# INTERNSHIP REPORT
# ON
# "PORT SCANNING"

**SUBMITTED TO:**

## MADHAV INSTITUTE OF TECHNOLOGY AND SCIENCE GWALIOR

**(A Govt. aided Autonomous Institute under RGPV, BHOPAL (M.P.) Established in (1957))**

**IN PARTIAL FULFILLMENT FOR THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF**

**BACHELOR OF TECHNOLOGY**

**IN**

**ELECTRONICS & TELECOMMUNICATION ENGINEERING**

**2022-2023**


**SUBMITTED BY:**
**KHUSHBU JAIN (0901ET191031)**

**GUIDED BY:**
**DR.LAXMI SHRIVASTAVA**
**ASSOCIATE PROFESSOR**

**DEPARTMENT OF ELECTRONICS ENGINEERING**
**MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE**
**GWALIOR-474005 (M.P.)**

# MADHAV INSTITUTE OF TECHNOLOGY AND SCIENCE
# GWALIOR

(A Govt. aided Autonomous Institute under RGPV, BHOPAL(M.P.) Established. in (1957))

## CERTIFICATE OF APPROVAL

This is to certify that the Internship is carried out in **Indian Institute of Technology, Indore** submitted by **KHUSHBU JAIN (0901ET191031)** student of **B.Tech. IV-Year (VIII Semester)** in partial fulfillment for the award of the degree of **Bachelor of Technology in Electronics & Telecommunication Engineering** under R.G.P.V., Bhopal. It is a record of their own work carried by them during internship.

26/5/23

**Supervised/Verified by**
**Dr. Laxmi Shrivastava**
**Associate Professor**

**Approved by**
**Dr. Vandana Vikas Thakare**
**H.O.D**

# MADHAV INSTITUTE OF TECHNOLOGY AND SCIENCE
## GWALIOR

(A Govt. aided Autonomous Institute under RGPV, BHOPAL (M.P.) Established in (1957)

## DECLARATION

We hereby declare that the work which has been carried out during the Internship in the company **Indian Institute of Technology, Indore** in partial fulfillment for the award of the degree of **Bachelor of Technology** in **Electronics & Telecommunication Engineering** from Madhav Institute of Technology & Science, Gwalior is an authenticated record of our work carried under the supervision /mentorship of **Prof. Neminath Hubbali** (Professor, IIT Indore) **& Dr. Laxmi Shrivastava** (Professor, MITS, Gwalior).The matter embodied in this internship report is not submitted for the award of any degree or diploma anywhere else.

Name & Signature of Students

Date: 26/05/23
Place: Gwalior

KHUSHBU JAIN
(0901ET191031)

## ACKNOWLEDGEMENT

We express our sincere gratitude and earnest indebtedness to Madhav Institute of Technology & Science, Gwalior (M.P.) for providing us the golden opportunity to complete our internship. We acknowledge with great pleasure and grateful indebtedness towards our internship mentor Prof. Neminath Hubbali (Professor, IIT Indore) & Dr. Laxmi Shrivastava ( Professor, MITS-Gwalior) for providing us with very useful and beneficial guidance throughout the Internship.

We also express our heartfelt gratitude to Dr. Vandana Vikas Thakare, Head of the Electronics Engineering Department for her profound guidance throughout the Internship.

We would also like to acknowledge our Director Dr. R. K. Pandit for helping us with the resources needed to accomplish this task. The environment at M.I.T.S. has been a valuable experience for us. With many difficulties, this Internship has blessed us with great knowledge in our field of interest. We also thank all those who have helped us in every path in the completion of this Internship and made this Internship a success.

Name & Signature of Students

Date: 26/05/23

Place: Gwalior

KHUSHBU JAIN

(0901ET191031)

# NOC


MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

Phone: 0751-2409362, Email id: [redacted]

(Training and Placement Cell)


Ref. T&P/21/1769

Date: 18/1/2021

To,

Professor

IIT Indore

Dear Sir/Ma'am,

We are grateful to the co-operation in imparting industrial training/internship/educational training to the Students of our institute. Industrial training/internship is a part of Academic Curriculum in the final and final year of B.Tech./MCA/MBA students and the progress of the same will be counted in their overall results and also gives them exposure & improves their skills and personality.

We will be highly obliged, if the following student is/are permitted to undergo training / internship at your esteemed Organization for a period of 23/01/2021 to 31/05/2021

| S.No | Name of the Student | Enrollment No | Course, Branch |
|---|---|---|---|
| 1 | [redacted] | [redacted] | B.Tech. (Computer Science & Communication Engineering) |

Hoping for your kind cooperation.

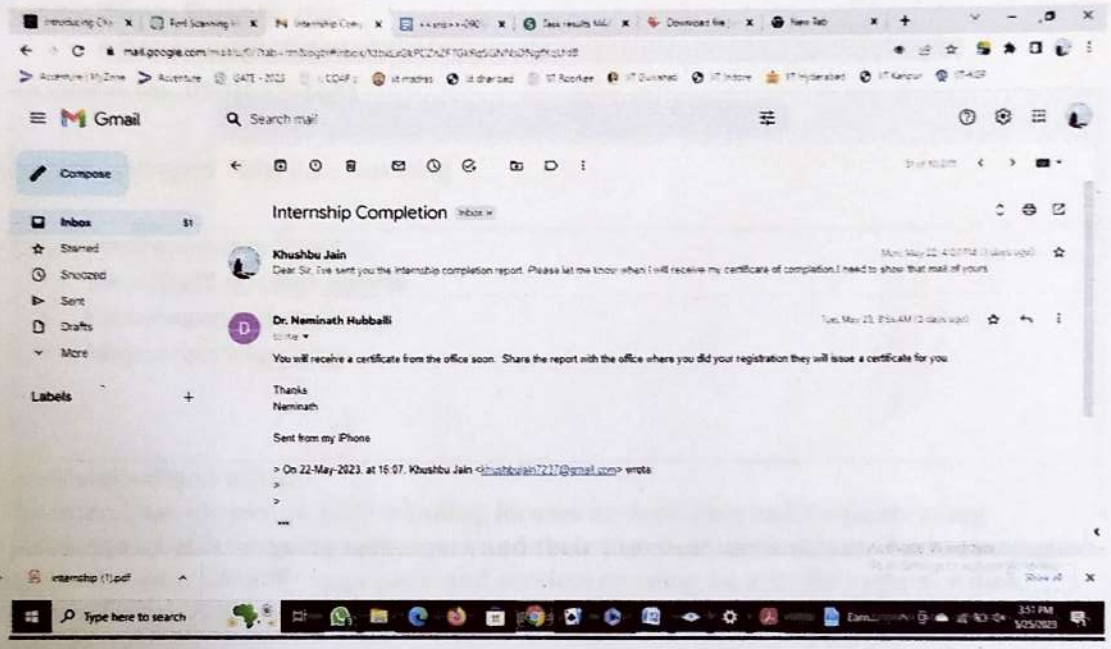
Best Regards!

Mr. Vikram Singh Rajput)
Training & Placement Officer

Kindly feel free to contact us for any further information.

*Important Declaration: This is a system generated letter with reference no. after the approval from the authority. There is no need for a signature and seal on hard copy.*

# CERTIFICATE



## Internship/ProjectExpectedOutcomes

Session:Jan–June2023

**Student Name: Khushbu Jain**

**Enrollment No.:**0901ET191031

**Internship/Project Title:** Port Scanning

| |
|---|
| **ObjectiveofInternship/Project:**<br>• **Identification ofopenports**<br>• **UnderstandanduseNmap**<br>• **Mapnetworktopology** |
| **BriefdetailsofInternship:**<br>**The internship project on port scanning focuses on exploring and understanding theconcept of port scanning techniques and their practical applications. Port scanning is amethod used to identify open ports and services running on a target system, which iscrucialfornetworkadministratorsto ensurethesecurity andproperfunctioning oftheirnetworks.** |
| **Expected/AchievedOutcomesofInternship/Project:**<br>• **Identifyingopenandcloseports**<br>• **Learning theuseofopenports**<br>• **Usenmap forfinding openports** |
| **Socialrelevance/ImpactofyourInternship/Project:**<br>• **Enhancingnetworksecurity**<br>• **Mitigatingcyberthreats**<br>• **EthicalHacking** |

**KhushbuJain**

**NameandSignatureofStudents**

**Laxmi Shrivastava, Associate Professor**

**NameandSignatureofInstitute Mentor**

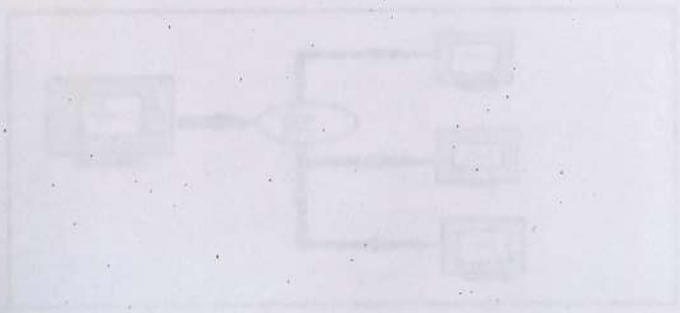
## CONTENT:

# ABSTRACT

Port Scanner is software designed to scan network hosts for open port. To monitor open ports we need to use a port scanner and the most accurate port scanner would be an online port scan. Port scanner and sniffer software are simple to use even if by a non-tech person. To check security of networks and by hacker to compromise it this is often used by administrators.

The purpose of this task is to identify port status for different ports by performing scans on various specified ports.

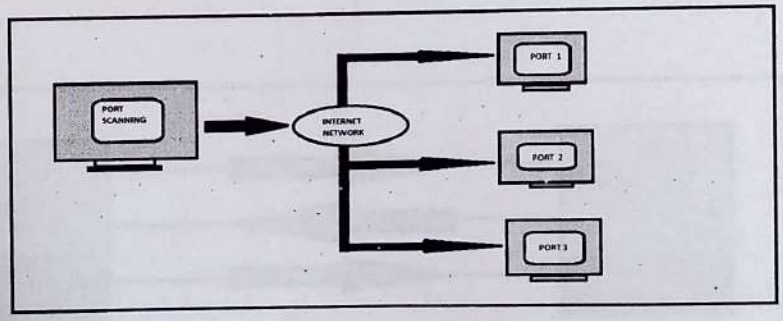
In my project, I've performed scanning on different IP addresses and checked the port status of those IP address and IP host.



# INTRODUCTION

Port scanning is an essential technique within the cyber-security field that is employed to identify open ports on computer systems or networks without plagiarizing any existing sources. Ports act as communication endpoints facilitating data exchange between devices. Through port scanning, security professionals can evaluate the accessibility and potential vulnerabilities of targeted systems.

The primary objective of port scanning is to map network topology and ascertain the services or applications operating on specific ports. Consequently, security practitioners can determine whether ports are open, closed, or filtered, providing critical insights into potential entry points for attackers. It empowers security professionals to identify misconfigured systems, outdated software, or unauthorized services that could pose security risks.



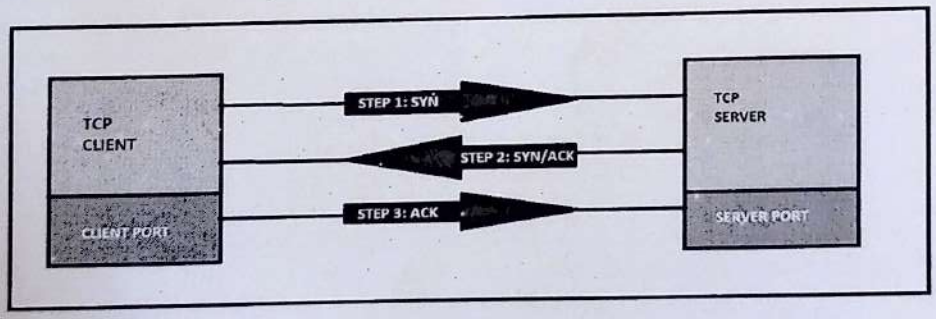
## THREE WAY HAND-SHAKE:

The three-way handshake is an essential process for establishing a TCP connection between a client and a server. In the context of port scanning, it plays a crucial role in determining the status of a specific port by analyzing the responses received during the handshake. The steps involved in the three-way handshake during port scanning are as follows:

- SYN (Synchronize) - In this step, the port scanner sends a TCP SYN packet to the target IP address and the specific port being scanned. The SYN flag is set in the packet, indicating the intention to establish a connection.

- SYN-ACK (Synchronize-Acknowledgment) - If the port being scanned is open, the target server responds with a SYN-ACK packet. This packet signifies that the server is willing to establish a connection and acknowledges the SYN packet received from the port scanner.

- ACK (Acknowledgment) - Upon receiving the SYN-ACK packet, the port scanner sends an ACK packet back to the server. This packet confirms the server's acknowledgment and completes the three-way handshake, establishing a successful TCP connection.

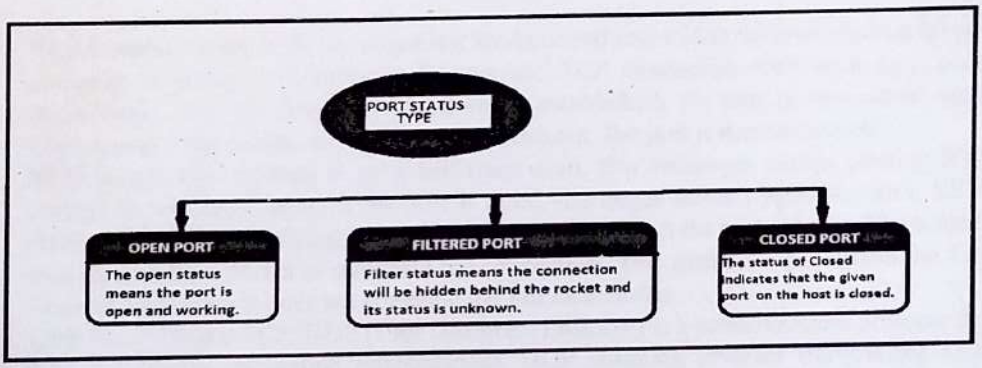



The responses received during the three-way handshake provide insights into the status of the port being scanned:

- Open Port: If the port scanner receives a SYN-ACK packet in response to the initial SYN packet, it indicates that the port is open and ready to establish a connection.

- Closed Port: When the port scanner receives a TCP RST (Reset) packet in response to the SYN packet, it signifies that the port is closed.

- Filtered Port: If the port scanner does not receive any response or encounters an ICMP unreachable error message, such as "port unreachable" or "host unreachable," it suggests that the port is filtered.



## PORT SCANNING TECHNIQUE

Port scanning techniques encompass a range of methods used to scan and analyze ports on a target system or network. These techniques empower security professionals to evaluate the accessibility and potential vulnerabilities of networked devices. Here are several common port scanning techniques:

1. **TCP Connect Scan:** This technique is a fundamental and widely utilized method for port scanning. It involves establishing a complete TCP connection with each port under examination. If a connection is successfully established, the port is considered open. Conversely, if the connection is refused or times out, the port is deemed closed.
2. **SYN Scan:** Also referred to as a half-open scan, this technique entails sending SYN packets to the target ports. If the port is open, the target server responds with a SYN-ACK packet, acknowledging the SYN packet received from the port scanner. The scanner then sends a RST packet to terminate the connection. This method is faster than the TCP Connect Scan since it does not complete the full handshake.
3. **UDP Scan:** Unlike TCP, UDP (User Datagram Protocol) is a connectionless protocol that does not require connection establishment. UDP scanning involves transmitting UDP packets to the target ports and examining the responses. If the port responds with an ICMP "port unreachable" message or does not respond at all, it indicates that the port is closed. If a response is received, further analysis is necessary to determine whether the port is open or filtered.
4. **FIN Scan:** This technique involves dispatching packets with the FIN flag set to the target ports. If the port is closed, it should respond with a TCP RST packet. However, if the port is open, it silently discards the packet, resulting in no response. The FIN Scan can be employed to avoid detection, as closed ports typically generate an RST packet in response.
5. **XMAS Scan:** Similar to the FIN Scan, the XMAS Scan sends packets with the FIN, PSH, and URG flags set. The scanning tool anticipates response behavior akin to the FIN Scan, where closed ports respond with a RST packet, while open ports remain unresponsive.
6. **NULL Scan:** In a NULL Scan, the scanning tool dispatches packets with no flags set (NULL packets) to the target ports. If the port is closed, it should respond with a TCP RST packet. However, if the port is open, it silently discards the packet, resulting in no response.
7. **Idle Scan:** The Idle Scan technique leverages IP ID sequence prediction to indirectly scan ports through a zombie or idle host. By sending spoofed packets from the idle host to the target, the received responses aid in determining the status of the target ports. This technique can help evade detection since the idle host serves as a proxy.

These examples represent only a selection of port scanning techniques. Each technique possesses its own advantages, disadvantages, and specific use cases. It is crucial to note that port scanning should be conducted solely on systems or networks with proper authorization and for legitimate security assessment purposes.

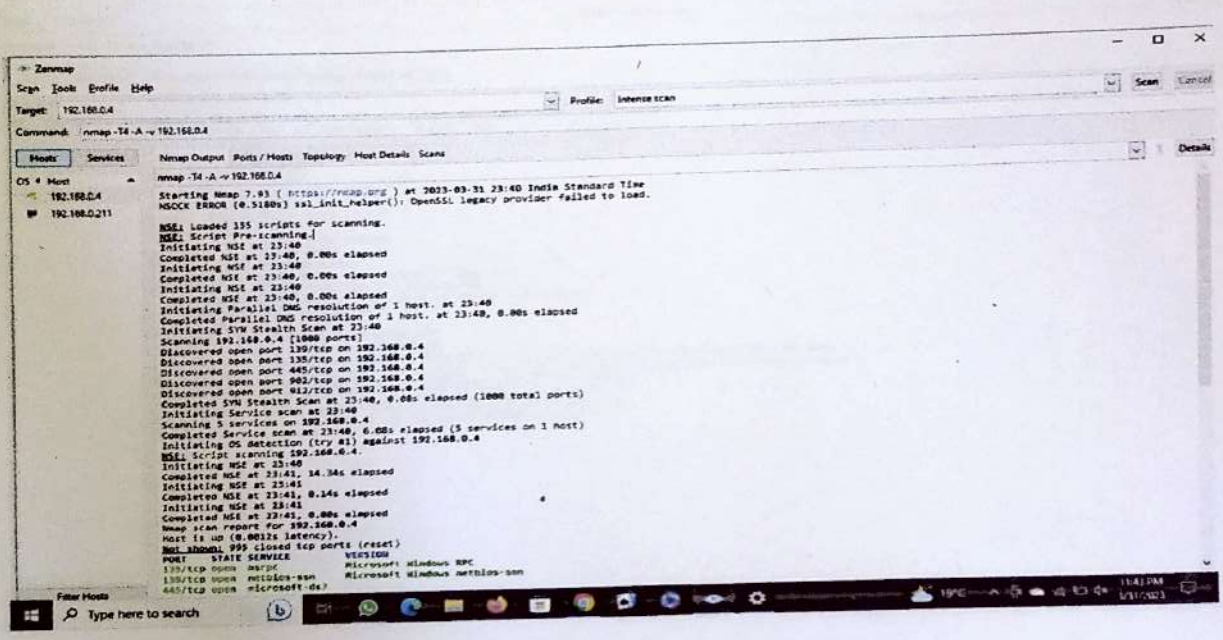
## PROTECTING AGAINST MALICIOUS PORT SCANNING

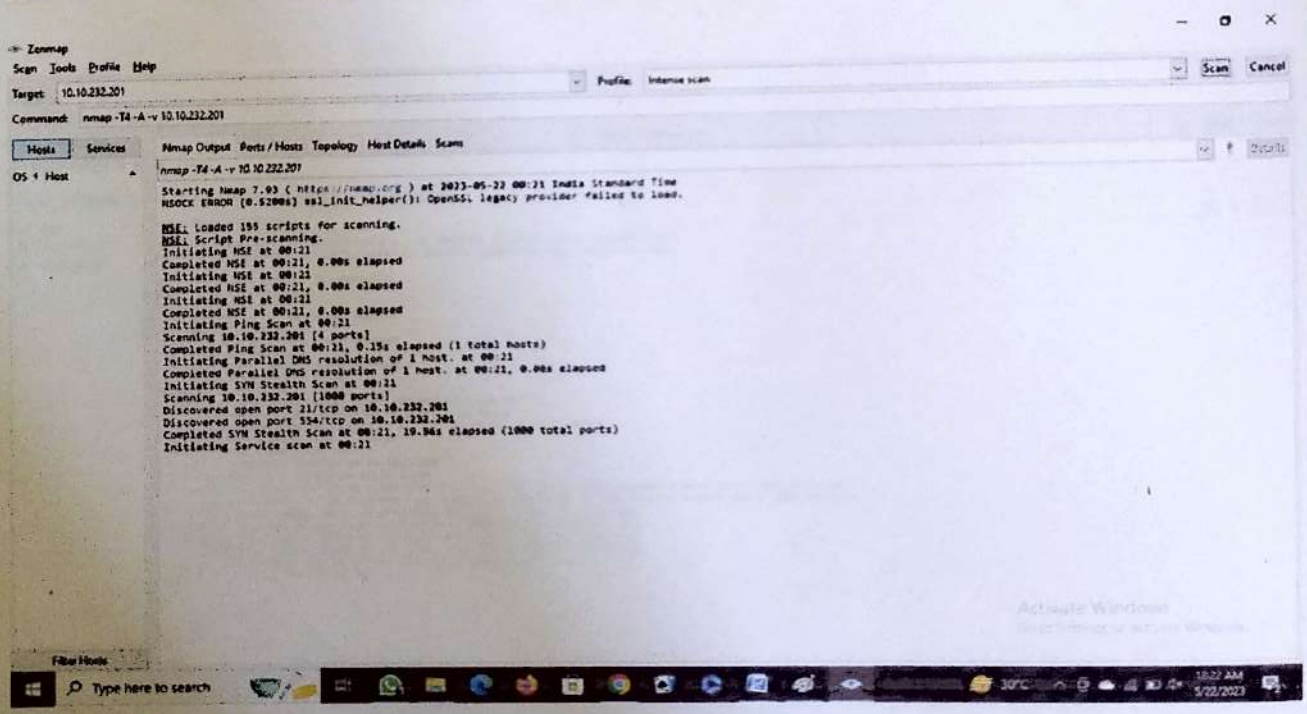
To safeguard against malicious port scanning, it is essential to employ a range of security measures. The following recommendations outline effective protections:

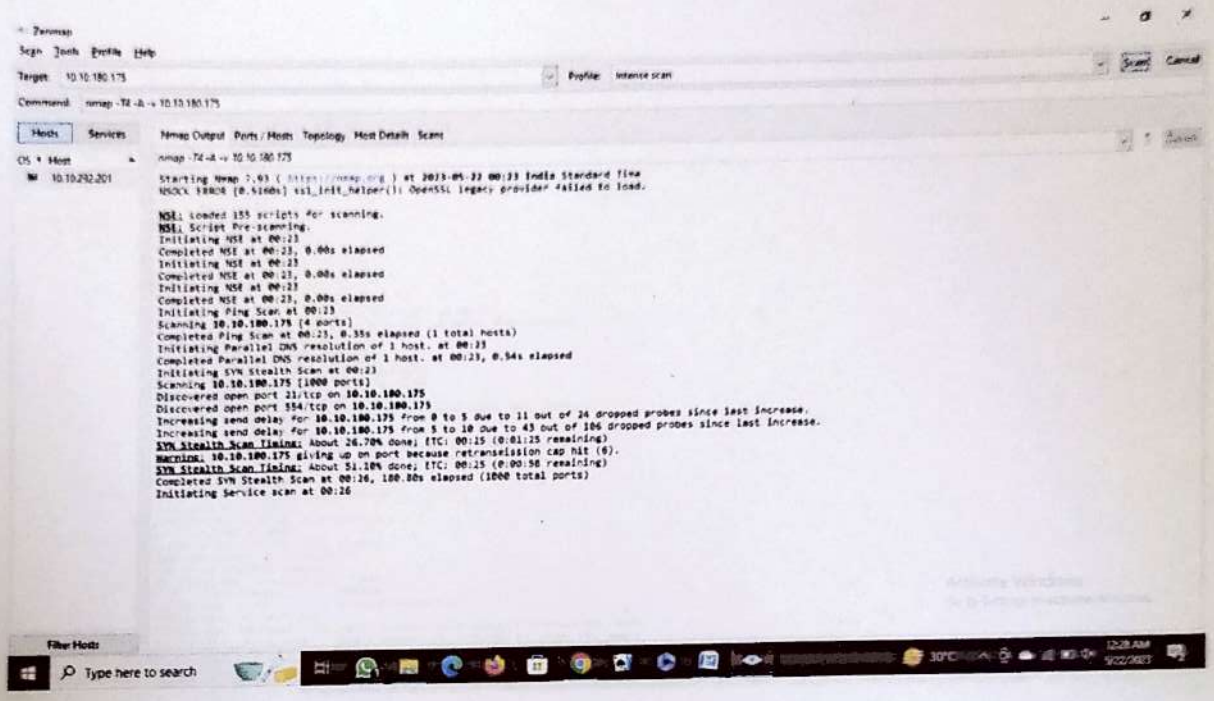
1. **Firewalls:** Deploy firewalls to filter incoming and outgoing network traffic. Customize firewall configurations to block or restrict access to unnecessary ports and services, permitting only essential ports for authorized communication. **Intrusion Detection/Prevention Systems (IDS/IPS):** Implement IDS/IPS solutions to monitor network traffic and identify potential port scanning attempts. These systems employ pattern recognition and signature analysis to detect port scanning activities, triggering alerts or automatically blocking offending IP addresses.
2. **Port Filtering:** Utilize port filtering mechanisms to explicitly allow or deny access to specific ports based on their necessity. By blocking access to unused or unnecessary ports, you reduce the attack surface and mitigate risks associated with port scanning.
3. **Network Monitoring:** Employ network monitoring tools to continuously oversee network traffic and identify any anomalous or suspicious behavior. Close scrutiny of network activity enables the detection of potential port scanning attempts, facilitating appropriate actions.
4. **Regular Patching and Updates:** Keep systems and applications up to date by promptly applying the latest patches and security updates. Regular patching addresses known vulnerabilities, diminishing the likelihood of exploitation through port scanning.
5. **Intrusion Prevention Best Practices:** Adhere to intrusion prevention best practices, including disabling unnecessary services, utilizing strong and unique passwords, implementing access controls, and employing encryption where appropriate.
6. **Network Segmentation:** Implement network segmentation by dividing the network into separate subnets or VLANs. This approach confines potential breaches and minimizes the impact of port scanning activities, as attackers would need to navigate additional security boundaries to access critical systems or information.
7. **Rate Limiting:** Enforce rate limiting techniques to restrict the number of connection requests from a single IP address within a defined time frame.
8. **Intrusion Response and Incident Handling:** Establish an incident response plan to promptly address and mitigate security incidents, including port scanning activities.
9. **Security Awareness and Training:** Educate employees and users about the risks associated with port scanning and emphasize the importance of adhering to security best practices. Training programs enhance individuals' ability to recognize and report suspicious activities, minimizing the impact of port scanning attempts.

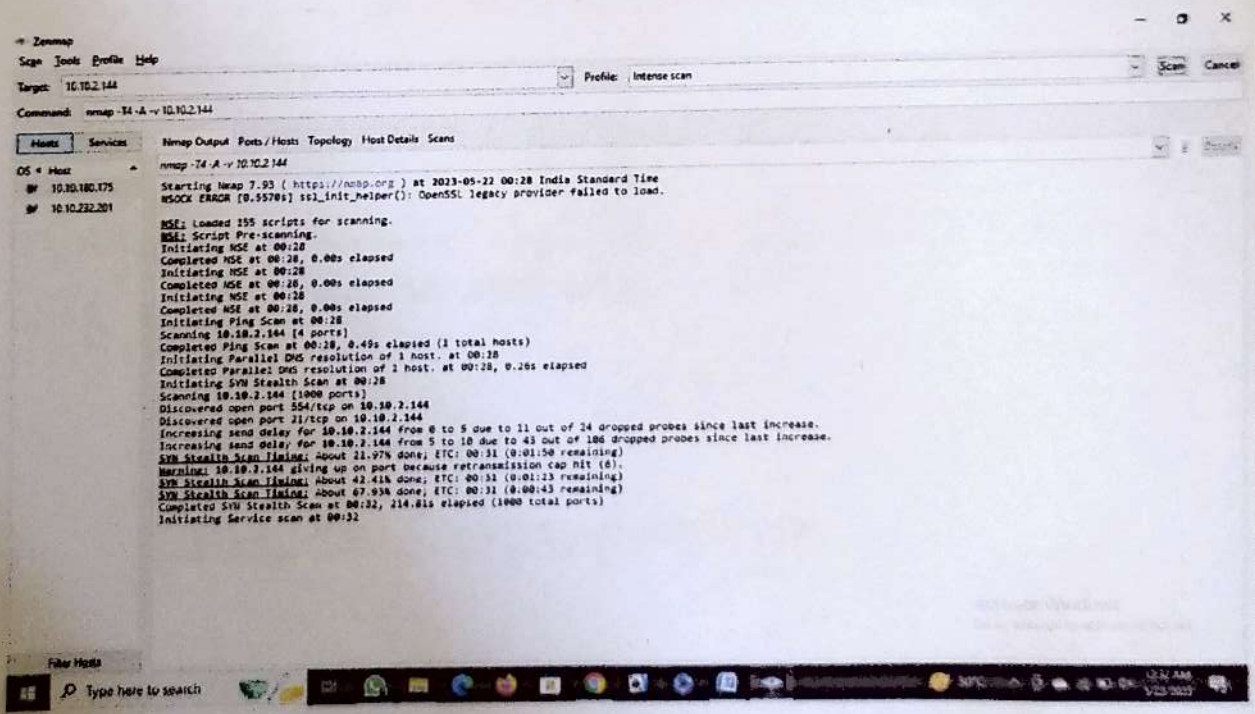
By implementing these protective measures, organizations can bolster their security posture and reduce the risks posed by malicious port scanning activities. Employing a multi-layered security approach and regularly updating and adapting these measures are crucial to address emerging threats and vulnerabilities.

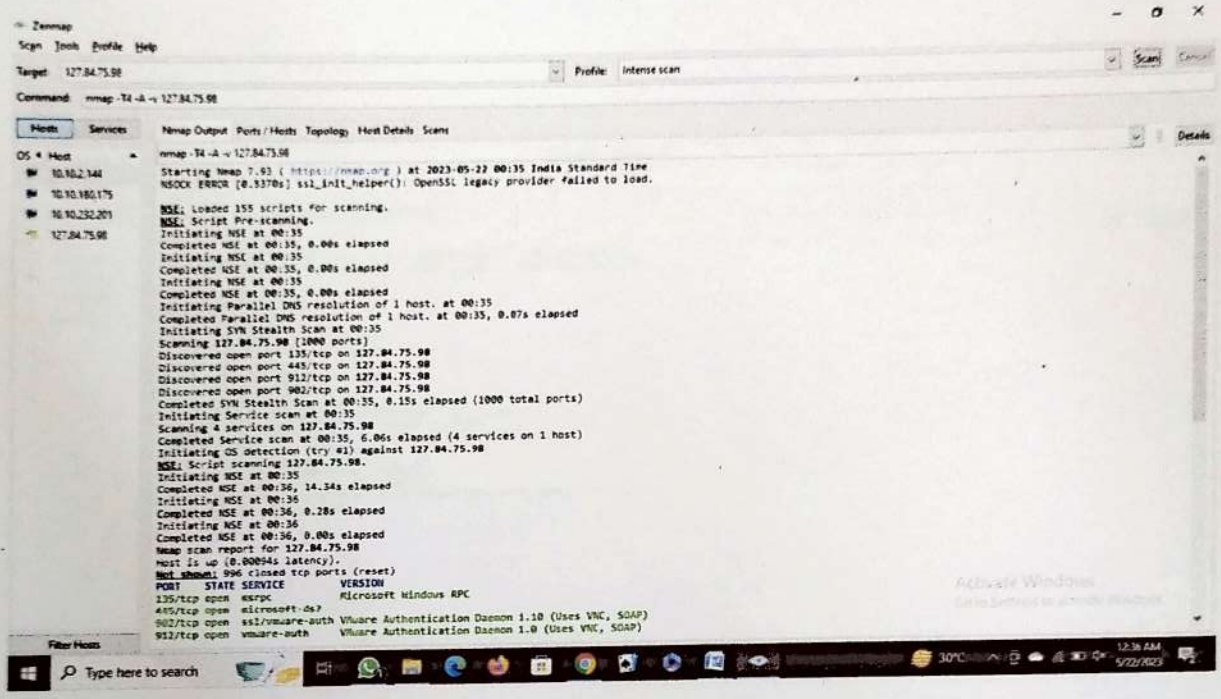
# PERFORMED PORT SCANS

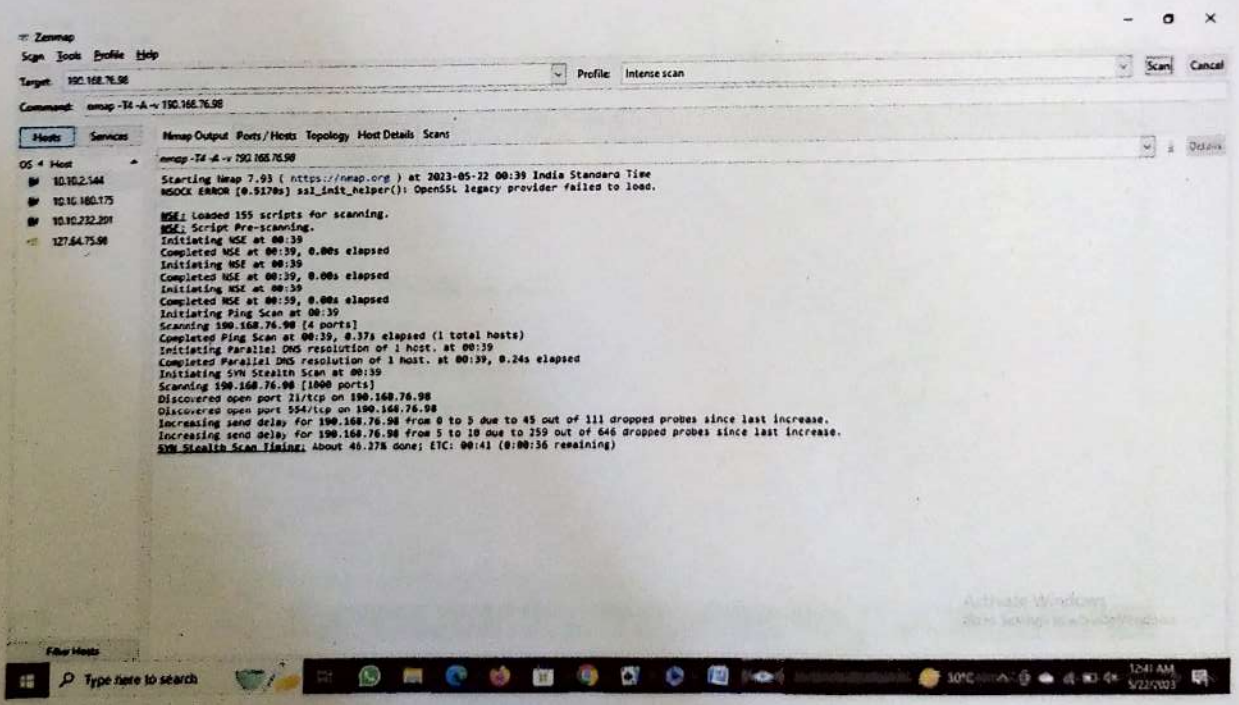


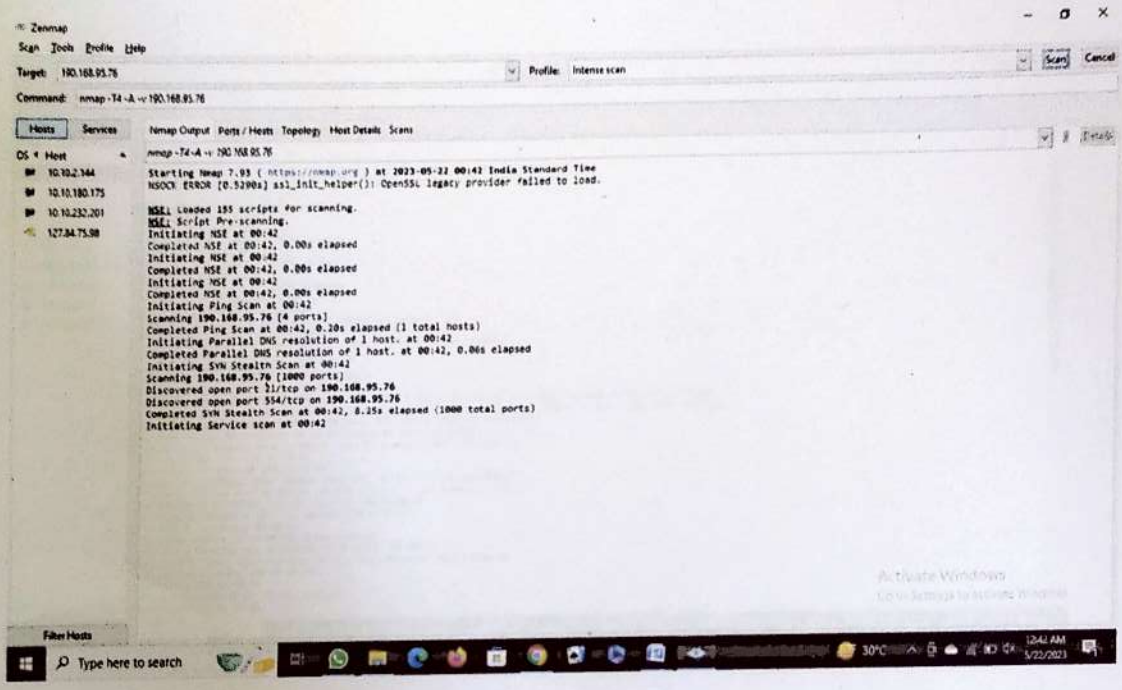



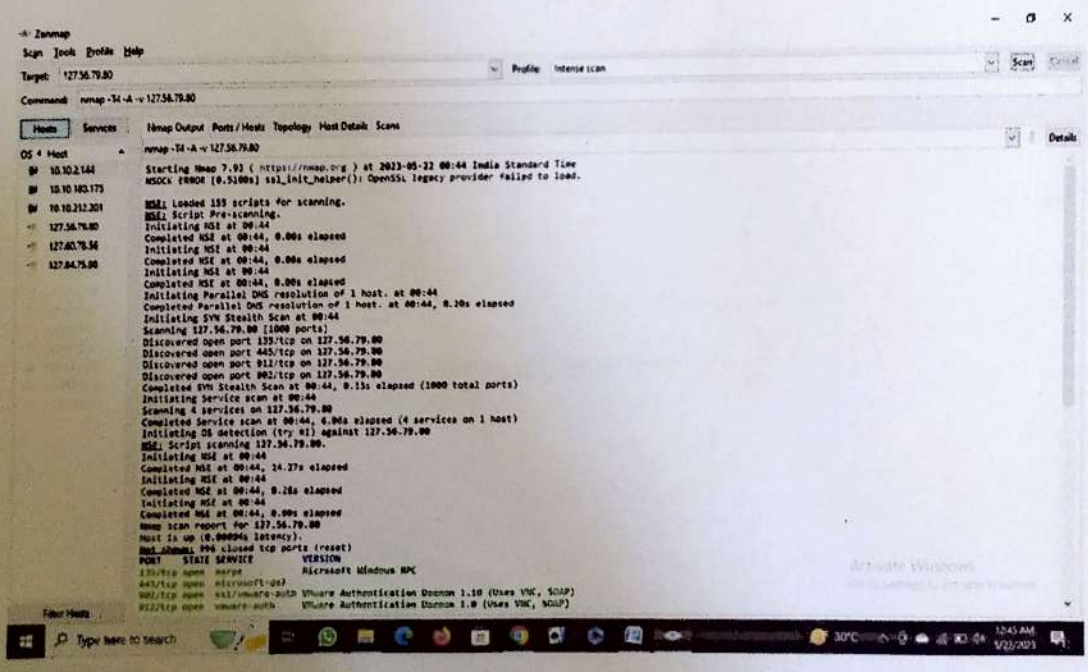

Zenmap
Scan Tools Profile Help
Target: 10.10.180.175
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 10.10.180.175
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS ▾ Host
10.10.232.201
nmap -T4 -A -v 10.10.180.175
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 00:23 India Standard Time
NSOCK ERROR [0.5160s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:23
Completed NSE at 00:23, 0.00s elapsed
Initiating NSE at 00:23
Completed NSE at 00:23, 0.00s elapsed
Initiating NSE at 00:23
Completed NSE at 00:23, 0.00s elapsed
Initiating Ping Scan at 00:23
Scanning 10.10.180.175 [4 ports]
Completed Ping Scan at 00:23, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:23
Completed Parallel DNS resolution of 1 host. at 00:23, 0.54s elapsed
Initiating SYN Stealth Scan at 00:23
Scanning 10.10.180.175 [1000 ports]
Discovered open port 21/tcp on 10.10.180.175
Discovered open port 554/tcp on 10.10.180.175
Increasing send delay for 10.10.180.175 from 0 to 5 due to 11 out of 24 dropped probes since last increase.
Increasing send delay for 10.10.180.175 from 5 to 10 due to 43 out of 106 dropped probes since last increase.
SYN Stealth Scan Timing: About 26.70% done; ETC: 00:25 (0:01:25 remaining)
Warning: 10.10.180.175 giving up on port because retransmission cap hit (6).
SYN Stealth Scan Timing: About 51.10% done; ETC: 00:25 (0:00:58 remaining)
Completed SYN Stealth Scan at 00:26, 180.80s elapsed (1000 total ports)
Initiating Service scan at 00:26
Filter Hosts
Type here to search

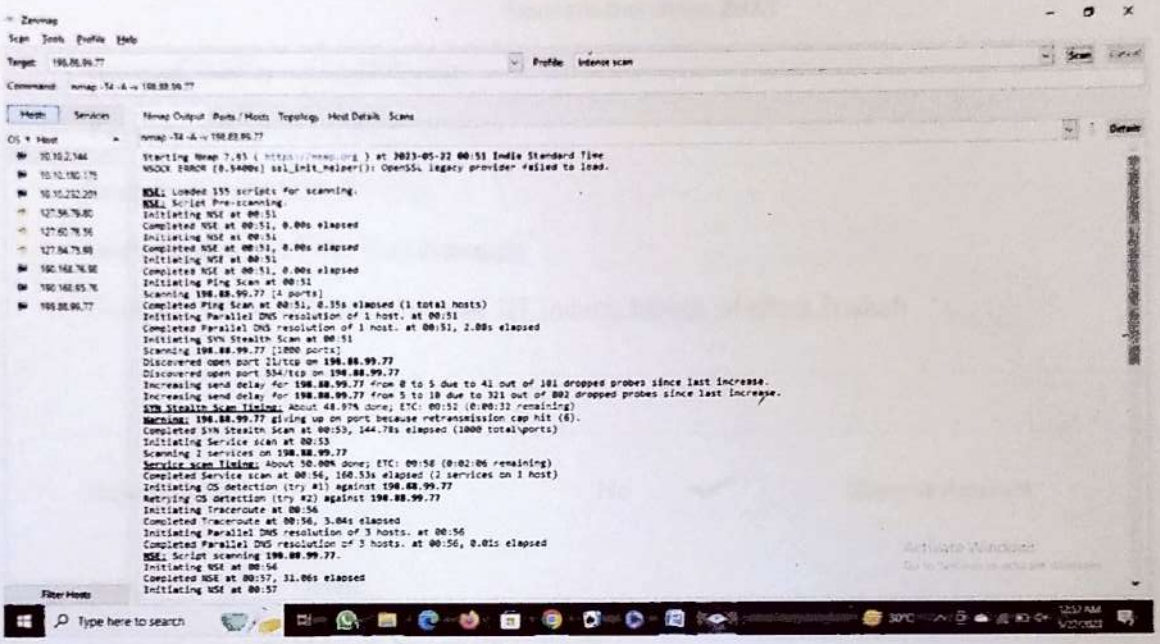

Zenmap
Scan Tools Profile Help
Target: 10.10.2.144
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 10.10.2.144
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS ▾ Host
10.10.180.175
10.10.232.201
nmap -T4 -A -v 10.10.2.144
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 00:28 India Standard Time
NSOCK ERROR [0.5570s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Initiating Ping Scan at 00:28
Scanning 10.10.2.144 [4 ports]
Completed Ping Scan at 00:28, 0.49s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:28
Completed Parallel DNS resolution of 1 host. at 00:28, 0.26s elapsed
Initiating SYN Stealth Scan at 00:28
Scanning 10.10.2.144 [1000 ports]
Discovered open port 554/tcp on 10.10.2.144
Discovered open port 21/tcp on 10.10.2.144
Increasing send delay for 10.10.2.144 from 0 to 5 due to 11 out of 24 dropped probes since last increase.
Increasing send delay for 10.10.2.144 from 5 to 10 due to 43 out of 106 dropped probes since last increase.
SYN Stealth Scan Timing: About 21.97% done; ETC: 00:31 (0:01:50 remaining)
Warning: 10.10.2.144 giving up on port because retransmission cap hit (6).
SYN Stealth Scan Timing: About 42.41% done; ETC: 00:32 (0:01:23 remaining)
SYN Stealth Scan Timing: About 67.93% done; ETC: 00:31 (0:00:43 remaining)
Completed SYN Stealth Scan at 00:32, 214.81s elapsed (1000 total ports)
Initiating Service scan at 00:32
Filter Hosts
Type here to search

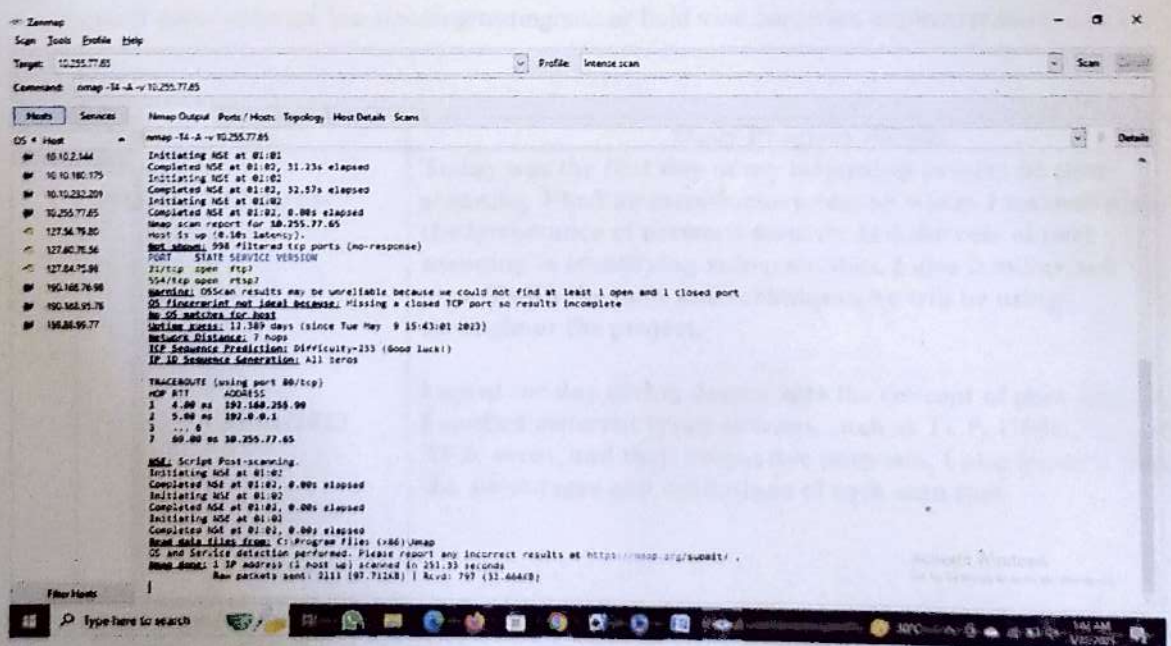

Zenmap
Scan Tools Profile Help
Target: 127.84.75.98
Profile: Intense scan
Scan
Command: nmap -T4 -A -v 127.84.75.98
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.2.144
10.10.160.175
10.10.232.201
127.84.75.98
nmap -T4 -A -v 127.84.75.98
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 00:35 India Standard Time
NSOCK ERROR [0.9370s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 00:35
Completed Parallel DNS resolution of 1 host. at 00:35, 0.07s elapsed
Initiating SYN Stealth Scan at 00:35
Scanning 127.84.75.98 [1000 ports]
Discovered open port 135/tcp on 127.84.75.98
Discovered open port 445/tcp on 127.84.75.98
Discovered open port 912/tcp on 127.84.75.98
Discovered open port 902/tcp on 127.84.75.98
Completed SYN Stealth Scan at 00:35, 0.15s elapsed (1000 total ports)
Initiating Service scan at 00:35
Scanning 4 services on 127.84.75.98
Completed Service scan at 00:35, 6.06s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 127.84.75.98
NSE: Script scanning 127.84.75.98.
Initiating NSE at 00:35
Completed NSE at 00:36, 14.34s elapsed
Initiating NSE at 00:36
Completed NSE at 00:36, 0.28s elapsed
Initiating NSE at 00:36
Completed NSE at 00:36, 0.00s elapsed
Nmap scan report for 127.84.75.98
Host is up (0.00054s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
Filter Hosts
Type here to search
30°C
12:36 AM
5/22/2023


Zenmap
Scan Tools Profile Help
Target: 192.168.76.98
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.76.98
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.2.144
10.10.160.175
10.10.232.201
127.84.75.98
nmap -T4 -A -v 192.168.76.98
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 00:39 India Standard Time
NSOCK ERROR [0.5170s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating Ping Scan at 00:39
Scanning 192.168.76.98 [4 ports]
Completed Ping Scan at 00:39, 0.37s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:39
Completed Parallel DNS resolution of 1 host. at 00:39, 0.24s elapsed
Initiating SYN Stealth Scan at 00:39
Scanning 192.168.76.98 [1000 ports]
Discovered open port 21/tcp on 192.168.76.98
Discovered open port 554/tcp on 192.168.76.98
Increasing send delay for 192.168.76.98 from 0 to 5 due to 45 out of 111 dropped probes since last increase.
Increasing send delay for 192.168.76.98 from 5 to 10 due to 259 out of 646 dropped probes since last increase.
SYN Stealth Scan Timing: About 46.27% done; ETC: 00:41 (0:00:36 remaining)
Filter Hosts
Type here to search
30°C
12:41 AM
5/22/2023


Zenmap
Scan Tools Profile Help
Target: 190.168.95.76
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 190.168.95.76
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.2.144
10.10.180.175
10.10.232.201
127.84.75.98
nmap -T4 -A -v 190.168.95.76
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 00:42 India Standard Time
NSOCK ERROR [0.5200s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:42
Completed NSE at 00:42, 0.00s elapsed
Initiating NSE at 00:42
Completed NSE at 00:42, 0.00s elapsed
Initiating NSE at 00:42
Completed NSE at 00:42, 0.00s elapsed
Initiating Ping Scan at 00:42
Scanning 190.168.95.76 [4 ports]
Completed Ping Scan at 00:42, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:42
Completed Parallel DNS resolution of 1 host. at 00:42, 0.06s elapsed
Initiating SYN Stealth Scan at 00:42
Scanning 190.168.95.76 [1000 ports]
Discovered open port 21/tcp on 190.168.95.76
Discovered open port 554/tcp on 190.168.95.76
Completed SYN Stealth Scan at 00:42, 8.25s elapsed (1000 total ports)
Initiating Service scan at 00:42
Filter Hosts
Type here to search
30°C
12:42 AM
5/22/2023


Zenmap
Scan Tools Profile Help
Target: 127.56.79.80
Profile: Intense scan
Scan
Command: nmap -T4 -A -v 127.56.79.80
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.2.144
10.10.180.175
10.10.232.201
127.56.79.80
127.60.79.56
127.84.75.98
nmap -T4 -A -v 127.56.79.80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 00:44 India Standard Time
NSOCK ERROR [0.5100s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 00:44
Completed Parallel DNS resolution of 1 host. at 00:44, 0.20s elapsed
Initiating SYN Stealth Scan at 00:44
Scanning 127.56.79.80 [1000 ports]
Discovered open port 139/tcp on 127.56.79.80
Discovered open port 445/tcp on 127.56.79.80
Discovered open port 912/tcp on 127.56.79.80
Discovered open port 902/tcp on 127.56.79.80
Completed SYN Stealth Scan at 00:44, 0.11s elapsed (1000 total ports)
Initiating Service scan at 00:44
Scanning 4 services on 127.56.79.80
Completed Service scan at 00:44, 6.00s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 127.56.79.80
NSE: Script scanning 127.56.79.80.
Initiating NSE at 00:44
Completed NSE at 00:44, 14.27s elapsed
Initiating NSE at 00:44
Completed NSE at 00:44, 0.28s elapsed
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
Nmap scan report for 127.56.79.80
Host is up (0.00004s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
Filter Hosts
Type here to search
30°C
12:45 AM
5/22/2023


Zenmap
Scan Tools Profile Help
Target: 198.88.99.77
Profile: Intense scan
Scan
Command: nmap -T4 -A -v 198.88.99.77
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS ▾ Host
nmap -T4 -A -v 198.88.99.77
10.10.2.144
10.10.180.175
10.10.232.209
127.56.79.80
127.60.78.56
127.84.75.98
198.168.76.98
198.168.95.76
198.88.99.77
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-22 00:51 India Standard Time
NSOCK ERROR [0.5400s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
Initiating Ping Scan at 00:51
Scanning 198.88.99.77 [4 ports]
Completed Ping Scan at 00:51, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:51
Completed Parallel DNS resolution of 1 host. at 00:51, 2.00s elapsed
Initiating SYN Stealth Scan at 00:51
Scanning 198.88.99.77 [1000 ports]
Discovered open port 21/tcp on 198.88.99.77
Discovered open port 554/tcp on 198.88.99.77
Increasing send delay for 198.88.99.77 from 0 to 5 due to 41 out of 101 dropped probes since last increase.
Increasing send delay for 198.88.99.77 from 5 to 10 due to 321 out of 802 dropped probes since last increase.
SYN Stealth Scan Timing: About 48.97% done; ETC: 00:52 (0:00:32 remaining)
Warning: 198.88.99.77 giving up on port because retransmission cap hit (6).
Completed SYN Stealth Scan at 00:53, 144.78s elapsed (1000 total ports)
Initiating Service scan at 00:53
Scanning 2 services on 198.88.99.77
Service scan Timing: About 50.00% done; ETC: 00:58 (0:02:06 remaining)
Completed Service scan at 00:56, 160.53s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 198.88.99.77
Retrying OS detection (try #2) against 198.88.99.77
Initiating Traceroute at 00:56
Completed Traceroute at 00:56, 3.04s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 00:56
Completed Parallel DNS resolution of 3 hosts. at 00:56, 0.01s elapsed
NSE: Script scanning 198.88.99.77.
Initiating NSE at 00:56
Completed NSE at 00:57, 31.06s elapsed
Initiating NSE at 00:57
Filter Hosts
Type here to search
30°C
12:57 AM
22-05-2023


Zenmap
Scan Tools Profile Help
Target: 10.255.77.65
Profile: Intense scan
Scan
Command: nmap -T4 -A -v 10.255.77.65
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS ▾ Host
nmap -T4 -A -v 10.255.77.65
10.10.2.144
10.10.180.175
10.10.232.209
10.255.77.65
127.56.79.80
127.60.78.56
127.84.75.98
198.168.76.98
198.168.95.76
198.88.99.77
Initiating NSE at 01:01
Completed NSE at 01:02, 31.23s elapsed
Initiating NSE at 01:02
Completed NSE at 01:02, 32.57s elapsed
Initiating NSE at 01:02
Completed NSE at 01:02, 0.00s elapsed
Nmap scan report for 10.255.77.65
Host is up (0.10s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp?
554/tcp open rtsp?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 17.389 days (since Tue May 9 15:43:01 2023)
Network Distance: 7 hops
TCP Sequence Prediction: Difficulty=233 (Good luck!)
IP ID Sequence Generation: All zeros
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 4.00 ms 192.168.250.90
2 5.00 ms 192.0.0.1
3 ... 6
7 60.00 ms 10.255.77.65
NSE: Script Post-scanning.
Initiating NSE at 01:02
Completed NSE at 01:02, 0.00s elapsed
Initiating NSE at 01:02
Completed NSE at 01:02, 0.00s elapsed
Initiating NSE at 01:02
Completed NSE at 01:02, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 251.33 seconds
Raw packets sent: 2113 (97.712kB) | Rcvd: 797 (31.664kB)
Filter Hosts
Type here to search
30°C
1:04 AM
22-05-2023

## Internship/Project Daily Diary

**Session: Jan–June 2023**

Name of Students: Khushbu Jain

Enrollment Number: 0901ET191031

Branch and Year: ET, IV Year

Internship/Project Title: Port Scanning

Company Name with Full Address: IIT Indore, Indore, Madhya Pradesh

.....

.....

Stipend Detail: Yes No ✓ Stipend Amount: .....

Industrial Mentor Detail:

Name of Industry Mentor: Neminath Hubbali

Email Address of Industry mentor: Neminath@iiti.ac.in

Students must mention the daily progress details with dates in the given format such as daily work done/ software learn/coding/testing/site or field visit/hardware implementation, etc.

| Month | Date | Daily Progress Details |
|---|---|---|
| Jan. 2023 | 23/01/23- | **Today was the first day of my internship project on port scanning. I had an introductory session where I learned about the importance of network security and the role of port scanning in identifying vulnerabilities. I also familiarized myself with the tools and techniques we will be using throughout the project.** |
| | 31/01/2023 | **I spent the day diving deeper into the concept of port scanning. I studied different types of scans, such as TCP, UDP, SYN, and ACK scans, and their respective purposes. I also learned about the advantages and limitations of each scan type.** |

| | | |
|---|---|---|
| Feb. 2023 | 01/02/23 | Today, I got hands-on experience with Nmap, one of the most popular port scanning tools. I practiced using various Nmap commands to perform scans on test systems and analyze the results. It was exciting to see how easily I could identify open ports and services running on those systems. |
| | 08/02/23 | I continued exploring Nmap and its advanced features. I focused on scanning techniques like stealth scanning and banner grabbing. I learned how to extract valuable information from banners, such as software versions and configurations, which can aid in vulnerability assessment. |
| | 14/02/23 | To solidify my understanding of port scanning, I conducted a series of practical exercises. I scanned a simulated network environment, documented the open ports, and analyzed the associated services. This exercise helped me gain confidence in my scanning abilities. |
| | 20/02/23 | Today marked the beginning of the second month of my internship project. I started by learning about other port scanning tools, such as hping and masscan. I compared their features, command structures, and use cases. |
| | 25/02/23 | I focused on mastering hping, a versatile command-line tool for port scanning and network testing. I practiced crafting custom packets, specifying flags, and using different scan techniques. I found hping to be a powerful tool for crafting specialized scans. |
| March 2023 | 1/03/23 | In today's session, I explored masscan, a high-speed port scanner. I learned how to optimize scan settings for maximum efficiency and how to deal with large-scale network scanning. Masscan's ability to scan thousands of hosts per second amazed me. |
| | 7/03/23 | I had the opportunity to work on a simulated network penetration testing exercise. I applied my knowledge of port scanning tools and techniques to identify vulnerabilities and assess the security of the target network. It was a challenging yet rewarding experience. |
| | 11/03/23 | To broaden my understanding, I researched and studied real-world port scanning case studies. I analyzed notable security incidents where port scanning played a crucial role in detecting vulnerabilities or identifying malicious activities. It was eye-opening to see the impact of port scanning in practical scenarios.<br>As I entered the third month of my internship, I shifted my |

| | | |
|---|---|---|
| | 17/03/23 | focus towards analyzing and interpreting scan results. I learned about common port numbers and associated services, allowing me to quickly identify potential vulnerabilities or misconfigurations based on the scan output. |
| | 21/03/23 | I had a session on the legal and ethical considerations surrounding port scanning. I learned about the importance of obtaining proper authorization, respecting privacy, and complying with relevant laws and regulations. Responsible disclosure practices were emphasized to ensure ethical scanning practices. |
| April 2023 | 1/04/23 | Today, I worked on a collaborative project with my fellow interns. We formed teams and conducted comprehensive scans on a shared network environment. We analyzed the combined results and prepared a report summarizing the vulnerabilities and recommended mitigation strategies. |
| | 9/04/23 | I had the opportunity to attend a guest lecture by a professional penetration tester who shared their experiences and insights. It was inspiring to hear about their real-world engagements and the role that port scanning played in their assessments. |
| | 14/04/23 | To further enhance my skills, I started exploring scripting and automation for port scanning. I learned about scripting languages like Python and how to leverage them to develop custom port scanning scripts. Automation would help streamline repetitive tasks in future projects. |
| | 22/04/23 | As the final month began, I revisited the fundamentals of port scanning to ensure a solid foundation. I reviewed different scan types, tools, and techniques, reinforcing my knowledge gained over the past few months. |
| | 26/04/23 | I conducted a research project on emerging port scanning trends and technologies. I explored topics like stealth scanning, evasion techniques, and the use of machine learning in port scanning detection. It was exciting to learn about the evolving landscape of port scanning. |

| | | |
|---|---|---|
| May 2023 | 1/05/23 | Incollaborationwiththesecurityteam,Iconductedanetwork-wideportscanonourorganization'sinfrastructure.Theresults provided valuable insights into potential security weaknesses and aided in strengthening our network's defenses. |
| | 10/05/23 | Ipreparedapresentationsummarizingmyinternshipproject on port scanning. I included key learnings, experiences, and notable findings. I was eager to share my knowledge and the impact port scanning can have on network security. |
| | 16/05/23 | Today marked the end of my internship project on port scanning. I presented my findings to the team and received valuablefeedback.Iexpressedmygratitudefortheopportunity to work on such an engaging and impactful project./ |

**KhushbuJain**

**NameandSignatureofStudents**

**Laxmi Shrivastava,**
**Associate Professor**

**Name&SignatureofInstituteMentor**

# MPR:

FORMAT

MONTHLY PROGRESS REPORT (MPR) FROM INDUSTRY MENTOR

| Name of student | Khushbu Jain | | Department | Department of Computer Science and Engineering | |
|---|---|---|---|---|---|
| Industry/Organization | IIT Indore | | Date/Duration | | |
| Criterion | Poor | Average | Good | Very Good | Excellent |
| Punctuality/Timely completion of assigned work | | | | ✓ | |
| Learning capacity/Knowledge up gradation | | | | ✓ | |
| Performance/Quality of work | | | | ✓ | |
| Behaviour/Discipline/Team work | | | | ✓ | |
| Sincerity/Hard work | | | ✓ | | |
| Comment on nature of work done/Area/Topic | Khushbu is working on the assignments given and progress is satisfactory | | | | |
| OVERALL GRADE (Any one) | POOR/AVERAGE/GOOD/VERY GOOD/EXCELLENT | | | | |
| Name of Industry Mentor | Neminath Hubbali | | | | |
| Signature of Industry Mentor | | | | | |

| Receiving Date | 25-01-23 | Name of Faculty Mentor | Dr. Laxmi Srivastava | Sign | |
|---|---|---|---|---|---|

**FORMAT**

**MONTHLY PROGRESS REPORT (MPR) FROM INDUSTRY MENTOR**

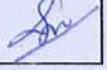
| Name of student | Khushbu Jain | | | Department of Computer Science and Engineering | |
|---|---|---|---|---|---|
| Industry/Organization | IIT Indore | | | Date/Duration - 15-02-2023 to 15-03-2023 | |
| Criterion | Poor | Average | Good | V.Good | Excellent |
| Punctuality/Timely completion of assigned work | | | | ✓ | |
| Learning capacity/Knowledge up gradation | | | | ✓ | |
| Performance/Quality of work | | | | ✓ | |
| Behaviour/Discipline/Team work | | | | ✓ | |
| Sincerity/Hard work | | | ✓ | | |
| Comment on nature of work done/Area/Topic | Khushbu is working on the assignments given and progress is satisfactory | | | | |
| OVERALL GRADE (Any one) | POOR/AVERAGE/GOOD/VERY GOOD/EXCELLENT | | | | |
| Name of Industry Mentor | Neminath Hubballi | | | | |
| Signature of Industry Mentor | | | | | |

| Receiving Date | 22/03/23 | Name of Faculty Mentor | Dr. Laxmi Shivaratan | Sign | |
|---|---|---|---|---|---|

**FORMAT**

**MONTHLY PROGRESS REPORT (MPR) FROM INDUSTRY MENTOR**

| Name of student | Khushbu Jain | | | Department of Computer Science and Engineering | |
|---|---|---|---|---|---|
| Industry/Organization | IIT Indore | | | Date/Duration - 25-03-2023 to 15-04-2023 | |
| Criterion | **Poor** | **Average** | **Good** | **V.Good** | **Excellent** |
| Punctuality/Timely completion of assigned work | | | | ✓ | |
| Learning capacity/Knowledge up gradation | | | | ✓ | |
| Performance/Quality of work | | | | ✓ | |
| Behaviour/Discipline/Team work | | | | ✓ | |
| Sincerity/Hard work | | | ✓ | | |
| Comment on nature of work done/Area/Topic | Khushbu is working on the assignments given and progress is satisfactory | | | | |
| OVERALL GRADE (Any one) | POOR/AVERAGE/GOOD/VERY GOOD/EXCELLENT | | | | |
| Name of Industry Mentor | Neminath Hubballi | | | | |
| Signature of Industry Mentor |  | | | | |

| Receiving Date | 23-04-23 | Name of Faculty Mentor | Dr. Laxmi Shrivastava | Sign |  |
|---|---|---|---|---|---|

## FORMAT

## MONTHLY PROGRESS REPORT (MPR) FROM INDUSTRY MENTOR

| Name of student | Khushbu Jain | | Department | Department of computer Science Engineering | |
|---|---|---|---|---|---|
| Industry/Organization | ET Infotech | | Date/Duration | 23/04/23-21/05/23 | |
| Criterion | Poor | Average | Good | Very Good | Excellent |
| Punctuality/Timely completion of assigned work | | | | | ✓ |
| Learning capacity/Knowledge up gradation | | | | ✓ | |
| Performance/Quality of work | | | | ✓ | |
| Behaviour/Discipline/Team work | | | | | ✓ |
| Sincerity/Hard work | | | | ✓ | |
| Comment on nature of work done/Area/Topic | Khushbu has completed her internship excellently ✓ | | | | |
| OVERALL GRADE (Any one) | POOR/AVERAGE/GOOD/VERY GOOD/EXCELLENT | | | | |
| Name of Industry Mentor | Prof. Narinath Hubballi | | | | |
| Signature of Industry Mentor | N | | | | |

| Receiving Date | 22/05/23 | Name of Faculty Mentor | Dr. Laxmi Shivaratra | Sign | |
|---|---|---|---|---|---|

turnitin

Similarity Report ID: oid:28506:36228569

PAPER NAME
internship (2).pdf

AUTHOR
Khushboo

WORD COUNT
3150 Words

CHARACTER COUNT
17968 Characters

PAGE COUNT
25 Pages

FILE SIZE
1.9MB

SUBMISSION DATE
May 26, 2023 11:46 AM GMT+5:30

REPORT DATE
May 26, 2023 11:46 AM GMT+5:30

## 17% Overall Similarity

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

- 5% Internet database
- Crossref database
- 15% Submitted Works database
- 3% Publications database
- Crossref Posted Content database

## Excluded from Similarity Report

- Bibliographic material
- Cited material
- Quoted material
- Small Matches (Less then 8 words)

turnitin

**Similarity Report ID:** oid:28506:36228569

## 17% Overall Similarity

Top sources found in the following databases:

- 5% Internet database
- Crossref database
- 15% Submitted Works database
- 3% Publications database
- Crossref Posted Content database

TOP SOURCES

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

| | | |
|---|---|---|
| 1 | **University of Technology, Sydney on 2023-05-19**<br>Submitted works | 5% |
| 2 | **Madhav Institute of Technology & Science on 2019-05-02**<br>Submitted works | 2% |
| 3 | **codemint.net**<br>Internet | 1% |
| 4 | **HCUC on 2023-05-24**<br>Submitted works | <1% |
| 5 | **Madhav Institute of Technology & Science on 2019-04-15**<br>Submitted works | <1% |
| 6 | **Angela Orebaugh, Becky Pinkard. "Nmap Scanning in the Real World", E...**<br>Crossref | <1% |
| 7 | **Staffordshire University on 2023-03-13**<br>Submitted works | <1% |
| 8 | **termpaperwarehouse.com**<br>Internet | <1% |

Sources overview

| | | |
|---|---|---|
| 9 | coursehero.com<br>Internet | <1% |
| 10 | University of Cincinnati on 2023-04-20<br>Submitted works | <1% |
| 11 | Victorian Institute of Technology on 2023-05-13<br>Submitted works | <1% |
| 12 | Rochester Institute of Technology on 2015-04-13<br>Submitted works | <1% |
| 13 | Staffordshire University on 2018-04-23<br>Submitted works | <1% |
| 14 | bkd00r.wordpress.com<br>Internet | <1% |
| 15 | Madhav Institute of Technology & Science on 2019-04-22<br>Submitted works | <1% |
| 16 | University of Maryland, University College on 2012-03-18<br>Submitted works | <1% |
| 17 | Liverpool John Moores University on 2023-04-12<br>Submitted works | <1% |
| 18 | Rochester Institute of Technology on 2014-10-17<br>Submitted works | <1% |
| 19 | University of Westminster on 2023-05-16<br>Submitted works | <1% |
| 20 | Zhai, Jiqiang, and Keqi Wang. "Design and implementation of dynamic ...<br>Crossref | <1% |

| | | |
|---|---|---|
| 21 | **pdfcoffee.com**<br>Internet | <1% |
| 22 | **South Bank University on 2023-03-30**<br>Submitted works | <1% |