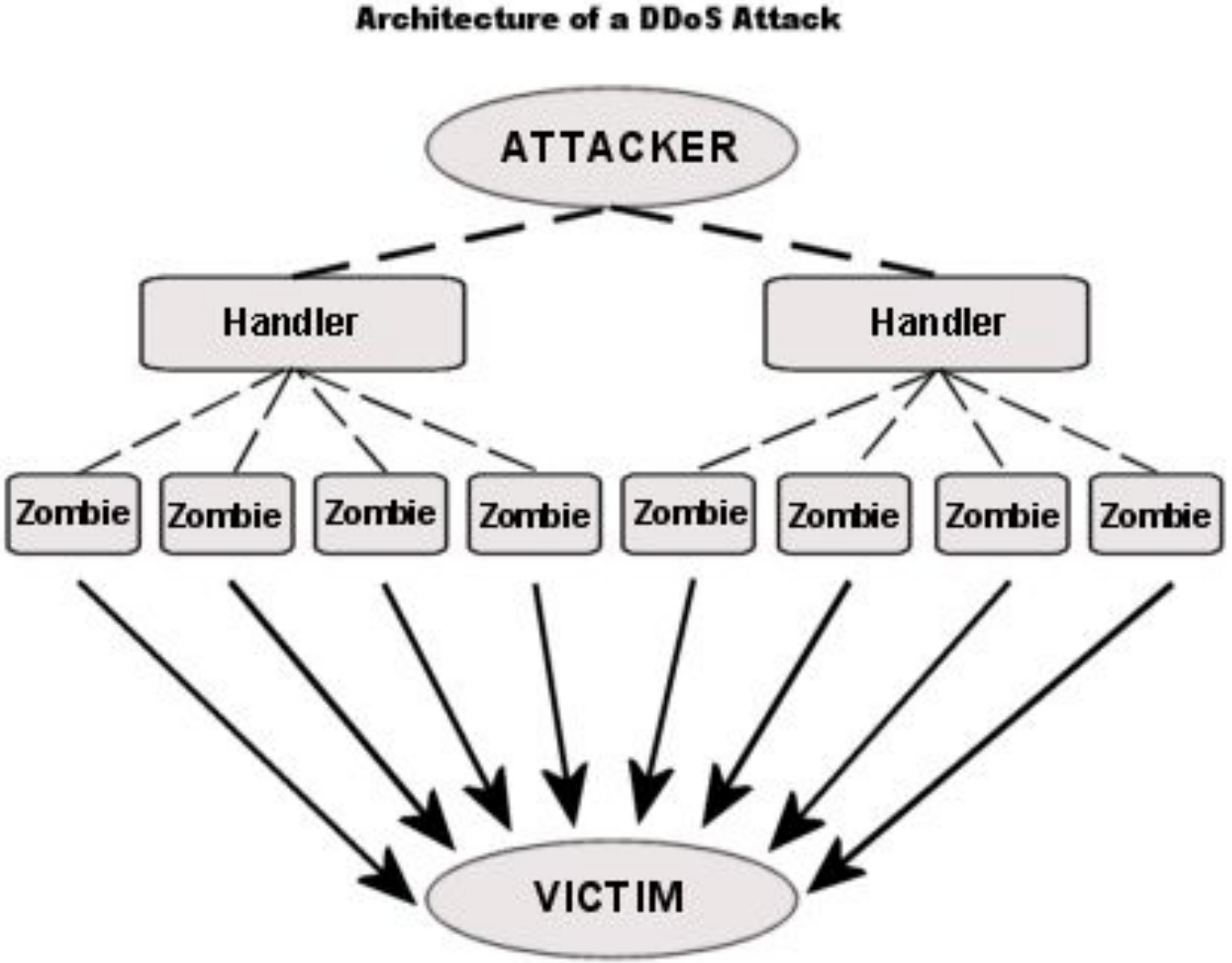
UDP Flood Attack

- UDP is a networking protocol that is both connectionless and session-less. Unlike TCP, UDP traffic does not require a three-way handshake. As such, it requires less overhead and is perfectly suited for traffic such as chat or VoIP that doesn't need to be checked and rechecked.
- The same properties that make UDP ideal for certain kinds of traffic also make it more susceptible to exploitation. Without an initial handshake to ensure a legitimate connection, UDP channels can be used to send a large volume of traffic to any host. There are no internal protections that can limit the rate of a UDP flood. As a result, UDP flood DOS attacks are exceptionally dangerous because they can be executed with a limited amount of resources.

UDP Flood Attack

- A UDP flood is a form of volumetric Denial-of-Service (DoS) attack where the attacker targets and overwhelms random ports on the host with IP packets containing User Datagram Protocol (UDP) packets.
- In this type of attack, the host looks for applications associated with these datagrams.
- When none are found, the host issues a “Destination Unreachable” packet back to the sender.
- The cumulative effect of being bombarded by such a flood is that the system becomes inundated and therefore unresponsive to legitimate traffic.

Distributed DoS (DDoS)



Cryptographic network protection

- Solutions above the transport layer
  - Examples: SSL and SSH
  - Protect against session hijacking and injected data
  - Do not protect against denial-of-service attacks caused by spoofed packets
- Solutions at network layer
  - Use cryptographically random ISNs [RFC 1948]
  - More generally: IPsec
  - Can protect against
    - session hijacking and injection of data.
    - denial-of-service attacks using session resets.