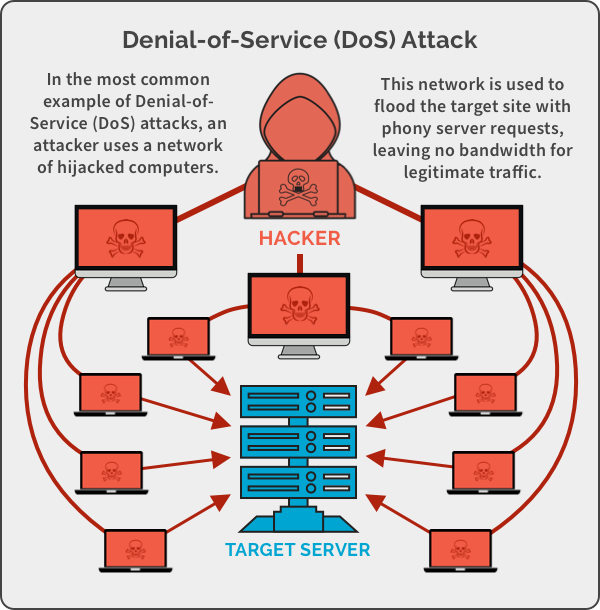
**Denial-of-service**

**What is DoS attack?**

It is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.

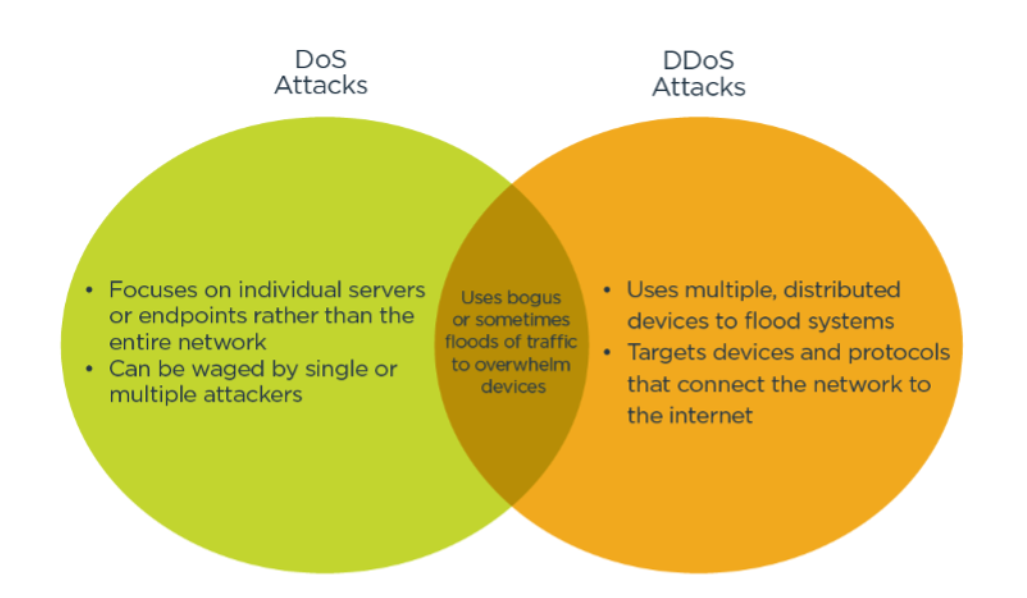


How DoS attack works?

A Denial of Service (DoS) attack floods a target system or network with excessive traffic, overwhelming its resources and causing it to become slow, unresponsive, or completely unavailable. Attackers typically exploit vulnerabilities or consume bandwidth, rendering the target incapable of handling legitimate requests from users.

**What is DDoS attack?**

A Distributed Denial of Service (DDoS) attack is a type of DoS attack where multiple compromised devices (often part of a botnet) are used to flood a target with massive traffic, making it difficult to defend against. DDoS attacks aim to overwhelm and disrupt services, causing widespread outages.



**Botnets:**

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

A botnet is a network of infected devices (bots) controlled by a central entity, called a "botmaster." These devices, often compromised through malware, can perform coordinated actions like launching DDoS attacks, sending spam, or stealing data. Botnets allow attackers to execute large-scale operations without direct control over each device.

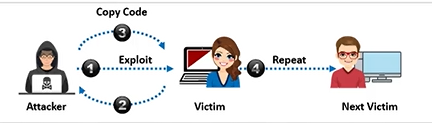
**Scanning methods for finding vulnerable machines:**

1. Random scanning
2. Hit-list scanning
3. Topological scanning
4. Local subnet scanning
5. Permutation scanning

**How Does Malicious Code propagate?**

Three techniques to do so:

1. Central Source propagation
2. Back-chaining Propagation



1. Autonomous propagation



**Basic categories of DoS/DDoS attack vectors:**

1. Volumetric attacks: measured in bits-per-second (bps)

Attack techniques:

1. UDP flood attack
2. ICMP flood attack
3. Ping of death and smurf attack
4. Pulse wave and zero-day attack
5. Protocol attacks: measured in packets-per-second (pps)

Attack techniques:

1. SYN flood attack
2. Fragmentation attack
3. Spoofed session flood attack
4. ACK flood attack
5. TCP SACK panic attack
6. Application layer attacks: measured in requests-per-second (rps)

Attack techniques:

1. HTTP GET/POST attack
2. Slowloris attack
3. UDP application layer flood attack
4. DDoS extortion attack

**UDP Flood attack:**

A UDP flood attack is a type of Denial of Service (DoS) attack where an attacker sends a large number of User Datagram Protocol (UDP) packets to random ports on a target system, overwhelming it and causing disruption.

Start

│

▼

Attacker initiates UDP flood

│

▼

Send UDP packets to random ports on the target server

│

▼

Target server receives packets

│

▼

Server checks for open ports

│

▼

If port is closed, server sends ICMP "Destination Unreachable" message

│

▼

Server consumes resources trying to process invalid requests

│

▼

Target becomes overwhelmed (CPU/Network resources exhausted)

│

▼

Service disruption (Denial of Service)

│

▼

Attack ends (when attacker stops or target mitigates)

│

▼

End

**ICMP Flood attack:**

An ICMP flood attack is a type of Denial of Service (DoS) attack where the attacker sends a large number of ICMP Echo Request (ping) packets to a target system. This overloads the target's resources, causing network congestion and disruption.

**Ping of Death and Smurf Attacks:**

A **Ping of Death** is a type of DoS attack where an attacker sends an oversized ICMP packet to a target system. When reassembled, the oversized packet can cause the system to crash or malfunction.

A **Smurf attack** is a type of DoS attack that exploits a network's broadcast address. An attacker sends spoofed ICMP echo requests to the broadcast address, causing numerous systems to send reply packets to the target, overwhelming it.

**Pulse Wave attacks:**

In a pulse wave DDoS attack, attackers send a highly repetitive, periodic train of packets as pulses to the target victim every 10 minutes, and each specific attack session can last for a few hours to days.

**Zero-day DDoS attack:**

A zero-day DDoS attack is a cyberattack that exploits a previously unknown vulnerability in a system's software or hardware to launch a DDoS attack. This means that the vulnerability has not been discovered or patched by the software or hardware vendor, leaving the system vulnerable to attack.

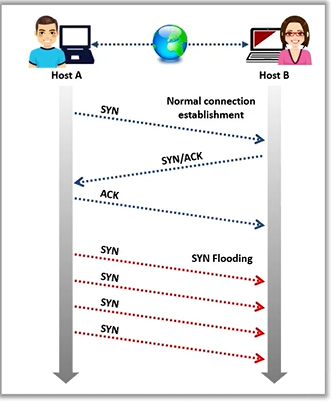
**Key characteristics of a Zero-Day DDoS Attack:**

* Exploits unknown vulnerabilities
* Prevents immediate defense
* Severe consequences

These attacks are particularly dangerous because they can be launched with little to no warning, and there may be no immediate way to mitigate the damage.

**SYN flood attack:**

A SYN flood attack is a type of denial-of-service (DoS) attack where an attacker overwhelms a target system with a large number of SYN (synchronize) packets. These packets initiate a TCP connection but never complete the handshake, filling up the target's connection queue and preventing legitimate users from connecting.



**Fragmentation Attack:**

A Fragmentation Attack is a type of DoS attack where an attacker sends a large number of fragmented packets to a target system. These fragmented packets overwhelm the system's resources as it tries to reassemble them. This can lead to system crashes, network outages, and denial of service.

**HTTP GET/POST Attacks:**

In this type of attack, the attacker sends malformed HTTP requests to a web server. These requests can either have delayed headers or incomplete bodies.

* **Delayed Headers:** The attacker sends an HTTP request with a delayed header, causing the server to wait for the complete header before processing the request. This ties up server resources and prevents it from handling other requests.
* **Incomplete Bodies:** The attacker sends an HTTP request with an incomplete body, leaving the server waiting for the complete body. This also ties up server resources and can lead to denial of service.

**Slowloris Attacks:**

In a Slowloris attack, the attacker sends a series of partial HTTP requests to a web server. Each request is only partially complete, but it's enough to establish a connection with the server. The server keeps these connections open, waiting for the complete requests. Over time, the server can become overwhelmed with these incomplete connections, leading to a denial of service.

The key difference between HTTP GET/POST and Slowloris attacks is the way they consume server resources. HTTP GET/POST attacks consume resources by keeping connections open for extended periods, while Slowloris attacks consume resources by maintaining a large number of half-open connections.

**UDP Application Layer Flood attack:**

The image lists UDP-based application layer protocols that attackers can use to flood target networks. These protocols include CharGEN, SNMPv2, QOTD, RPC, SSDP, CLDAP, TFTP, NetBIOS, NTP, Quake Network Protocol, Steam Protocol, and VoIP. By exploiting these protocols, attackers can overwhelm target systems with excessive traffic, leading to denial-of-service conditions.

**Multi-vector DDoS attack:**

Multi-vector DDoS attacks combine volumetric, protocol, and application-layer attacks to overwhelm targets. Attackers rapidly switch between attack types or launch them simultaneously to confuse defenses and deplete resources. This makes them harder to mitigate than single-vector attacks.

**Peer-to-Peer attack:**

Attackers instruct clients of peer-to-peer file sharing hubs (like DC++) to disconnect from their network and connect to a fake website. This floods the target website with traffic, overwhelming it and causing a denial-of-service attack.

**Permanent Denial-of-Service Attack:**

This attack aims to permanently damage the target system's hardware, rendering it unusable. Attackers often use fraudulent firmware updates to trick victims into installing malicious code that bricks their devices. This requires replacing or reinstalling the damaged hardware.

**TCP SACK Panic Attack:**

This attack exploits a vulnerability in Linux systems by sending malformed TCP Selective Acknowledgment (SACK) packets with a low Maximum Segment Size (MSS). This causes the system's socket buffer to overflow, leading to a kernel panic and system crash.

**Distributed Reflection Denial-of-Service (DRDoS) attack:**

In a Distributed Reflection Denial-of-Service (DRDoS) attack, attackers use multiple intermediary and secondary machines to launch a DDoS attack on a target. The attacker sends requests to intermediary hosts, which then redirect them to secondary victims, who unknowingly reflect the traffic to the target. This amplifies the attack and makes it harder to trace back to the attacker.

**DDoS extortion attacks:**

DDoS extortion attacks, also known as ransom DDoS (RDDoS), involve attackers threatening organizations with DDoS attacks unless they pay a ransom. Attackers send ransom notes with payment instructions and warnings of future attacks. They may also exploit known vulnerabilities or threaten to expose sensitive data.

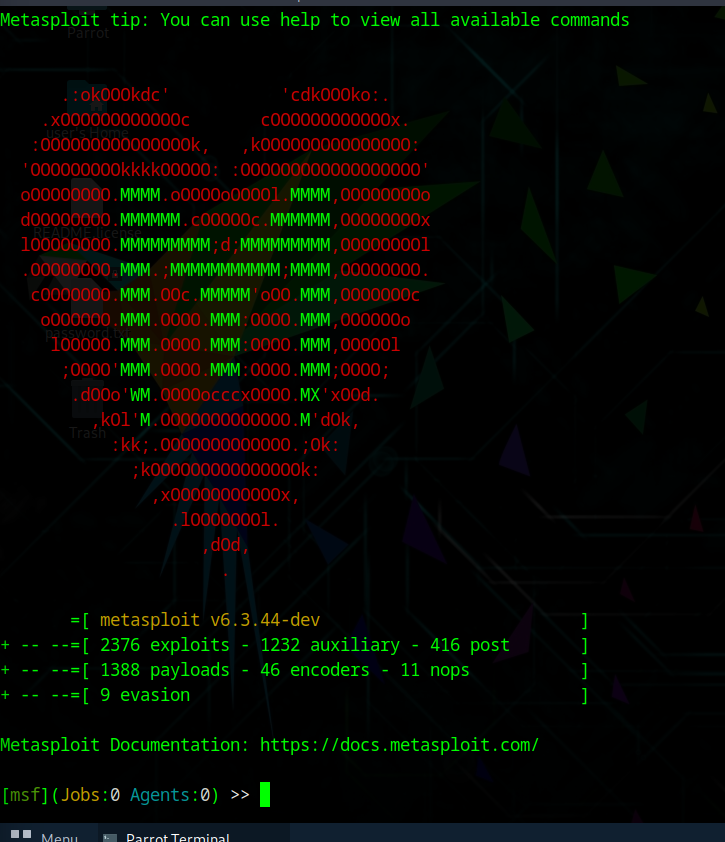
Tools for it:

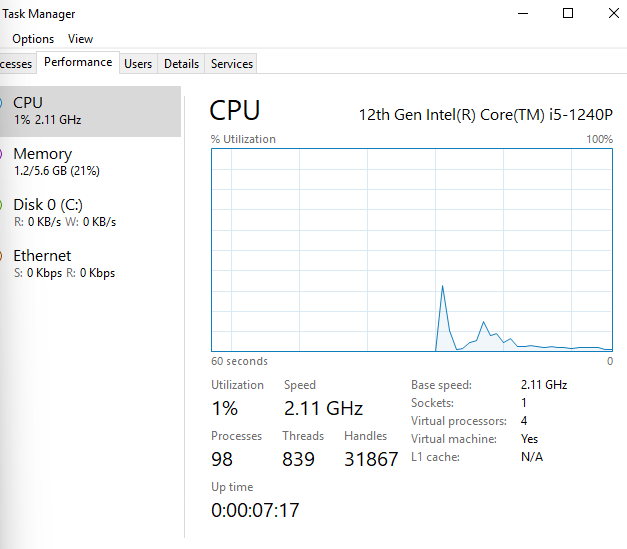
1. HOIC
2. LOIC
3. XOIC
4. Metasploit

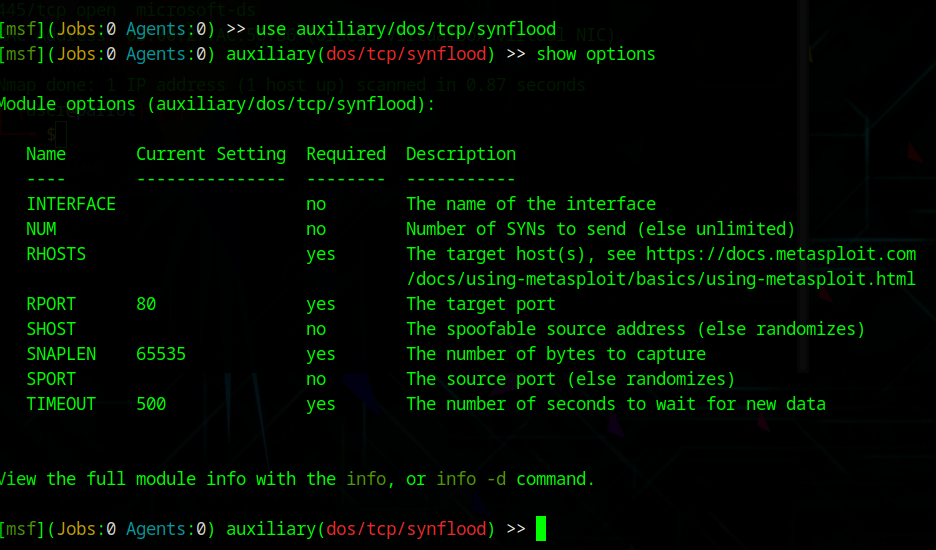
**DoS/DDoS countermeasure strategies:**

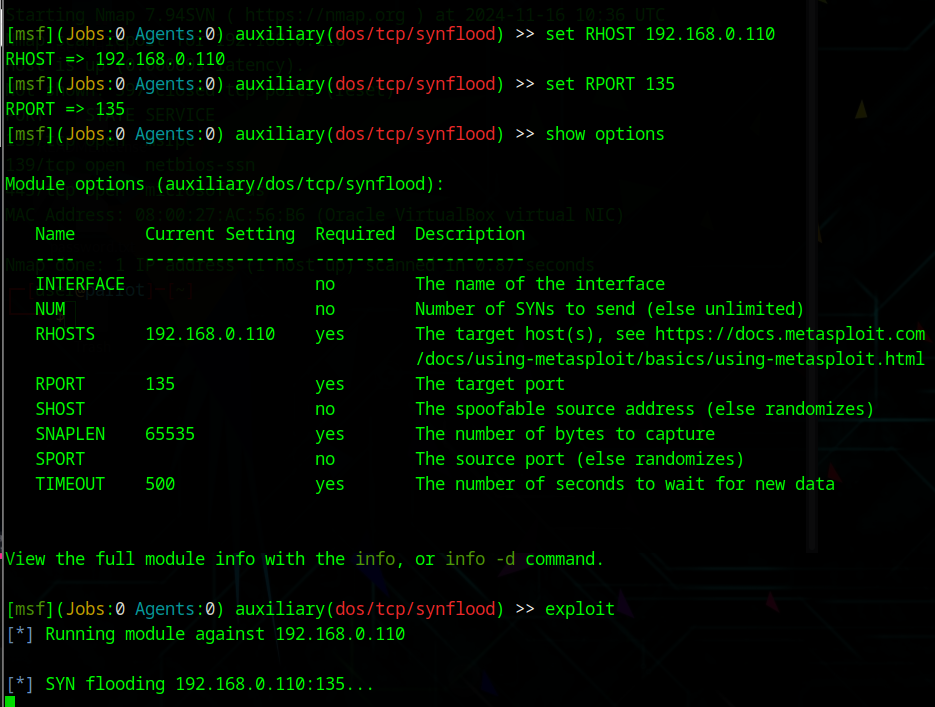
1. Absorbing the attack
2. Degrading services
3. Shutting down the services

**DOS attack (synflood) using Metasploit:**

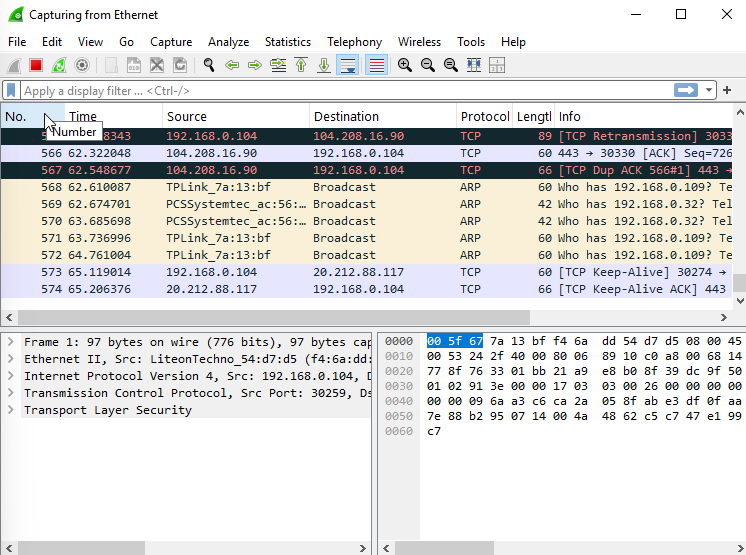
****

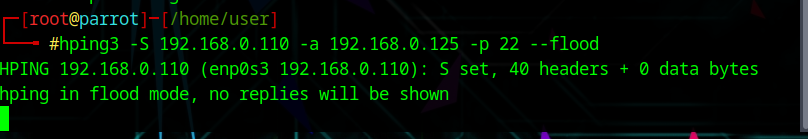
****

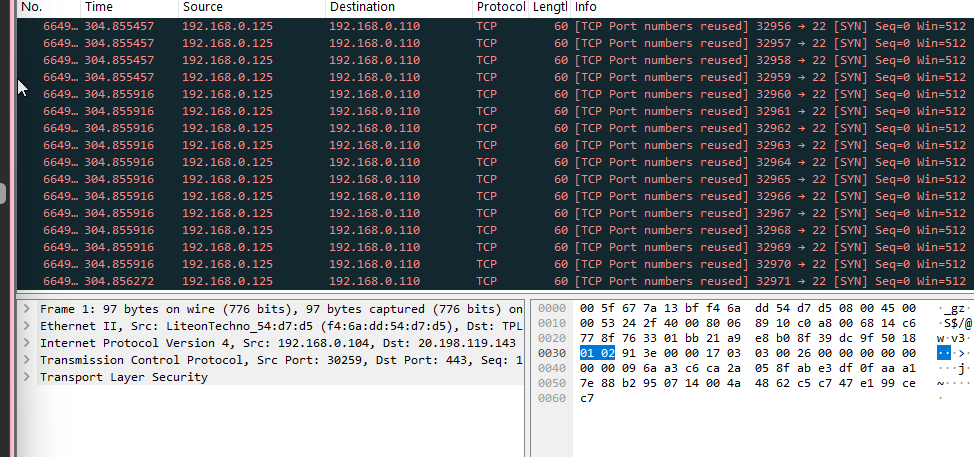
****

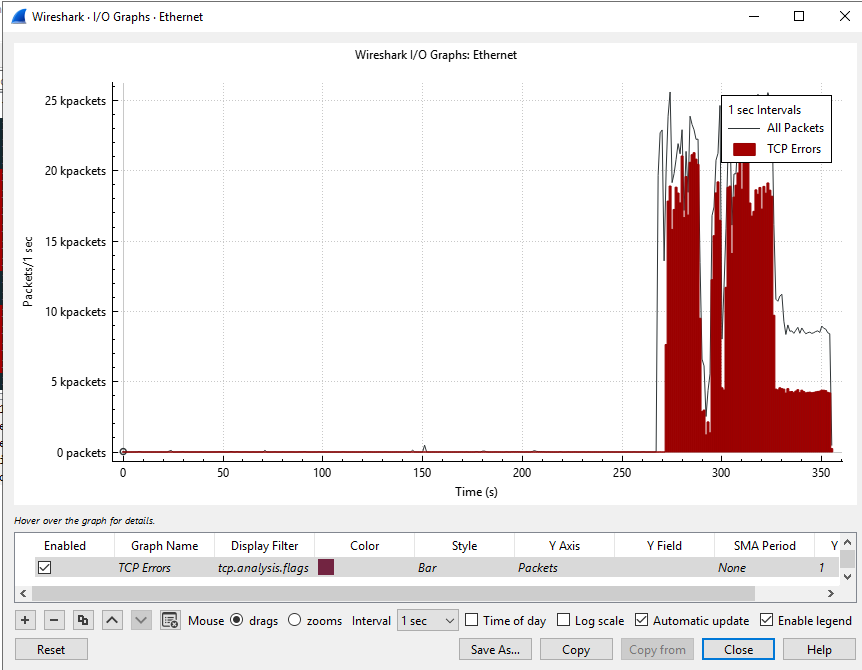
****

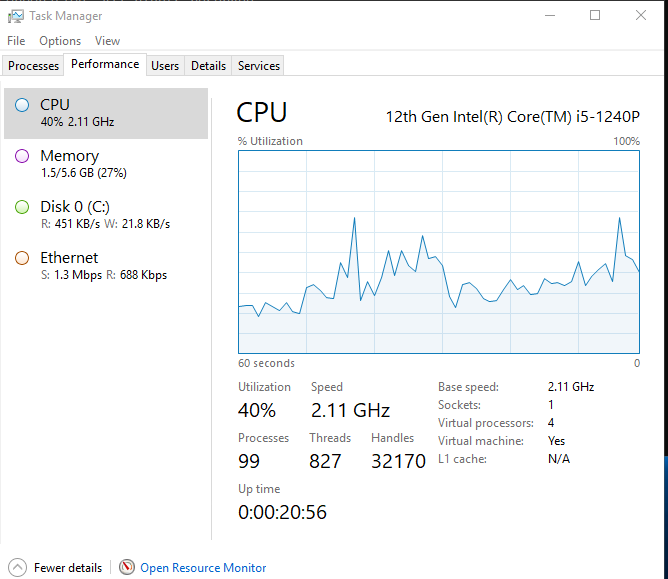
**Perform a DoS attack on a target host using hping3:**

****

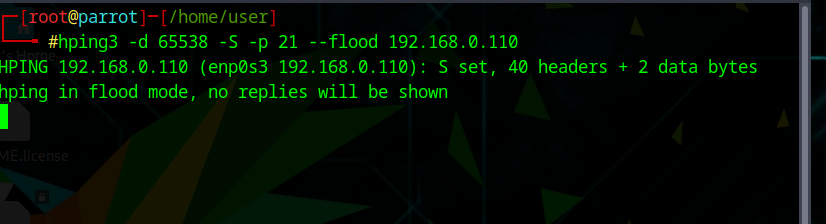
****

****

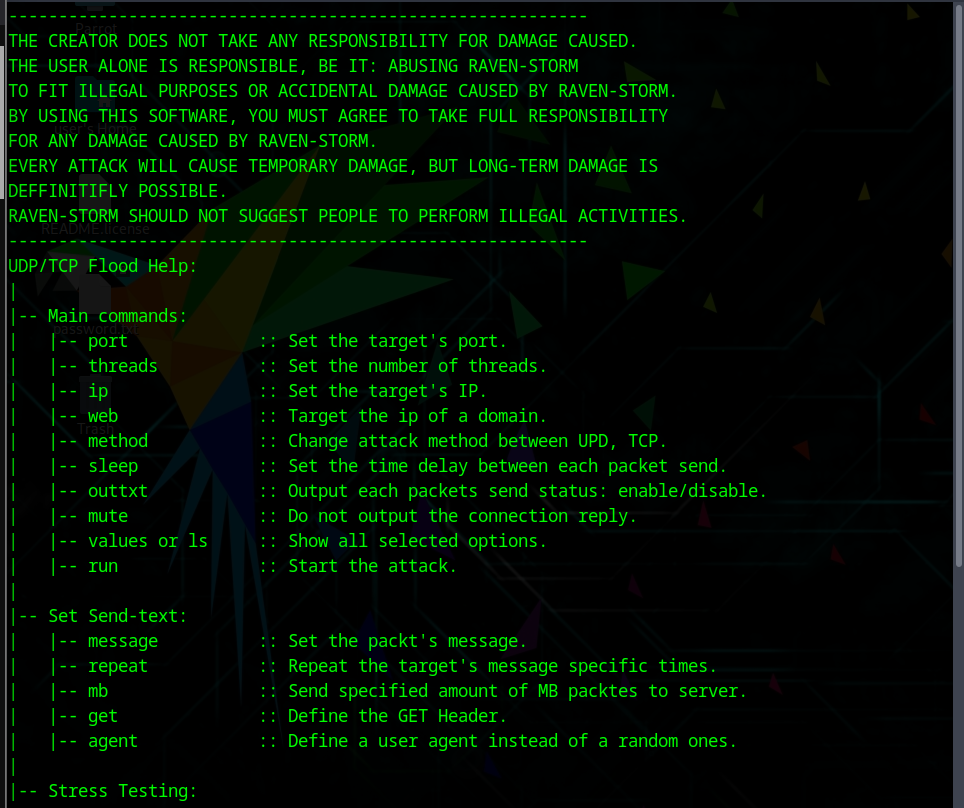
****

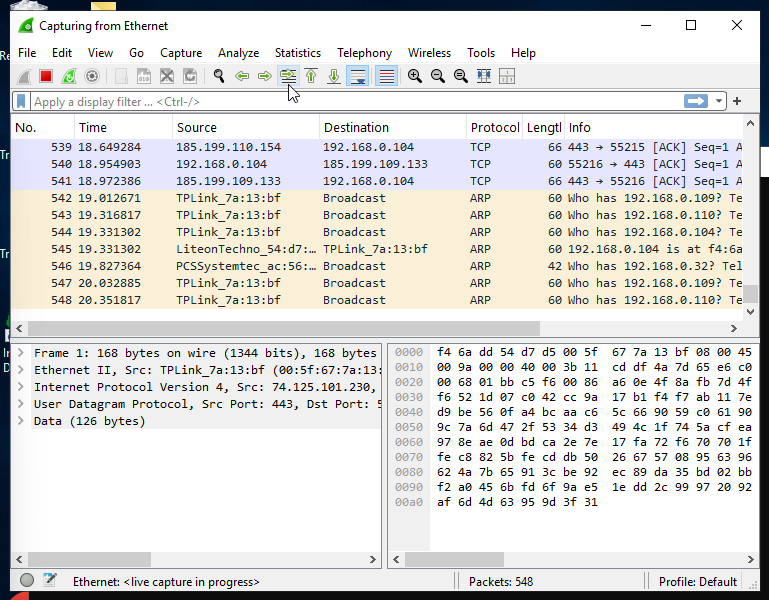
****

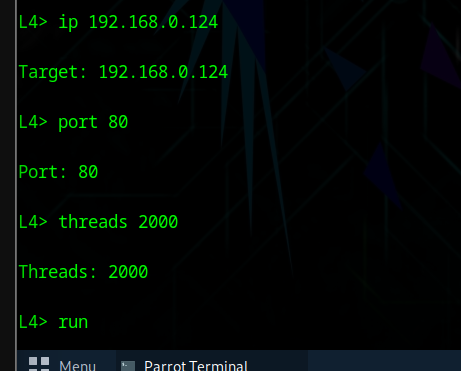
Similarly we can perform POD attack using hping3:

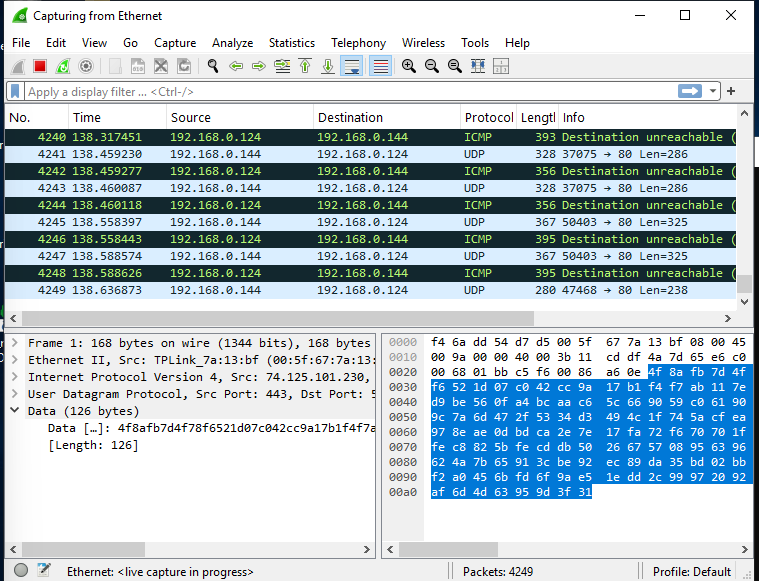
****

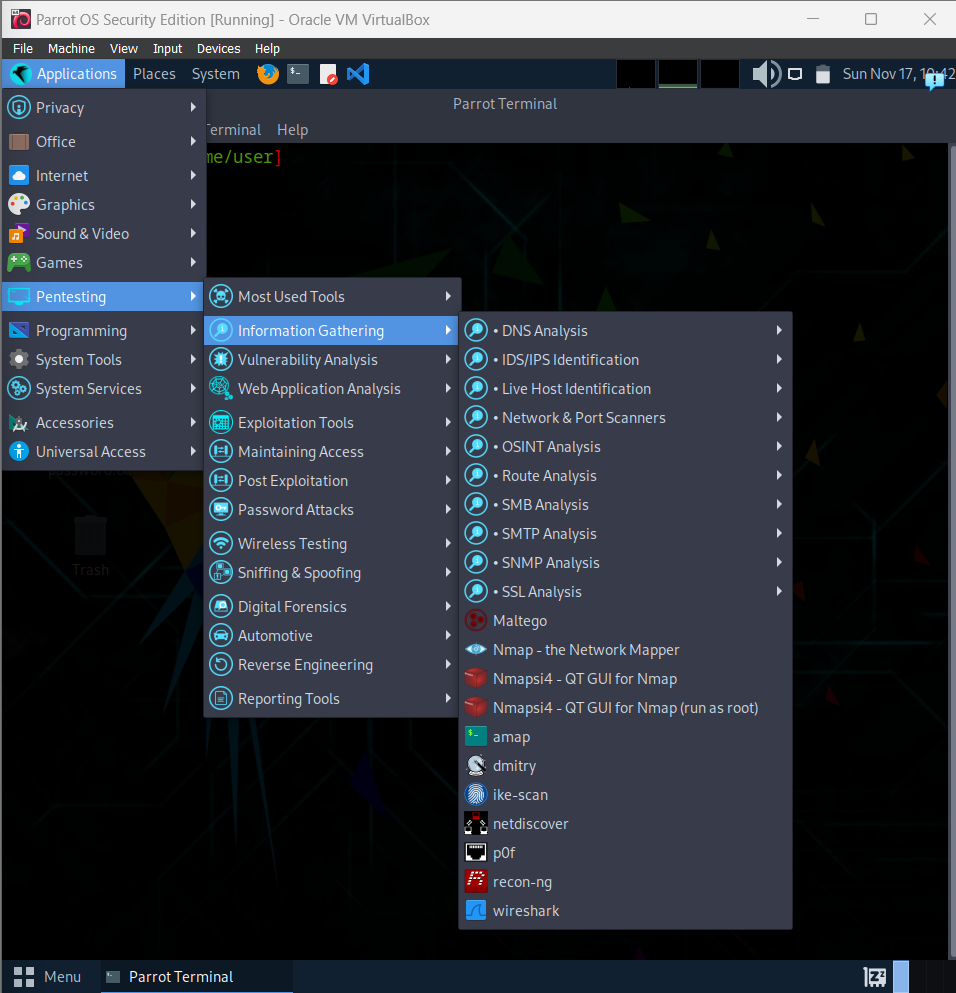
**Perform a DoS attack using Raven-Storm:**

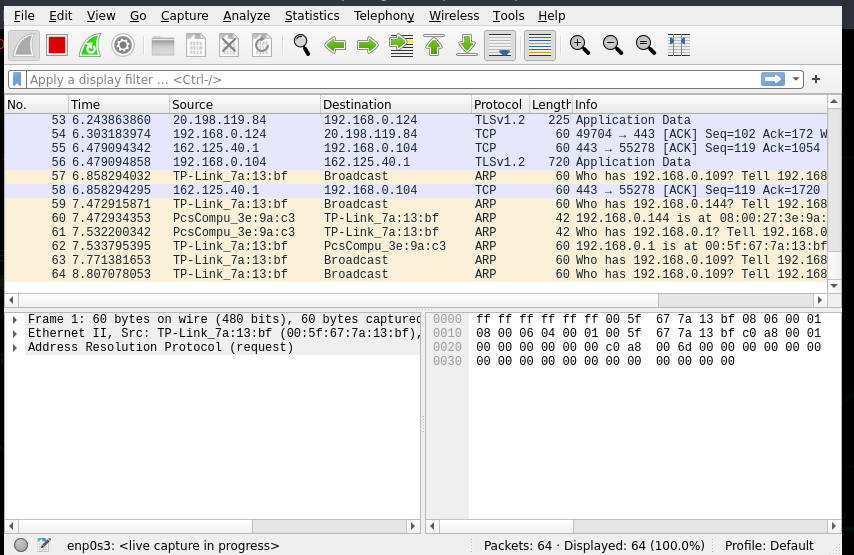
****

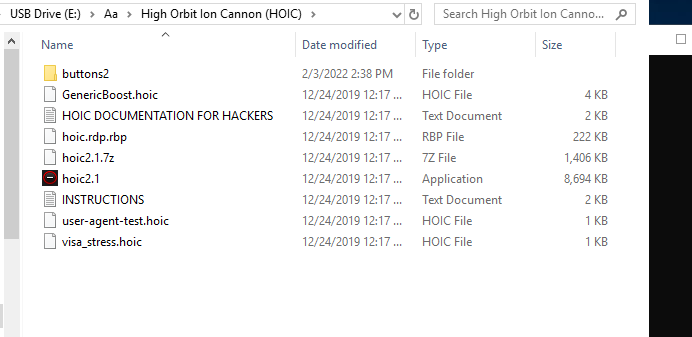
****

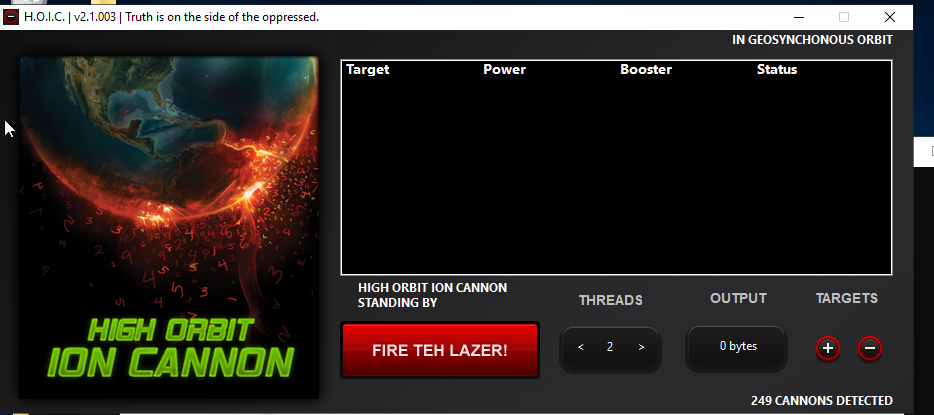
****

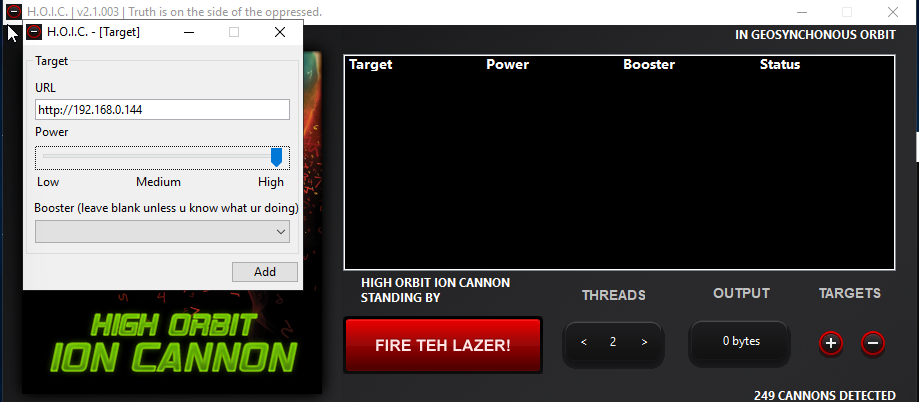
****

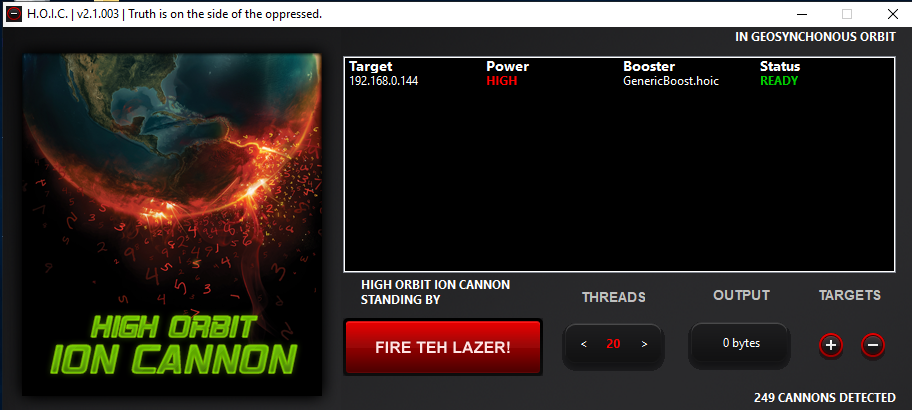
**Perform a DDoS attack using HOIC:**

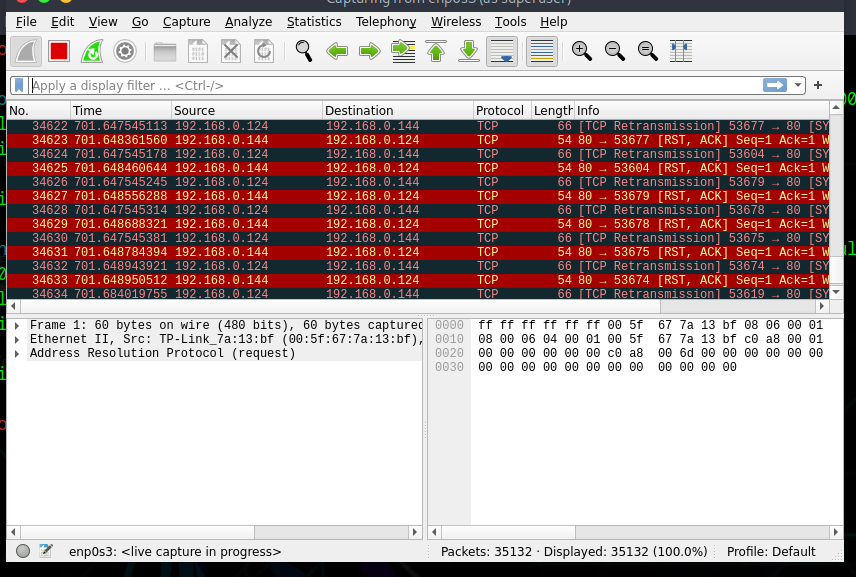
****

****

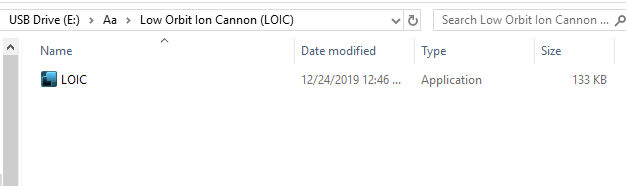
****

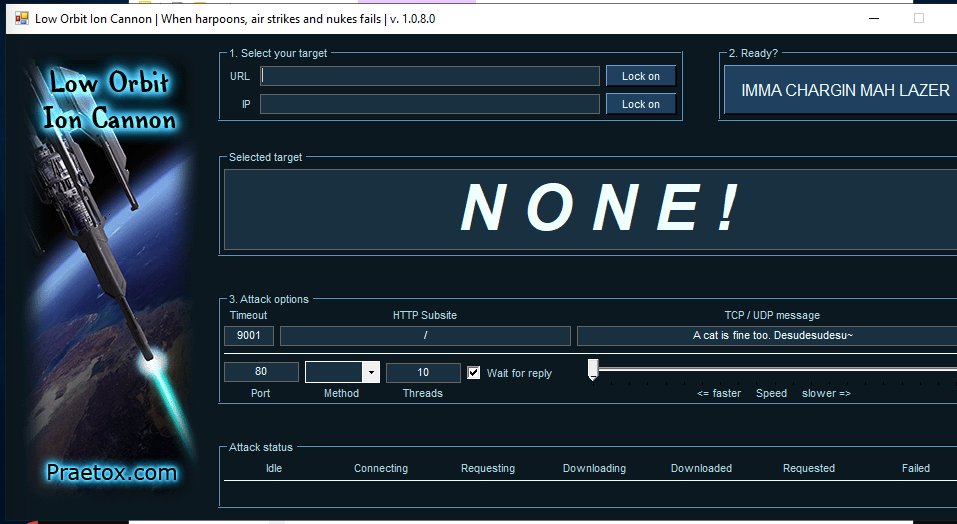
****

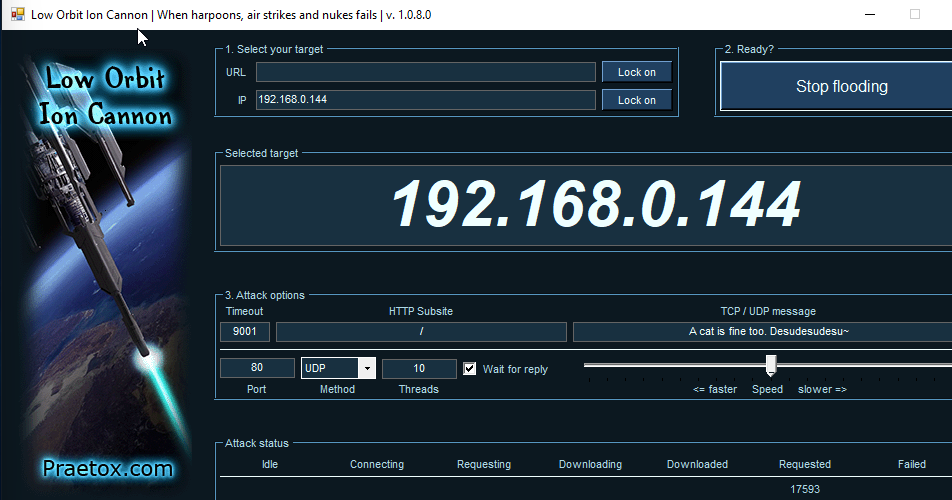
****

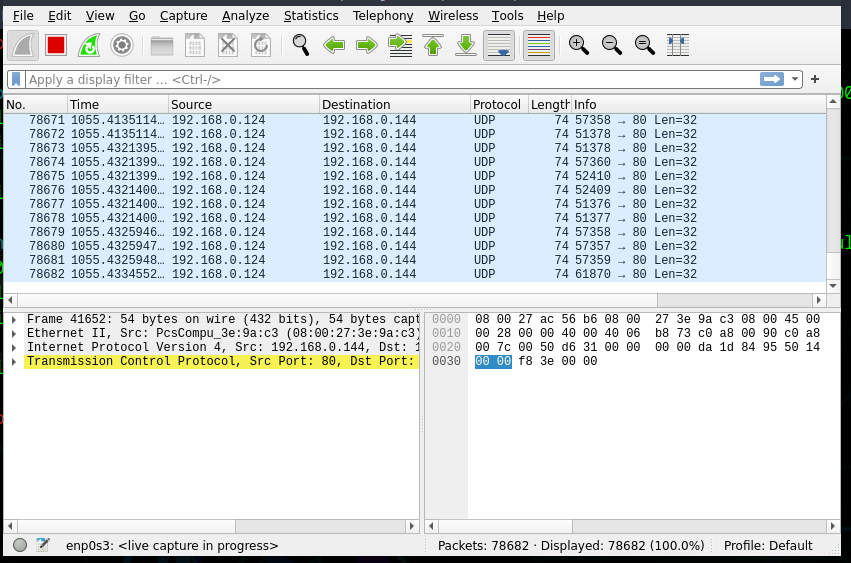
****

**Perform a DDoS Attack using LOIC:**

****

****

****

****