Week 3: Network Scanning, Footprinting and Enumeration

Name: V. Risvanth

Introduction

In the realm of cybersecurity, reconnaissance and scanning are crucial steps in assessing the security posture of a target network. This report focuses on conducting various scanning techniques to gather critical information about a system, including active hosts, open ports, running services, and potential vulnerabilities. The objective is to identify security gaps that could be exploited by attackers and provide insights for strengthening network defenses.

Scope of the Task

The study involves performing a series of active scans using **Nmap** and other open-source tools to compare results and gain a comprehensive understanding of the target network. The tasks include:

- Identifying the target **IP range** for scanning.
- Conducting **ping scans** to detect active hosts.
- Performing **port scanning** to discover open ports.
- Executing **service enumeration** to determine the versions of running services.
- Using **banner grabbing** to extract additional information about these services.
- Conducting **OS fingerprinting** to identify the target operating system.
- Gathering **network footprinting data** using tools like whois, dig, and nslookup.
- Performing a **vulnerability assessment** to detect security flaws.
- Comparing the output of Nmap scans with results from other open-source tools.
- Conducting **five additional active scans** with Nmap and documenting the findings.

Tools Used

This study employs **Nmap (Network Mapper)**—one of the most powerful open-source tools for network discovery and security auditing. Additionally, other open-source tools will be used for comparative analysis to evaluate differences in scanning accuracy and efficiency.

Importance of the Nmap

Cyber attackers often leverage the same reconnaissance techniques to gather intelligence before launching an attack. By proactively performing these scanning techniques, organizations can:

- Identify and remediate security vulnerabilities before they are exploited.
- Strengthen their network security posture by understanding potential attack vectors.
- Enhance security monitoring and incident response strategies.

Commands Used

1.Identifying Target IP Range:

- Objective: Determine the target IP range for scanning
- Command: ip a | grep inet
- Analysis: Identifies the network subnet for scanning

2.Performing Ping Scan :

- Objective: Identify active hosts within the target IP range.
- Command: nmap -sn 44.228.249.3
- Analysis: Displays active devices on the network using ICMP packets.

3. Performing Port Scanning:

- Objective: Identify open ports on the active hosts
- Command: nmap -p- 44.228.249.3
- Analysis: Scans all 65,535 ports to detect open ones.

4. Service Enumeration:

- Objective: Detect the version of services running on open ports.
- Command: nmap -sV 44.228.249.3
- Analysis: Identifies service versions and helps in vulnerability detection.

5. Banner Grabbing:

- Objective: Extract banners from open ports
- Command: nmap --script=banner 44.228.249.3
- Analysis: Provides software details that may contain vulnerabilities.

6. OS Fingerprinting:

- Objective: Identify the operating system of the target.
- Command: nmap -O 44.228.249.3
- Analysis: Determines if the target is Windows, Linux, or another OS.

7. Footprinting:

- Objective: Domain Gathering Information
- Command: dig testphp.vulnweb.com
  (or)
- Command: nslookup teestphp.vulnweb.com
- Analysis: Provides domain owner details and DNS records.

8. Vulnerability Assessment:

- Objective: To find the vulnerability using nmap
- Command: nmap --script=vuln 44.228.249.3
- Analysis: Identifies security flaws and misconfigurations.

9. Comparing Nmap with Other Open Source Tools:

- Nmap - it is used for Scanning, Enumeration, Vulnerability Analysis
- Nikto - it is used for Web vulnerability scanner
- OpenVAS – it is used for full vulnerability assessment
- Metasploit – it is used for Exploit and penetration testing
- Masscan - it is used for high speed network scanning

10. Performing 5 More Active Scans and Analysis:

Scan 1: TCP SYN Scan:

- Command: nmap -sS 44.228.249.3
- Analysis: Stealth scan to detect open TCP ports.

Scan 2: UDP Scan:

- Command: nmap -sU 44.228.249.3
- Analysis: Identifies UDP-based services like DNS and SNMP.

Scan 3: Aggressive Scan:

- Command: nmap -A 44.228.249.3
- Analysis: Performs multiple scans in one command.

Scan 4: Evading Firewalls with Fragmentation:

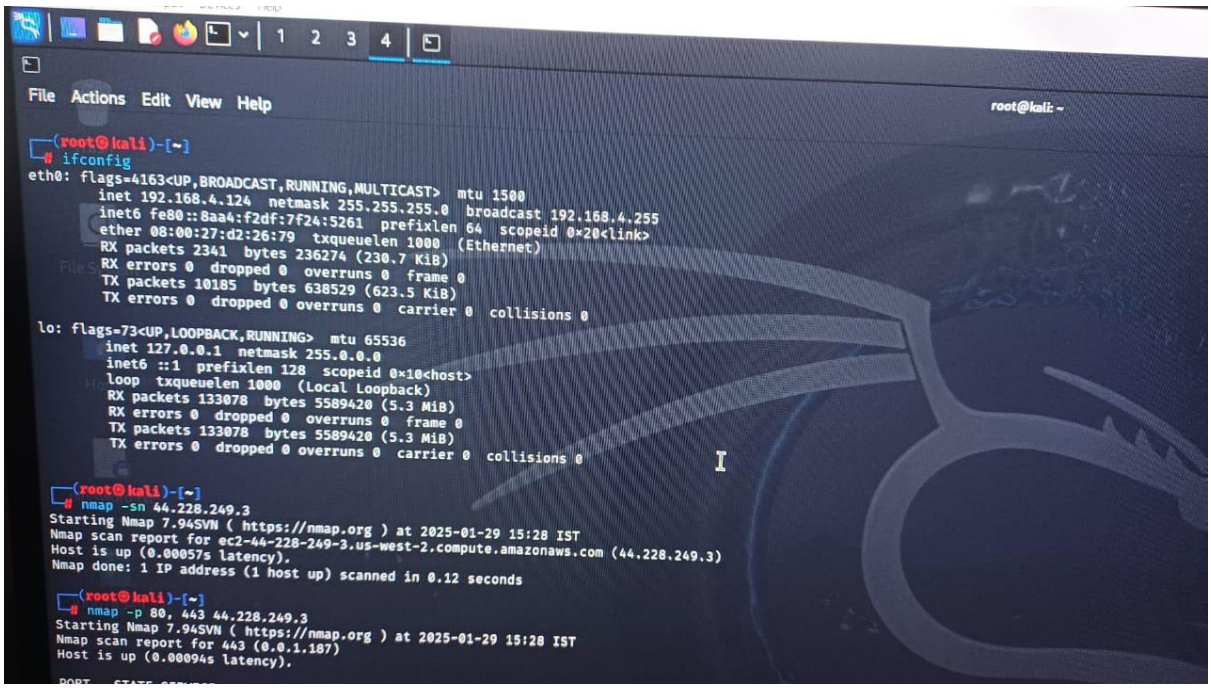
- Command: nmap -f 44.228.249.3
- Analysis: Helps bypass intrusion detection systems.

Scan 5: Spoofing Source IP for Anonymous Scanning

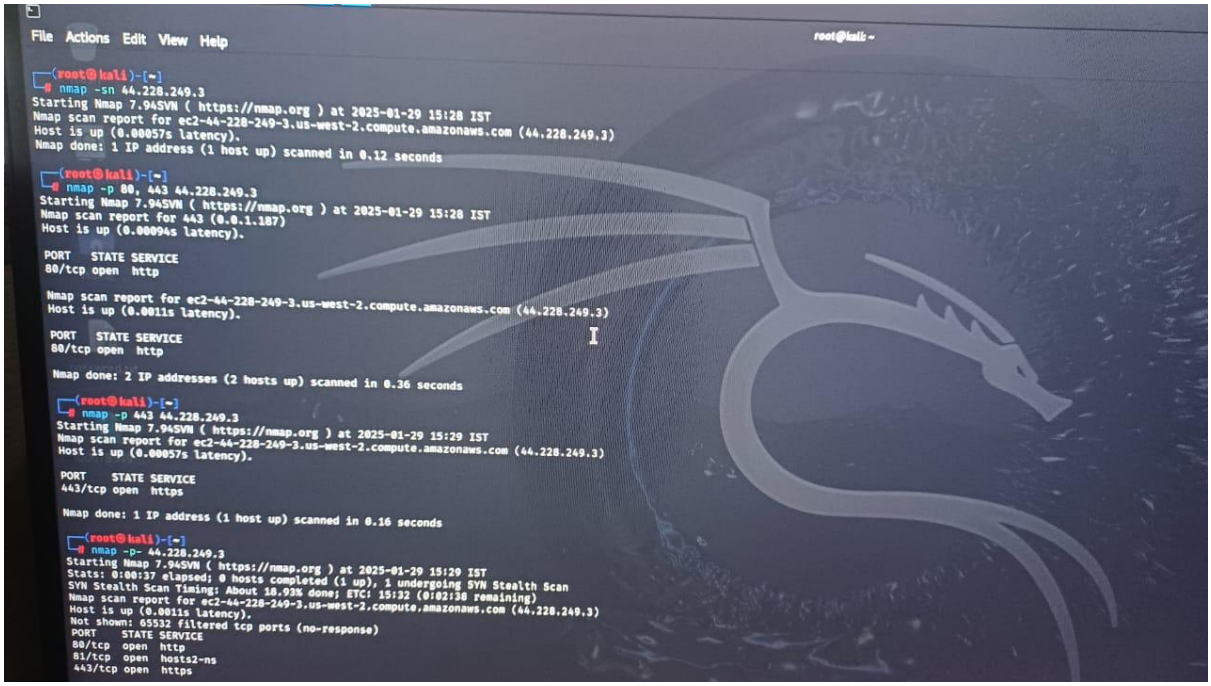
- Command: nmap -S 192.168.4.124 44.228.249.3
- Analysis: Hides the real scanner identity.

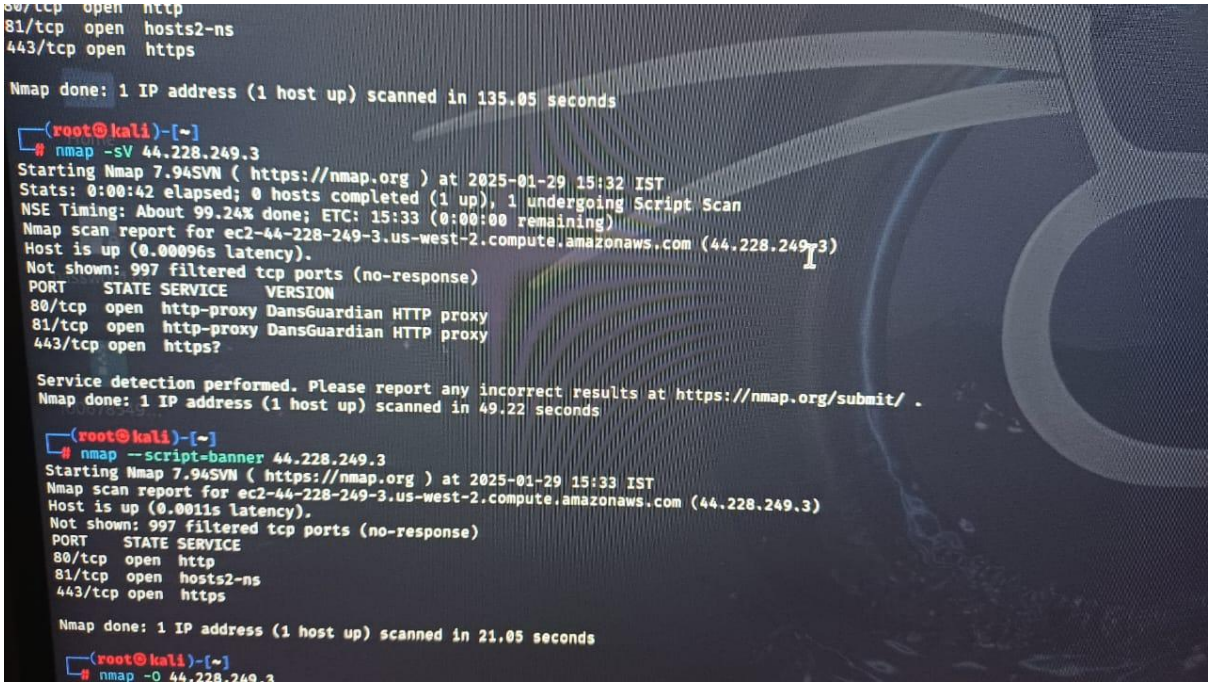
All the Commands for this task are included with working functionality

Screenshots



1. Using ifconfig command and checked the ip address





2. Through Nmap I checked with the Ip address what are the hosts all are alive and checking thee ports which is open

1.Performing Ping Scan :

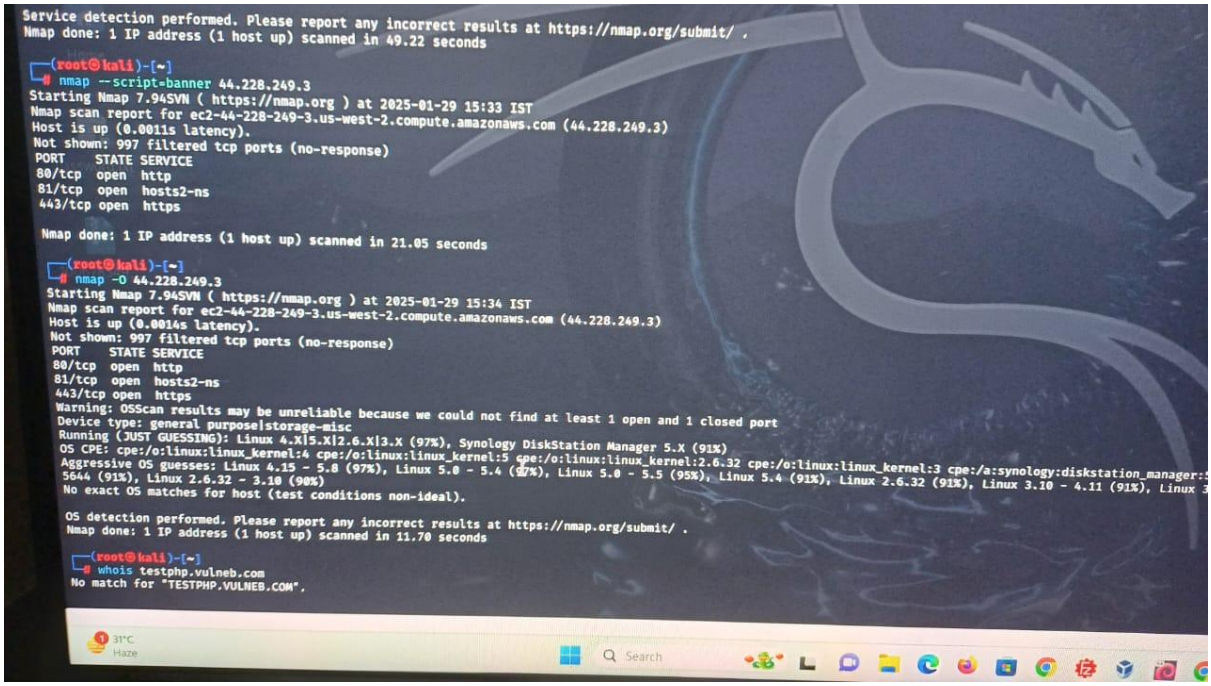
- Objective: Identify active hosts within the target IP range.
- Command: nmap -sn 44.228.249.3
- Analysis: Displays active devices on the network using ICMP packets.

2. Performing Port Scanning:

- Objective: Identify open ports on the active hosts
- Command: nmap -p- 44.228.249.3
- Analysis: Scans all 65,535 ports to detect open ones.

3. Service Enumeration:

- Objective: Detect the version of services running on open ports.
- Command: nmap -sV 44.228.249.3
- Analysis: Identifies service versions and helps in vulnerability detection.



1. Banner Grabbing:

- Objective: Extract banners from open ports
- Command: nmap --script=banner 44.228.249.3

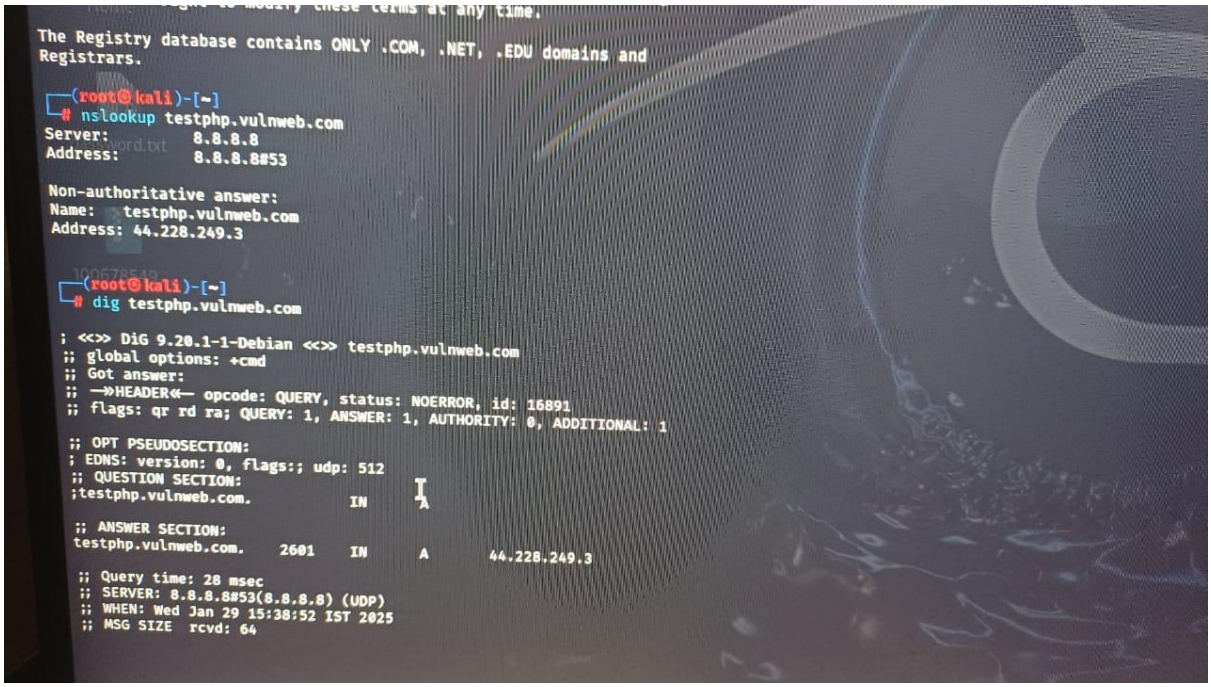
● Analysis: Provides software details that may contain vulnerabilities.

2. OS Fingerprinting:

● Objective: Identify the operating system of the target.

● Command: nmap -O 44.228.249.3

● Analysis: Determines if the target is Windows, Linux, or another OS.



1. Footprinting:

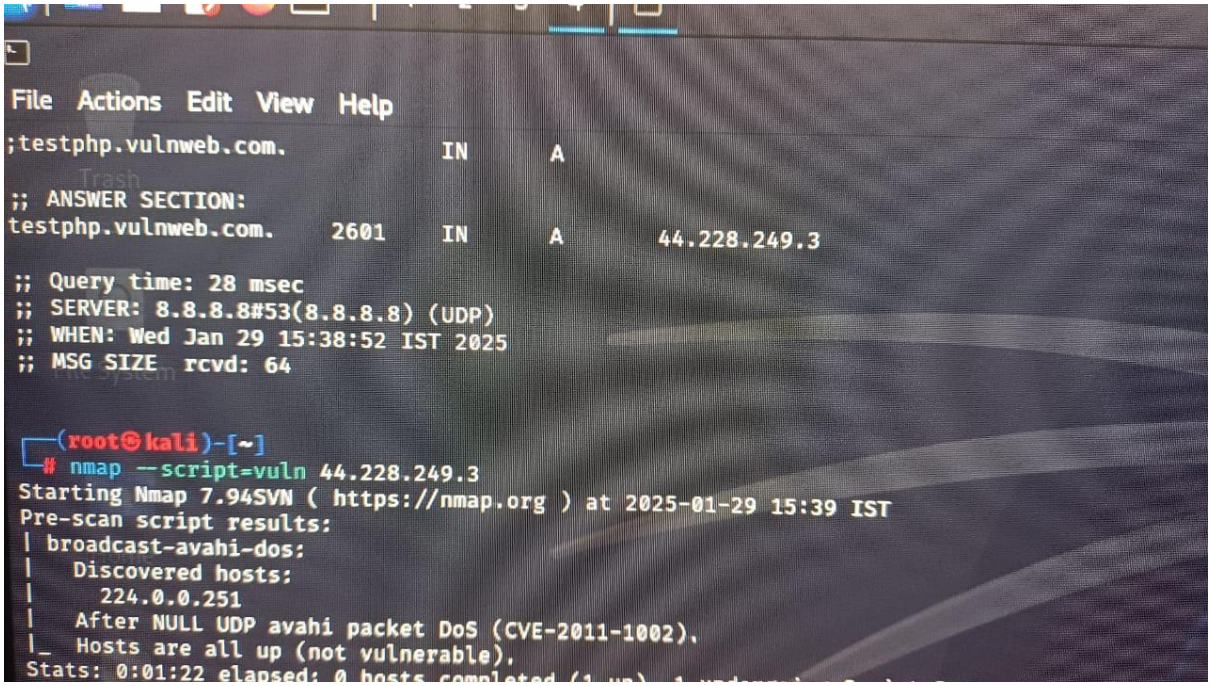
● Objective: Domain Gathering Information

● Command: dig testphp.vulnweb.com

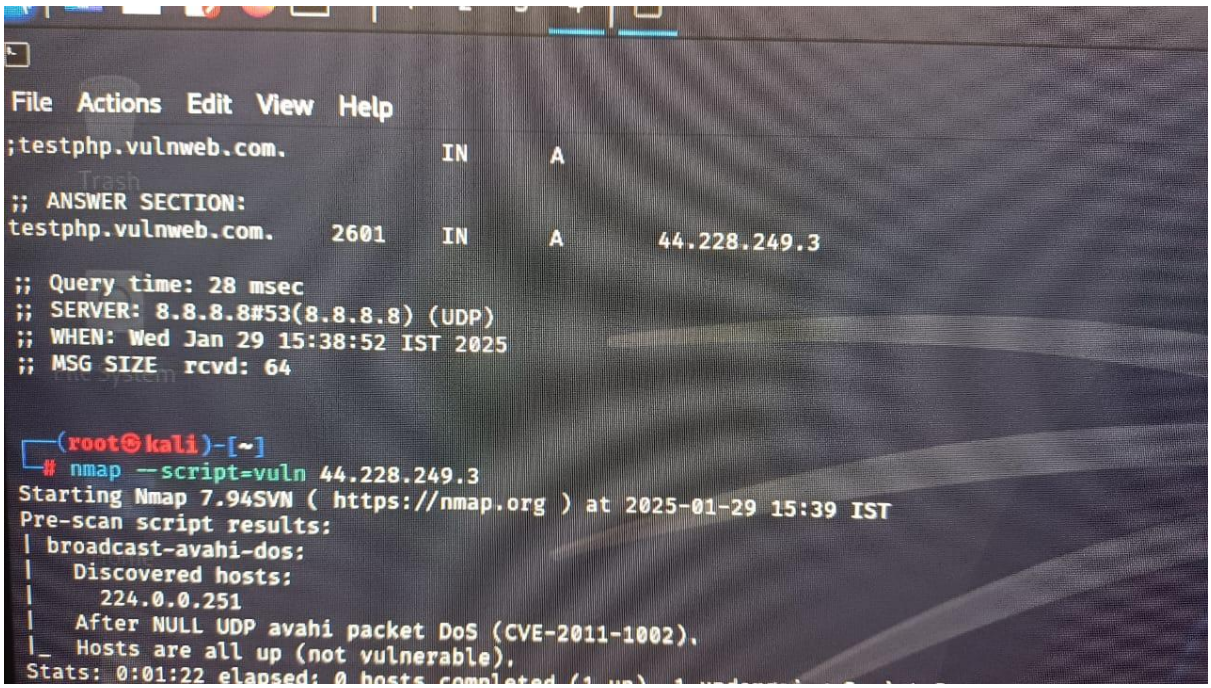
(or)

● Command: nslookup teestphp.vulnweb.com

● Analysis: Provides domain owner details and DNS records.

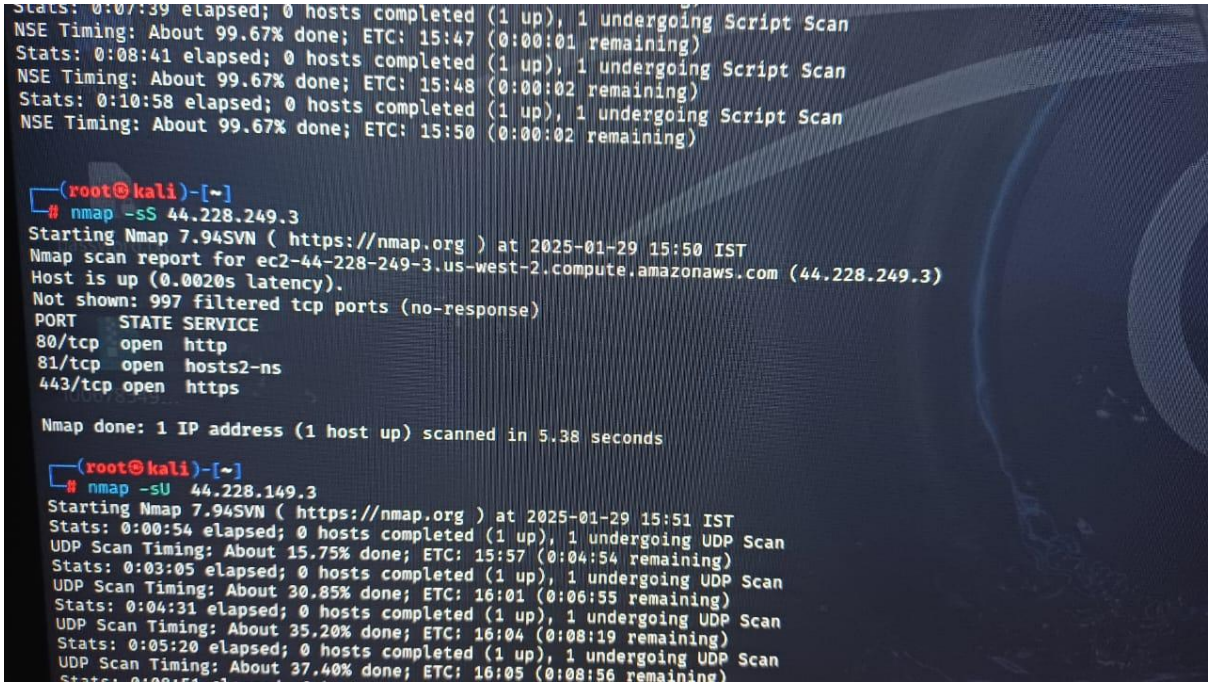

File Actions Edit View Help
;testphp.vulnweb.com. IN A
;; ANSWER SECTION:
testphp.vulnweb.com. 2601 IN A 44.228.249.3
;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Jan 29 15:38:52 IST 2025
;; MSG SIZE rcvd: 64
(root㉿kali)-[~]
nmap --script=vuln 44.228.249.3
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-29 15:39 IST
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).

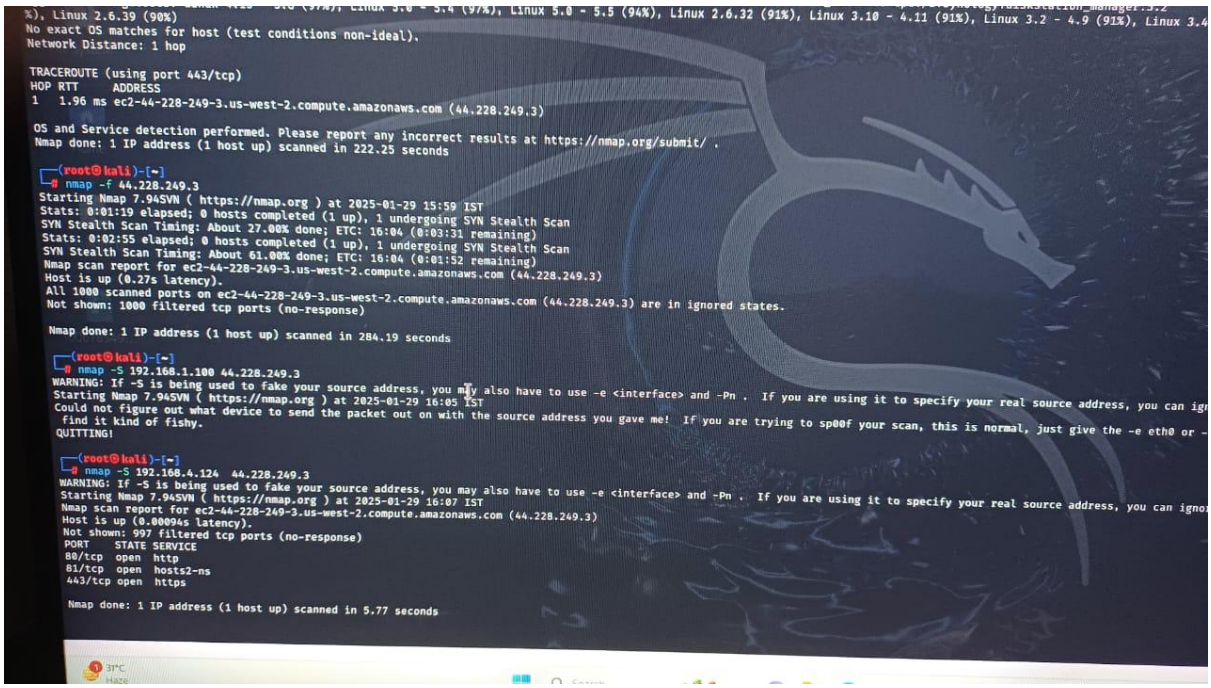
.

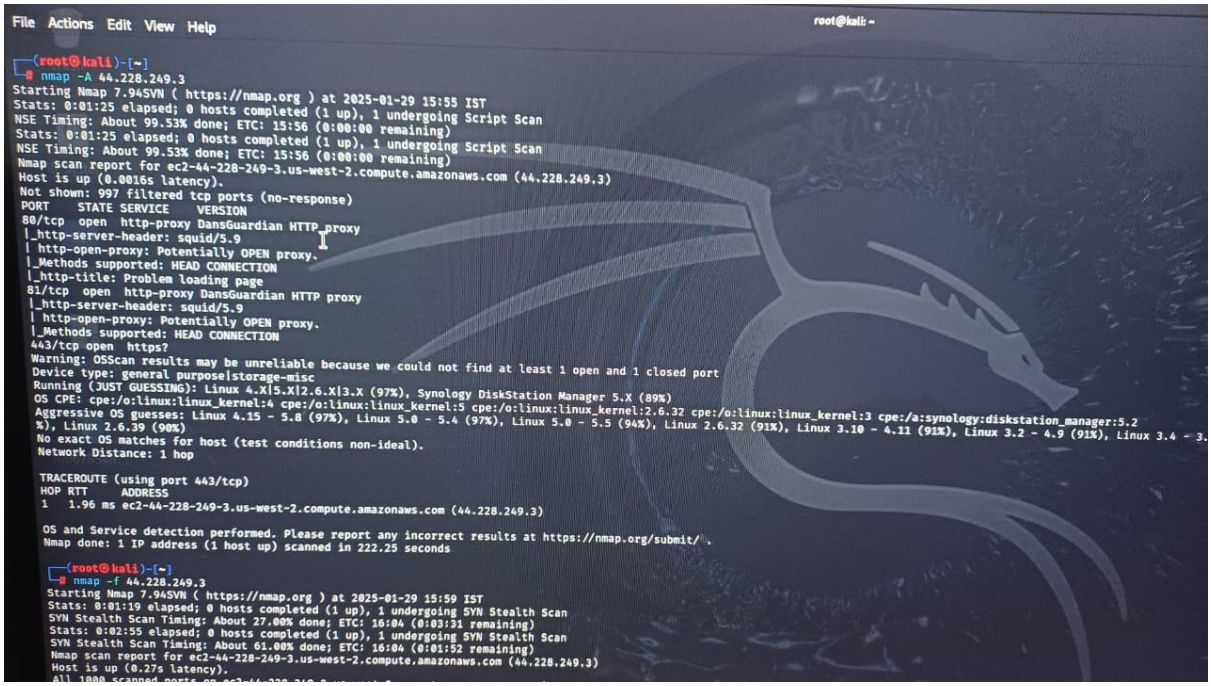

File Actions Edit View Help
;testphp.vulnweb.com. IN A
;; ANSWER SECTION:
testphp.vulnweb.com. 2601 IN A 44.228.249.3
;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Jan 29 15:38:52 IST 2025
;; MSG SIZE rcvd: 64
(root㉿kali)-[~]
nmap --script=vuln 44.228.249.3
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-29 15:39 IST
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).

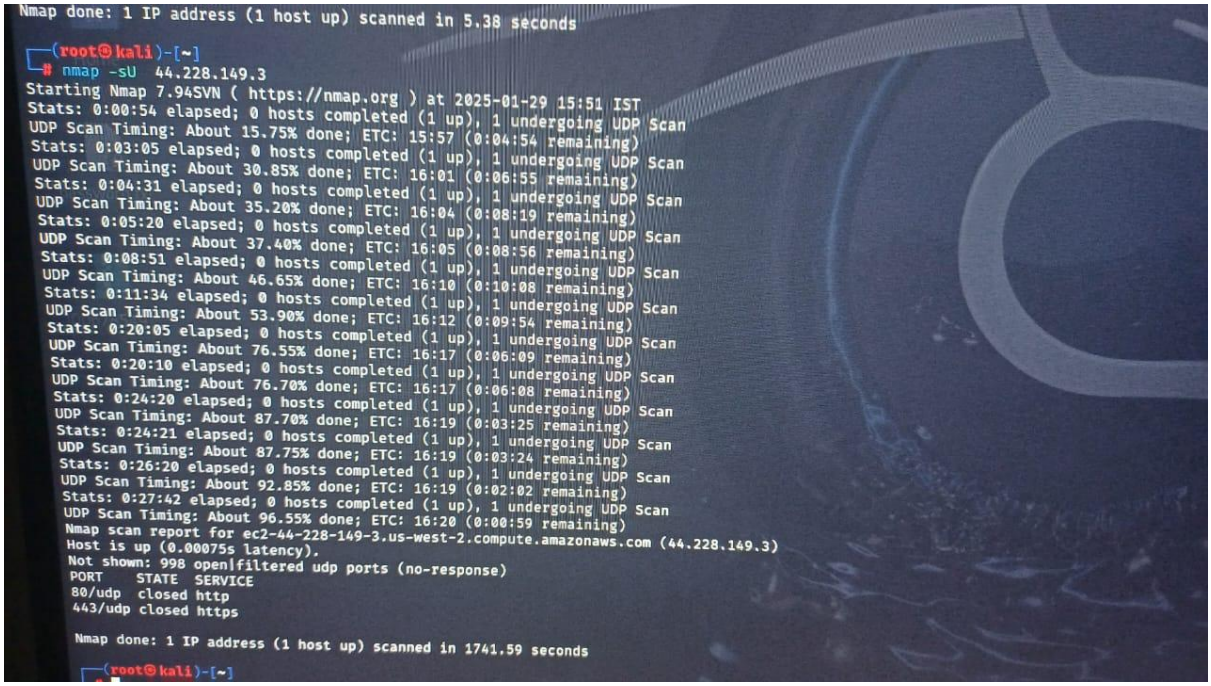
1. Vulnerability Assessment:

- Objective: To find the vulnerability using nmap
- Command: nmap --script=vuln 44.228.249.3
- Analysis: Identifies security flaws and misconfigurations.









1.. Performing 5 More Active Scans and Analysis:

Scan 1: TCP SYN Scan:

- Command: nmap -sS 44.228.249.3

- Analysis: Stealth scan to detect open TCP ports.

Scan 2: UDP Scan:

- Command: nmap -sU 44.228.249.3
- Analysis: Identifies UDP-based services like DNS and SNMP.

Scan 3: Aggressive Scan:

- Command: nmap -A 44.228.249.3
- Analysis: Performs multiple scans in one command.

Scan 4: Evading Firewalls with Fragmentation:

- Command: nmap -f 44.228.249.3
- Analysis: Helps bypass intrusion detection systems.

Scan 5: Spoofing Source IP for Anonymous Scanning

- Command: nmap -S 192.168.4.124 44.228.249.3
- Analysis: Hides the real scanner identity.

Conclusion

The network scanning and security assessment conducted in this task provided valuable insights into the security posture of the target environment. By systematically performing **ping scans, port scans, service enumeration, banner grabbing, OS fingerprinting, footprinting, and vulnerability assessments**, we identified active hosts, open ports, running services, and potential vulnerabilities.

The use of **Nmap** and other open-source tools allowed us to compare outputs, assess tool accuracy, and determine the effectiveness of different scanning techniques. Through **banner grabbing and OS fingerprinting**, we gained deeper visibility into system configurations and potential weaknesses. Additionally, the **footprinting phase** using tools like **whois, dig, and nslookup** helped gather external intelligence on the target domain.

By performing multiple **active scans with Nmap**, we observed various network behaviors and security gaps. These findings emphasize the importance of **regular network scanning and vulnerability assessments** to proactively detect and mitigate security risks.

Overall, this assessment highlights the critical need for **continuous monitoring, proper network hardening, and security best practices** to protect against cyber threats. The insights from this report can be used to strengthen security defenses and improve overall network resilience.
