LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5009NI Cyber Security in

Computing

Assessment Weightage & Type

60% Group Coursework 02

Year and Semester

Student Name	London Met ID
Prashant Shah	22085574
Aman Adhikari	23047306
Rahul Chaudhary	23047310
Santosh Katwal	23047517

2024 -25 Autumn Semester

Assignment Due Date: March 19, 2025

Assignment Submission Date: April 22, 2025

Word Count (Where Required): 4537

I confirm that I understand my coursework needs to be submitted online via My Second Teacher under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgement

We thank Mr. Samrid Budathoki, our lecturer and Mr. Sugam Giri our tutor, for their guidance, support, and valuable insights throughout this coursework. Their skill and dedication have played an essential part in developing our understanding of Cloud Computing and IOT and guiding us through the investigation and content of this study. We also want to thank from the bottom of our hearts for all the help and guidance they gave us. Their advice and support have been very helpful in guiding us through this project's challenges and ensuring it is finished successfully.

Abstract

This report presents a comprehensive walkthrough of a SYN flood Denial-of-Service (DoS) attack and its corresponding mitigation strategies within a controlled virtual lab environment. The attack was executed using Kali Linux as the attacker system and Windows Server as the target. The demonstration included reconnaissance using tools like Nmap, launching attacks with Metasploit and Hping3, and monitoring network traffic using Wireshark. The impact of the attack was evaluated by observing resource usage and system behavior, confirming the effectiveness of the attack. Various mitigation techniques, such as blocking SMB traffic, implementing custom firewall rules, and using tools like RdpGuard, were deployed to secure the target system. Post-attack analysis confirmed that the applied security measures successfully prevented further attacks. This experiment emphasizes the importance of layered defense and real-time monitoring in protecting systems from DoS attacks.

Table of Contents

Acknowledgement i

Abstract ii

1. Introduction 1

1.1 Aim 3

1.2 Objectives 3

1.3 Technological terminologies 4

1.3.1 Dos Attack Tool (Slowloris, LOIC, HOIC) 4

1.3.2 Botnet 4

1.3.3 Packet Flooding 4

1.3.4 Amplification Attack 4

1.3.5 Intrusion Detection System (IDS) 4

1.3.6 Rate Limiting 5

1.3.7 Firewall 5

1.3.8 SYN Flood 5

1.3.9 Intrusion Prevention System (IPS) 5

2. Background 6

2.1 Types of DDoS Attack 6

2.1.1 Smurf Attack 6

2.1.2 SYN Flood 6

2.1.3 Layer 7 DDoS Attack 6

2.2 History and Evolution of DoS attack 7

2.3 Impact of DoS Attack 7

2.4 Case Study – GitHub attack on 2018 9

3. Demonstration 10

3.1 Lab Setup 10
3.2 Attack Procedure 10
3.2.1 Initial Connectivity Test 10
3.2.2 Ping the machine 11
3.2.3 Tools Installation 12
3.2.4 Confuring the Attack 13
3.3 Impact Observation 18
3.3.1 Victim System Behavior 18
3.3.2 Resource Usage (CPU, Memory, Network) 19
3.3.3 Wireshark Observation 20
4. Mitigation 21
4.1 Prevention methods 21
4.1.1 Server Message Block (SMB) 21
4.1.2 Firewall rules 22
4.1.3 RdpGuard 23
4.2 Response during Attack 24
4.3 Post Attack Measures 24
4.4 Post Security Attack Check 25
4.5 Pros and cons 26
4.5.1 Pros 26
4.5.2 Cons 27
5. Testing 28
6. Conclusion 32
References 33

Table of Figures

Figure 1 Cost effect by different industries 1
Figure 2 Process of DoS attack 2
Figure 3 behind data breach. 3
Figure 4 Graph of Dos attack on GitHub. 9
Figure 5: screenshot of ipconfig of windows server 10
Figure 6: screenshot of ipconfig of kali linux 11
Figure 7: Screenshot of pinging 11
Figure 8: Screenshot of install Nmap 12
Figure 9: Screenshot of install Wireshark 12
Figure 10: Screenshot of install metasploit framework 13
Figure 11: Screenshot of install Hping3 13
Figure 12: screenshot of Nmap scanning 14
Figure 13: screenshot of monitoring wireshark 14
Figure 14: Screenshot of running metasploit framework 15
Figure 15: screenshot of search syn flood 15
Figure 16: screenshot of selecting module 0 16
Figure 17: screenshot of listing configurable variable 16
Figure 18Screenshot of set Rhosts, Rport, and Shost 17
Figure 19: Screenshot of execute attack 17
Figure 20: Screenshot of execute attack by Hping3 method 17
Figure 21: Screenshot of monitoring system behavior before attack 18
Figure 22: Screenshot of monitoring system behavior before attack using metasploit framework 18
Figure 23: Screenshot of monitoring system behavior before attack using Hping3 19
Figure 24: Screenshot of viewing windows server performance after attack 19
Figure 25 Screenshot of monitoring Wireshark before the attack 20
Figure 26: Screenshot of monitoring Wireshark after the attack 20
Figure 27: screenshot of Block port 445 traffic 21
Figure 28: Screenshot of filtering traffic using Cmd 22
Figure 29: Screenshot of tuning firewall on 22

Figure 30: Screenshot of enable FTP protection 23
Figure 31: Screenshot of choosing enable 23
Figure 32: Screenshot of block user IP 24
Figure 33: Screenshot of post check security attack measures 25
Figure 34: Screenshot of attack execute 28
Figure 35: Monitoring after attack 28
Figure 36: screenshot of applying ICMP packet 29
Figure 37 post monitor of victim machine 29
Figure 38: Screenshot of attack execute 30
Figure 39: Monitor after attack 30
Figure 40: open firewall to mitigate 31
Figure 41: monitoring after attack 31

Table of Tables

Table 1: Table of lab setup 10
Table 2: Table of Server message block 21
Table 3: Table of filters incoming and outgoing traffic 22
Table 4: Table of Rdp guard enable 23
Table 5: Table of block user IP while attack happen 24
Table 6 Table of testing ping of death attack 28
Table 7: Table of fragmented packet attack 30

1. Introduction

In today's interconnected world, cybersecurity is essential for both individuals and businesses. Cybersecurity entails leveraging multiple technologies, methods, and policies to prevent or counteract the impact of cyberattacks, protecting systems, devices, data, financial assets, and personal information from attacks like ransomware, malware, phishing, and data breaches. The increased rate and sophistication of cyberattacks only help to underscore the necessity of cybersecurity since such attacks lead to identity theft, financial loss, and disruption of operations. For instance, the average cost of a data breach was **$4.88 million in 2024**, up **10%** from the year before. With improvements in technology, there are also emerging challenges in terms of ensuring the systems are secure. Increased adoption of cloud computing and IoT devices introduces new vulnerabilities that require perpetual upgrading and strengthening of security controls. To deal with these challenges, businesses must adopt modern security technology, build knowledge about security, and form skilled teams. Prioritizing cybersecurity safeguards assets, guarantees corporate operations, and establishes trust in an increasingly digital environment (IBM, 2024).

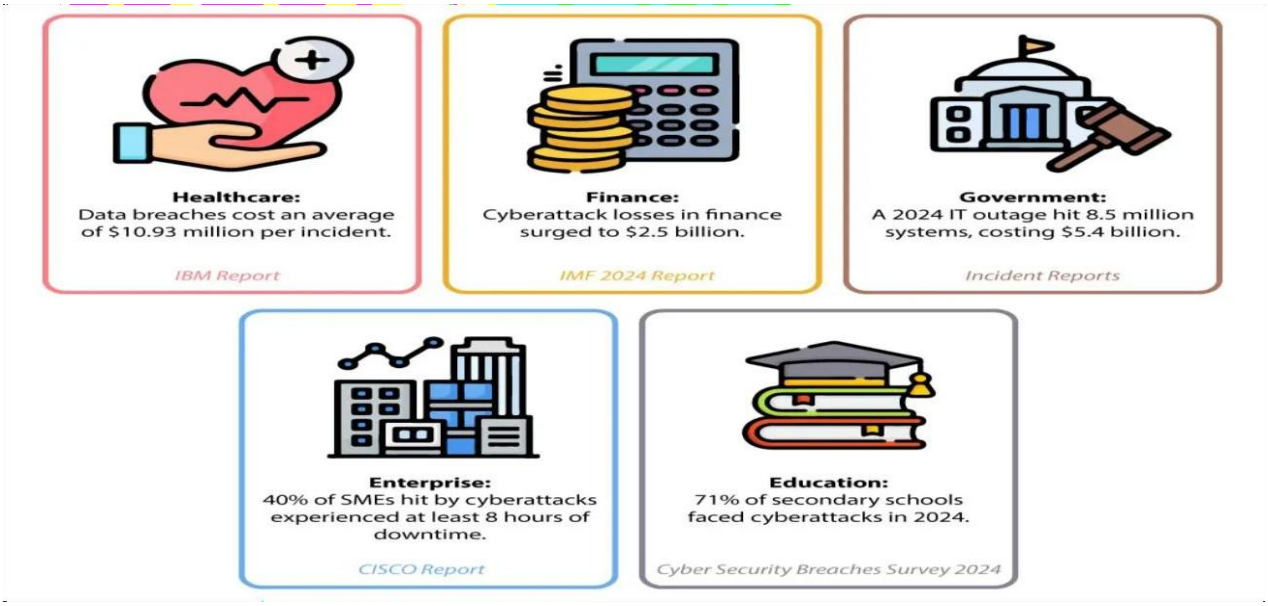

Figure 1 Cost effect by different industries

Denial-of-service (DoS) is an attack in which a cyber threat actor prohibits

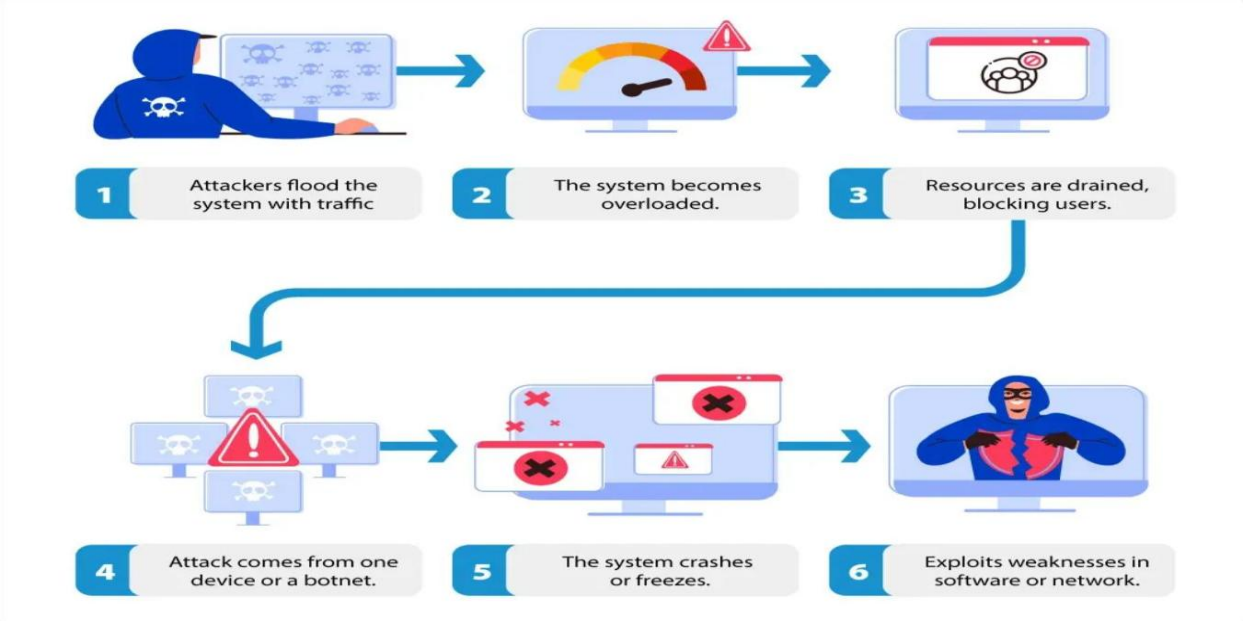

Figure 2 Process of DoS attack

legitimate users from accessing systems, devices, or network resources through overwhelming them with traffic. This may impact emails, websites, banking, and other services, incurring operational and financial losses. High-visibility attacks like the 2016 **Mirai botnet attack** on Twitter and Netflix highlight the rising threat.

Ongoing DDoS threats in geopolitical dispute further highlight the influence on company, government, and essential infrastructure (Cybersecurity & Infrastructure Security Agency) (Surfshark, 2020).Denial-of-service (DoS) attacks remain a major cybersecurity threat, disrupting businesses, financial institutions, and government services worldwide. According to the FBI's Internet Crime Reports, from 2015 to 2023, an average of **2,000** victims per year were affected, with a **49%** increase in reported cases during the **2020 COVID-19** pandemic. Although the average financial loss per victim dropped to **$254** in 2020, it increased to $41,500 in 2023, which indicates a higher economic impact (Surfshark, 2020). Between 2018 and 2020, DoS attacks were also among the primary security threats, with the most significant effect experienced in the Asia-Pacific, China, and Japan **(57%)**, followed by Europe, the Middle East, and Africa **(45%)** (warburton, 2021)

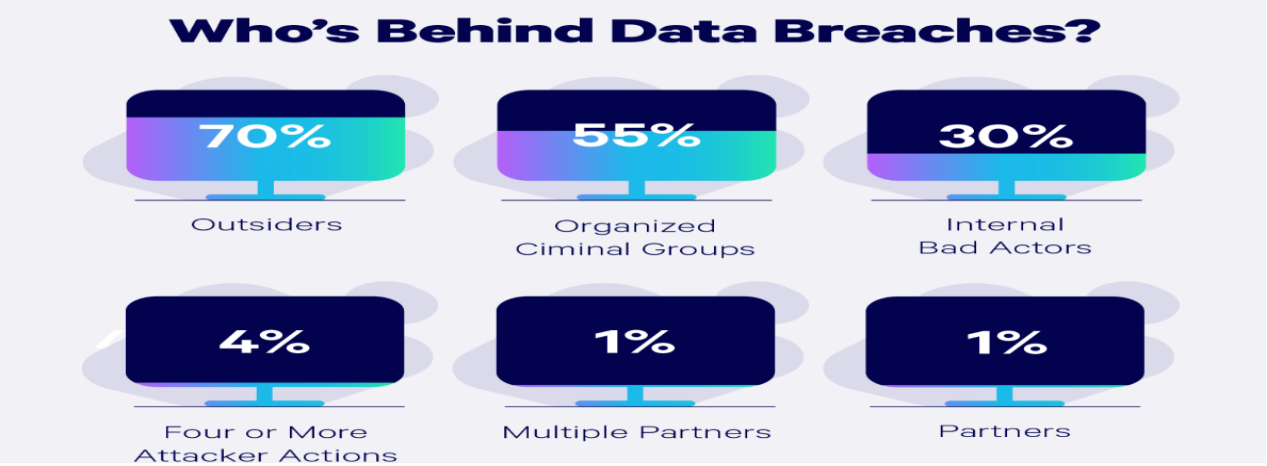

Figure 3 behind data breach.

Furthermore, organizations operating in industries such as finance, healthcare, and e-commerce have been targeted on a regular basis. The financial sector has witnessed increased attacks, with the hackers exploiting the vulnerabilities to knock down banking activities and web-based transactions. Cloud computing and IoT devices have further expanded the attack surface with even more vulnerabilities so that it has become significantly easy for the attackers to launch DoS campaigns. These trends emphasize the critical requirement for robust security controls such as traffic filtering, rate limiting, and early threat detection to combat the threats emanating from DoS attacks.

1.1 Aim

The main aim of this report is to analyze denial-of-service (DoS) attacks against Linux and Windows devices and systems. This task include understanding the methods used in these attacks, their implications on IT infrastructure, and identifying possibilities for control or mitigation of their impacts.

1.2 Objectives

- Define and explain DoS attacks, including their characteristics and common techniques.
- Analyze the impact of DoS attacks on IT devices, networks, and system availability.
- Demonstrate different types of DoS attacks with real-world examples and case studies.

- Identify and evaluate various security measures to prevent or mitigate DoS attacks.
- Assess the effectiveness of different DoS mitigation strategies.
- Provide recommendations for securing IT systems against DoS attacks.

1.3 Technological terminologies

While explaining Denial-of-Service (DoS) assaults in your report, the technological terminologies part is to clarify the key concepts, technologies, and tools involved in the topic. This is for clarification to readers who are not familiar with terminologies because it will benefit them in understanding the technical report content.

1.3.1 Dos Attack Tool (Slowloris, LOIC, HOIC)

DoS attack tools like LOIC (Low Orbit Ion Cannon), HOIC (High Orbit Ion Cannon), and Slowloris are programs that can generate large amounts of traffic or issue slow requests in an attempt to flood and disable a target system. These tools can be utilized by attackers to execute DoS or DDoS attacks.

1.3.2 Botnet

A botnet is a collection of compromised devices (computers, mobile devices, IoT devices) under the control of an attacker remotely after being infected with malware. These compromised devices may be used to launch mass attacks, for instance, DDoS attacks, without the awareness of the owners.

1.3.3 Packet Flooding

Packet flooding is a technique where an attacker sends an overwhelming number of packets to a target system, consuming its resources and causing it to crash or become unresponsive. Common flooding attacks include TCP SYN floods and UDP floods.

1.3.4 Amplification Attack

An amplification attack takes advantage of vulnerabilities in certain protocols to amplify the amount of traffic that is sent to the victim. The attacker sends small requests to a vulnerable server, and the server responds with much larger responses, amplifying the impact of the attack.

1.3.5 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a network security solution employed to detect

and track policy violations or suspicious activity within a system. IDS systems scan incoming network traffic for patterns that might signal potential attacks, including DoS or DDoS.

1.3.6 Rate Limiting

Rate limiting is a security technique used to control the number of requests a server or application can handle within a specified time period. It helps protect systems from being overwhelmed by excessive traffic, especially during DoS attacks.

1.3.7 Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. Firewalls are used to block malicious traffic and prevent unauthorized access, which can help mitigate DoS attacks.

1.3.8 SYN Flood

A SYN flood is a type of DoS attack where an attacker sends a series of SYN requests (part of the TCP handshake) to a target system without completing the handshake. This causes the target server to allocate resources for each incomplete connection, leading to resource exhaustion.

1.3.9 Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is similar to an IDS, but in addition to detecting suspicious activity, an IPS can also take immediate action to block or prevent the attack. IPS systems are proactive in defending against DoS attacks.

2. Background

A denial-of-service (DoS) attack is an attack technique of overloading a machine or network to make it inaccessible. Attackers achieve this by sending more traffic than the target can process, thereby crashing into it making it incapable of providing service to its users. Possible targets may include mail, internet banking, websites, or any other service reliant on a targeted network or computer.

There are different forms of DoS attacks, such as resource exhaustion and flood attacks. Resource exhaustion attacks utilize all the accessible memory or storage of the victim infrastructure, disabling it completely. Flood attacks overflow the system with an overloading quantity of packets more than a server can handle.

A distributed denial-of-service (DDoS) is a DoS attack in which the traffic that is used to overload the target is coming from many distributed sources. The method suggests the attack can't be stopped by simply blocking traffic sources. Attack that target distributed denial of service often make use of botnets (Extrahop, 2024).

2.1 Types of DDoS Attack

2.1.1 Smurf Attack

A Smurf attack is a DDoS that will transmit packets that spoof the victim's source IP. When the devices on the network attempt to respond, the volume of traffic slows the targeted device to the point where it is unusable.

2.1.2 SYN Flood

A SYN flood attack establishes numerous connections with the target server and never finishes them. The attacker initiates a SYN message as a client. When the server responds to a SYN-ACK, the malicious client does not send any ACK message. In this way, the server is forced to keep numerous connections open, wasting its resources until killed.

2.1.3 Layer 7 DDoS Attack

A Layer 7 DDoS attack or application attack aims to target one specific service, not a network. These types of attacks are becoming more popular compared to random network attacks.The first recorded DoS attack occurred in 1996, targeting Panix when the ancient internet service provider (ISP) Panix was attacked. Panix's service was brought down for its users, demonstrating the possibility of crashing internet services through

malicious traffic.

2.2 History and Evolution of DoS attack

Cybercriminals have developed more powerful and advanced techniques of carrying out DoS attacks over the years. Some of the most popular DoS's attacks include:

- **Mafiaboy's Attack (2000):** Mafiaboy attacked major corporations including Yahoo, eBay, CNN, and Amazon with a distributed denial-of-service (DDoS) attack. For one hour, these websites were not functioning properly.
- **The Estonia cyberattacks (2007):** A politically charged cyberattack was launched on the banks, news websites, and government institutions of Estonia. Botnets were utilized to overload Estonian networks, making them unavailable for weeks. It was the first time that a DDoS attack had been used as cyber warfare between states.
- **The Mirai Botnet Attack (2016):** There was new malware called Mirai that infected thousands of Internets of Things (IoT) devices, such as routers and smart cameras. One of the biggest DDoS attacks ever seen on Dyn DNS, a prominent internet service provider. The attack brought down popular platforms like Twitter, Netflix, and Reddit and exposed the dangers of having exposed smart devices.

2.3 Impact of DoS Attack

Service Disruption

A DoS attack overloads a particular object (such as a website or server) through numerous requests to render it inaccessible .Single-origin DoS attacks differ from DDoS attacks because they operate from only one source though they damage both personal websites and vital services and small businesses. Server crashes at online stores prevent customers from making purchases which results in instant financial loss along with customer dissatisfaction. Business operations can suffer damages regardless of how brief the outage is when backup systems are absent (Labs, 2024).

Financial Losses

A direct financial strike occurs when DoS attacks target business operations. Customer transactions automatically decrease whenever a business requires downtime for its online operations. The costs of emergency IT support as well as server upgrades together with any ransom demands from attackers prove to be expensive. Small businesses usually bear the highest impact since their limited cybersecurity resources lead to extended system outages. Multiple attacks against a company result in higher insurance costs while preventing investors from doing business with the organization which produces ongoing financial challenges (Plurilock, 2021).

Reputation Harm

Online service reliability remains a customer requirement due to which frequent website crashes because of DoS attacks result in lost trust. Small enterprises face major difficulties when trying to recover their reputation following damage because they lack the resources large corporations possess. Company growth in the long term suffers when negative reviews appear with online backlash from customers and the loss of frequent consumers. It requires at least several months before a business can restore its credibility after clients decide to move to their competitor's services. The public perception of weak security endures even when the problem has been resolved causing obstacles to gain new clients (Burke, 2025).

Security Vulnerabilities Exposed

The success of a DoS attack usually reveals security deficiencies within the system. The insufficient strength of firewalls, traffic filters or server capacity indicates that one attacker can target and disable the system. Attacks originating from weak security weaknesses provide hackers potential opportunities to launch future data theft or malware attacks. Companies that survive a DoS attack without losing data must use their funds on security assessments and software updates that eat into their capability for expansion. Some perpetrators of DoS attacks utilize this method to establish a gateway for more destructive breaches to occur (Government of canada, 2020).

2.4 Case Study – GitHub attack on 2018

On **February 28 2018**, the **GitHub** Attack was one of the biggest Distributed Denial of Service (DDoS) attacks ever recorded. GitHub is a platform for software developers. Attackers utilized a **Memcached-based amplification technique**. The Memcached DDoS attack techniques is particularly as it provide an amplification factor-attacker's request size to the amount of DDoS attack traffic generated-of up to a staggering **51,200 times**. The attack generated **1.35 terabits per second (Tbps)** of traffic. The attackers exploited vulnerable Memcached servers, which is used to cache database queries for speeding up network performances. Memcached servers are usually open to the internet, thus allowing attackers to easily send small requests that triggered large responses, flooding GitHub's platform with rising traffic. The attackers used IP spoofing, which complicates identifying the source of the attack (A10 staff, 2022).

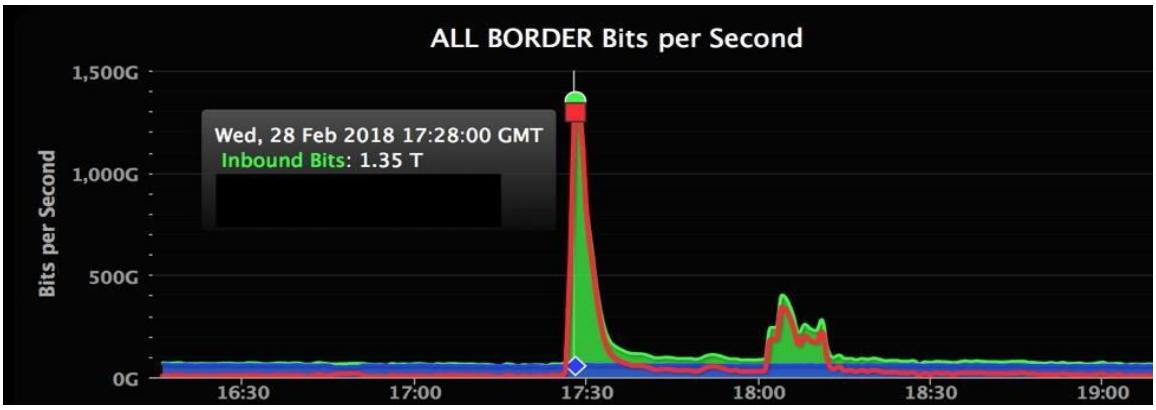

Figure 4 Graph of Dos attack on GitHub.

GitHub's IT security team responded quickly and detecting the attack within 10 minutes. They immediately rerouted traffic to Akamai. It is a cloud-based DDOs mitigation service, which absorbed the massive influx of traffic. It mitigated the attack within minutes and ensure that GitHub experienced only a few minutes of disruption. This quick response prevented any significant downtime or lasting damage. Following the incident, security researchers and organization worked to patch exposed Memcached servers, while internet service providers (ISPs) and security firms began blocking UDP traffic from these server to prevent similar attacks.

3. Demonstration

This section illustrates how the simulated DoS attack was executed in a virtual lab using Kali Linux and a Windows system. It leads through setting up the environment, installing tools like Nmap, Wireshark, Metasploit, and Hping3, and the attack execution. Each step has screenshots to demonstrate what was performed and how the victim system reacted.

3.1 Lab Setup

Component	Specification
Attack Machine	Kali Linux
Victim Machine	Windows
Network Devices	VMware
Network Interface	Bridge

Table 1: Table of lab setup

3.2 Attack Procedure

3.2.1 Initial Connectivity Test

At the Windows level, just use ipconfig at the Command Prompt. It displays the IP address and other network parameters of all adapters connected, which is convenient for checking your network configuration. Where allocated IP is (100.64.244.8).

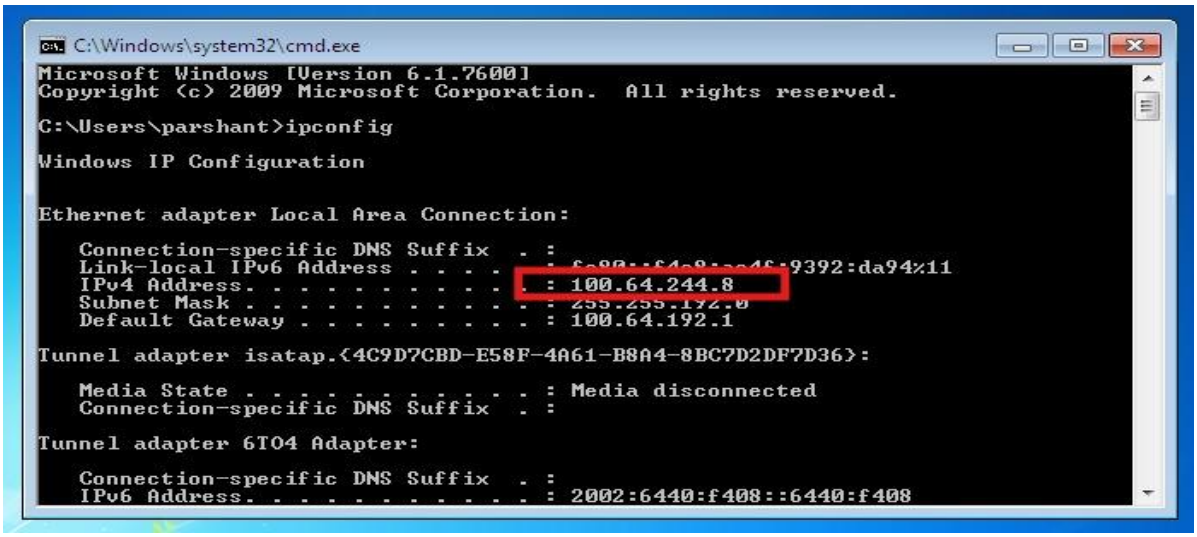

Figure 5: screenshot of ipconfig of windows server

At the Linux level, you can perform the lookup through ifconfig or ip a. The ifconfig command gives you general network interface details, and ip a offers more detailed information. They both are terminal commands used to find your system IP address.

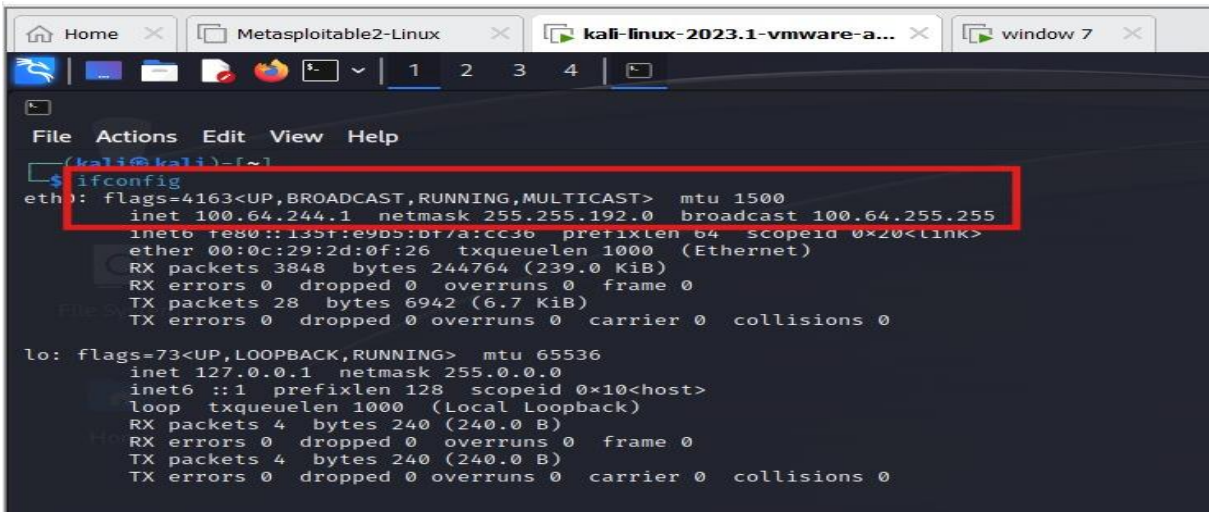

Figure 6: screenshot of ipconfig of kali linux

3.2.2 Ping the machine

The screenshot shows a successful ping from the Kali Linux box to the Windows victim. This confirms that the victim is network accessible and ready to be scanned or exploited.

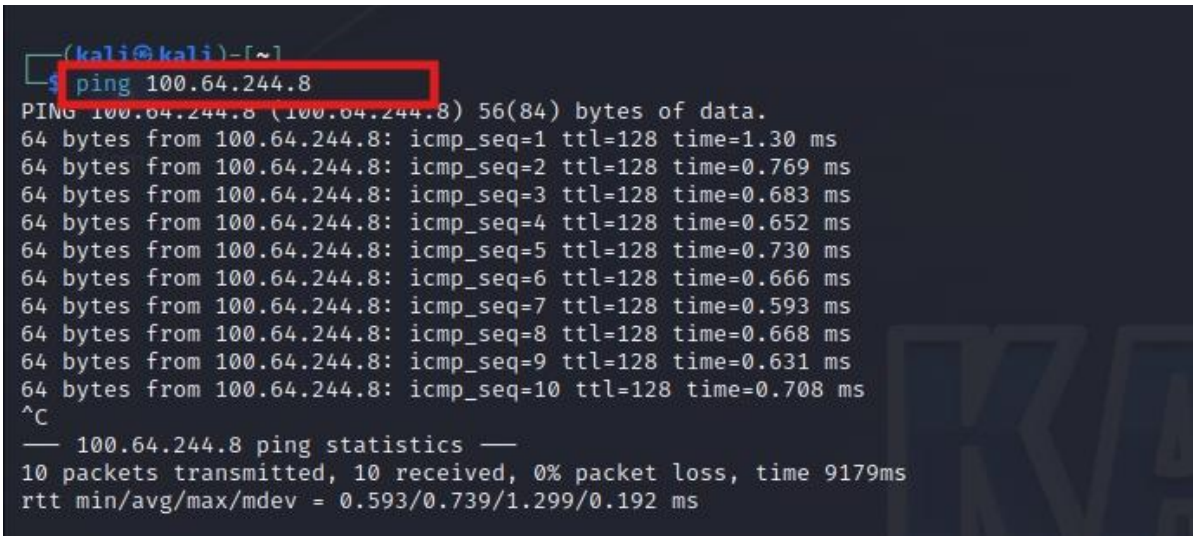

Figure 7: Screenshot of pinging

3.2.3 Tools Installation

- **Nmap:** This screenshot displays the terminal after running **sudo apt install nmap**, confirming that the Nmap tool was installed successfully for port scanning and version detection.

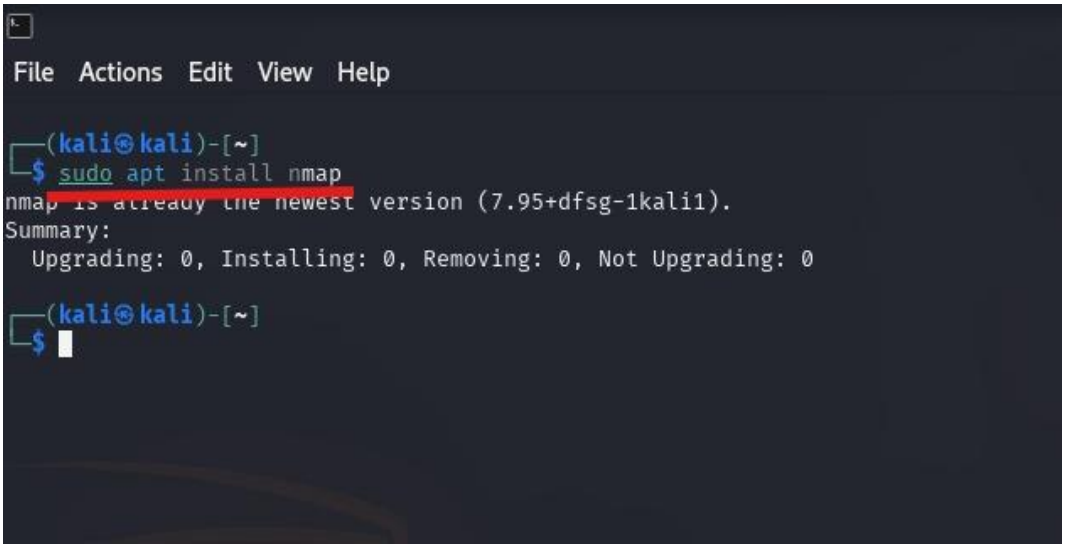

Figure 8: Screenshot of install Nmap

- **WireShark:** It shows the Wireshark installation process using sudo apt install wireshark, used for network traffic monitoring.

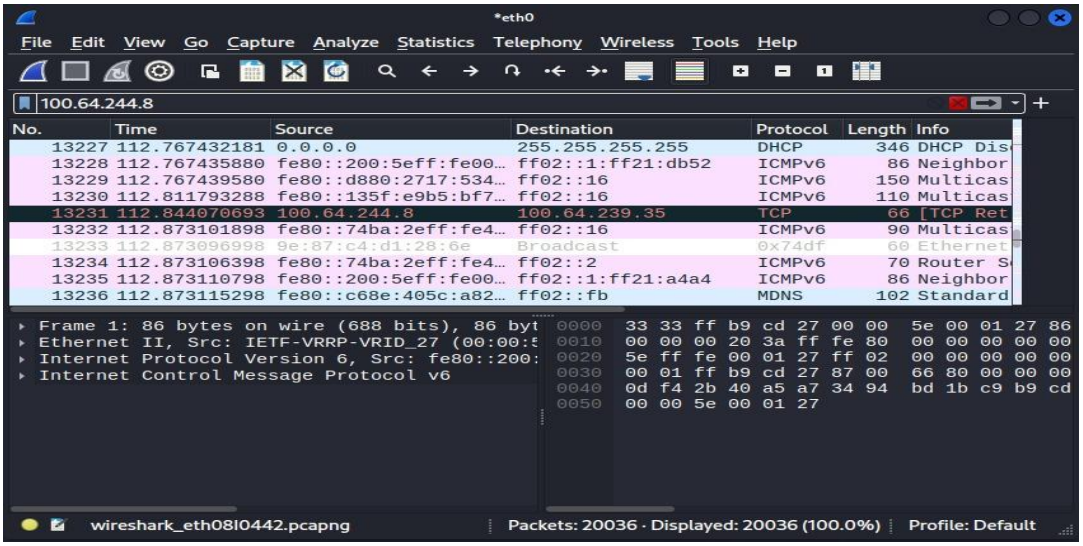

Figure 9: Screenshot of install Wireshark

- **Msfconsole:** The screenshot confirms Metasploit Framework installation, which is used for launching exploits like SYN flood.

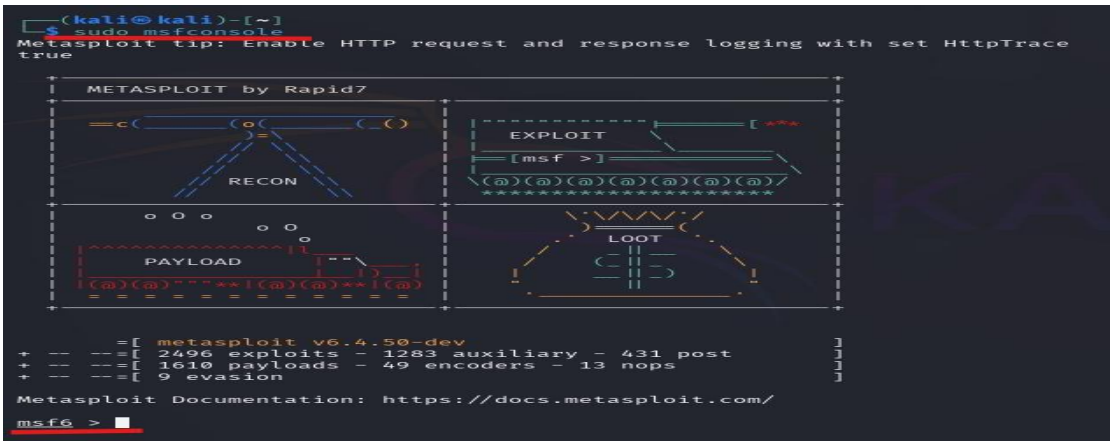

Figure 10: Screenshot of install metasploit framework

- **Hping3:** Demonstrates that hping3, a packet crafting tool with the capability of simulating SYN flood and more, has installed successfully.

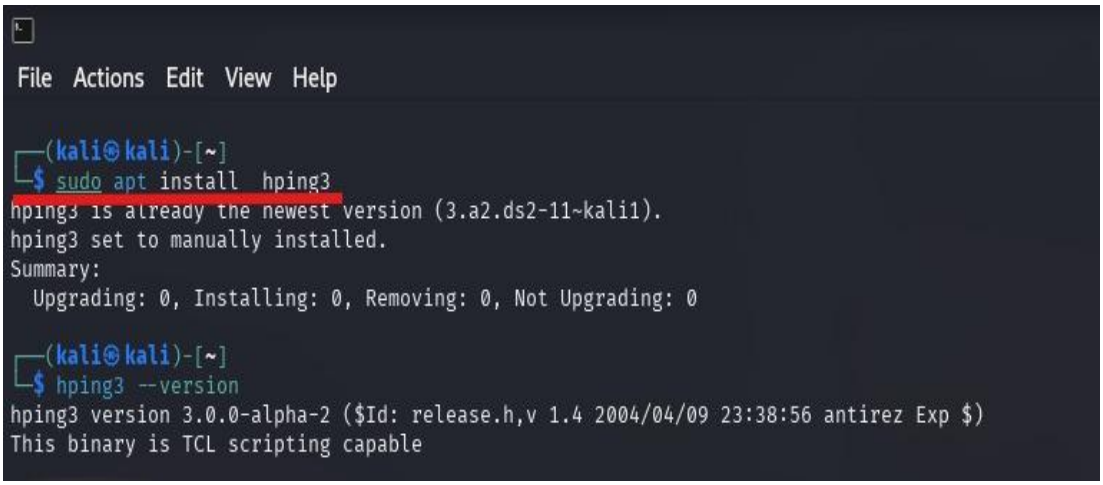

Figure 11: Screenshot of install Hping3

3.2.4 Confuring the Attack

Step1: Nmap

It show the network setup and configuration on both attacker and victim systems. It includes checking local IP addresses with open ports and TCP handshake with Wireshark and preparing the tools for the attack.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  100.64.244.8
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-21 05:39 EDT
Nmap scan report for 100.64.244.8
Host is up (0.0021s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: PARSHANT-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.09 seconds
```

Figure 12: screenshot of Nmap scanning

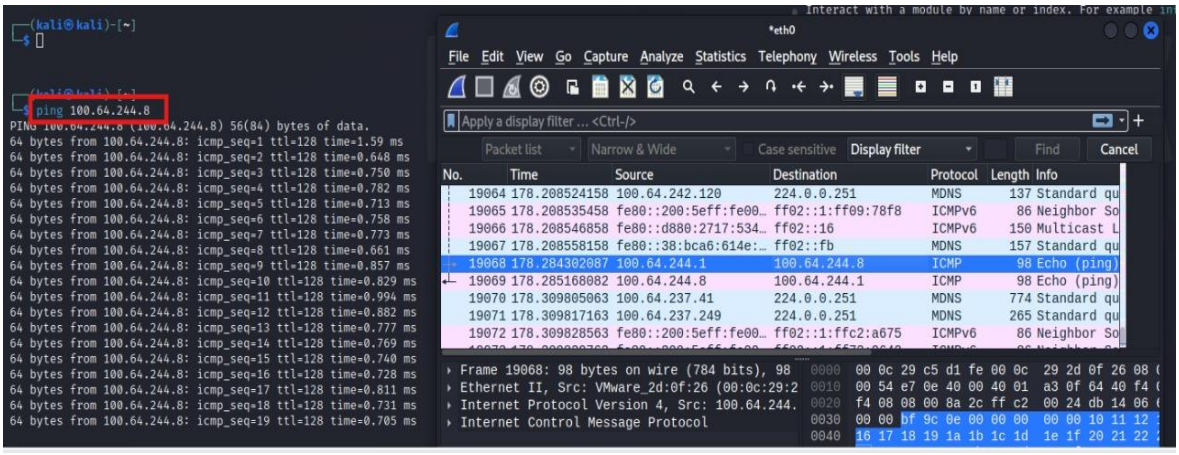

Figure 13: screenshot of monitoring wireshark

Step 2: Attack by Msfconsole and Hping3

Step 2.1: By Msfconsole

Displaying the command sudo msfconsole being run and the Metasploit Framework console loading.

Figure 14: Screenshot of running metasploit framework

Step 2.2: Search SYN Flood

Showing the output of search SYN flood, which lists related modules in the Metasploit database.

Figure 15: screenshot of search syn flood

Step 2.3: Use 0

This screenshot demonstrates selecting the module auxiliary/dos/tcp/synflood with the **use 0** command.

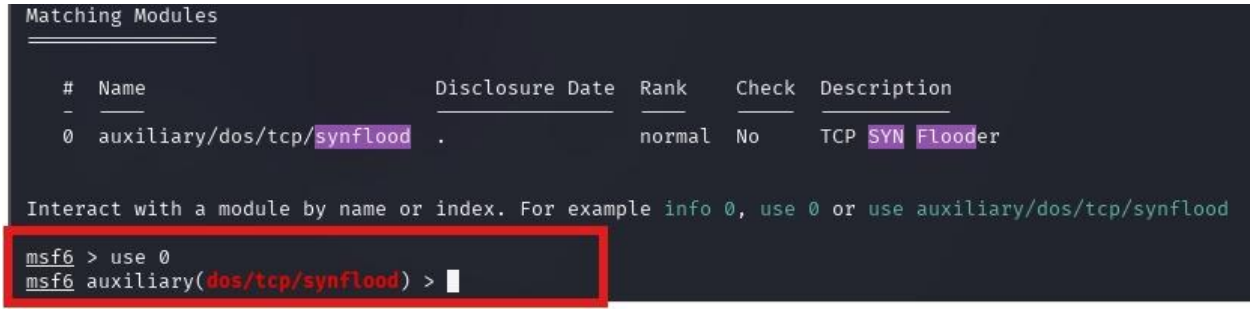

Figure 16: screenshot of selecting module 0

Step 2.4: Show Options

Displaying the show options output, listing configurable variables like RHOST, SHOST and RPORT for the target machine.

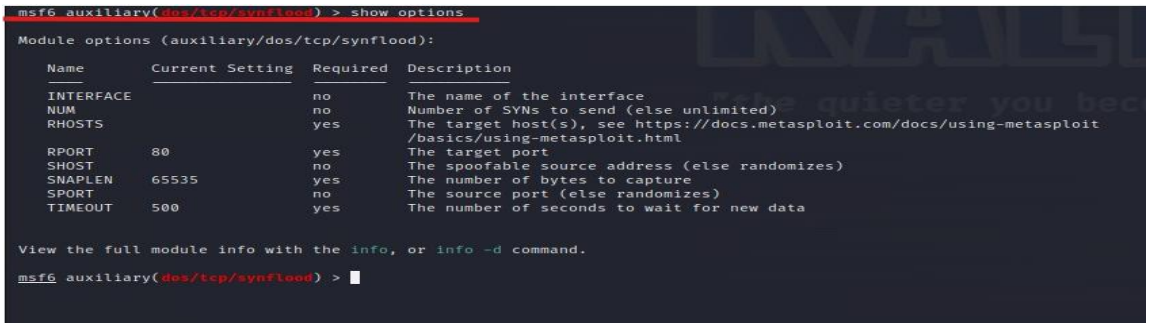

Figure 17: screenshot of listing configurable variable

Step 2.5: Set Host

The screenshot shows the use of the set RHOST, RPORT, and SHOST command to configure the target.

RHOST= **100.64.244.8**

SHOST= **10.0.20.30**

RPORT= **445**

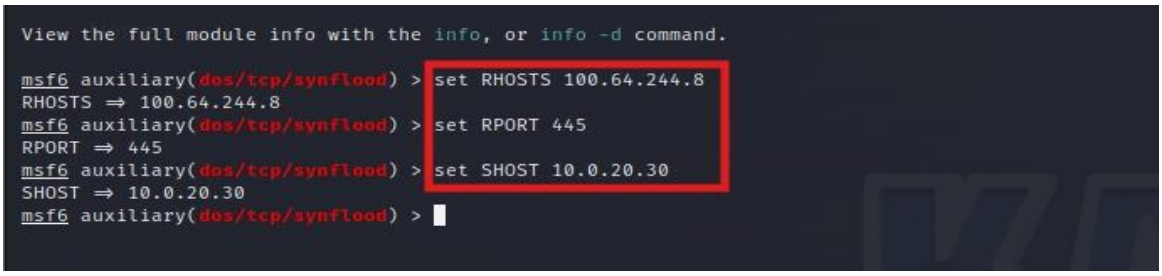

Figure 18Screenshot of set Rhosts, Rport, and Shost

Step 2.6: Execute the Attack

This screenshot confirms the attack execution using the run command. The exploit sends SYN packets to the target port on the victim system.

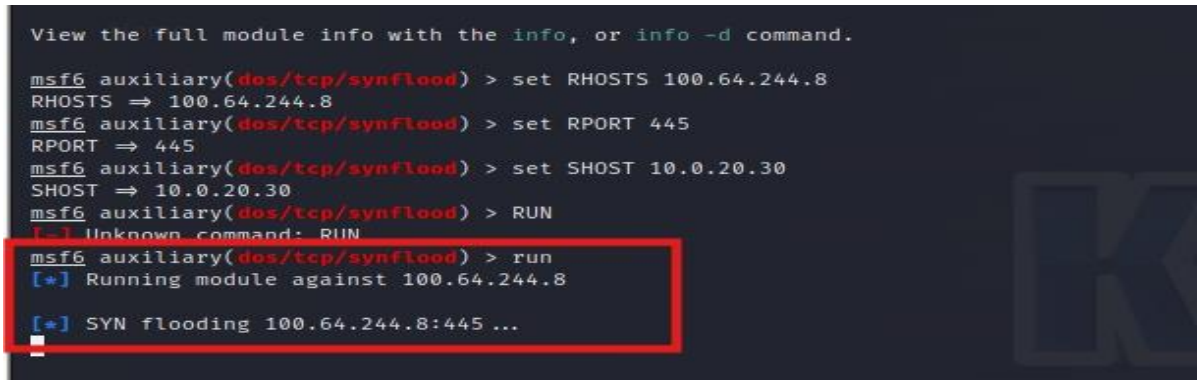

Figure 19: Screenshot of execute attack

Step 2.7: Now, attack by **Hping3**

When we executed command in the Kali terminal. It sends a continuous flood of TCP SYN packets to the victim's port 445 simulating a denial-of-service attack.

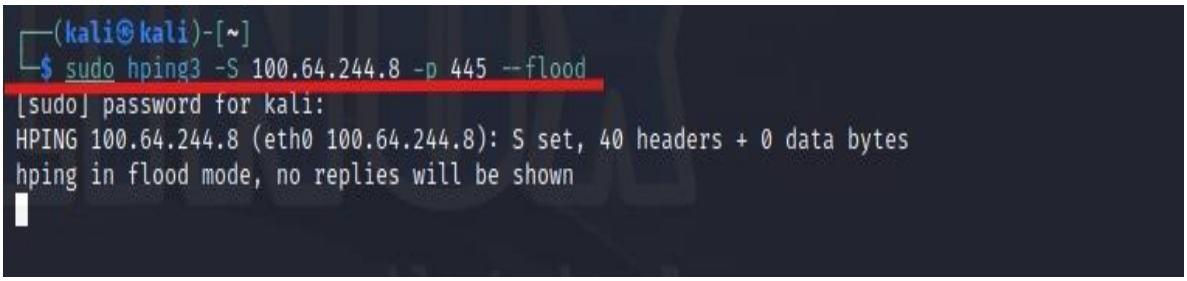

Figure 20: Screenshot of execute attack by Hping3 method

3.3 Impact Observation

3.3.1 Victim System Behavior

Before

The victim machine running normally with responsive services or system utilities.

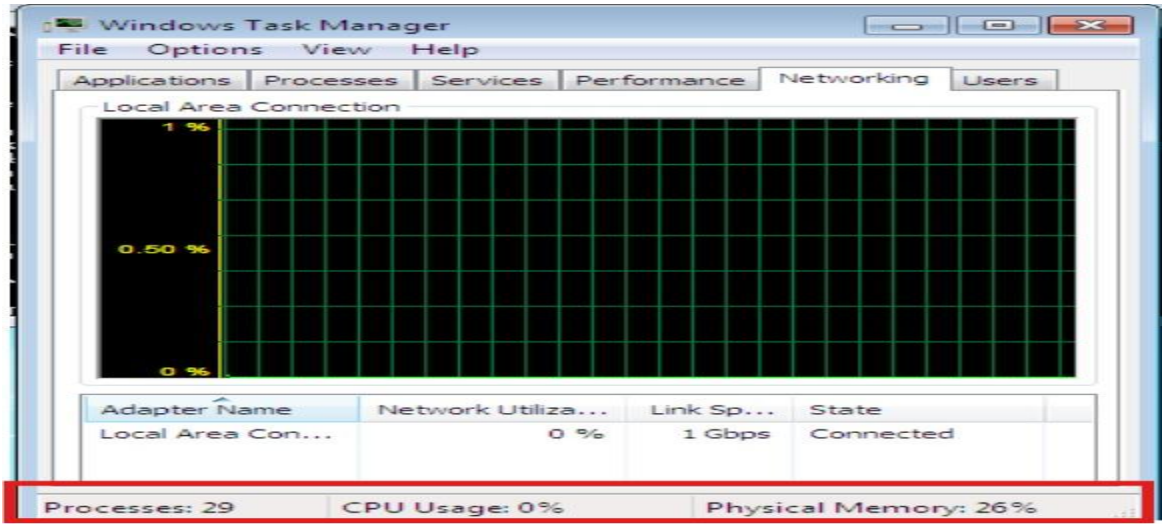

Figure 21: Screenshot of monitoring system behavior before attack

After

The victim system under heavy load or unresponsive due to the flood of SYN packets. Services in the victim device hang, and CPU usage spike with both attack msfconsole and Hping3.

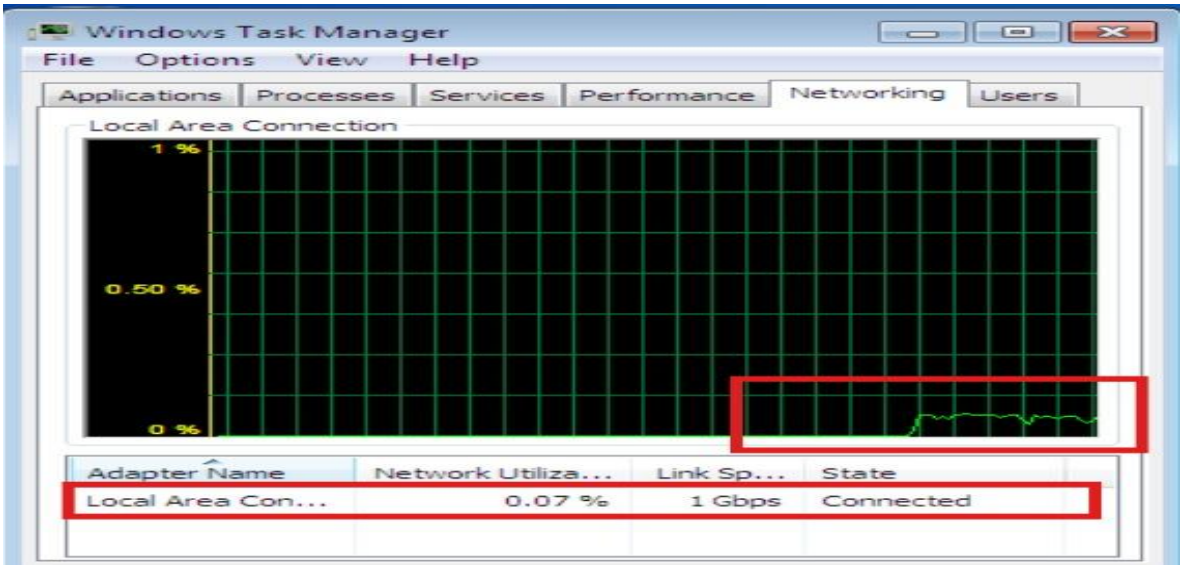

Figure 22: Screenshot of monitoring system behavior before attack using metasploit framework

By hping3

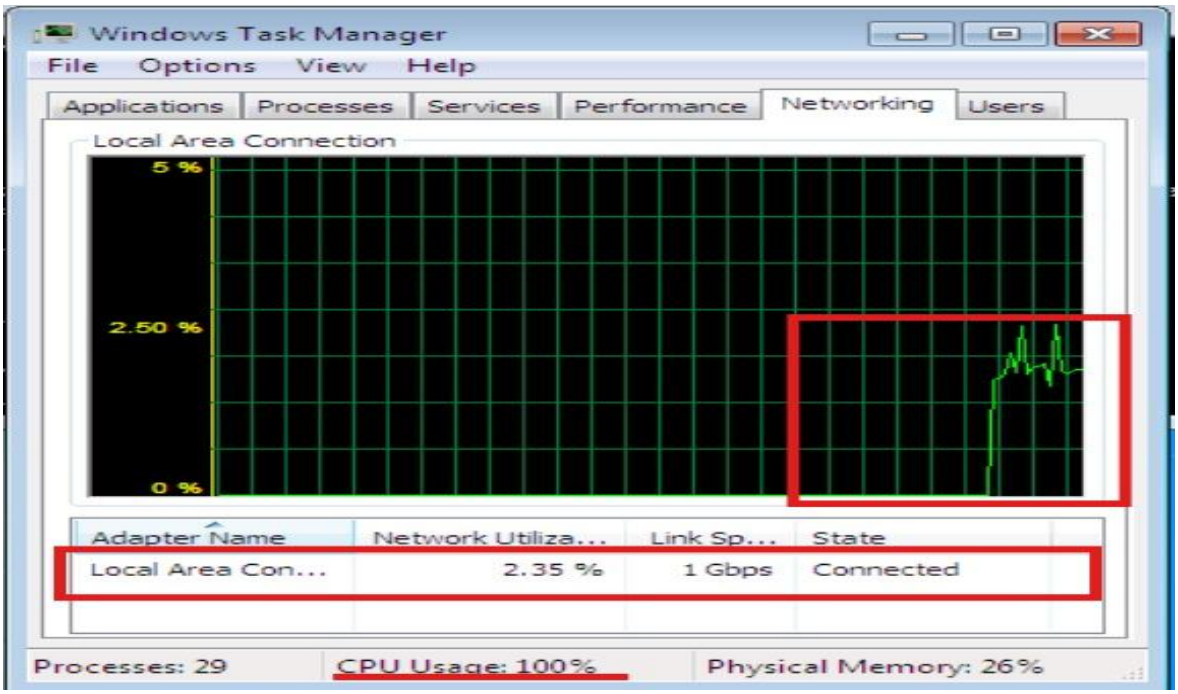

Figure 23: Screenshot of monitoring system behavior before attack using Hping3

3.3.2 Resource Usage (CPU, Memory, Network)

This Task Manager Screenshot of the victim indicates greater consumption of resources, specifically 100% of CPU and 26% of Memory, which confirms the burden created by the SYN flood attack.

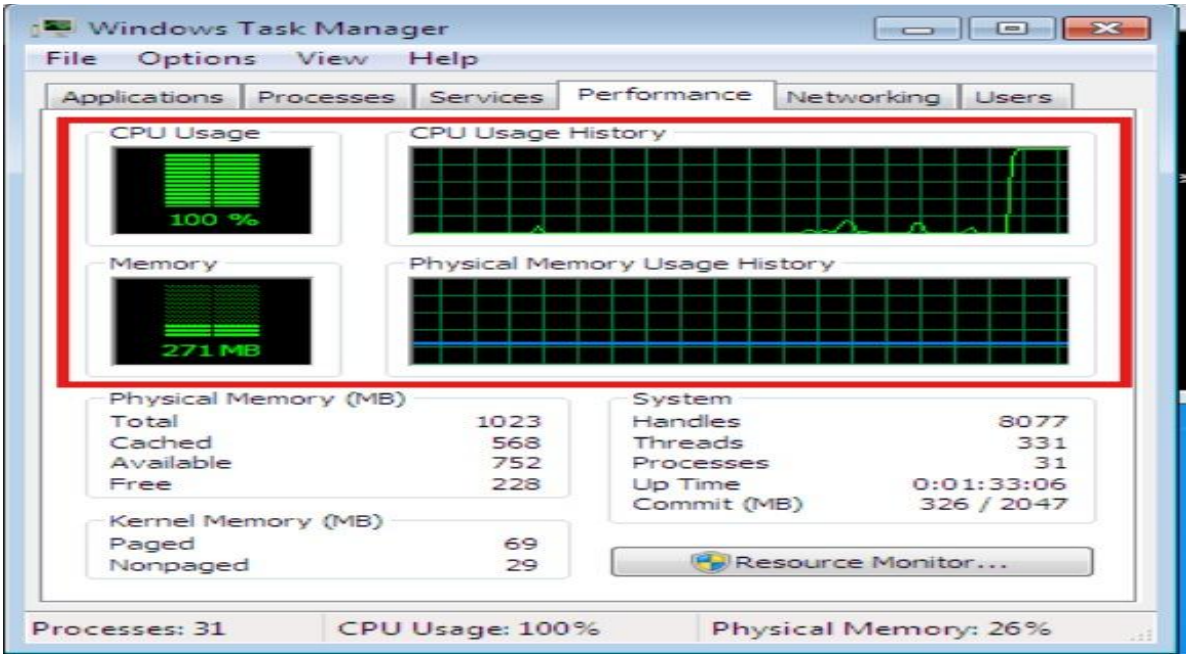

Figure 24: Screenshot of viewing windows server performance after attack

3.3.3 Wireshark Observation

Wireshark captures proving multiple incoming SYN packets to **port 445** on the attacker IP. The capture confirms a SYN flood as subsequent ACK replies are seen, indicating complete TCP handshakes with more than **17000** packets and Spoofing IP address (**10.0.20.30).**

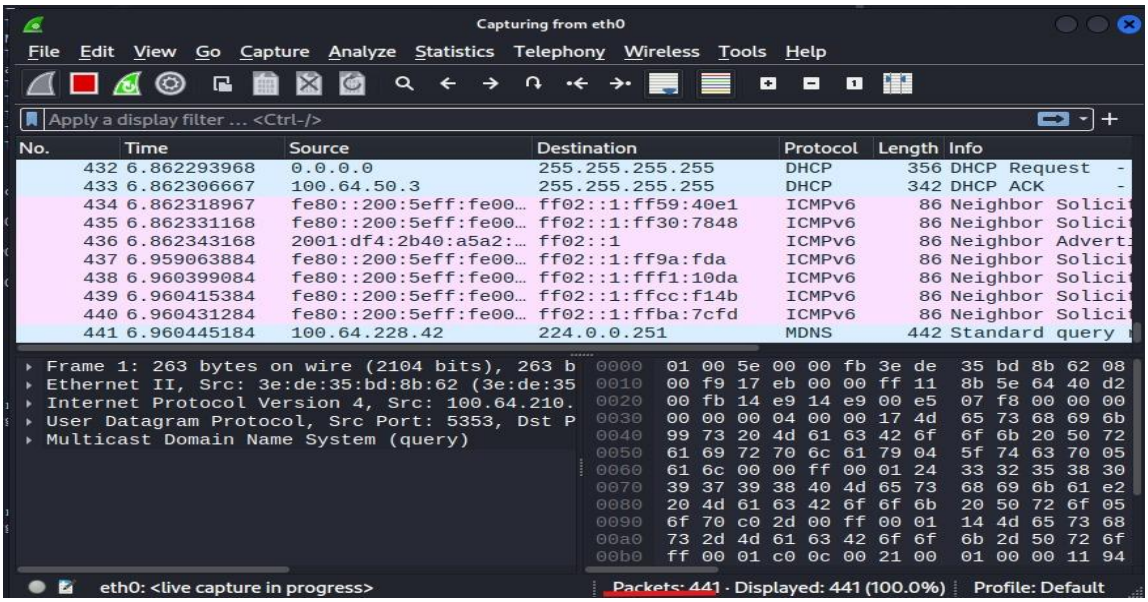

Figure 25 Screenshot of monitoring Wireshark before the attack

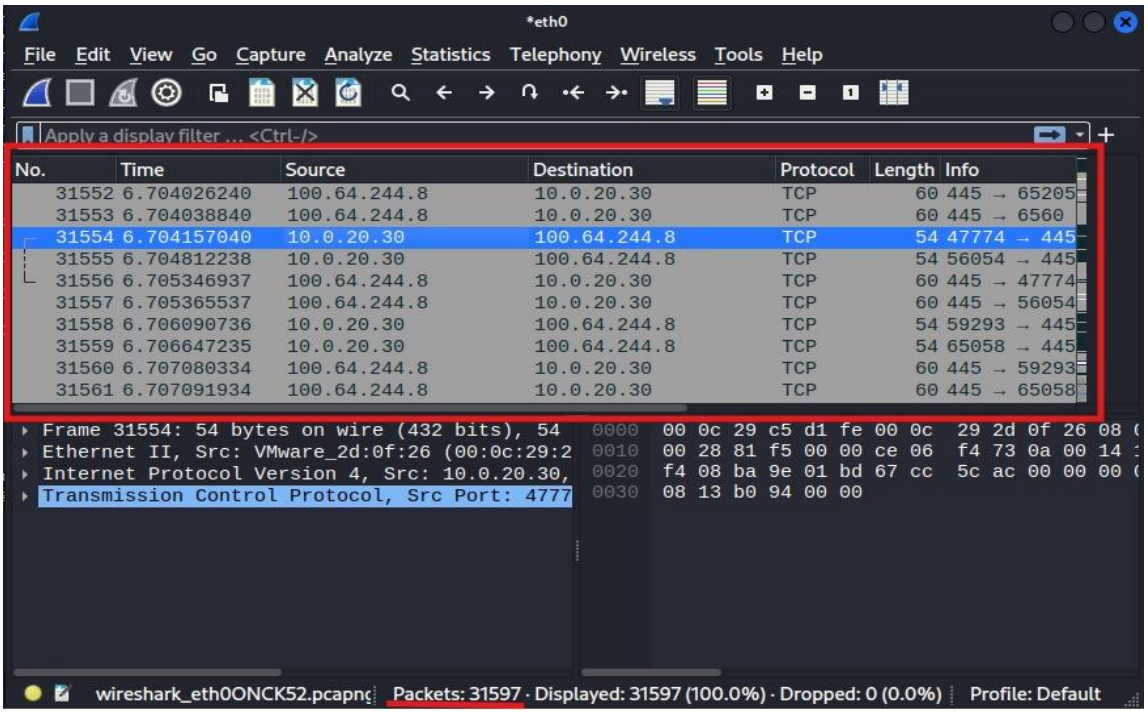

Figure 26: Screenshot of monitoring Wireshark after the attack

4. Mitigation

4.1 Prevention methods

4.1.1 Server Message Block (SMB)

A network protocol known as Server Message Block (SMB) is utilized in order to make the sharing of resources like printers and files easy for users and applications across the network. It normally operates on TCP/IP port 445 and uses a client-server model. Despite the fact that SMB, a native protocol of Windows, makes it easy to share and access resources, its extensive use needs more security (digitalguardian, 2024).

Goal	Limit excessive connections to port **445 (SMB)**.
Method Name	Service Message Block
Tools	Windows Firewall
Command	netsh advfirewall firewall add rule name="Block SMB Port" protocol=TCP dir=in localport=445 action=block
What it Does	Blocks port **445** traffic; allows access only to trusted IPs.

Table 2: Table of Server message block

Screenshot:

Here you can see **(ok)** on yellow line which means mitigation is successful.

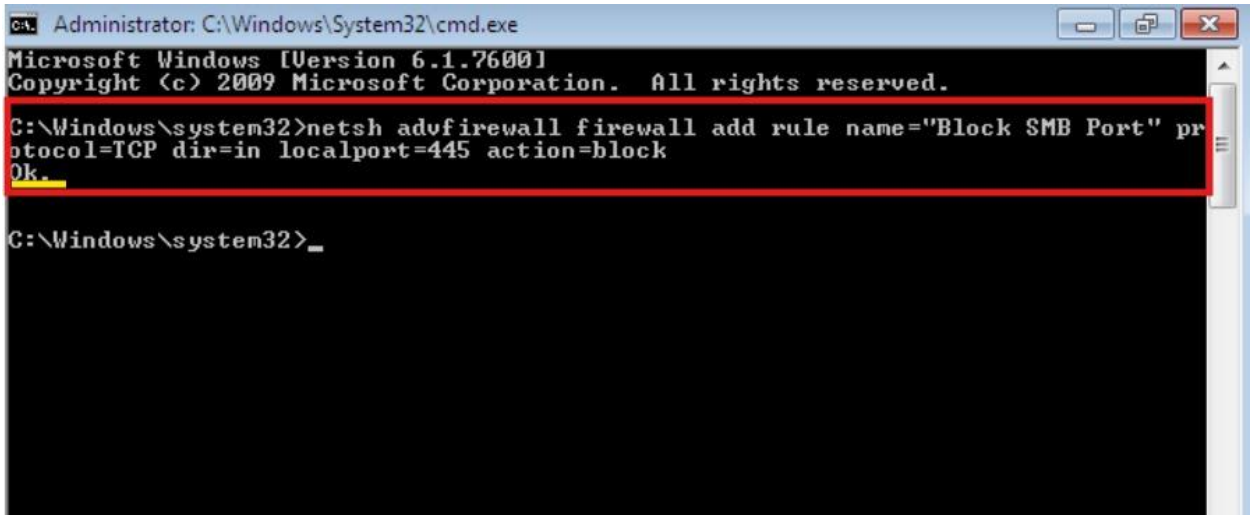

Figure 27: screenshot of Block port 445 traffic

4.1.2 Firewall rules

Network administrators create firewall rules that tell a firewall to process inbound and outbound network traffic communications. Network security relies on firewall instructions decided by network administrators through specifications of IP addresses as well as ports and protocols. Rules defined for firewalls work through a privilege-based principle. Such policies lower the exposure to external and internal attacks and unauthorized entry by enabling permissions solely at necessary times (Palo Alto Networks, 2024).

Goal	Filters incoming/outgoing traffic
Method Name	Firewall Rules
Tools	Windows CMD
Command	netsh advfirewall firewall add rule name="Allow SMB from Trusted IP" dir=in action=allow protocol=TCP localport=445 remoteip=100.64.244.1
What it Does	Filters incoming/outgoing traffic based on rules.

Table 3: Table of filters incoming and outgoing traffic

Screenshot:

Figure 28: Screenshot of filtering traffic using Cmd

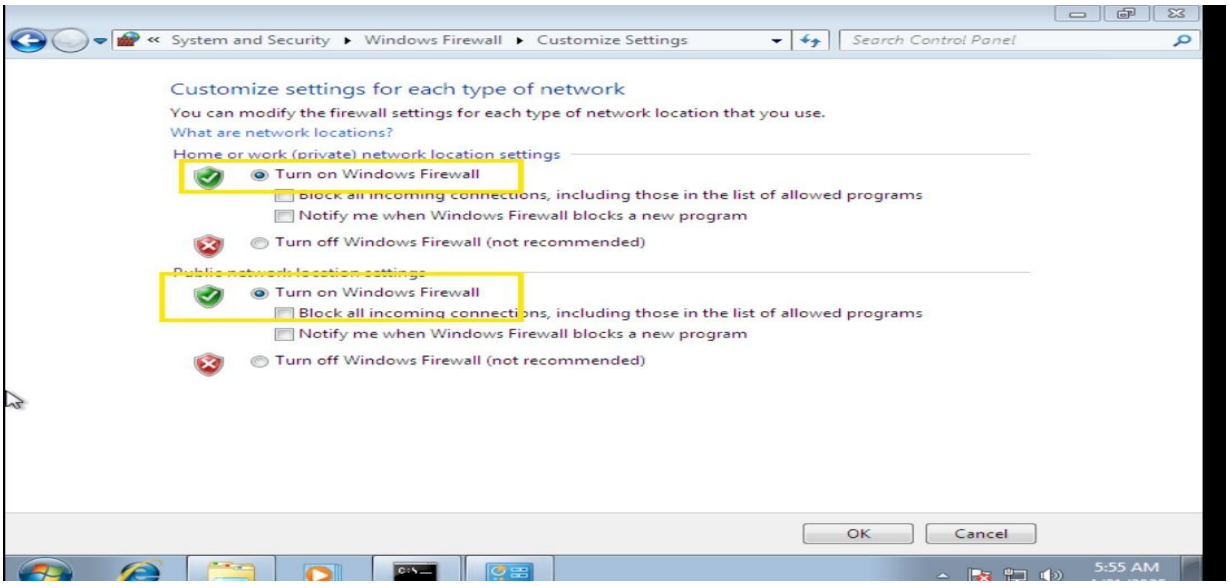

Figure 29: Screenshot of tuning firewall on

4.1.3 RdpGuard

RdpGuard functions as a host-based intrusion prevention system (HIPS) which guards Windows Servers against brute-force attacks that target RDP and 18 other specified protocols and services (RDP, FTP, IMAP, POP3, SMTP, MySQL, MS-SQL, IIS Web Login, ASP.NET Web Forms, MS Exchange, RD Web Access, VoIP/SIP, SSH, etc). The system performs server log monitoring to identify sequence breakdowns in login attempts. The system blocks attacker IP addresses when a specific number of failed logon attempts originate from the same address for a particular time duration (Rdpguard, 2024).

Goal	Mitigate port and different service
Method Name	Enable RdpGuard
Tools	RdpGuard Software
Command	Enable or Disable
What it Does	Block attack imidetialy close port.

Table 4: Table of Rdp guard enable

Figure 30: Screenshot of enable FTP protection

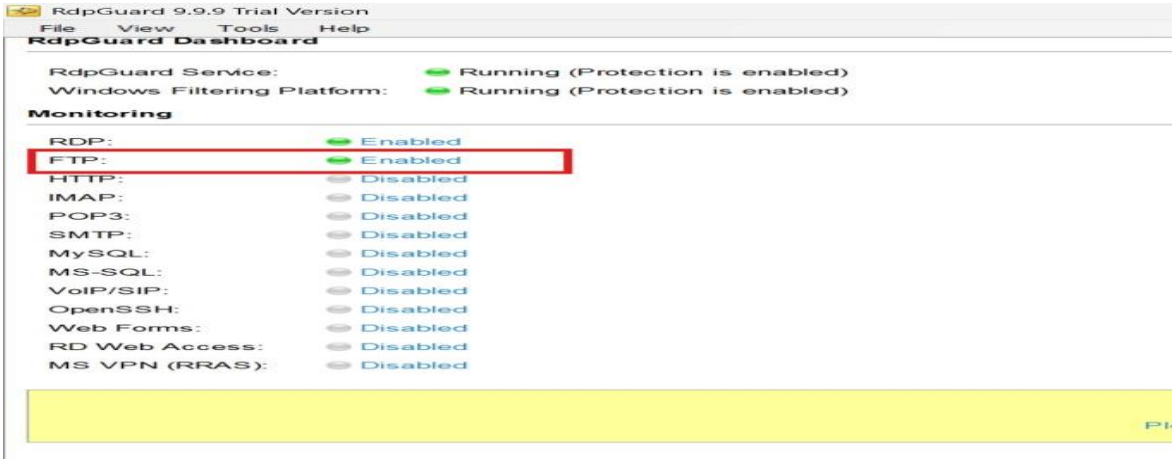

Figure 31: Screenshot of choosing enable

4.2 Response during Attack

Block user IP

Goal	Block user IP while attack
Method Name	Windows firewall rule
Tools	Command line interface
Command	**netsh advfirewall firewall add rule name="Block Attacker IP" dir=in remoteip=100.64.244.1 action=block**
What it Does	Immediately stops traffic from the attacker's IP.

Table 5: Table of block user IP while attack happen

Screenshot:

Figure 32: Screenshot of block user IP

4.3 Post Attack Measures

- The restart of important services through **(services.msc)** enabled File Sharing together with Remote Desktop to operate normally.

- System reboot procedures were carried out to eliminate half-open sockets and stabilize network performance.

- We checked and reactivated all firewall parameters together with blocking configurations to protect the system post-attack.

- Task Manager graph provided important data to track the attack and confirm system performance and detect unusual behavior.

- A security check and testing regimen took place to confirm stability and establish protection for future threats after executing full system updates.

4.4 Post Security Attack Check

The security measures were verified through post-mitigation tests that executed ping and **SYN flood attacks** from Kali Linux attack machine to the victim machine with IP address **100.64.244.8.** The ping test with **16 packets** experienced complete packet loss because **ICMP** traffic survived the blocking attempts. About **60,000 SYN flood packets** were sent through **hping3** toward **port 445** but the victim machine remained unresponsive and failed to respond to all packets. The simulated attack demonstrated that the firewall rules combined with other protective mitigation successfully blocked all kinds of connection attempts to the victim machine thus securing it.

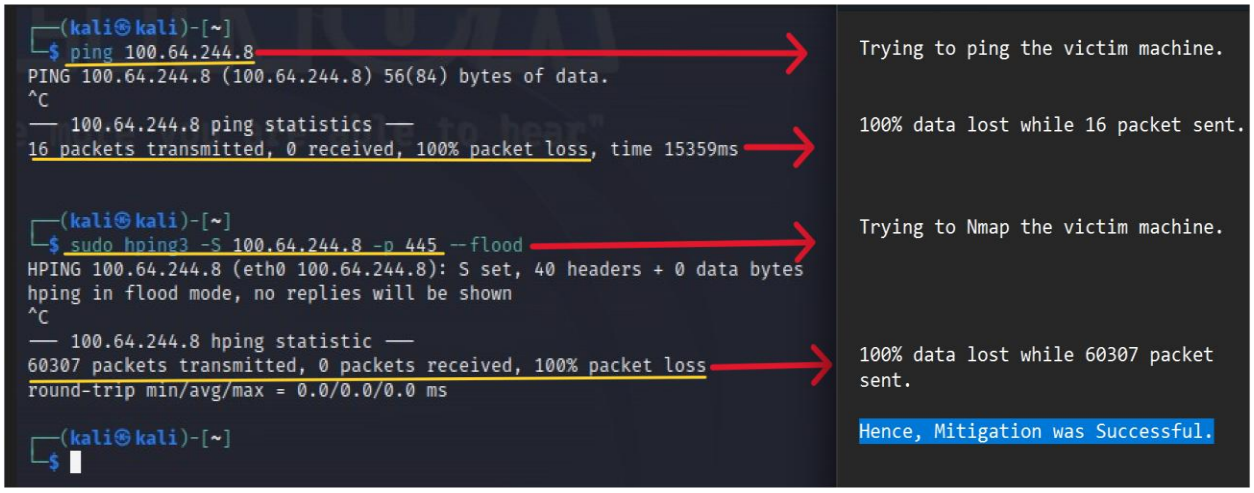

Figure 33: Screenshot of post check security attack measures

4.5 Pros and cons

4.5.1 Pros

- **Effective Mitigation**
    - The proper application of Firewall rules serves to block harmful traffic which includes SYN flood attacks.
    - The system operates more securely from threats because IP blocking prevents known attackers from accessing its network.
    - Right implementations of these security methods lower the susceptibility to DoS threats efficiently.
- **Lightweight Tools**
    - The user-friendly tools netsh, iptables along with RdpGuard permit smooth installation and setup processes.
    - These security tools need small computer system resources for stable performance.
    - Ideal for quick deployment in both small and large environments.
- **Immediate Response**
    - Operators can instantly block attackers' IP addresses throughout active incidents.
    - An instant command allows users to deactivate vulnerable services and ports to interrupt an attack.
    - During emergency situations these tools decrease the amount of system time unavailability as well as diminish the impact of security breaches.
- **Flexible Testing**
    - Safety simulations of live network attacks happen through Metasploit and Hping3.
    - Useful for penetration testing and defense validation.
    - The testing capabilities aid security personnel to develop their protective systems while enhancing their preparedness.

4.5.2 Cons

- **Manual Effort**
    - Technical skill is necessary to perform firewalls and tools configuration tasks.
    - Connecting networks manually creates higher opportunities for user mistakes to occur.
    - Application of critical settings without expert knowledge might lead to critical mistakes when implementing rules.
- **False Positives**
    - Strict security rules might prevent genuine users from accessing the network.
    - Such disruptions might negatively impact trusted user and client access to services.
    - The implementation of security measures creates obstacles for maintaining access regulation.
- **Limited Scope**
    - Firewalls cannot stop attacks that use fake IP addresses through the blocking technique.
    - The distributed attacks (DDoS) circumvent simple blocking methods because they use numerous IP addresses.
    - Advanced and large-scale threats cannot be addressed by using these methods independently.
- **Temporary Fixes**
    - The basic procedures of restarting services and blocking ports act as temporary measures that stop only visible problems.
    - Such measures do not establish sustainable solutions for continuous vulnerabilities.
    - The core reason which brought about the problem does not receive resolution.

5. Testing

Test 1- Ping of death/ICMP Flood

Step	Details
Attack	**CMD:** sudo hping3 --icmp --flood -d 3200 **192.168.18.137** **Goal:** Flood the victim with oversize ICMP Packets.
Check	Monitor server stability, CPU/memory usage, and check task manager for dropped packets.
Mitigate	Apply firewall rules to limit or block ICMP packets.
Result	The attack was mitigated. CPU, Memory remained stable.

Table 6 Table of testing ping of death attack

Note:

- **Sudo –** Runs the command with administrator rights.
- **hping3 –** The tool used to send custom network packets.
- **--icmp –** Sends ICMP packets (like a ping).
- **--flood –** Sends packets very quickly, one after another.
- **-d 3200 –** Makes each packet very large (3200 bytes).
- **target-ip –** Replace this with the IP address of the target machine.

Step1- Attack Command

Running Hping3 cmd in terminal.

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --icmp --flood -d 3200 192.168.18.137
HPING 192.168.18.137 (eth0 192.168.18.137): icmp mode set, 28 headers + 3200 data bytes
hping in flood mode, no replies will be shown
```

Figure 34: Screenshot of attack execute

Step2- System Check after attack

System, CPU, memory use.

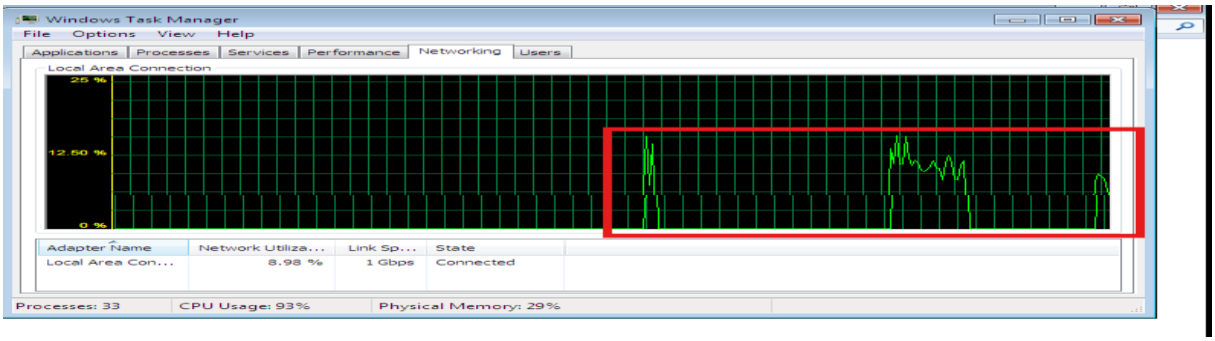

Figure 35: Monitoring after attack

Step3- Mitigation

Applying Firewall

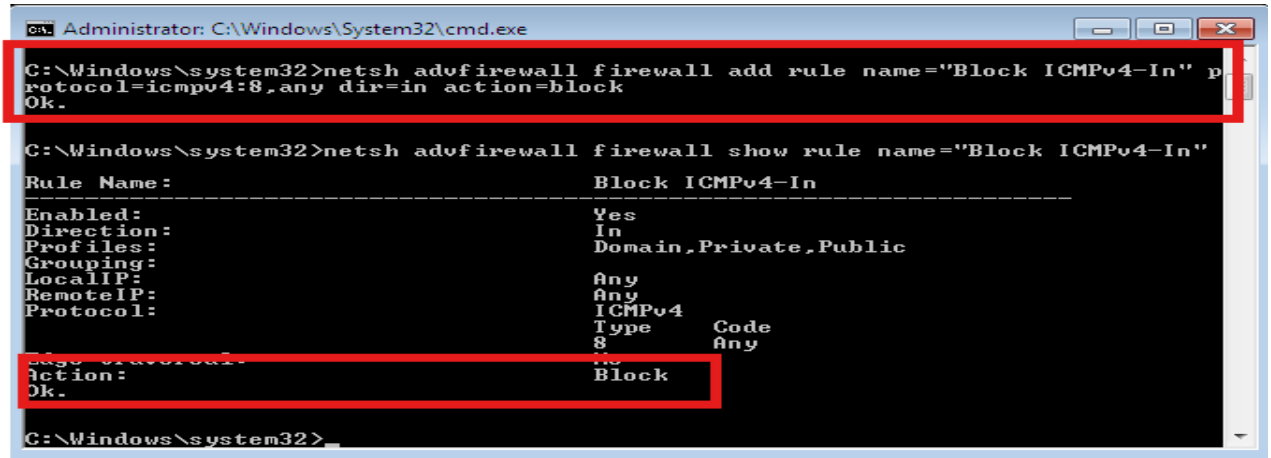

Figure 36: screenshot of applying ICMP packet

Step4- Success Proof after blocking ICMP packet

Task manager showing ICMP packets blocked, or rate limited in graph.

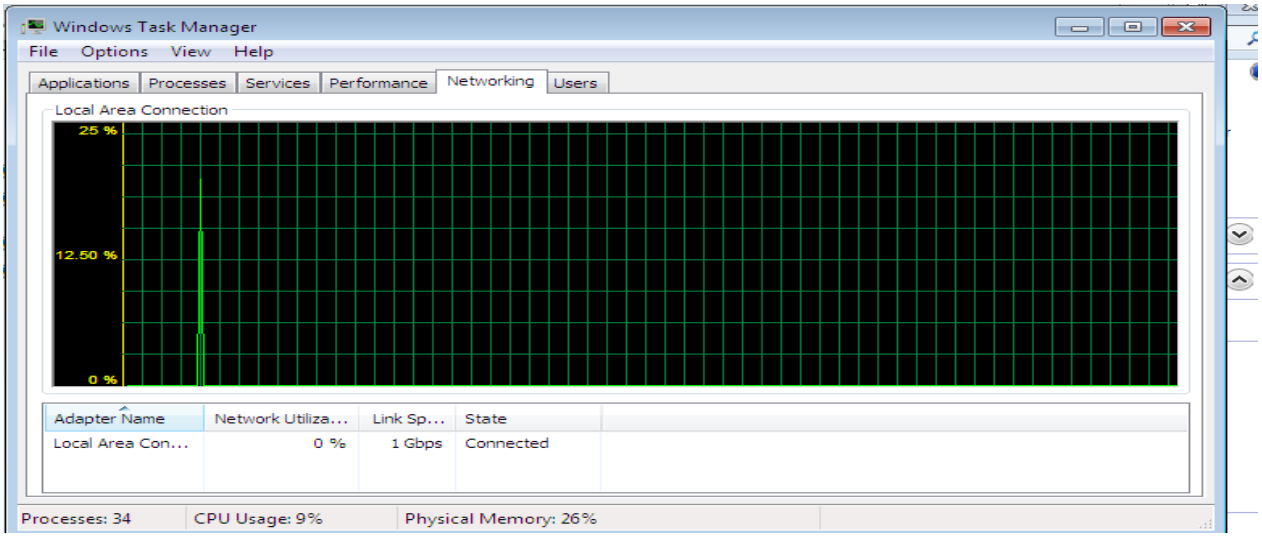

Figure 37 post monitor of victim machine

The test was successful.

Test 2- Fragmented Packet Attack

Step	Details
Attack	**CMD: sudo hping3 -f -S -p 445 192.168.18.137** **Goal:** Try to confuse the server.
Check	Look at CPU and memory on the server before and during the attack.
Mitigate	Apply firewall rules to block fragmented packets.
Result	The attack was mitigated. CPU, Memory remained stable.

Table 7: Table of fragmented packet attack

Note:

- **sudo –** Run as admin/root.
- **hping3 –** Tool to send custom network packets.
- **-f –** Fragment the packets.
- **-S –** Set the SYN flag (start a TCP connection).
- **-p 445 –** Target port 445 (web server).
- **target-ip –** IP address of the target machine.

Step1- Attack Command

Running Hping3 cmd in terminal.

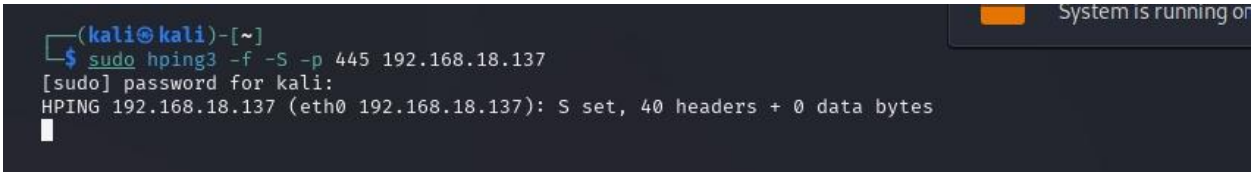

Figure 38: Screenshot of attack execute

Step2- System Check after attack

System, CPU, memory use.

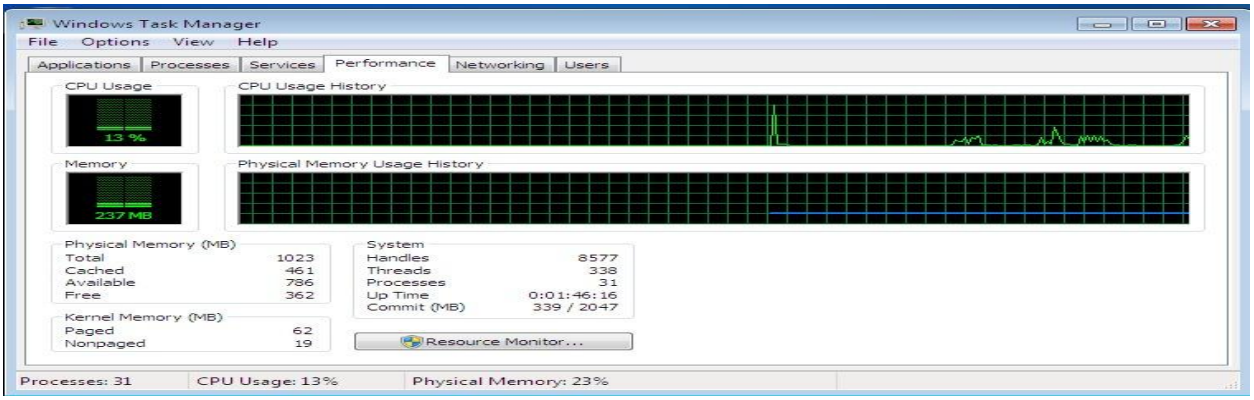

Figure 39: Monitor after attack

Step3- Mitigation

Applying Firewall

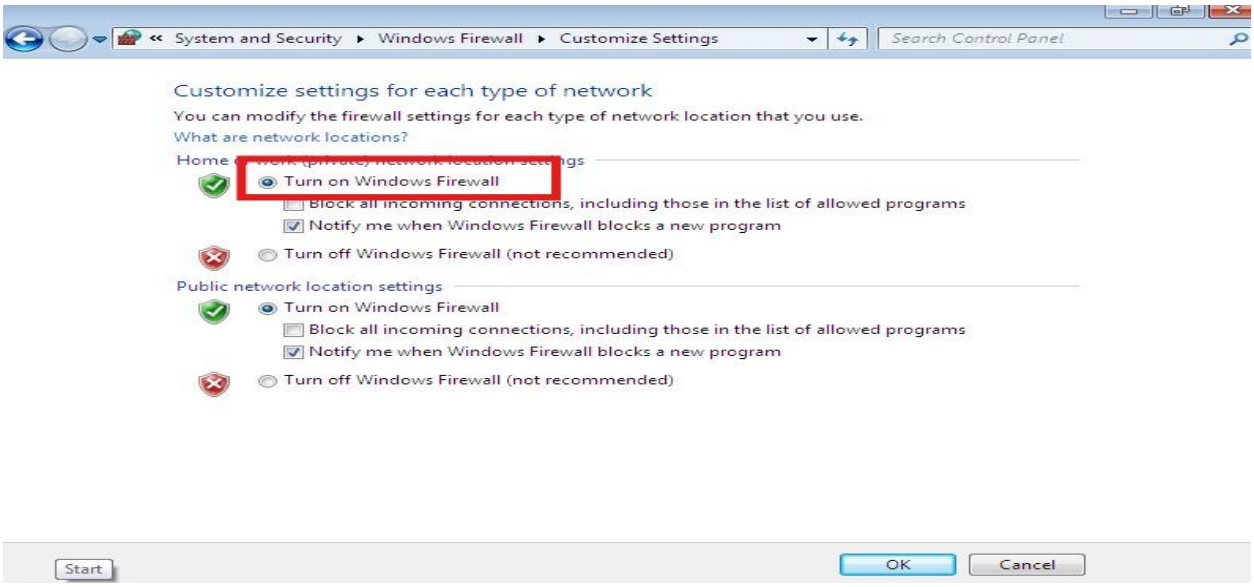

Figure 40: open firewall to mitigate

Step4- Success Proof after blocking ICMP packet

Task manager showing ICMP packets blocked, or rate limited.

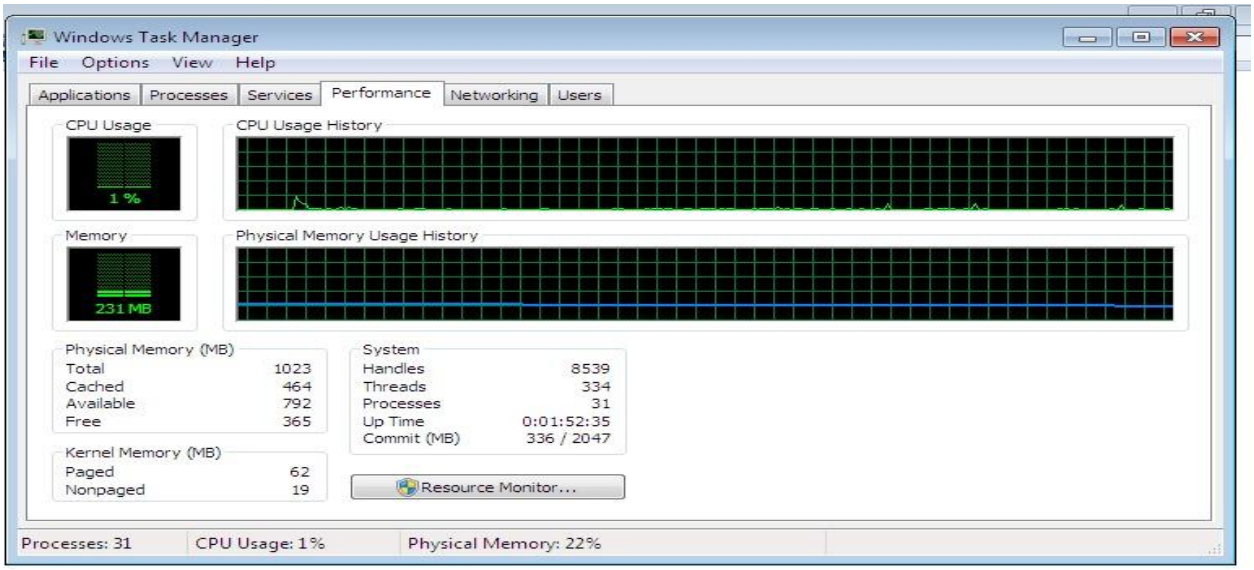

Figure 41: monitoring after attack

The test was successful.

6. Conclusion

The research demonstrated successful security detection approaches for blocking SYN flood denial-of-service attacks along with their reduction techniques within virtual network setup. The Windows operating system received the attack through a SYN flood process controlled by Metasploit and Hping3 from Kali Linux. The attacker system resources depleted as service access got blocked according to Wireshark network capture data and system performance testing records.

Sandboxing SMB connections along with IP address limits protected the system along with RdpGuard to make up the security against this attack. Research simulations proved the defensive measures effective as they completely prevented both connection attempts and traffic congestion from reaching victim systems.

Proactive network defense and proper access controls and continuous monitoring form the system defense requirements for protecting against common DoS threats according are done in the report.

References

A10 staff, 2022. *A10networks.com.* [Online]
Available at: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/
[Accessed 20 4 2025].

Burke, A., 2025. *Quest Technology Management.* [Online]
Available at: https://questsys.com/security-blog/Understanding-the-Different-Types-of-DDoS-Attacks/#:~:text=Reputational%20Damage:%20Customers%20expect%20reliable%20service%20from,it%20harder%20to%20retain%20and%20attract%20customers
[Accessed 20 4 2025].

digitalguardian, 2024. *What is the server message block protocol?.* [Online]
Available at: https://www.digitalguardian.com/blog/what-server-message-block-protocol
[Accessed 20 4 2025].

Extrahop, 2024. *Extrahop.com.* [Online]
Available at: https://www.extrahop.com/resources/attacks/dos
[Accessed 22 4 2025].

Government of canada, 2020. *Canadian Centre for Cyber Security.* [Online]
Available at: https://www.cyber.gc.ca/en/guidance/protecting-your-organization-against-denial-service-attacks-itsap80100
[Accessed 20 4 2025].

IBM, 2024. *Ibm.com.* [Online]
Available at: https://www.ibm.com/think/topics/cyber-attack
[Accessed 20 4 2025].

Labs, K., 2024. *Keepnet Labs.* [Online]
Available at: https://keepnetlabs.com/blog/what-is-a-denial-of-service-do-s-attack
[Accessed 20 4 2025].

Palo Alto Networks, 2024. *What are firewall rules?.* [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/what-are-firewall-rules#:~:text=Firewall%20rules%20are%20specific%20directives,complies%20with%20these%20set%20parameters
[Accessed 20 4 2025].

Plurilock, 2021. *Plurilock.com.* [Online]
Available at: https://plurilock.com/deep-dive/denial-of-service-dos-attack/#:~:text=The%20economic%20impact%20of%20DoS,cost%20of%20implementing%20remediation%20measures
[Accessed 20 4 2025].
Rdpguard, 2024. *Rdpguard.com.* [Online]
Available at: https://rdpguard.com/
[Accessed 20 4 2025].
Surfshark, 2020. *Surfshark.com.* [Online]
Available at: https://surfshark.com/research/cybercrime-risks/crime-denial-of-service
[Accessed 20 4 2025].
warburton, d., 2021. *F5 labs.* [Online]
Available at: https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020
[Accessed 20 4 2025].