Task 01: Networking Fundamentals, Nmap Scanning & Automation Scripting

Objective

The objective of this task is to build a strong foundation in networking concepts, gain hands-on experience with Nmap scanning techniques, and develop automation skills using Python. The activity focuses on identifying open ports, running services, associated security risks, and automating the scanning process in an authorized lab environment.

Tools & Environment

• Operating System: Linux
• Nmap Version: 7.80
• Python Version: 3.8.10
• Python Library: python-nmap

Networking Concepts Applied

This task involved understanding IP addressing, TCP and UDP protocols, well-known service ports, and how exposed services increase an organization’s attack surface.

Nmap Scans Performed

Multiple Nmap scans were performed, including TCP Connect (-sT), SYN (-sS), and UDP (-sU -F) scans to enumerate live hosts, open ports, and running services.

Scan Findings Summary

Port	Protocol	Service
22	TCP	SSH
25	TCP	SMTP
53	TCP	DNS
80	TCP	HTTP
110	TCP	POP3
111	TCP	RPCBind
143	TCP	IMAP
993	TCP	IMAPS
995	TCP	POP3S

Security Observations

The presence of multiple mail services increases exposure to credential-based attacks. RPCBind services can be abused for enumeration, while DNS and NTP services may be leveraged for amplification attacks if not properly secured. Service hardening and firewall controls are strongly recommended.

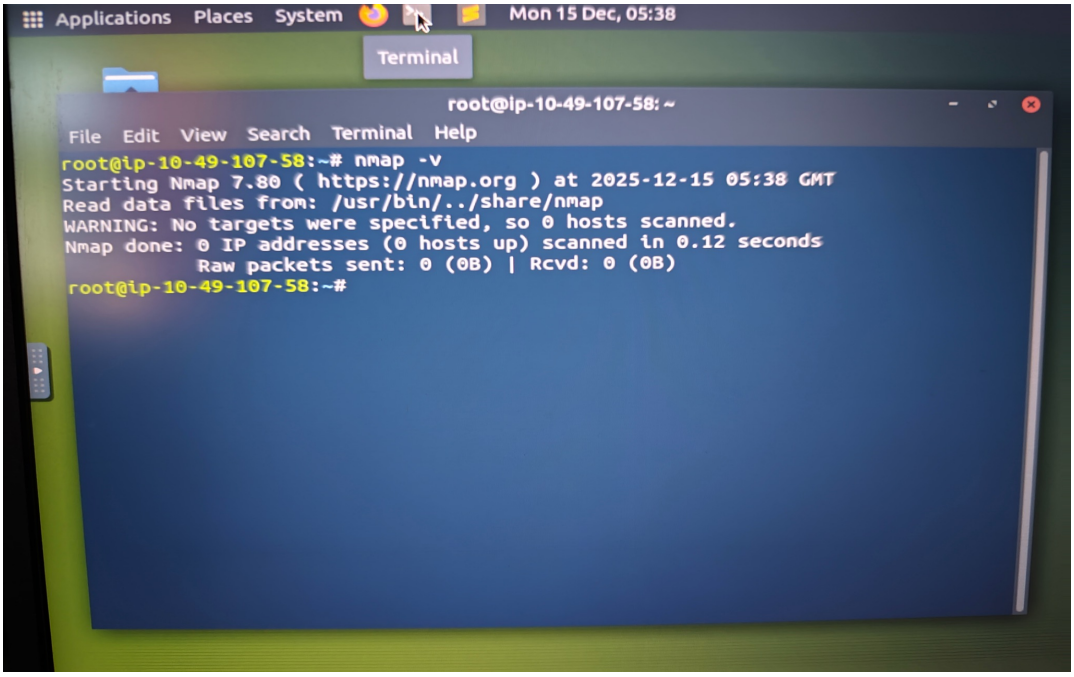
Python Automation

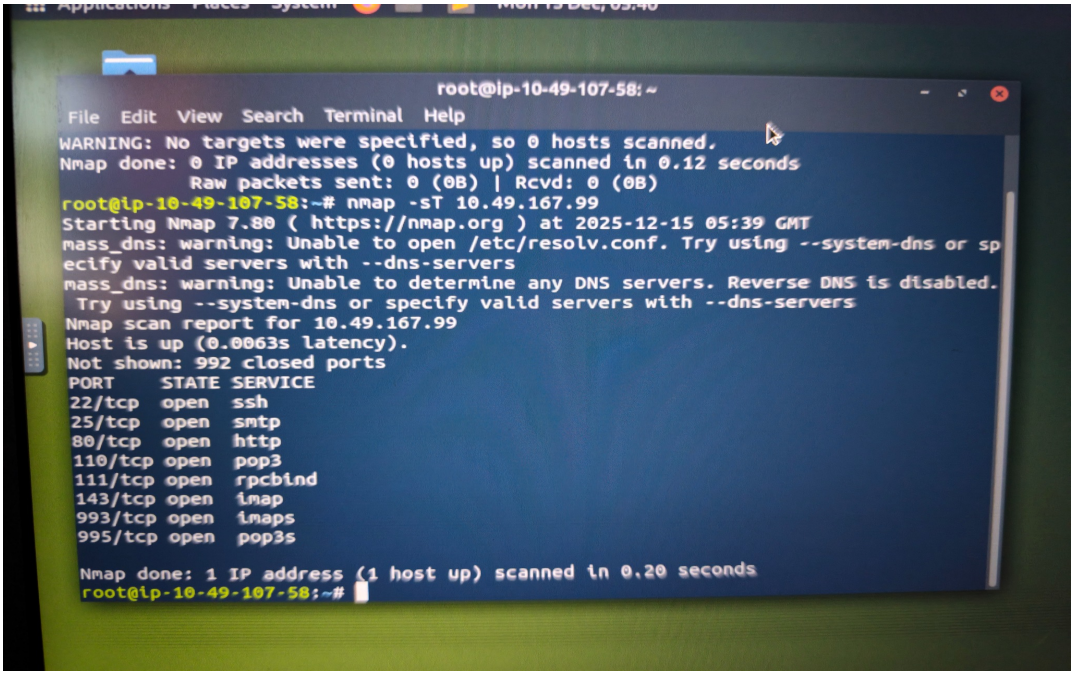
A Python script using the python-nmap library was developed to automate SYN scans. The script accepts a target IP address, executes the scan, parses results, and generates a timestamped scan report.

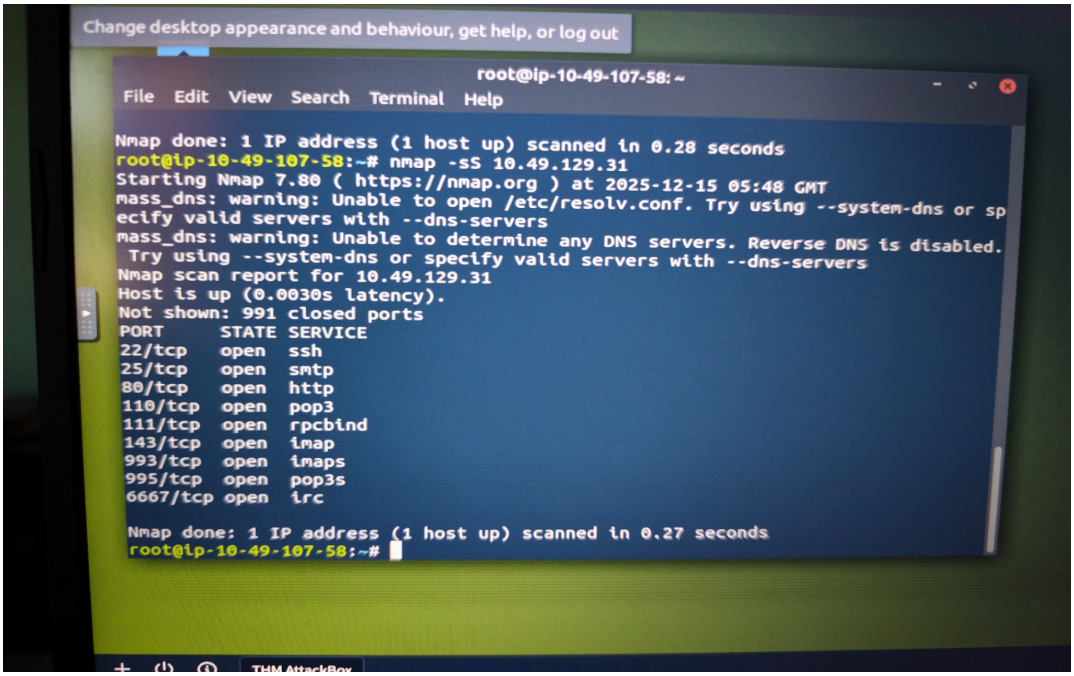
Error Encountered and Resolution

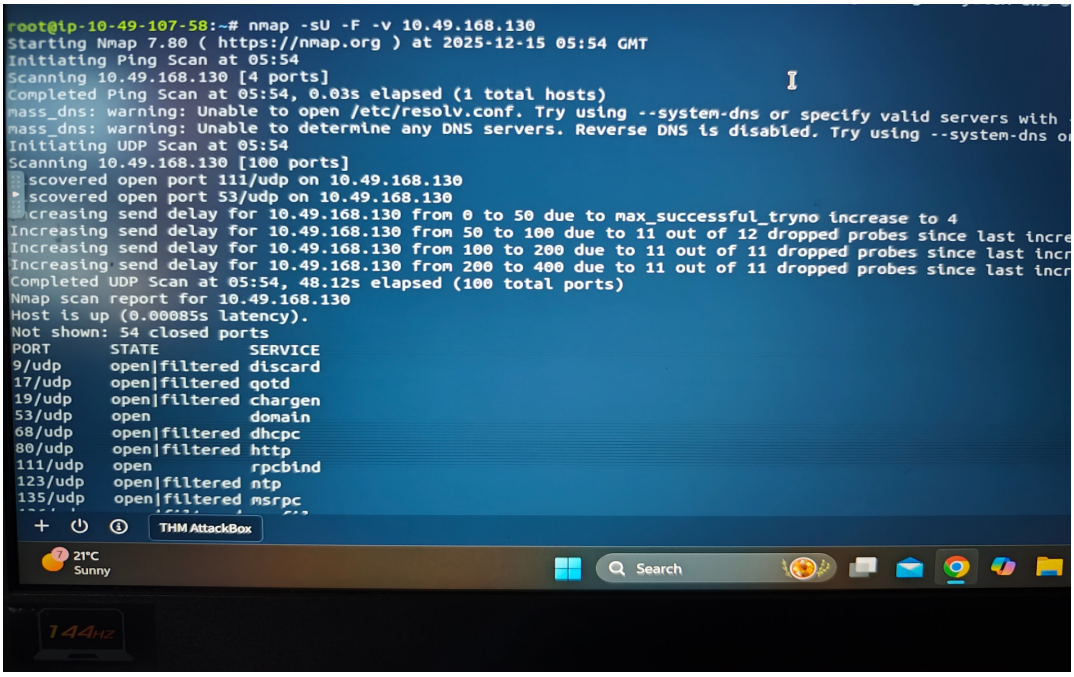
During script execution, a ModuleNotFoundError was encountered due to the absence of the python-nmap library. Although Nmap was installed at the system level, the required Python wrapper was missing. This issue was resolved by installing the python-nmap package using pip, after which the script executed successfully.

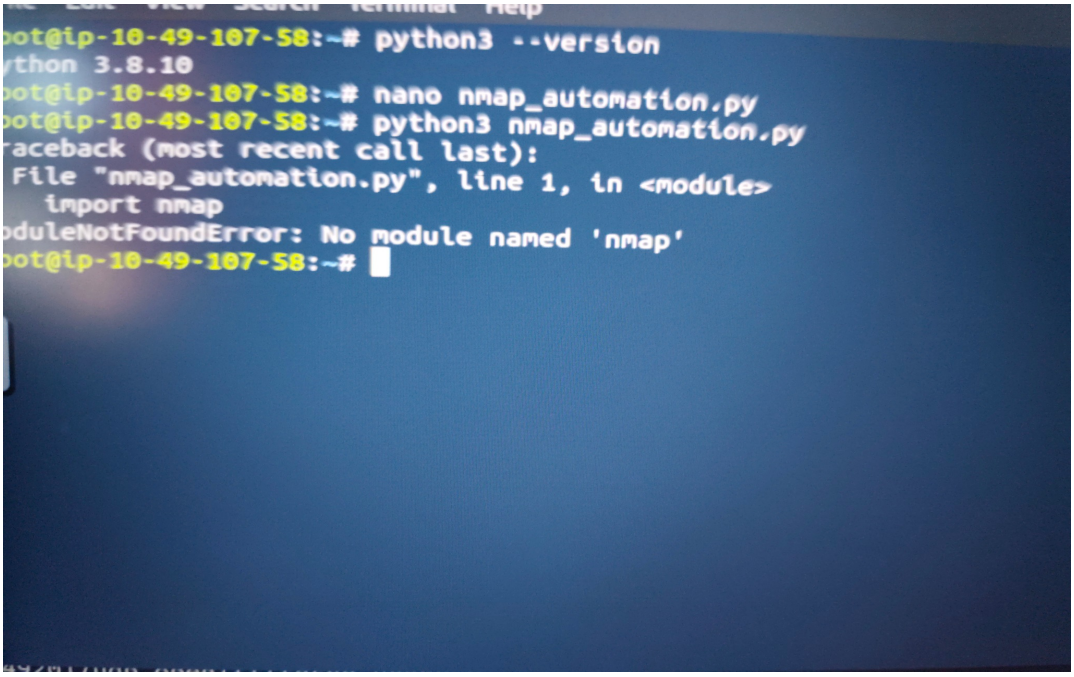
Evidence Screenshots

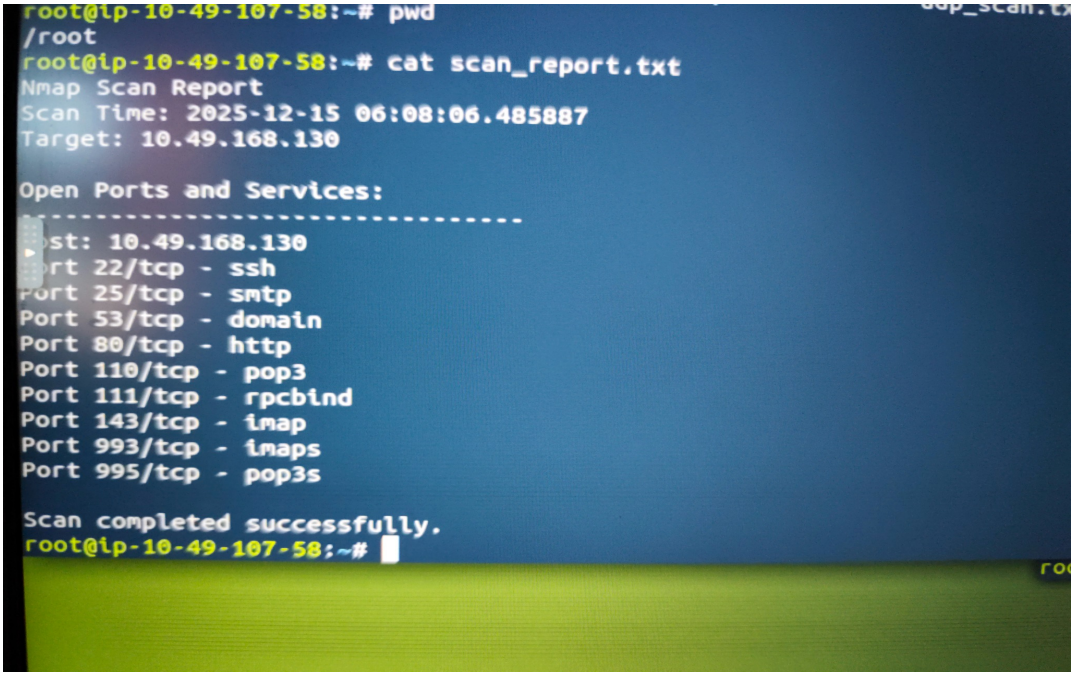




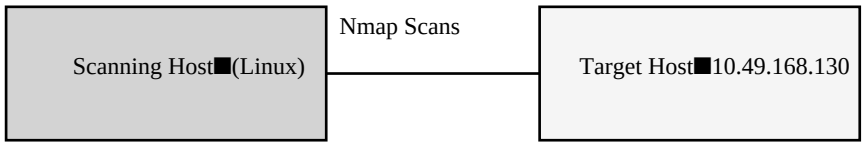

Change desktop appearance and behaviour, get help, or log out
root@ip-10-49-107-58: ~
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@ip-10-49-107-58:~# nmap -sS 10.49.129.31
Starting Nmap 7.80 (https://nmap.org) at 2025-12-15 05:48 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.49.129.31
Host is up (0.0030s latency).
Not shown: 991 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
80/tcp open http
110/tcp open pop3
111/tcp open rpcbind
143/tcp open imap
993/tcp open imaps
995/tcp open pop3s
6667/tcp open irc
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@ip-10-49-107-58:~#


root@ip-10-49-107-58:~# nmap -sU -F -v 10.49.168.130
Starting Nmap 7.80 (https://nmap.org) at 2025-12-15 05:54 GMT
Initiating Ping Scan at 05:54
Scanning 10.49.168.130 [4 ports]
Completed Ping Scan at 05:54, 0.03s elapsed (1 total hosts)
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns o
Initiating UDP Scan at 05:54
Scanning 10.49.168.130 [100 ports]
scovered open port 111/udp on 10.49.168.130
scovered open port 53/udp on 10.49.168.130
creasing send delay for 10.49.168.130 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 10.49.168.130 from 50 to 100 due to 11 out of 12 dropped probes since last incre
Increasing send delay for 10.49.168.130 from 100 to 200 due to 11 out of 11 dropped probes since last incr
Increasing send delay for 10.49.168.130 from 200 to 400 due to 11 out of 11 dropped probes since last incr
Completed UDP Scan at 05:54, 48.12s elapsed (100 total ports)
Nmap scan report for 10.49.168.130
Host is up (0.00085s latency).
Not shown: 54 closed ports
PORT STATE SERVICE
9/udp open|filtered discard
17/udp open|filtered qotd
19/udp open|filtered chargen
53/udp open domain
68/udp open|filtered dhcpc
80/udp open|filtered http
111/udp open rpcbind
123/udp open|filtered ntp
135/udp open|filtered msrpc
THM AttackBox
21°C
Sunny
Search
144Hz


oot@ip-10-49-107-58:~# python3 --version
ython 3.8.10
oot@ip-10-49-107-58:~# nano nmap_automation.py
oot@ip-10-49-107-58:~# python3 nmap_automation.py
raceback (most recent call last):
File "nmap_automation.py", line 1, in <module>
import nmap
oduleNotFoundError: No module named 'nmap'
oot@ip-10-49-107-58:~#


root@ip-10-49-107-58:~# pwd
/root
root@ip-10-49-107-58:~# cat scan_report.txt
Nmap Scan Report
Scan Time: 2025-12-15 06:08:06.485887
Target: 10.49.168.130
Open Ports and Services:
st: 10.49.168.130
rt 22/tcp - ssh
ort 25/tcp - smtp
Port 53/tcp - domain
Port 80/tcp - http
Port 110/tcp - pop3
Port 111/tcp - rpcbind
Port 143/tcp - imap
Port 993/tcp - imaps
Port 995/tcp - pop3s
Scan completed successfully.
root@ip-10-49-107-58:~#

Network Diagram



Conclusion

This task provided hands-on exposure to network reconnaissance and security assessment techniques. By combining manual Nmap analysis with Python-based automation, the exercise reflects real-world cybersecurity workflows and demonstrates readiness for entry-level cybersecurity roles and internships.