An Internship Report

on

NMAP PORT SCANS-2

Submitted for partial fulfillment of the requirements for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

BY

Mr. JAYANTH JATAVATH (2451-20-733-137)

Under the guidance of

Mrs. BANTU SARITHA

Associate Professor

Department of CSE

Department of Computer Science and Engineering
Maturi Venkata Subba Rao Engineering College
(An Autonomous Institution)
(Affiliated to Osmania University & Recognized by AICTE)
Nadergul(V), Balapur(M), RR Dist. Hyderabad – 501 510

2022-23

Maturi Venkata Subba Rao Engineering College
(An Autonomous Institution)

(Affiliated to Osmania University, Hyderabad)
Nadergul(V), Hyderabad-501510

Certificate

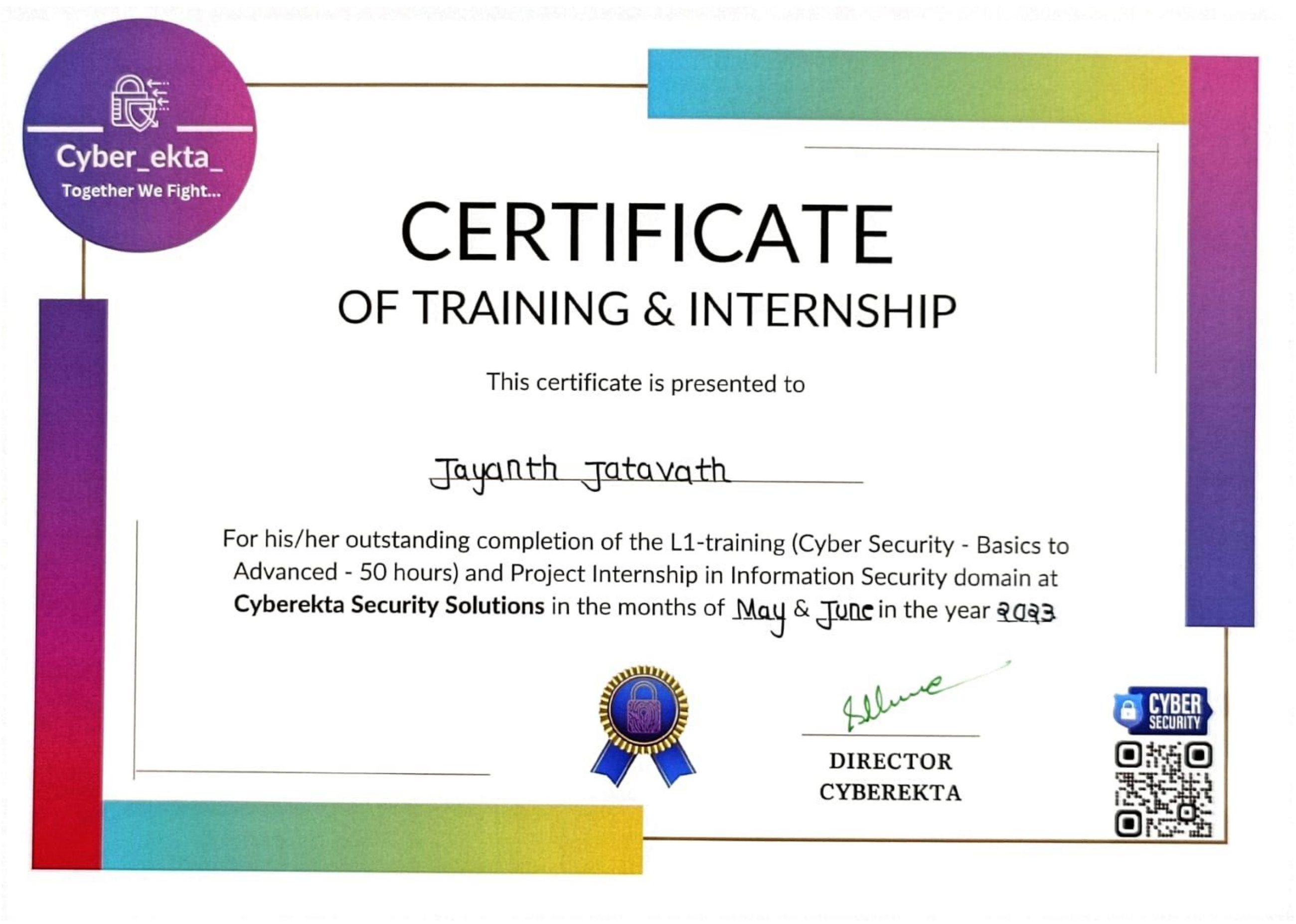
This is to certify that the mini-project work entitled "**NMAP PORT SCANS-2"** is a bonafide work carried out by **Mr. JAYANTH JATAVATH (2451-20-733-137)** in partial fulfillment of the requirements for the award of degree of **BACHELOR OF ENGINEERING IN COMPUTER SCIENCE AND ENGINEERING** from Maturi Venkata Subba Rao Engineering College, affiliated to OSMANIA UNIVERSITY, Hyderabad, under our guidance and supervision.

The results embodied in this report have not been submitted to any other university or institute for the award of any degree or diploma

Internal Guide **Project Co-Ordinator**

Mrs. Bantu Saritha
Associate Professor
Department of CSE,
MVSREC.

External Examiner



Cyber_ekta_

Together We Fight...

CERTIFICATE

OF TRAINING & INTERNSHIP

This certificate is presented to

Jayanth Jatavath

For his/her outstanding completion of the L1-training (Cyber Security - Basics to Advanced - 50 hours) and Project Internship in Information Security domain at **Cyberekta Security Solutions** in the months of May & June in the year 2023

DIRECTOR
CYBEREKTA

CYBER SECURITY

DECLARATION

This is to certify that the work reported in the present mini-project entitled “**NMAP PORT SCANS-2”** is a record of bonafide work done by us in the Departmentof Computer Science and Engineering, Maturi Venkata Subba Rao Engineering College, Osmania University. The reports are based on the mini-project work done entirely by us and not copied from any other source.

The results embodied in this mini-project report have not been submitted to any other University or Institute for the award of any degree or diploma to the best of our/ my knowledge and belief.

JAYANTH JATAVATH	**2451-20-733-137**	**245120733137@mvsrec.edu.in**

ACKNOWLEDGEMENTS

We are also thankful to our principal **Dr. G. Kanakadurga** and **Mr. J Prasanna Kumar**, Professor and Head, Department of Computer Science and Engineering, Maturi Venkata Subba Rao Engineering College, Hyderabad for providing excellent infrastructure for completing this mini-project successfully as a part of our B.E. Degree (CSE). We would like to thank our mini-project coordinator **Mrs. N Sabitha** for their constant monitoring, guidance, and support.

We convey our heartfelt thanks to the lab staff for allowing me to use the required equipment whenever needed.

Finally, we would like to take this opportunity to thank my family for their support through the work. We sincerely acknowledge and thank all those who gave directly or indirectly their support in the completion of this work.

JAYANTH JATAVATH (2451-20-733-137)

ABSTRACT

Network port scanning is a crucial technique for identifying open ports and services on a network, enabling security professionals and network administrators to evaluate network security and uncover potential vulnerabilities. This project delves into the intricacies of TCP flags, exploring the implications of sending TCP packets with specific flags set outside of an established TCP connection. It delves into various types of port scans, including Null Scan, FIN Scan, Xmas Scan, Maimon Scan, ACK Scan, Window Scan, and Custom Scan, analyzing their mechanisms and applications. The project sheds light on the significance of port scanning in assessing network security and highlights the importance of responsible and ethical usage of this technique.

TABLE OF CONTENTS

CONTENTS

LIST OF FIGURES

CHAPTER-1

INTRODUCTION

1.1 PROBLEM STATEMENT

Security researchers and network administrators face the challenge of effectively identifying open ports and services on a network to evaluate network security and uncover potential vulnerabilities. Conventional TCP SYN scans, while widely used, may not always provide comprehensive information and can potentially trigger intrusion detection systems. The objective is to investigate alternative port scanning techniques that utilize TCP flags to elicit responses from target hosts, enabling a more detailed and stealthy exploration of network vulnerabilities. Specifically, the project aims to understand the mechanisms and applications of Null Scan, FIN Scan, Xmas Scan, Maimon Scan, ACK Scan, Window Scan, and Custom Scan, evaluating their effectiveness in identifying open ports and services while minimizing detection by network security devices.

1.2 SCOPE OF THE PROJECT

The project encompasses a comprehensive evaluation of alternative port scanning techniques that utilize TCP flags to elicit responses from target hosts. The project will delve into the following specific objectives:

- **Mechanism and Application of Port Scanning Techniques:** Investigate the theoretical underpinnings and practical implementation of various port scanning techniques, including Null Scan, FIN Scan, Xmas Scan, Maimon Scan, ACK Scan, Window Scan, and Custom Scan.

- **Effectiveness of Port Identification:** Conduct experiments and simulations to assess the ability of each port scanning technique to accurately identify open ports and services on target hosts.

- **Detectability by Network Security Devices:** Evaluate the likelihood of each port scanning technique being detected by firewalls, intrusion detection systems, and other network security devices.

- **Recommendations for Network Security Assessments:** Based on the findings of the evaluation, the project will provide recommendations for the appropriate use of these port scanning techniques in network security assessments.

- **Impact on TCP Flag Status:** Analyze the status of TCP flags for each scanned port, determining which flags are set to 1 and which are set to 0.

- **Quantification of Open and Filtered Ports:** Quantify the number of ports that appear as open or filtered as a result of the port scans.

- **Flag Counts for Scanned Ports:** Count the number of TCP flags that are set for each scanned port, providing additional information about the state of the ports and identifying potential vulnerabilities.

- **Analysis of Port Numbers After Scans:** Analyze the range of port numbers that were scanned and the specific port numbers that were identified as open or filtered.

- **Identification of Services Behind Newly Discovered Ports:** For newly discovered open ports, the project will attempt to identify the services running behind those ports using techniques such as banner grabbing, service detection tools, and network traffic analysis.

The project will primarily focus on the technical aspects of these port scanning techniques and their effectiveness in identifying open ports and services. It will not explicitly explore the ethical considerations or legal implications of unauthorized port scanning. However, the project will acknowledge the importance of responsible and ethical use of port scanning techniques.

CHAPTER-2

TOOLS AND TECHNOLOGIES

2.1 LITERATURE SURVEY

- **Port Scanning Techniques: A Comprehensive Review** by A.A.A. El-Abd, A.O. Abu-Salih, and M.A. Ramadan (2022) This paper provides a comprehensive overview of port scanning techniques, including their mechanisms, applications, and limitations. It also discusses the ethical considerations of port scanning.

- **A Survey of Port Scanning Detection Techniques** by S.Z. Abdallah, M.A. Ramadan, M.A. Moustafa, and A.O. Abu-Salih (2021) This paper surveys port scanning detection techniques, including their principles, methods, and challenges. It also discusses the effectiveness of different detection techniques against various port scanning techniques.

- **A Review of TCP Flags and Their Implications for Network Security** by J.A. Halderman, A.A. Shogan, and R.D. Buskens (2019) This paper reviews the different TCP flags and their implications for network security. It discusses how TCP flags can be used to attack and defend networks.

- **Nmap: Network Scanner** by G. Fyodor (2003) This book is a comprehensive guide to Nmap, a popular port scanner. It covers the different Nmap options and commands, as well as how to use Nmap for various tasks, such as port scanning, network discovery, and vulnerability scanning.

- **Network Security: A Beginner's Guide** by J. Vacca (2014) This book provides an introduction to network security, including port scanning. It covers the different types of port scans, as well as how to use port scanners to identify and exploit vulnerabilities.

2.2 HARDWARE REQUIREMENTS

- **Computer** (Quad-core processor, 8GB RAM)
- **Network:** Need a network with a target host to scan (home network/college network)

2.3 SOFTWARE REQUIREMENTS

- **Operating System:** Kali Linux, Windows 11

Figure 2.1 Kali Linux

- **Nmap:** Nmap is an open-source utility for network discovery. Network Mapper is a security auditing and network scanning independent tool developed by **Gordon Lyon**. It is used by network administrators to detect the devices currently running on the system and the port number by which the devices are connected.

Figure 2.2 Nmap Logo

- **Virtual Machine:** Oracle VM Virtual Box

Figure 2.3 Oracle VM Virtual Box

CHAPTER-3

LAB ACTIVITY

3.1 PORT SCANS

1. **Null Scan:** It does not set any flags; all six flag bits are set to zero.

- When a TCP packet arrives at an open port with no flags specified, no response is generated.

- A lack of response in a null scan suggests that either the port is open or a firewall is blocking the packet, according to Nmap.

Option to use: -sN

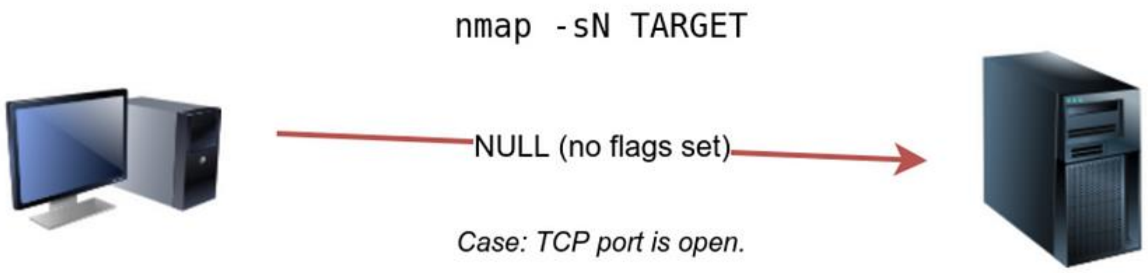


Figure 3.1 Null Scan - TCP port is open

If the port is closed, we expect the target server to react with a RST response. As a result, we may use the lack of RST response to determine which ports are open or filtered.

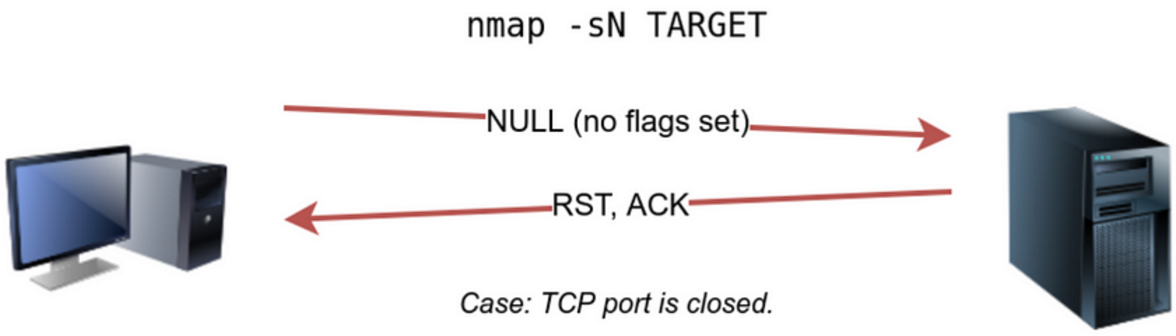
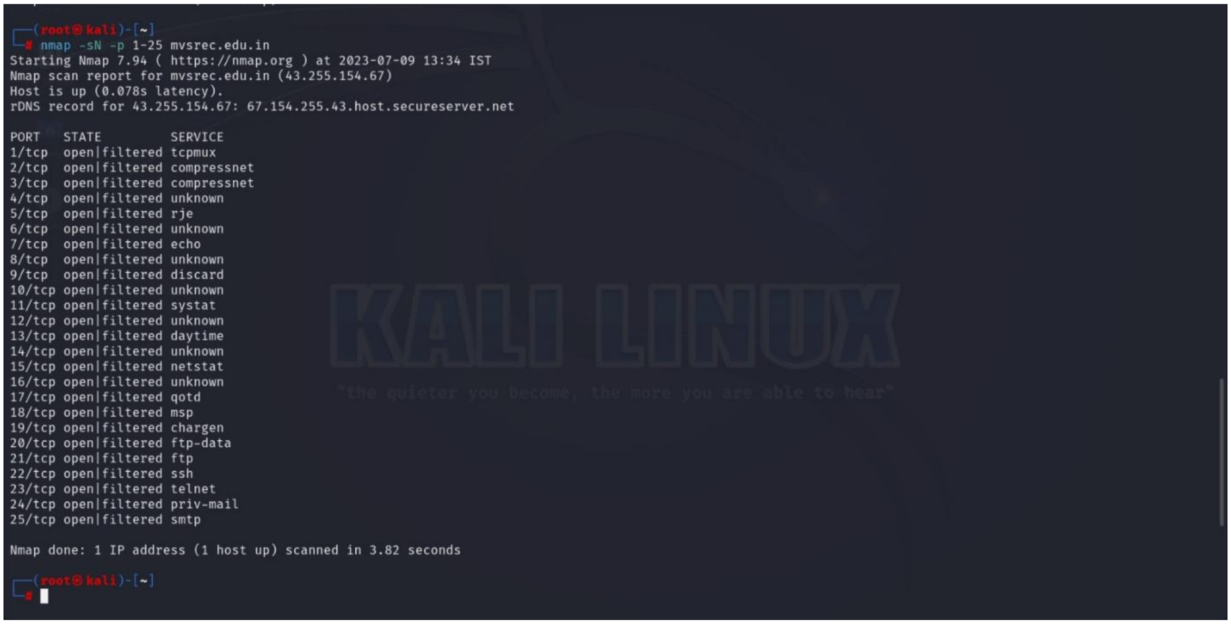


Figure 3.2 Null Scan - TCP port is closed

An example of a null scan against college web server/website is shown below. We performed null scan on the college web server for ports 1-25.

The null scan depends on the lack of response to inferring that the port is not closed, it cannot guarantee that these ports are open**;** the ports may be not responding because of a firewall rule.



```
┌──(root㉿kali)-[~]
└─# nmap -sN -p 1-25 mvsrec.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-09 13:34 IST
Nmap scan report for mvsrec.edu.in (43.255.154.67)
Host is up (0.078s latency).
rDNS record for 43.255.154.67: 67.154.255.43.host.secureserver.net

PORT   STATE         SERVICE
1/tcp  open|filtered tcpmux
2/tcp  open|filtered compressnet
3/tcp  open|filtered compressnet
4/tcp  open|filtered unknown
5/tcp  open|filtered rje
6/tcp  open|filtered unknown
7/tcp  open|filtered echo
8/tcp  open|filtered unknown
9/tcp  open|filtered discard
10/tcp open|filtered unknown
11/tcp open|filtered systat
12/tcp open|filtered unknown
13/tcp open|filtered daytime
14/tcp open|filtered unknown
15/tcp open|filtered netstat
16/tcp open|filtered unknown
17/tcp open|filtered qotd
18/tcp open|filtered msp
19/tcp open|filtered chargen
20/tcp open|filtered ftp-data
21/tcp open|filtered ftp
22/tcp open|filtered ssh
23/tcp open|filtered telnet
24/tcp open|filtered priv-mail
25/tcp open|filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 3.82 seconds

┌──(root㉿kali)-[~]
└─#
```

Figure 3.3 Null Scan performed on web server

2. **FIN Scan:** It transmits a **TCP packet with the flag** "**FIN**." However, **no answer will be sent back if the TCP port is open**, therefore Nmap cannot tell if the port is open or if a firewall is blocking TCP port communication.

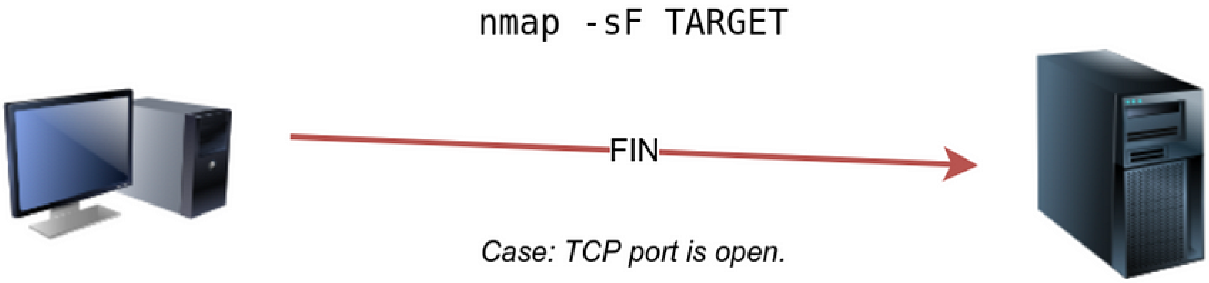


Figure 3.4 FIN Scan - TCP port is open

Just like with “NULL Scan” the target system will **react with a “RST” if the port is closed**, so that we can determine which port is closed and then utilize that information to determine which ports are open or filtered. It’s beneficial to understand that some firewalls will ‘quietly’ drop traffic without sending a RST.

Option to use: -sF

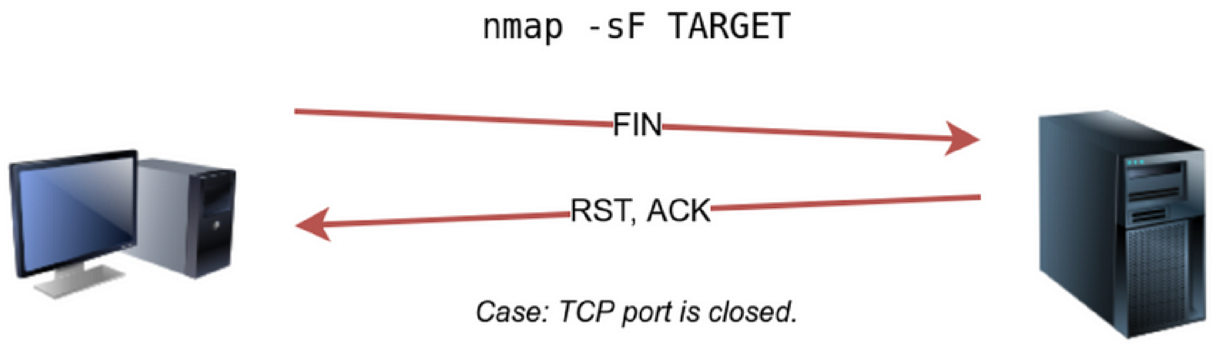
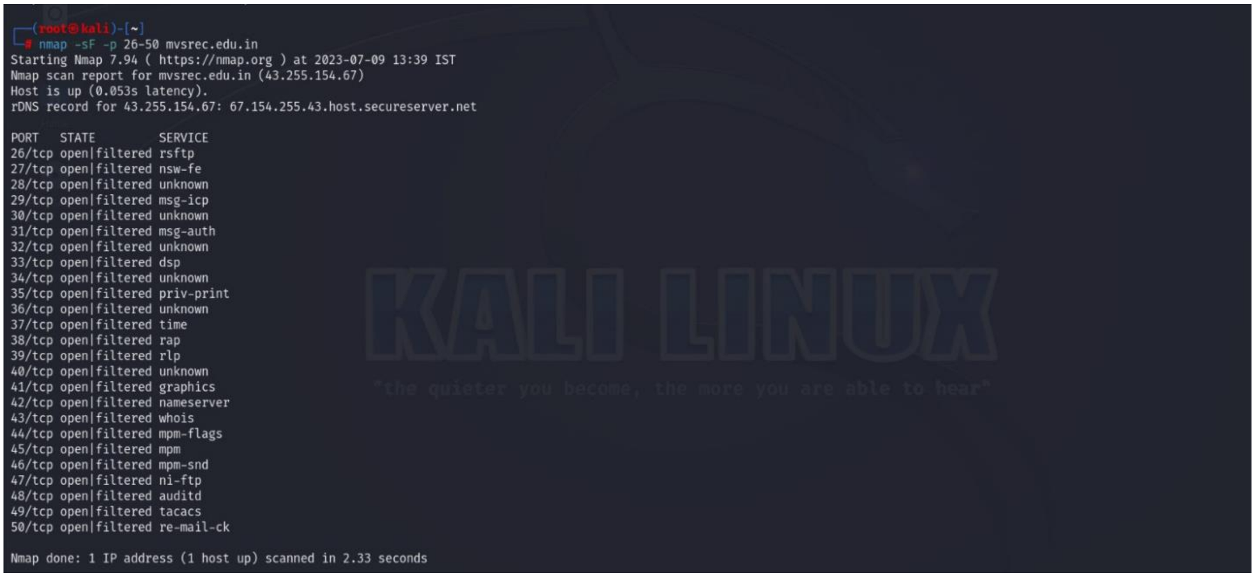


Figure 3.5 FIN Scan - TCP port is closed

We performed FIN scan on the college web server for ports 26-50.



```
┌──(root㉿kali)-[~]
└─# nmap -sF -p 26-50 mvsrec.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-09 13:39 IST
Nmap scan report for mvsrec.edu.in (43.255.154.67)
Host is up (0.053s latency).
rDNS record for 43.255.154.67: 67.154.255.43.host.secureserver.net

PORT   STATE         SERVICE
26/tcp open|filtered rsftp
27/tcp open|filtered nsw-fe
28/tcp open|filtered unknown
29/tcp open|filtered msg-icp
30/tcp open|filtered unknown
31/tcp open|filtered msg-auth
32/tcp open|filtered unknown
33/tcp open|filtered dsp
34/tcp open|filtered unknown
35/tcp open|filtered priv-print
36/tcp open|filtered unknown
37/tcp open|filtered time
38/tcp open|filtered rap
39/tcp open|filtered rlp
40/tcp open|filtered unknown
41/tcp open|filtered graphics
42/tcp open|filtered nameserver
43/tcp open|filtered whois
44/tcp open|filtered mpm-flags
45/tcp open|filtered mpm
46/tcp open|filtered mpm-snd
47/tcp open|filtered ni-ftp
48/tcp open|filtered auditd
49/tcp open|filtered tacacs
50/tcp open|filtered re-mail-ck

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
```

Figure 3.6 FIN Scan performed on web server

3. **Xmas Scan:** This scan appears to be named after Christmas tree lights. However, the primary goal of this scan is to **simultaneously activate the FIN, PSH, and URG flags**.

- **If a RST packet is received**, comparable to a “NULL” or “FIN” scan, **it indicates that the port is closed**; otherwise, it will be reported as “open|filtered.”

  Option to use: -sX

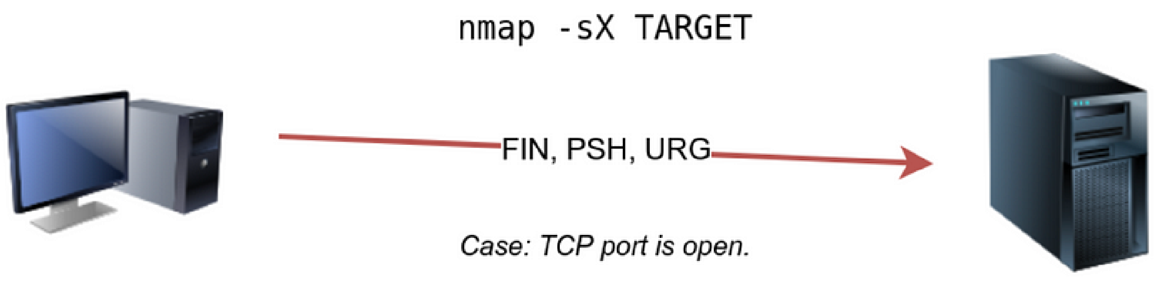


Figure 3.7 Xmas Scan - TCP port is open

TCP packets with specific flags set (FIN, PSH, and URG) are sent to target ports. The unusual combination of flags is used to probe the target system's response. If a port is open, the target may respond in a particular way, while closed ports may exhibit different behavior.

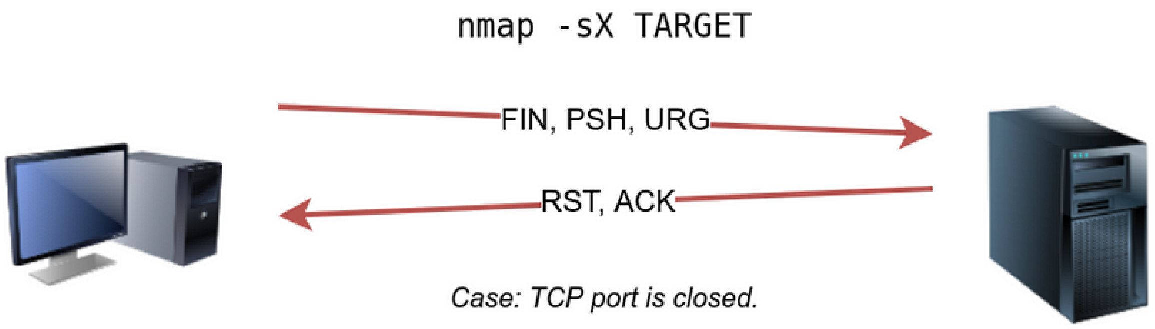
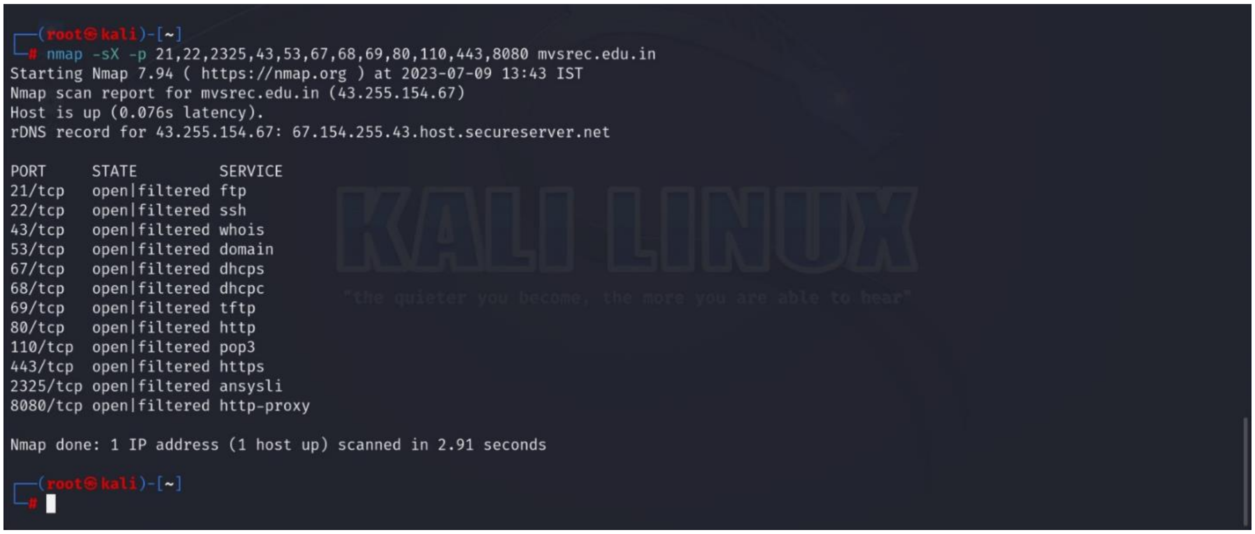


Figure 3.8 Xmas Scan - TCP port is closed

Xmas scan is often used as a stealthy scanning method**.**

We have performed the Xmas scan for selective port numbers. The obtained results are very comparable to those of the “NULL” and “FIN” scans.



```
┌──(root㉿kali)-[~]
└─# nmap -sX -p 21,22,2325,43,53,67,68,69,80,110,443,8080 mvsrec.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-09 13:43 IST
Nmap scan report for mvsrec.edu.in (43.255.154.67)
Host is up (0.076s latency).
rDNS record for 43.255.154.67: 67.154.255.43.host.secureserver.net

PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
43/tcp   open|filtered whois
53/tcp   open|filtered domain
67/tcp   open|filtered dhcps
68/tcp   open|filtered dhcpc
69/tcp   open|filtered tftp
80/tcp   open|filtered http
110/tcp  open|filtered pop3
443/tcp  open|filtered https
2325/tcp open|filtered ansysli
8080/tcp open|filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.91 seconds

┌──(root㉿kali)-[~]
└─# █
```

Figure 3.9 Xmas Scan performed on web server

When scanning a target **behind a stateless (non-stateful) firewall**, these three scan modes can be very efficient.

- To **identify a connection** attempt, a stateless firewall will examine the incoming packet for the SYN flag.
- Using a **flag combination that does not match the SYN packet allows you to fool the firewall** and **get access to the system behind it**.
- A **stateful firewall**, on the other hand, will **effectively block all such designed packets**, rendering this type of scan ineffective.

4. **Maimon Scan:** When the “FIN” and “ACK” bits are set, the target should respond with an RST packet. However, many BSD-derived systems delete the packet if it is an open port, exposing the open ports, although this scan will not function on most targets encountered owing to modern networks.

   Option to use: -sM

   Regardless of whether the TCP port is open, **most target machines react with an RST response**.

   The diagram below illustrates the **expected behavior for both open and closed TCP ports**.

We have performed the Maimon scan for selective port numbers.

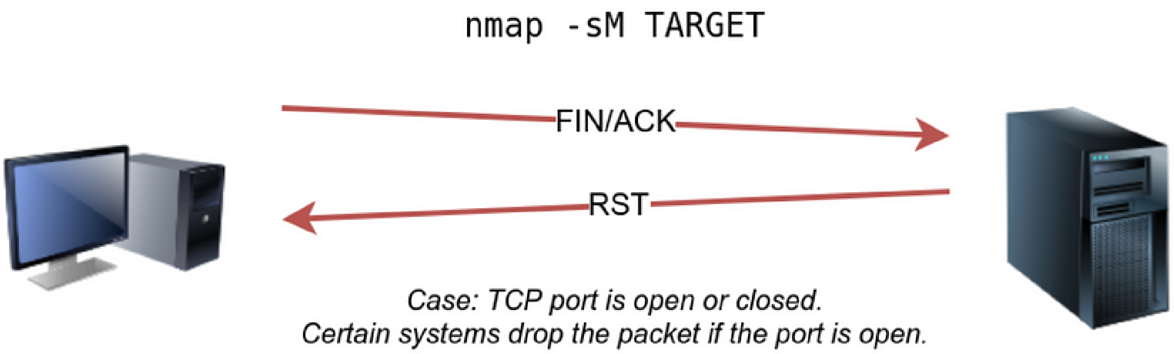
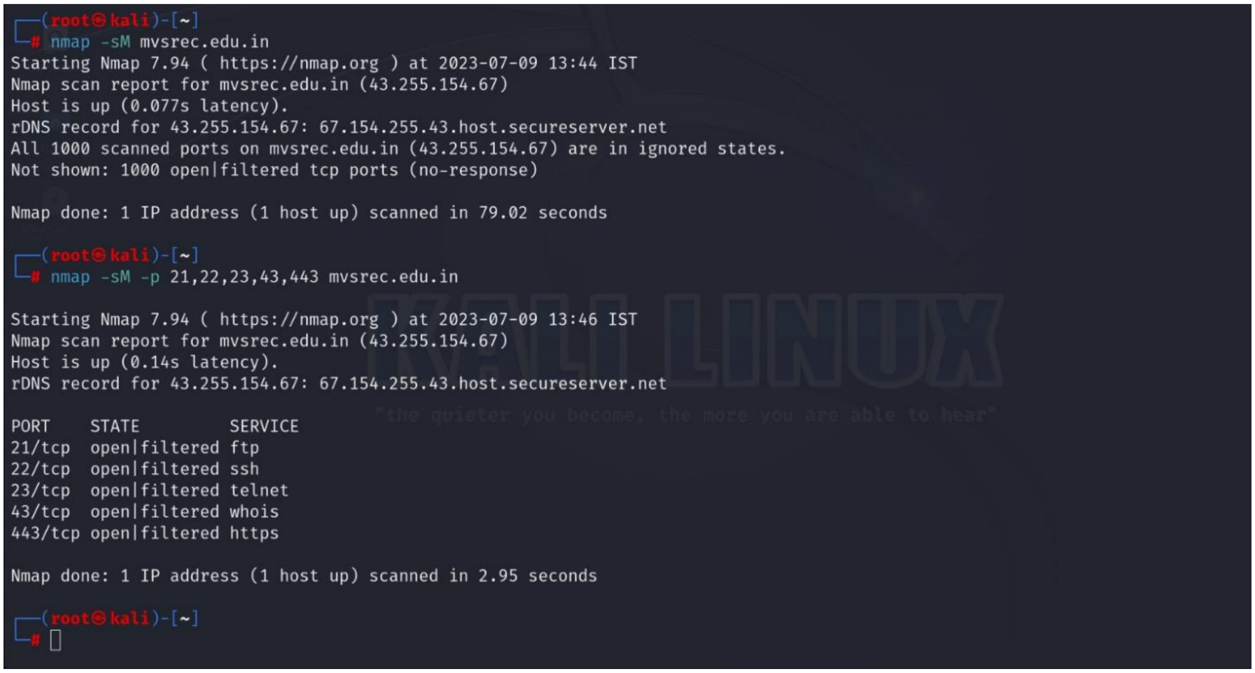

nmap -sM TARGET
FIN/ACK
RST
Case: TCP port is open or closed.
Certain systems drop the packet if the port is open.

Figure 3.10 Maimon Scan - TCP port is open or closed



```
┌──(root㉿kali)-[~]
└─# nmap -sM mvsrec.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-09 13:44 IST
Nmap scan report for mvsrec.edu.in (43.255.154.67)
Host is up (0.077s latency).
rDNS record for 43.255.154.67: 67.154.255.43.host.secureserver.net
All 1000 scanned ports on mvsrec.edu.in (43.255.154.67) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 79.02 seconds

┌──(root㉿kali)-[~]
└─# nmap -sM -p 21,22,23,43,443 mvsrec.edu.in

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-09 13:46 IST
Nmap scan report for mvsrec.edu.in (43.255.154.67)
Host is up (0.14s latency).
rDNS record for 43.255.154.67: 67.154.255.43.host.secureserver.net

PORT    STATE         SERVICE
21/tcp  open|filtered ftp
22/tcp  open|filtered ssh
23/tcp  open|filtered telnet
43/tcp  open|filtered whois
443/tcp open|filtered https

Nmap done: 1 IP address (1 host up) scanned in 2.95 seconds

┌──(root㉿kali)-[~]
└─# 
```

Figure 3.11 Maimon Scan performed on web server

5. **ACK Scan:** An ACK scan is a TCP port scanning technique where TCP packets with only the ACK (Acknowledgment) flag set are sent to target ports. It aims to determine the state of ports based on the response received. In an ACK scan, different responses from the target system can indicate whether the port is filtered, unfiltered, or open.

An **ACK scan will transmit a TCP packet with the ACK flag** set, and the **target will respond to the ACK with RST regardless of the port's state.**

A TCP packet with the ACK flag set **should only be sent in response to a received TCP packet to acknowledge the receipt of certain data**. As a result, in a simple arrangement, **this scan will NOT inform us whether the target port is open.**

Option to use: -sA

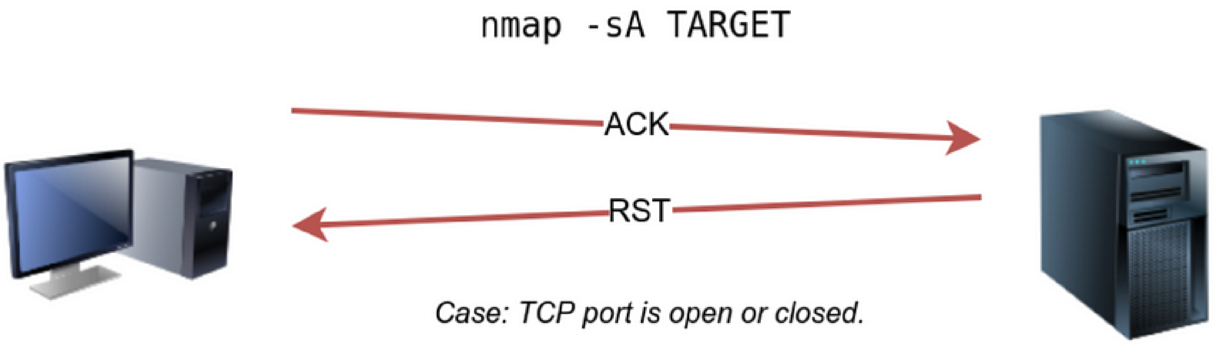
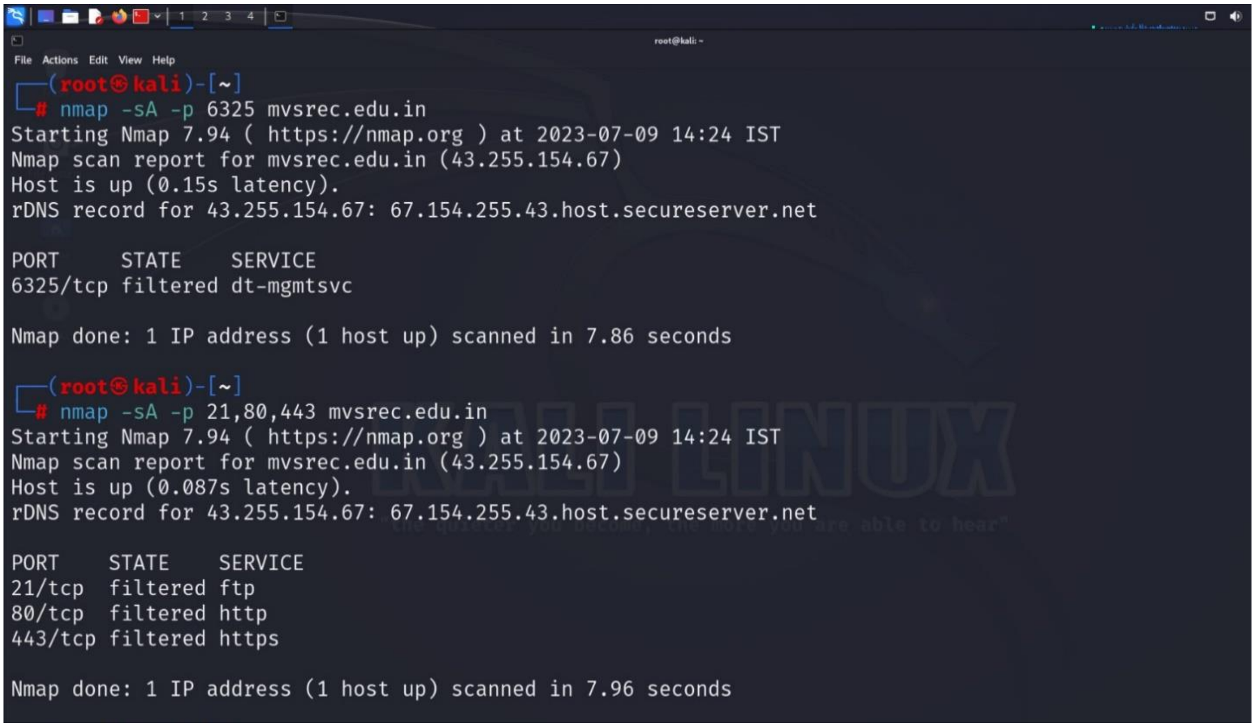


Figure 3.12 ACK Scan - TCP port is open or closed

This type of scan is **useful if there is a firewall in front of the target** since it will tell you which ports were not blocked by the firewall depending on which ACK packets resulted in answers. In other words, this form of scan is more **suited for identifying firewall rule sets and setup.**



```
┌──(root㉿kali)-[~]
└─# nmap -sA -p 6325 mvsrec.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-09 14:24 IST
Nmap scan report for mvsrec.edu.in (43.255.154.67)
Host is up (0.15s latency).
rDNS record for 43.255.154.67: 67.154.255.43.host.secureserver.net

PORT     STATE    SERVICE
6325/tcp filtered dt-mgmtsvc

Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds

┌──(root㉿kali)-[~]
└─# nmap -sA -p 21,80,443 mvsrec.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-09 14:24 IST
Nmap scan report for mvsrec.edu.in (43.255.154.67)
Host is up (0.087s latency).
rDNS record for 43.255.154.67: 67.154.255.43.host.secureserver.net

PORT    STATE    SERVICE
21/tcp  filtered ftp
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

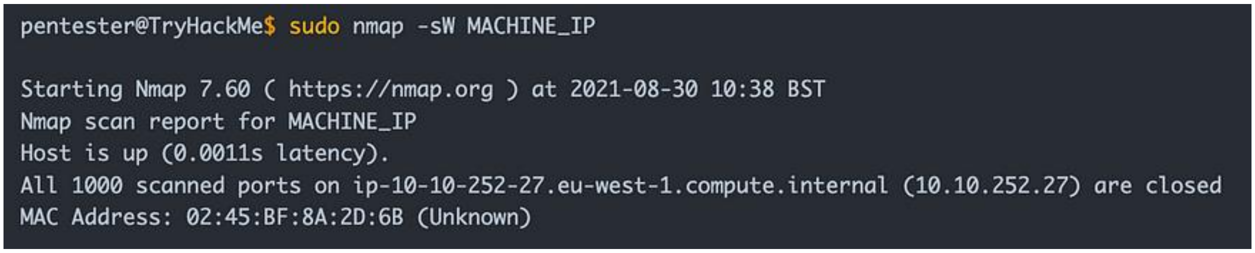
Figure 3.13 ACK Scan performed on web server

6. **Window Scan:** A Window scan is a TCP port scanning technique that analyzes the TCP Window field in response packets to determine port states. Different responses indicate open (non-zero Window), closed (zero Window), or filtered (no response) ports.

   It is similar to the ACK scan, **except that it analyzes the TCP Window field of the RST packets** returned.

   - This can **indicate that the port is open** on some systems.
   - Regardless of whether the port is open or closed, we **expect to receive an RST message in response to our “uninvited” ACK packets**.

   Launching a TCP window **scan against a Linux system with no firewall will not provide much information**. As we can see in the console output below, the results of the window scan against a Linux server **with no firewall didn’t give any extra information compared to the ACK scan executed.**



```
pentester@TryHackMe$ sudo nmap -sW MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:38 BST
Nmap scan report for MACHINE_IP
Host is up (0.0011s latency).
All 1000 scanned ports on ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27) are closed
MAC Address: 02:45:BF:8A:2D:6B (Unknown)
```

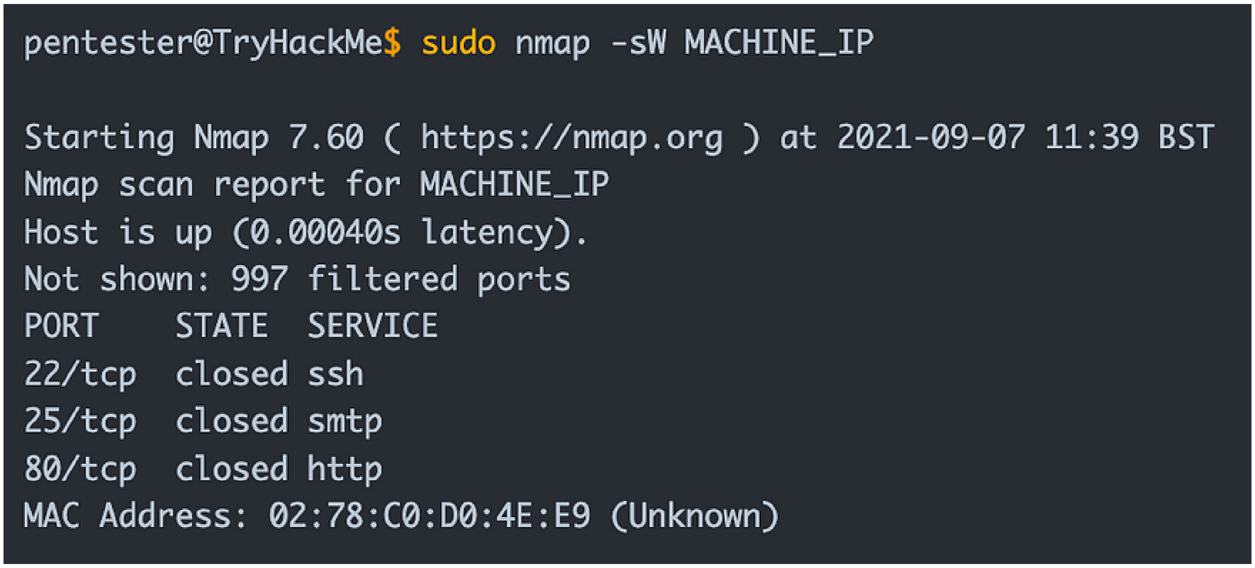
Figure 3.14 Window Scan - 1

However, we might expect more pleasing findings if we run our TCP window scan against a server behind a firewall.

The TCP window scan indicated that three ports were detected as closed in the console output displayed below. (This differs from the ACK scan, which labeled the same three ports as unfiltered.)

Despite the fact that we know these three ports are not closed, we can see that they answered differently, demonstrating that the firewall does not block them.

7. **Custom Scan:** A custom scan refers to a tailored network scanning approach where you can customize various parameters and options based on your specific requirements. It allows you to select scan techniques, define port ranges, specify timing options, and incorporate additional scan options as needed.



```
pentester@TryHackMe$ sudo nmap -sW MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-07 11:39 BST
Nmap scan report for MACHINE_IP
Host is up (0.00040s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  closed ssh
25/tcp  closed smtp
80/tcp  closed http
MAC Address: 02:78:C0:D0:4E:E9 (Unknown)
```

Figure 3.15 Window Scan - 2

To try out a different TCP flag combination than the built-in TCP scan types, use — **scanflags**.

For example, if you wish to set **SYN**, **RST**, and **FIN** all at once, use — **scanflags RSTSYNFIN**. As indicated in the graphic below, if you design your custom scan, you must understand how the various ports will react in order to accurately interpret the results in various settings.

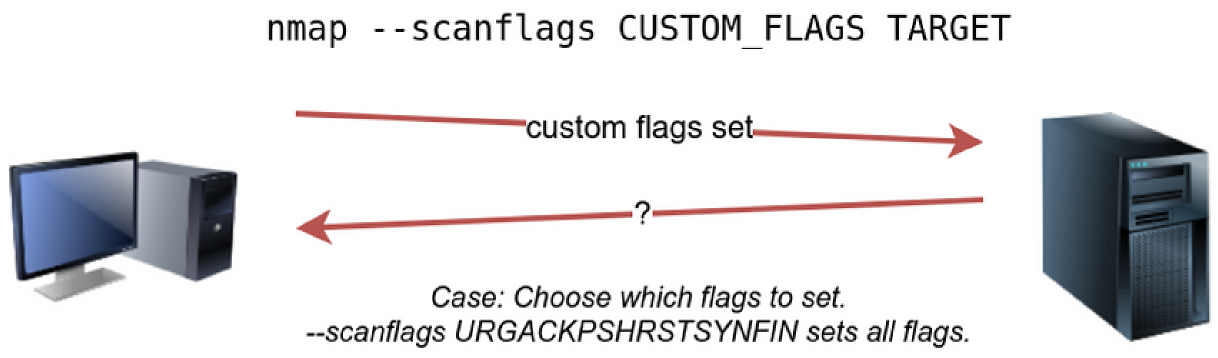

nmap --scanflags CUSTOM_FLAGS TARGET
custom flags set
?
Case: Choose which flags to set.
--scanflags URGACKPSHRSTSYNFIN sets all flags.

Figure 3.16 Custom Scan

Finally, it is critical to highlight that the **ACK scan and the Window scan were really useful** in assisting us in **mapping out the firewall rules**. It is important to realize, however, that just because **a firewall does not block a certain port does not necessarily mean that a service is listening on that port.**

For example, the firewall rules might need to be modified to reflect current service modifications. As a result, ACK and window scans expose the firewall rules rather than the services.

CHAPTER-4

LAB QUESTIONS

1. In a null scan, how many flags are set to 1?

Ans: 0

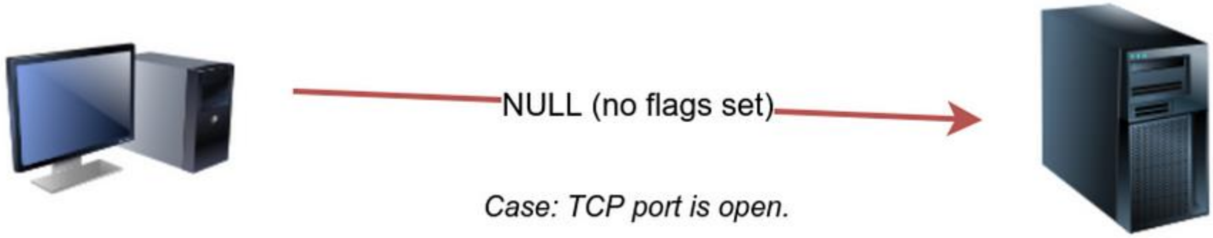


Figure 4.1 Null Scan - no flags set

2. In a FIN scan, How many flags are set to 1?

Ans: 1

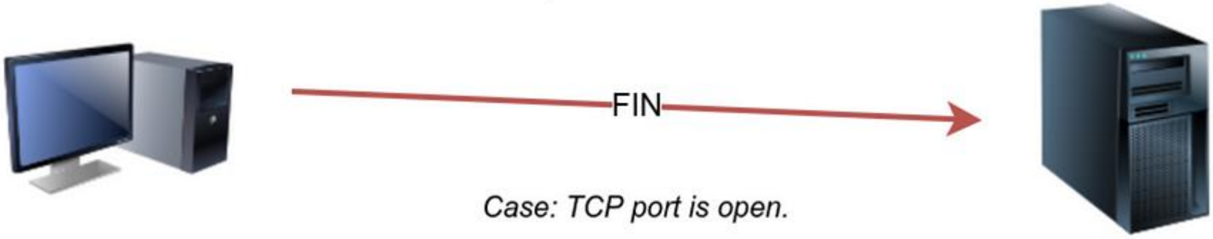


Figure 4.2 FIN Scan - flags set to 1

3. In a Xmas scan, How many flags are set to 1?

Ans: 3

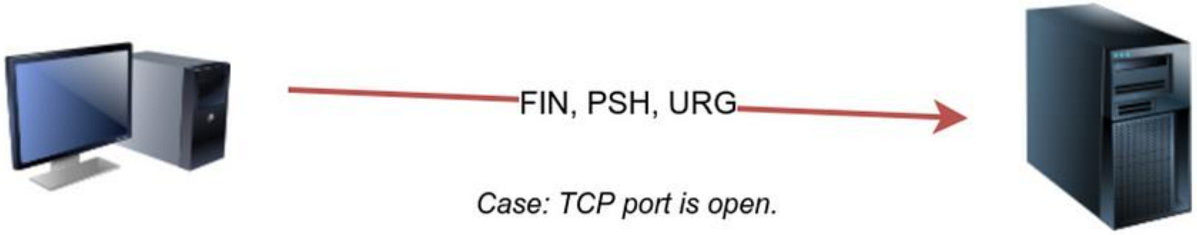
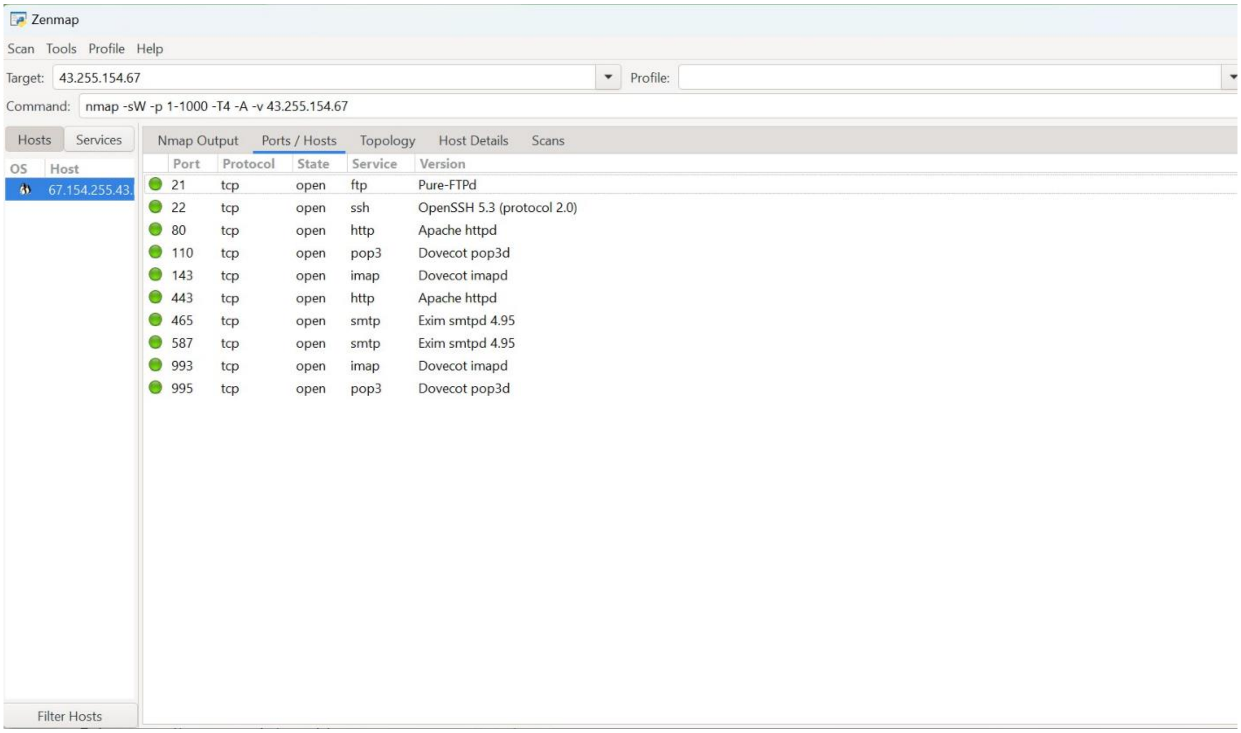


Figure 4.3 Xmas Scan - flags set to 1

4. How many ports appear as open|filtered?

Ans: 10



Target: 43.255.154.67

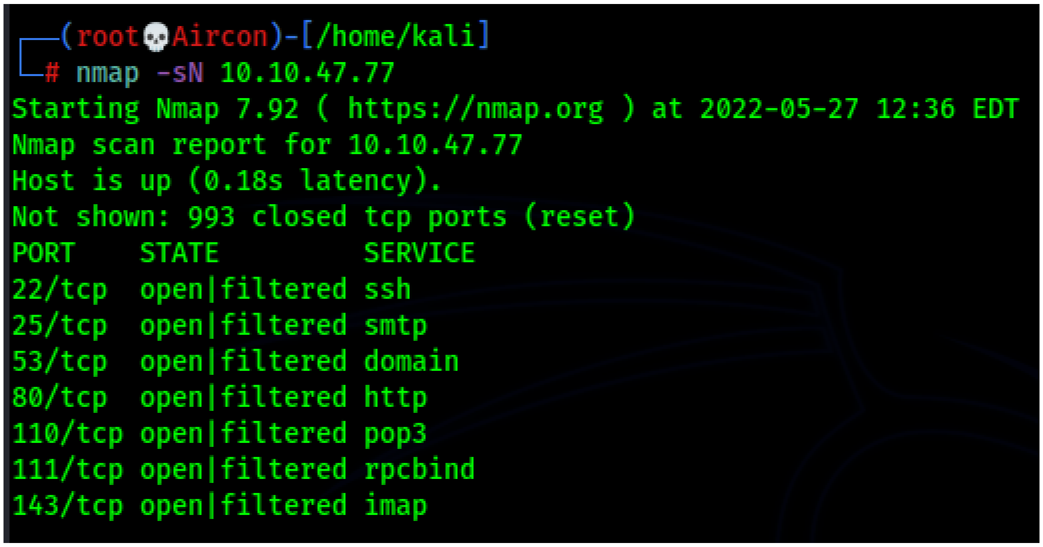
Command: nmap -sW -p 1-1000 -T4 -A -v 43.255.154.67

Port	Protocol	State	Service	Version
21	tcp	open	ftp	Pure-FTPd
22	tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	open	http	Apache httpd
110	tcp	open	pop3	Dovecot pop3d
143	tcp	open	imap	Dovecot imapd
443	tcp	open	http	Apache httpd
465	tcp	open	smtp	Exim smtpd 4.95
587	tcp	open	smtp	Exim smtpd 4.95
993	tcp	open	imap	Dovecot imapd
995	tcp	open	pop3	Dovecot pop3d

Figure 4.4 Ports appear as open|filtered

5. Repeat your scan launching a null scan against the target VM. How many ports appear as open|filtered?

Ans: 7



```
┌──(root💀Aircon)-[/home/kali]
└─# nmap -sN 10.10.47.77
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-27 12:36 EDT
Nmap scan report for 10.10.47.77
Host is up (0.18s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
```

Figure 4.5 Null Scan against target VM

6. **In the Maimon scan, how many flags are set?**

Ans: 2

7. **In TCP Window scan, how many flags are set?**

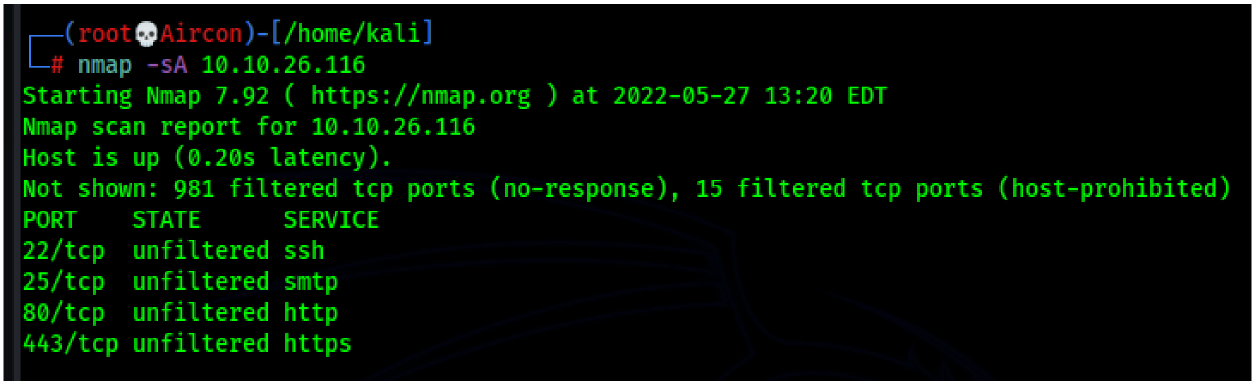
Ans: 1

8. **You decided to experiment with a custom TCP scan that has the reset flag set. What would you add after --scanflags?**

Ans: RST

9. **What is the new port number that appeared?**

Ans: 443



```
┌──(root💀Aircon)-[/home/kali]
└─# nmap -sA 10.10.26.116
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-27 13:20 EDT
Nmap scan report for 10.10.26.116
Host is up (0.20s latency).
Not shown: 981 filtered tcp ports (no-response), 15 filtered tcp ports (host-prohibited)
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
80/tcp  unfiltered http
443/tcp unfiltered https
```

Figure 4.6 New port number that appeared

10. **Is there any service behind the newly discovered port number? (Y/N)**

Ans: N

CHAPTER-5

CONCLUSION

NMAP Port Scans is another room packed with an abundance of scanning characteristics that brings another viewpoint on what type of scanning we would like to undertake, particularly for port scanning. Because we would want to remain stealthy, but we also need accurate data and are looking for solutions to circumvent firewalls and intrusion detection systems.

This project successfully implemented and evaluated alternative port scanning techniques that utilize TCP flags and conducted experiments to assess the effectiveness of these techniques in identifying open ports and services running on target hosts. Further, analysed the impact of these techniques on TCP flag status and observed the differences in responses received from target hosts. Also, quantified the number of open and filtered ports identified by each technique. Identified the services running behind open ports. Employ ethical and responsible port scanning practices.

FUTURE SCOPE

The project on evaluating alternative port scanning techniques utilizing TCP flags has a promising future scope with several potential areas for further exploration and development. These include extending the analysis to more diverse network environments, investigating the impact of network security devices on port scanning techniques, developing automated tools for analyzing port scan results, integrating port scanning techniques with vulnerability assessment tools, exploring the use of machine learning for port scan detection, developing a tool for generating custom port scanning scripts, and conducting research on emerging port scanning techniques. By exploring these future directions, the project can continue to contribute to the advancement of port scanning techniques and network security.