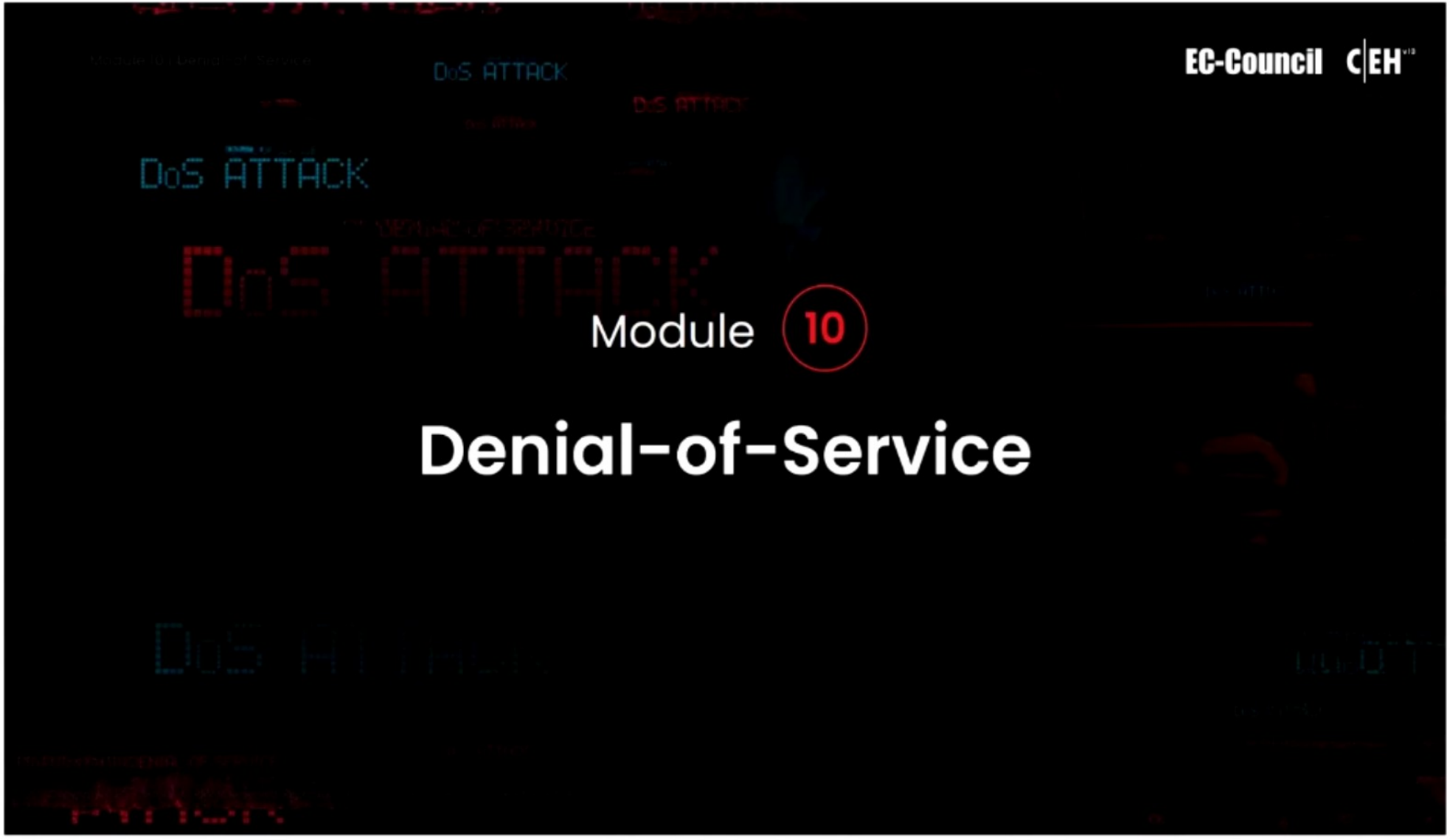

EC-Council
C|EH
DoS ATTACK
DoS ATTACK
DoS ATTACK
Module 10
Denial-of-Service

Learning Objectives

01 Summarize DoS/DDoS Concepts

02 Demonstrate Different DoS/DDoS Attack Techniques

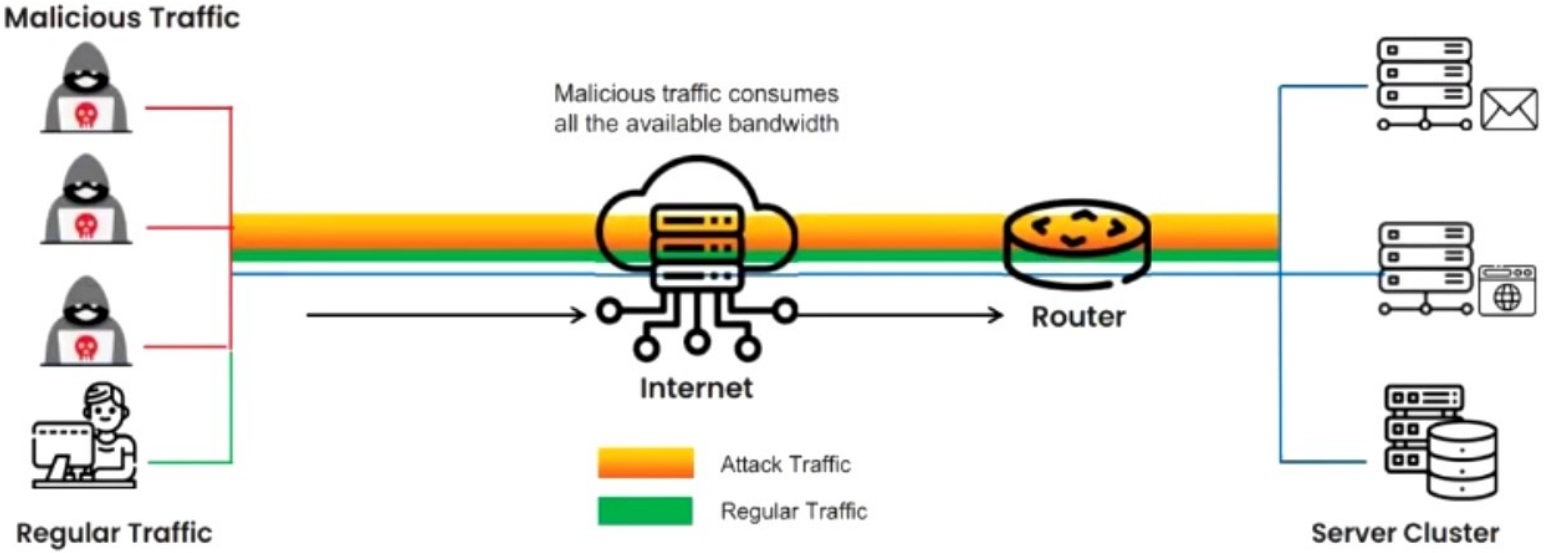
03 Explain DoS/DDoS Attack Countermeasures

Objective 01

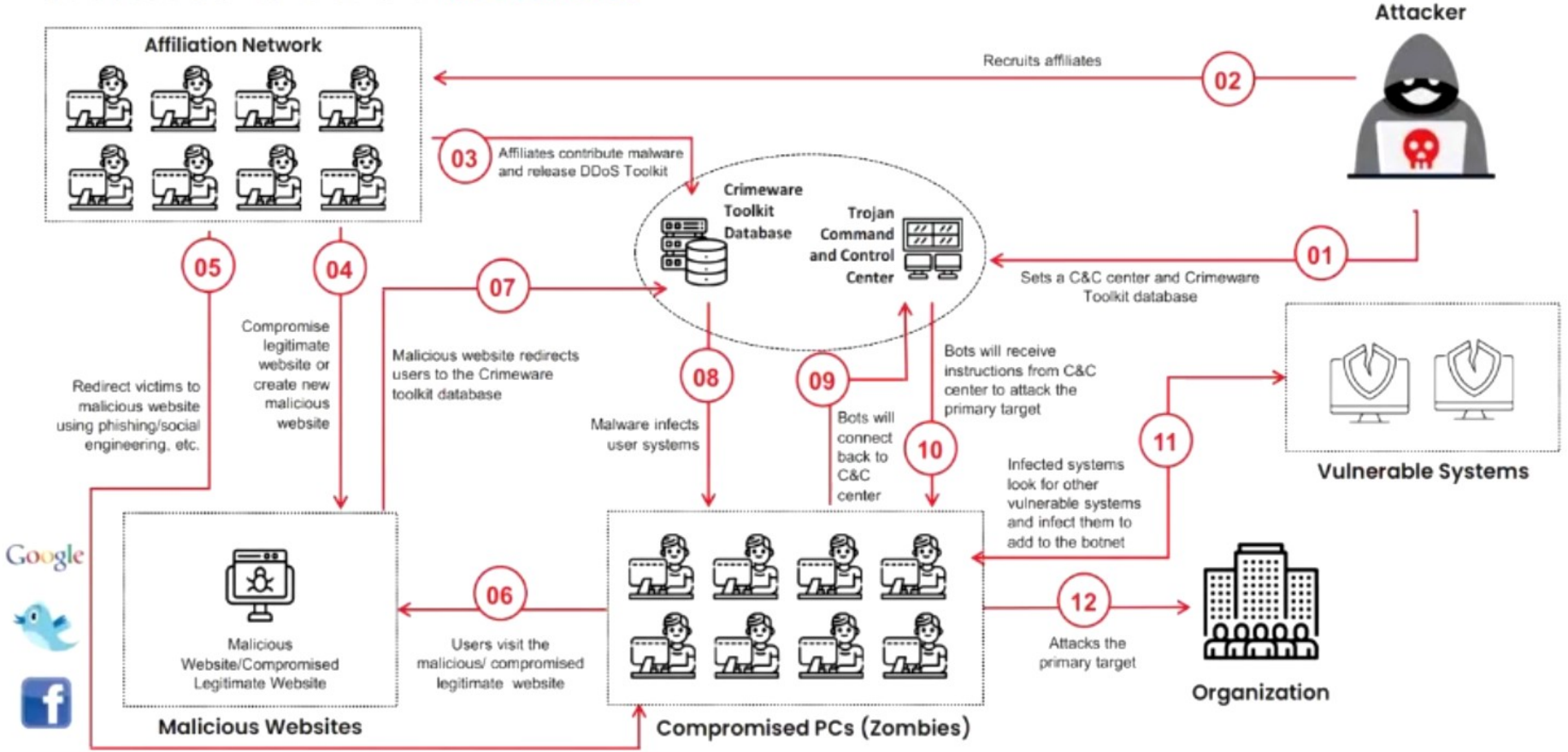
Summarize DoS/DDoS Concepts

What is a DoS Attack?

- Denial-of-Service (DoS) is an attack on a computer or network that **reduces, restricts, or prevents** accessibility of system resources to its legitimate users
- In a DoS attack, attackers flood the victim system with **non-legitimate service requests or traffic** to overload its resources
- The impact of DoS attacks include loss of goodwill, network outages, financial losses, and operational disruptions



What is a DDoS Attack?



Scanning Methods for Finding Vulnerable Machines

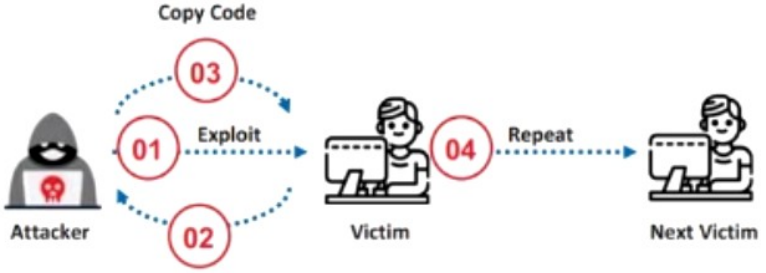
Random Scanning	The infected machine probes **IP addresses** randomly from the **target network IP range** and checks for vulnerabilities
Hit-list Scanning	An attacker first collects a list of **potentially vulnerable machines** and then scans them to find vulnerable machines
Topological Scanning	It uses **information obtained from an infected machine** to find new vulnerable machines
Local Subnet Scanning	The infected machine looks for **new vulnerable machines in its own local network**
Permutation Scanning	It uses a **pseudorandom permutation list of IP addresses** to find new vulnerable machines

How Does Malicious Code Propagate?

Attackers use three techniques to propagate malicious code to newly discovered vulnerable systems

Attackers place an **attack toolkit on the central source**, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system

Central Source Propagation



Back-chaining Propagation

An attacker places an **attack toolkit on his/her own system**, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system

The attacking **host itself transfers** the attack toolkit to the newly discovered vulnerable system **at the exact time that it breaks** into that system

Autonomous Propagation

00:59

Use of Mobile Devices as Botnets for Launching DDoS Attacks

- Android devices are passively **vulnerable to various malware** such as Trojan, bots, and RATs, which are often found in third-party application stores
- These unsecured Android devices are becoming primary targets for attackers to **enlarge their botnet** because they are **highly vulnerable to malware**
- Malicious Android applications found in the **Google Play store** and **drive-by downloads** are just a few examples of **infection methods**
- The attacker **binds the malicious APK server** to the Android application package (**APK file**), **encrypts** it, and **removes unwanted features** and **permissions** before distributing the malicious package to a **third-party app store** like the Google Play Store
- Once the user is **tricked into downloading and installing** such an application, the attacker can gain full control of the victim's device, **enslaving the targeted device** into the **attacker's mobile botnet** to perform malicious activities such as **launching DDoS attacks** and **web injections**

Objective 02

Demonstrate Different DoS/DDoS Attack Techniques

00:59

Basic Categories of DoS/DDoS Attack Vectors

Volumetric Attacks

- Consume the bandwidth of a target network or service
- The magnitude of attack is measured in **bits-per-second (bps)**
- Types of bandwidth depletion attacks:
  - Flood attacks
  - Amplification attacks

Attack Techniques

- **UDP flood attack**
- **ICMP flood attack**
- **Ping of Death and Smurf attack**
- **Pulse wave and zero-day attack**
- **NTP amplification attack**

Protocol Attacks

- Consume other types of resources like **connection state tables** present in network infrastructure components such as **load-balancers**, **firewalls**, and **application servers**
- The magnitude of attack is measured in **packets-per-second (pps)**

Attack Techniques

- **SYN flood attack**
- **Fragmentation attack**
- **Spoofed session flood attack**
- **ACK flood attack**
- **TCP SACK panic attack**

Application Layer Attacks

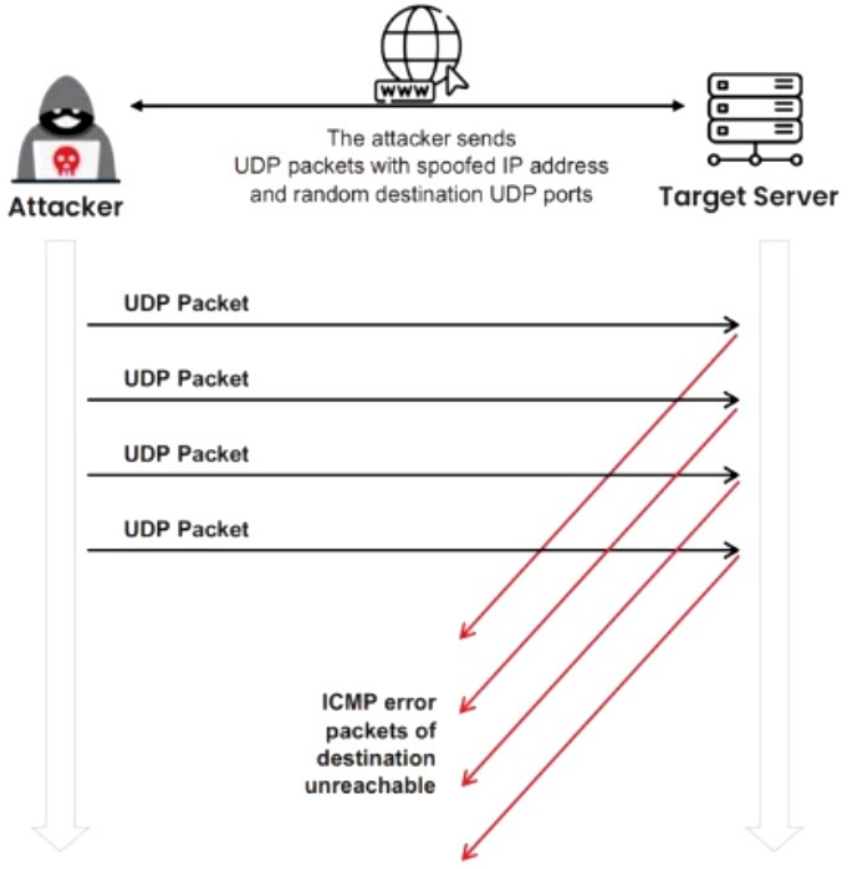
- Consume the **resources or services of an application**, thereby making the application unavailable to other legitimate users
- The magnitude of attack is measured in **requests-per-second (rps)**

Attack Techniques

- **HTTP GET/POST attack**
- **Slowloris attack**
- **UDP application layer flood attack**
- **DDoS extortion attack**

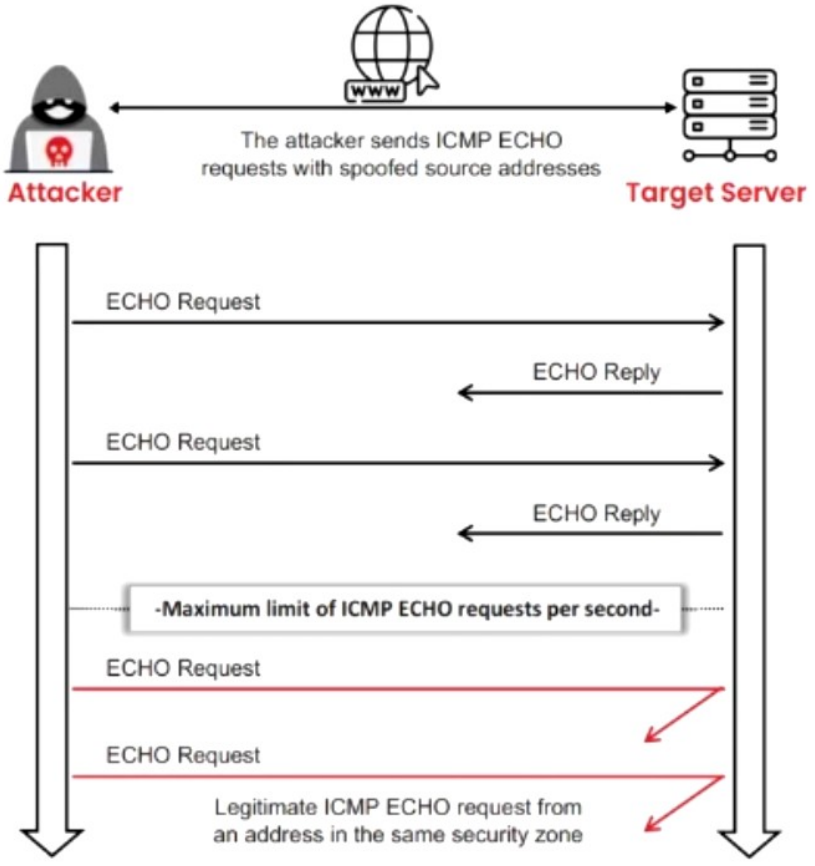
UDP Flood Attack

- An attacker sends **spoofed UDP packets** at a very high packet rate to a remote host on random ports of a target server using a large source IP range
- The flooding of UDP packets causes the server to repeatedly check for **non-existent applications** at the ports
- Legitimate applications are inaccessible by the system and give an **error reply** with an ICMP "Destination Unreachable" packet
- This attack consumes **network resources** and available bandwidth, exhausting the network until it goes offline



ICMP Flood Attack

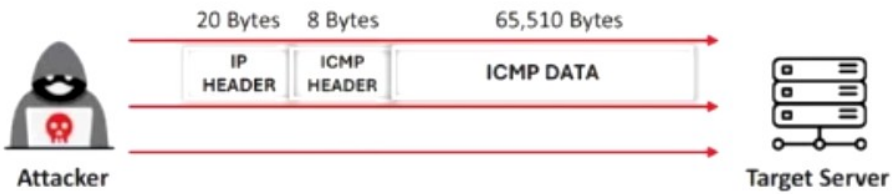
- Network administrators use ICMP primarily for IP operations and troubleshooting, and error messaging is used for **undeliverable packets**
- ICMP flood attacks are a type of attack in which attackers send large volumes of **ICMP echo request packets** to a victim system directly or through reflection networks
- These packets signal the victim's system to reply, and the resulting combination of traffic saturates the bandwidth of the victim's network connection, causing it to be overwhelmed and **subsequently stop** responding to legitimate TCP/IP requests
- To protect against ICMP flood attacks, set a **threshold limit** that invokes an ICMP flood attack protection feature when exceeded



Ping of Death and Smurf Attacks

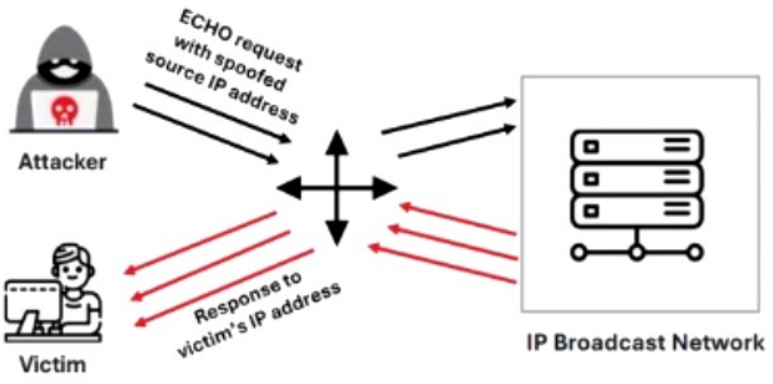
Ping of Death Attack

- In a Ping of Death (PoD) attack, an attacker tries to crash, destabilize, or freeze the targeted system or service by **sending malformed or oversized packets** using a simple ping command
- For instance, the attacker sends a packet which has a size of 65,538 bytes to the target web server. This **packet size exceeds** the size **limit prescribed** by **RFC 791 IP**, which is 65,535 bytes. The reassembly process of the receiving system might cause the system to crash



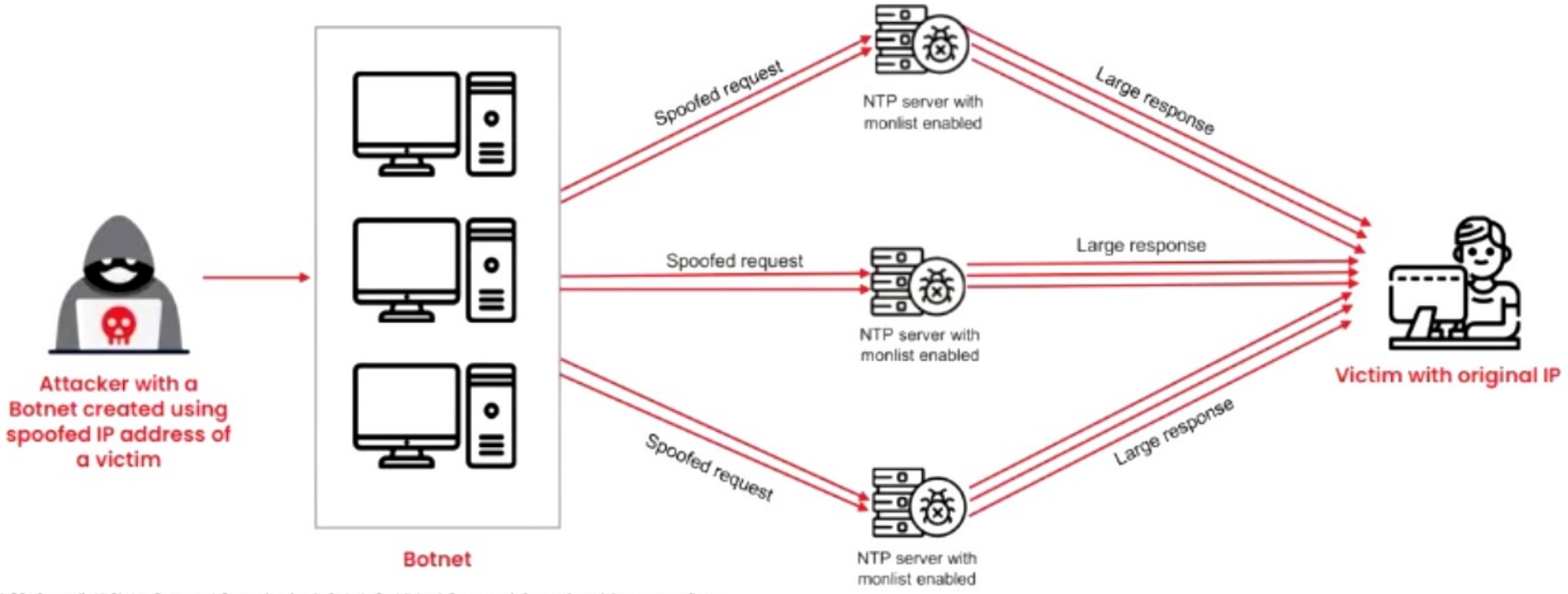
Smurf Attack

- In a Smurf attack, the attacker spoofs the **source IP address** with the victim's IP address and sends a **large number of ICMP ECHO request packets** to an IP broadcast network
- This causes all the hosts on the broadcast network to respond to the received **ICMP ECHO** requests. These responses will be sent to the victim machine, ultimately causing the machine to crash



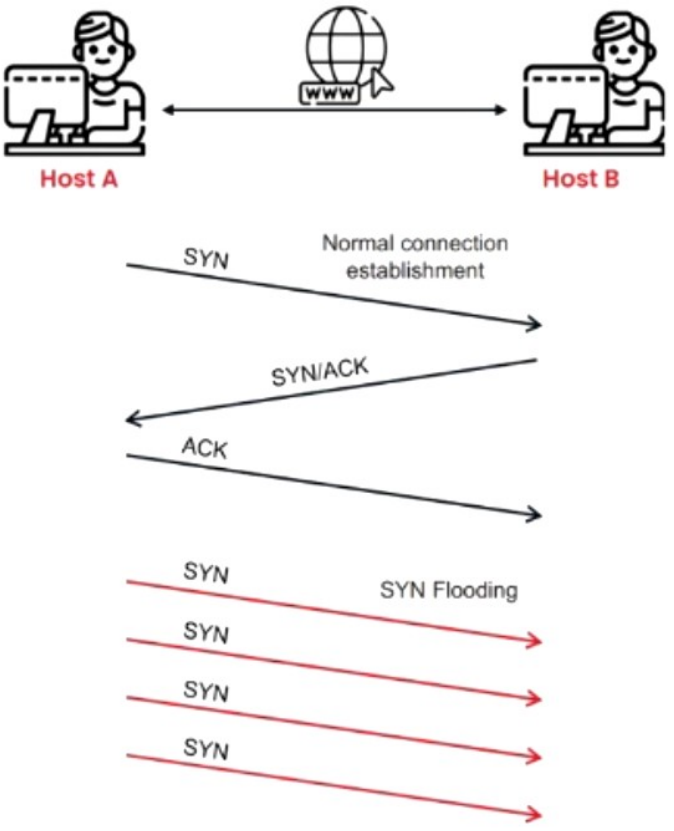
NTP Amplification Attack

- In an NTP amplification attack, the attacker uses a botnet to send large UDP packets through a **spoofed IP address** to the NTP server
- This attack is often initiated through an NTP server that has its **monlist command enabled**
- Each UDP packet triggers a request to the NTP server via the monlist command, which results in the production of **large response packets**



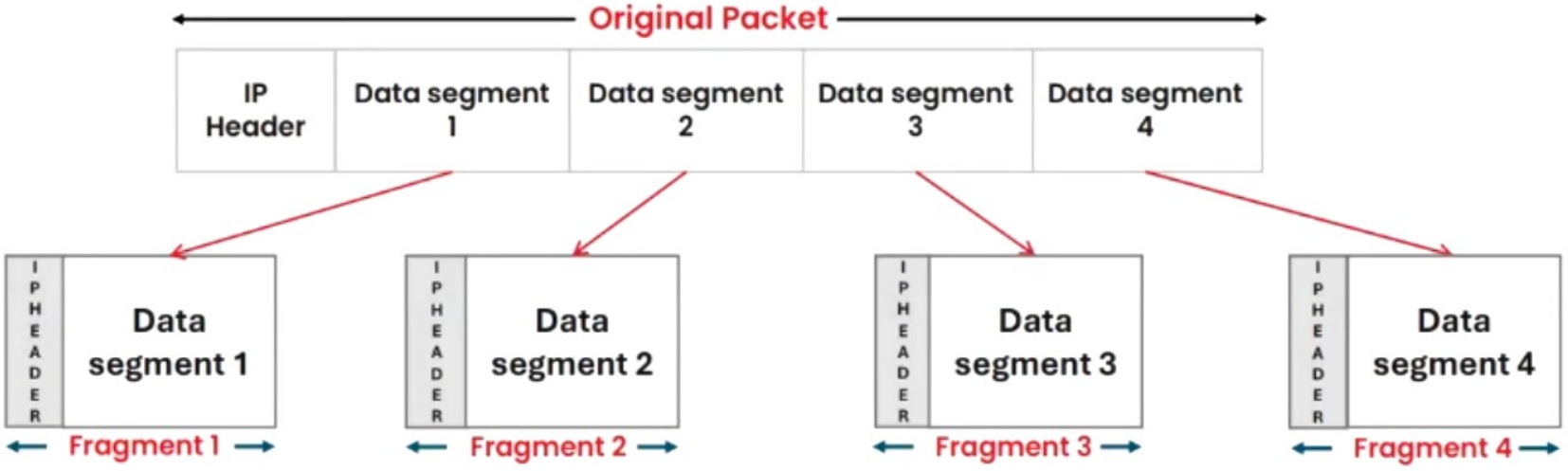
SYN Flood Attack

- The attacker sends a large number of **SYN requests** with **fake source IP addresses** to the target server (victim)
- The target machine sends back a **SYN/ACK** in **response to the request** and waits for the ACK to complete the session setup
- The target machine **does not get the response** because the **source address is fake**
- SYN flooding takes advantage of a flaw in the implementation of the **TCP three-way handshake** in most hosts
- When **Host B** receives the **SYN** request from Host A, it must keep track of the partially opened connection in a **"listen queue"** for **at least 75 seconds**
- A malicious host can exploit the small size of the listen queue by **sending multiple SYN requests** to a host, but **never replying to the SYN/ACK**
- The victim's listen queue is quickly filled up
- The ability to **delay** each incomplete **connection for 75 seconds** can be used cumulatively as a **Denial-of-Service attack**



Fragmentation Attack

- These attacks stop a victim from being able to **re-assemble fragmented packets** by flooding the target system with TCP or UDP fragments, resulting in reduced performance. Attackers send a large number of fragmented (1500+ byte) packets to a **target web server** with a relatively small packet rate
- Because the protocol allows for fragmentation, these packets usually pass uninspected through network equipment such as routers, firewalls, and IDS/IPS
- Reassembling and inspecting these large fragmented packets consumes excessive resources. Moreover, the **content in the packet fragments** will be randomized by the attacker, which in turn makes the process consume more resources, causing the system to crash



Spoofed Session Flood Attack

- Attackers **create fake or spoofed TCP sessions** by carrying multiple **SYN**, **ACK**, and **RST or FIN packets**
- Attackers employ this attack to **bypass firewalls** and **perform DDoS attacks** against the target network, exhausting its network resources

Multiple SYN-ACK Spoofed Session Flood Attack

Attackers create a fake session with **multiple SYN and multiple ACK packets** along with **one or more RST or FIN packets**

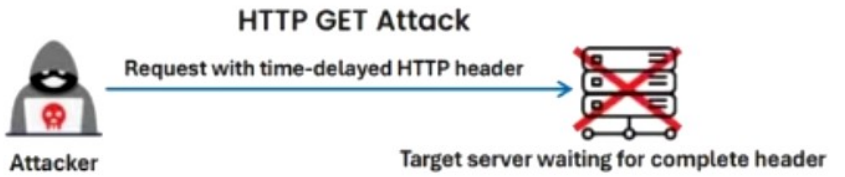
Multiple ACK Spoofed Session Flood Attack

Attackers create a fake session by **completely skipping the SYN packets** and using only **multiple ACK packets** along with **one or more RST or FIN packets**

HTTP GET/POST and Slowloris Attacks

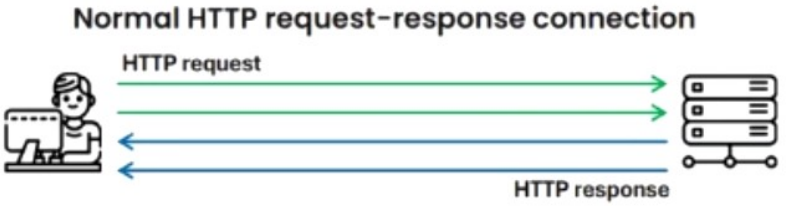
HTTP GET/POST Attack

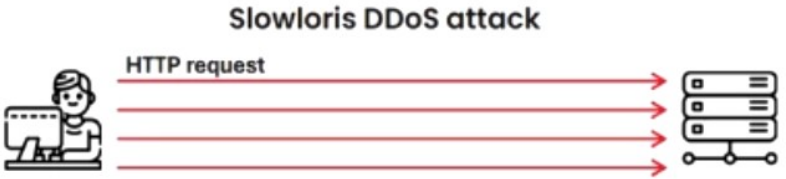
- HTTP clients such as web browsers connect to a web server through the HTTP protocol to send HTTP requests. These requests can be either HTTP GET or HTTP POST
- In an HTTP GET attack, attackers use a time-delayed HTTP header to maintain HTTP connections and exhaust web server resources
- In an HTTP POST attack, attackers send HTTP requests with complete headers but with incomplete message bodies to the target web server or application, prompting the server to wait for the rest of the message body



Slowloris Attack

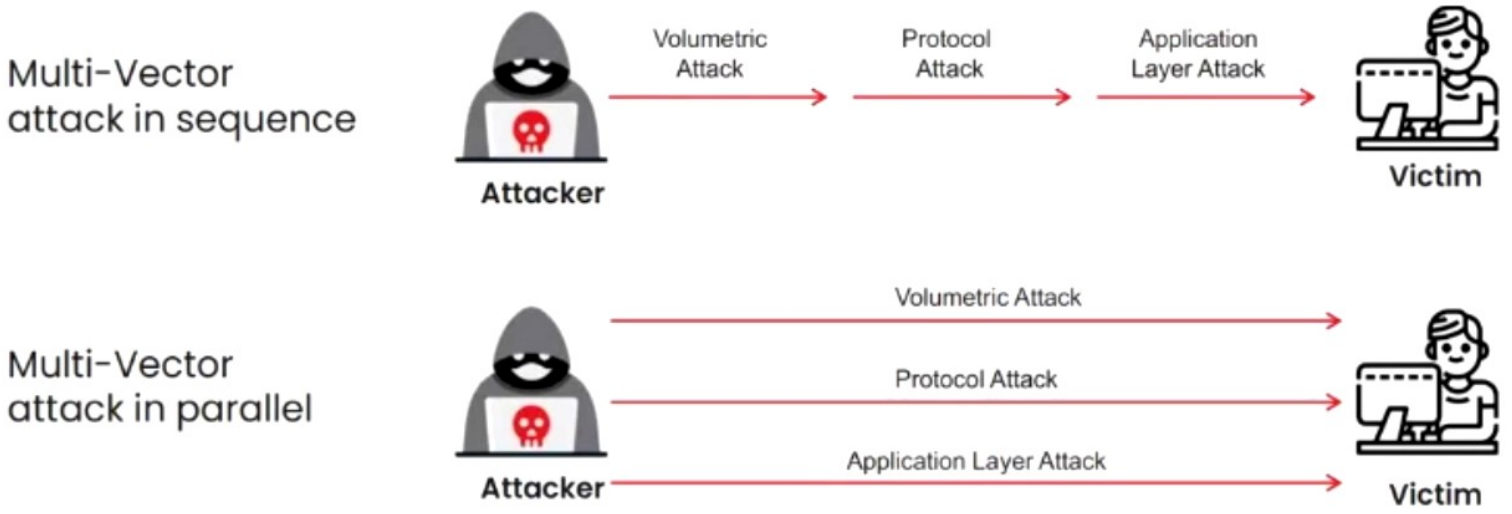
- In the Slowloris attack, the attacker sends partial HTTP requests to the target web server or application
- Upon receiving the partial HTTP requests, the target server opens multiple open connections and keeps waiting for the requests to complete
- These requests will not be complete, and as a result, the target server's maximum concurrent connection pool will be exhausted, and additional connection attempts will be denied





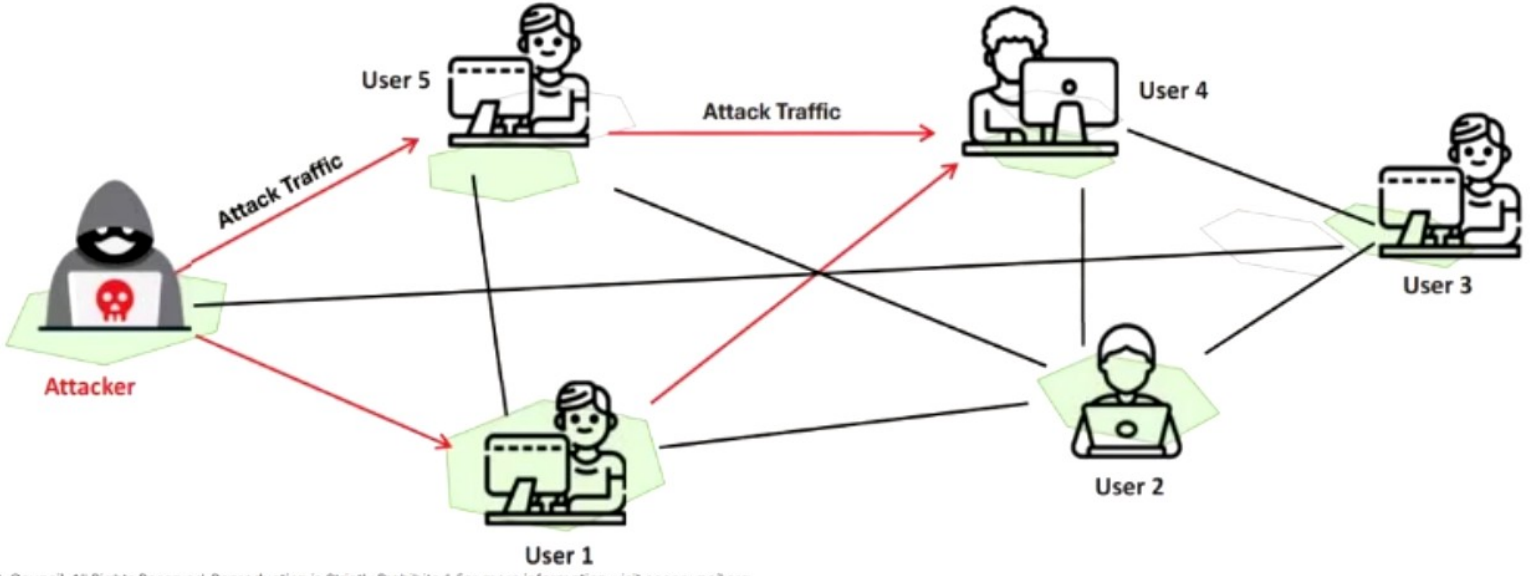
Multi-Vector Attack

- In multi-vector DDoS attacks, the attackers use **combinations of volumetric**, protocol, and application-layer attacks to disable the target system or service
- Attackers rapidly and repeatedly change the form of their DDoS attack (e.g., SYN packets, Layer 7)
- These attacks are either **launched one vector at a time** or in parallel to confuse a company's IT department and exhaust their resources with their focus diverted to the wrong solution



Peer-to-Peer Attack

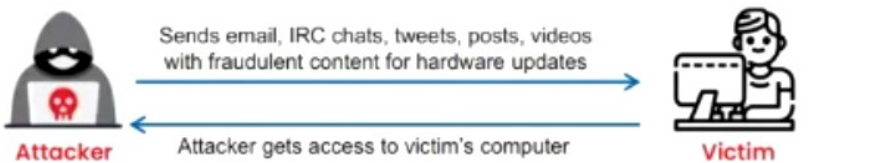
- Using peer-to-peer attacks, attackers **instruct clients of peer-to-peer file sharing hubs** to disconnect from their peer-to-peer network and to connect to the victim's fake website
- Attackers **exploit flaws** found in the network using the DC++ (Direct Connect) protocol, which is used for sharing all types of files between instant messaging clients
- Using this method, attackers launch **massive denial-of-service attacks** and compromise websites



Permanent Denial-of-Service Attack and TCP SACK Panic Attack

Permanent Denial-of-Service Attack

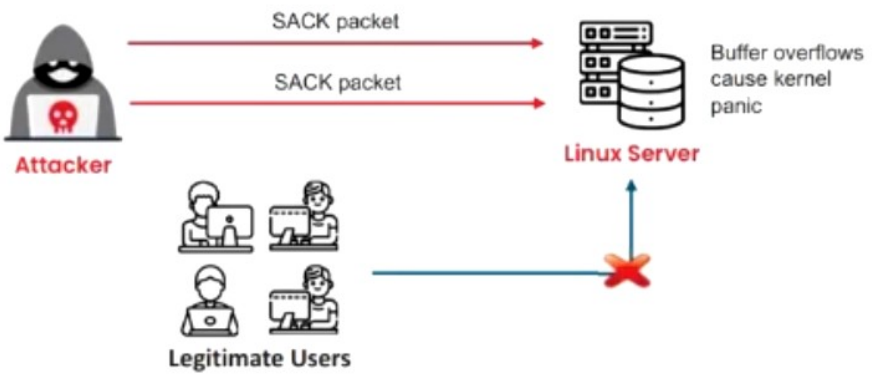
- Permanent DoS, also known as **phlashing**, refers to attacks that cause irreversible damage to system hardware
- Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware
- This attack is carried out using a method known as "**bricking a system**"
- Using this method, attackers send **fraudulent hardware updates** to the victims



(Malicious code is executed)

TCP SACK Panic Attack

- In TCP SACK panic attack, attackers attempt to crash the target Linux machine by **sending SACK packets** with malformed maximum segment size (MSS)
- This attack exploits an **integer overflow vulnerability** in Linux **Socket Buffer (SKB)**, which can lead to kernel panic
- Attackers send SACK packets in sequence to the target server by setting MSS to the **lowest value (48 bytes)**
- The socket buffer exceeds the limit and triggers integer overflow causing a **kernel panic** that leads to denial of service

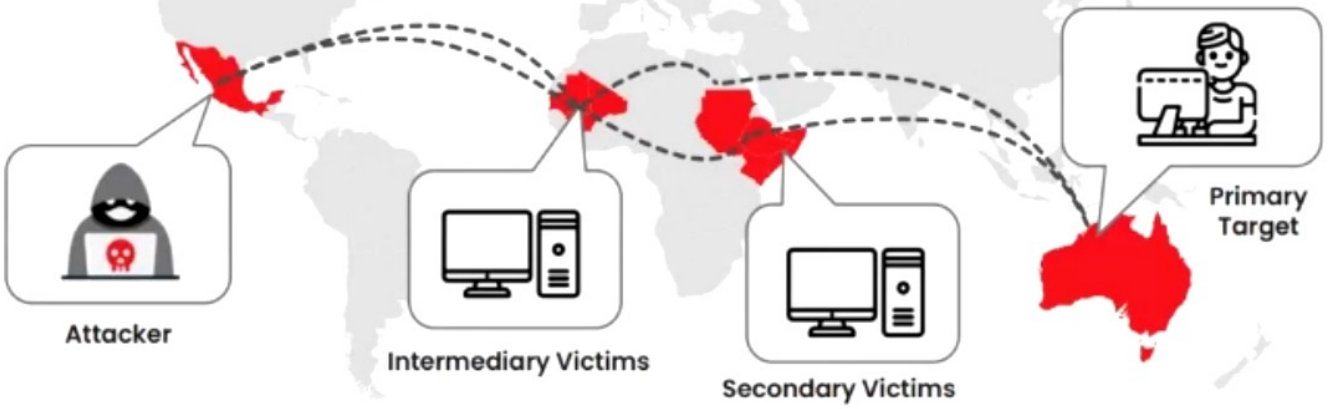


Distributed Reflection Denial-of-Service (DRDoS) Attack

- A distributed reflection denial-of-service attack (DRDoS), also known as a spoofed attack, involves the **use of multiple intermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application
- Attackers launch this attack by sending requests to the intermediary hosts, which then redirect the requests to the secondary machines, which in turn **reflect the attack traffic to the target**

Advantage

- The primary target seems to be directly attacked by the secondary victim rather than the actual attacker
- Multiple intermediary victim servers are used, which results in an increase in attack bandwidth



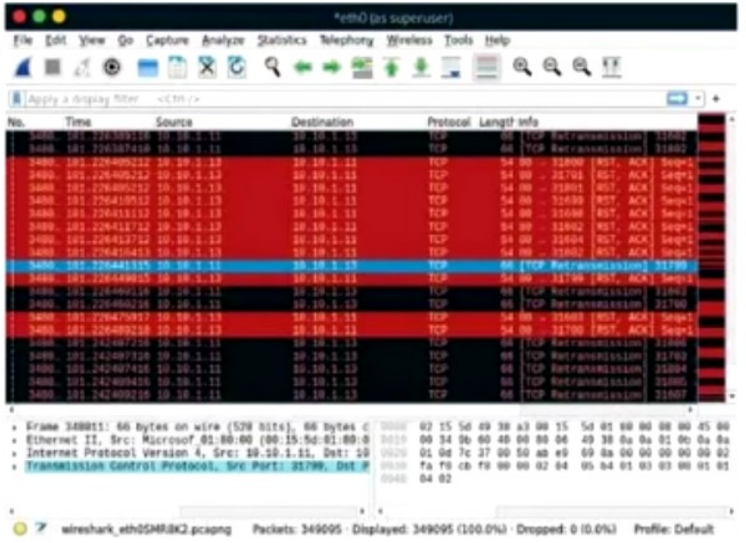
DoS/DDoS Attack Toolkits in the Wild

ISB ISB (I'm so bored) is a **software utility** that helps attackers to perform **HTTP, UDP, TCP** and **ICMP flood** attacks on the target network

https://sourceforge.net

UltraDDOS-v2 UltraDDOS-v2 provides a simple GUI interface where attackers can enter target IP address, port number and number of packets that they desire to transmit

https://sourceforge.net



DoS/DDoS Attack Tools

High Orbit Ion Cannon (HOIC) (*https://sourceforge.net*)

Low Orbit Ion Cannon (LOIC) (*https://sourceforge.net*)

HULK (*https://github.com*)

Slowloris (*https://github.com*)

UFONet (*https://ufonet.03c8.net*)

Objective 03

Explain DoS/DDoS Attack Countermeasures

Detection Techniques

- Detection techniques are based on **identifying and discriminating illegitimate traffic increases** and flash events from legitimate packet traffic
- All detection techniques define an attack as an **abnormal and noticeable deviation** from a threshold of normal network traffic statistics

Activity Profiling

- Activity profiling is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields
- Activity profiles are obtained by monitoring network packet header information
- An attack is indicated by the following:
  - An increase in activity levels among the **network flow clusters**
  - An increase in the overall number of **distinct clusters** (DDoS attack)

Sequential Change-Point Detection

- Change-point detection algorithms isolate changes in network traffic statistics and in the traffic flow rate caused by attacks
- The algorithms filter the **target traffic data** by address, port, or protocol and store the resultant flow as a time series
- The sequential change-point detection technique uses the Cusum algorithm to identify and locate **DoS attacks**
- This technique can also be used to identify the typical scanning activities of network worms

Wavelet-Based Signal Analysis

- Wavelet analysis describes an input signal in terms of **spectral components**
- Analyzing each spectral window's energy determines the presence of anomalies
- Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise

DoS/DDoS Countermeasure Strategies

Absorbing the Attack	• Use additional capacity to absorb the attack • **Requires preplanning** and **additional resources**
Degrading Services	• Identify **critical services** to maintain functionality while stopping non-critical services
Shutting Down the Services	• Shut down all services until the **attack has subsided**

DDoS Attack Countermeasures

Protect Secondary Victims

- Monitor security regularly to remain protected from **DDoS agent software**
- Install **anti-virus** and **anti-Trojan** software and keep them up-to-date
- Increase awareness regarding security issues and prevention techniques among all Internet users
- Disable unnecessary services, uninstall unused applications, and scan all files received from external sources
- Properly configure and **regularly update** the built-in defensive mechanisms in the core hardware and software of systems

Detect and Neutralize Handlers

Network Traffic Analysis

- Analyze communication protocols and traffic patterns between handlers and clients or handlers and agents in order to **identify the network nodes** that might be infected by the handlers

Neutralize Botnet Handlers

- There are usually fewer **DDoS handlers deployed** compared to the number of agents. Neutralizing a few handlers can possibly **render multiple agents** useless, thus thwarting DDoS attacks

Spoofed Source Address

- There is a decent probability that the spoofed source address of DDoS attack packets will not represent a **valid source address of the definite sub-network**

DDoS Attack Countermeasures: Prevent Potential Attacks

Egress Filtering

- Egress filtering **scans the headers of IP packets** leaving a network
- Egress filtering ensures that **unauthorized or malicious traffic** never leaves the internal network
- The packets will not reach the targeted address if they do not meet the necessary specifications

Ingress Filtering

- Ingress filtering **prevents the source address spoofing** of Internet traffic
- It **protects against flooding attacks** originating from valid prefixes (IP addresses)
- It allows the originator to be traced to its true source

TCP Intercept

- TCP intercept features in routers protect TCP servers from TCP SYN-flooding attacks
- Configuring TCP Intercept features **prevents DoS attacks** by intercepting and validating TCP connection requests

Rate Limiting

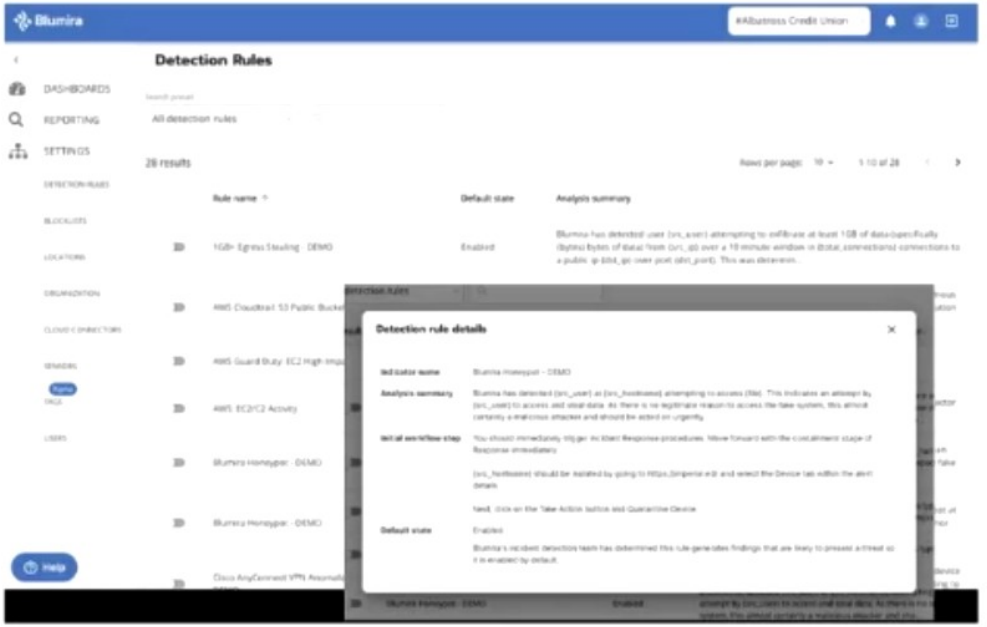
- Rate limiting c**ontrols the rate of outbound or inbound traffic** of a network interface controller
- It **reduces the high-volume inbound traffic** caused by DDoS attacks

DDoS Attack Countermeasures: Deflect Attacks

- Systems that are set up with limited security, also known as **Honeypots**, act as an enticement for an attacker
- Honeypots serve as a means of **gaining information** about attackers, **attack techniques**, and tools by storing a record of the system activities
- The defense-in-depth approach is used with IPSes at different network points to divert **suspicious DoS traffic** to several honeypots

Blumira Honeypot Software

Blumira honeypot software helps security professionals **detect unauthorized access attempts** and the attackers' lateral movement



https://www.blumira.com

DDoS Attack Countermeasures: Mitigate Attacks

Load Balancing

- Increase bandwidth on **critical connections** to absorb additional traffic generated by an attack
- **Replicate servers** to provide additional failsafe protection
- Balance loads on each server in a **multiple-server architecture** to mitigate DDoS attacks

Throttling

- Set routers to access a server with a logic that throttles **incoming traffic** levels to be safe for the server
- Throttling helps in preventing damage to servers by controlling **DoS traffic**
- This method helps routers manage **heavy incoming traffic**, so that the server can handle it
- It filters legitimate user traffic from fake **DDoS attack traffic**

Drop Requests

- In this technique, servers and routers **drop packets** when load increases
- System causes requester to drop the request by making it to solve a difficult puzzle that requires a lot of **memory or computing** power before it can continue with the request

DDoS Attack Countermeasures: Post-Attack Forensics

Traffic Pattern Analysis	• Traffic pattern analysis can help network administrators to develop new **filtering techniques** for preventing attack traffic from entering or leaving their networks • The output of traffic pattern analysis helps in **updating load balancing** and **throttling countermeasures** to enhance efficiency and protection ability
Packet Traceback	• Packet Traceback is similar to **reverse engineering** • It helps in identifying the true **source of attack** and taking necessary steps to block further attacks
Event Log Analysis	• Event log analysis helps in identifying the source of **DoS traffic** • This allows network administrators to recognize the type of DDoS attack, or a combination of attacks used

Techniques to Defend against Botnets

RFC 3704 Filtering

- RFC 3704 filtering limits the impact of DDoS attacks by denying traffic with **spoofed addresses**
- Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link

Cisco IPS Source IP Reputation Filtering

- Reputation services help in determining if an **IP or service** is a source of threat
- Cisco IPS regularly **updates its database** with known threats such as botnets, botnet harvesters, and malwares, and helps in filtering DoS traffic

Black Hole Filtering

- A "black hole" refers to a network node where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient
- Black hole filtering refers to **discarding packets** at the routing level

DDoS Prevention Offerings from ISP or DDoS Service

- **Enable IP Source Guard** (in CISCO) or similar features in other routers to filter traffic based on the **DHCP snooping binding database** or IP source bindings, preventing a bot from succeeding with spoofed packets

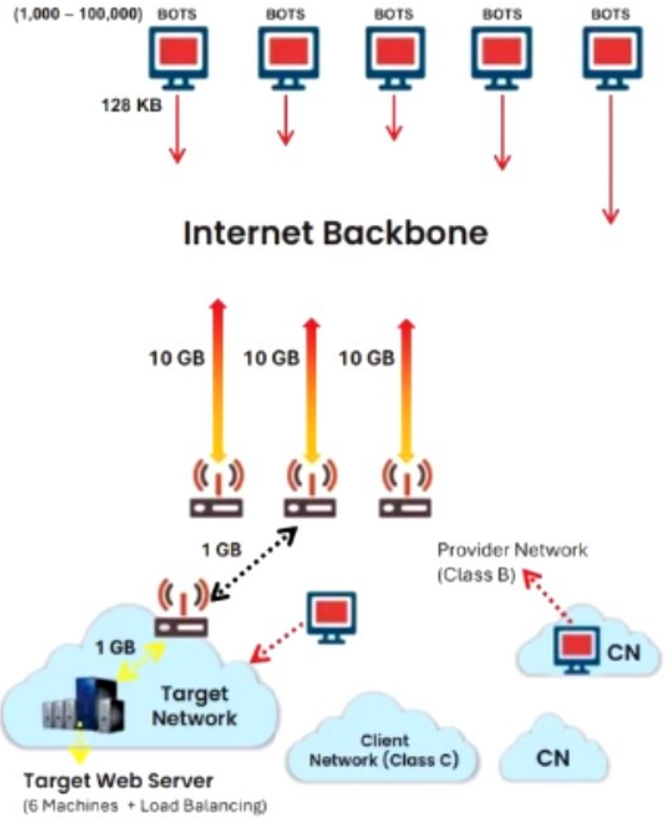
DoS/DDoS Protection at ISP Level

Most ISPs simply block all requests during a **DDoS attack**, **denying even the legitimate traffic** from accessing the service

ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become **saturated by the attack**

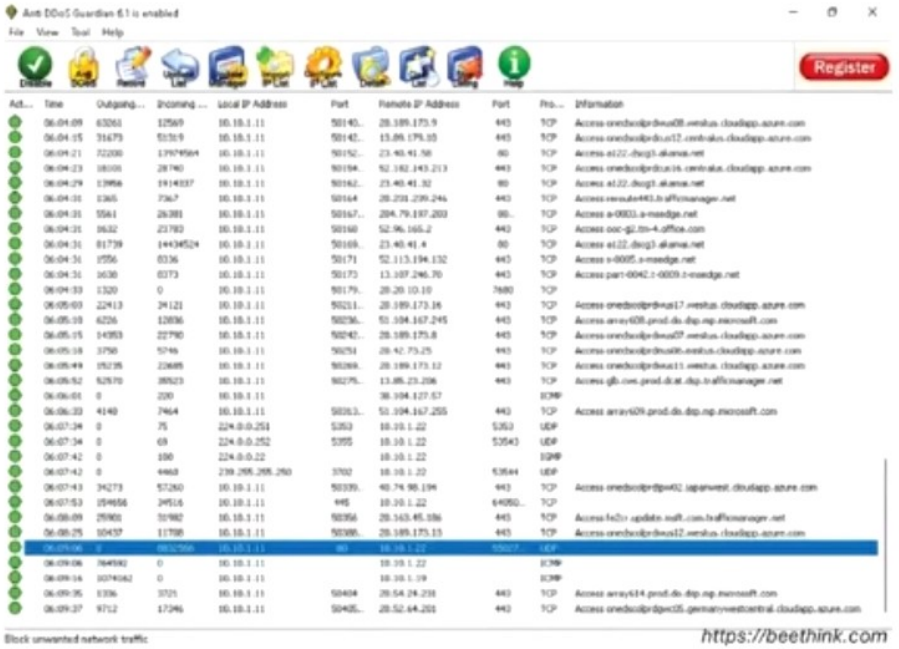
In-the-cloud DDoS protection **redirects attack traffic** to the ISP during the attack and sends it back

Administrators can **request ISPs** to block the original affected IP and move their site to another IP after performing DNS propagation



DoS/DDoS Protection Tools

Anti DDoS Guardian — A DDoS attack protection tool that protects **IIS servers**, **Apache serves**, game servers, Camfrog servers, **mail servers**, FTP servers, VOIP PBX, SIP servers, and other systems



https://beethink.com

DDoS-Guard
https://ddos-guard.net

DOSarrest's DDoS protection service
https://www.dosarrest.com

Radware DefensePro X
https://www.radware.com

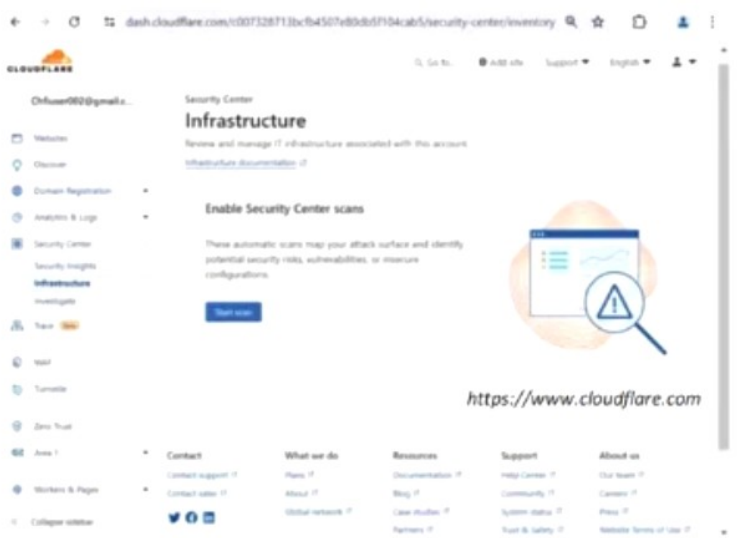
Gatekeeper
https://github.com

F5 DDoS Attack Protection
https://www.f5.com

DoS/DDoS Protection Services

Cloudflare

Cloudflare helps organizations defend against DDoS attacks and secure their networks with a **100 Tbps infrastructure**



Akamai DDoS Protection

Akamai DDoS Protection uses **dedicated infrastructure** to protect Internet-facing **applications** and **systems**, ensuring fast, secure, and always-available DNS services

Additional Services

Stormwall PRO
(*https://stormwall.network*)

Imperva DDoS Protection
(*https://www.imperva.com*)

Nexusguard
(*https://www.nexusguard.com*)

BlockDoS
(*https://www.blockdos.net*)

Module Summary

- In this module, we have discussed the following:
  - ✓ Concepts of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
  - ✓ Concept of botnets along with the botnet ecosystem
  - ✓ Various types of DoS/DDoS attacks
  - ✓ Various DoS/DDoS attack tools
  - ✓ A detailed DDoS case study, namely, the DDoS Attack on Google Cloud - HTTP/2 'Rapid Reset' Attack
  - ✓ We concluded with a detailed discussion on various countermeasures that are to be employed to prevent DoS/DDoS attacks along with various hardware and software DoS/DDoS protection tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform session hijacking to steal a valid session ID