**Practical question paper for using Nmap**

Report Date: 22nd September 2024

Report Time: 5.30 PM

Reported by: **Sanjana Inchalmath**

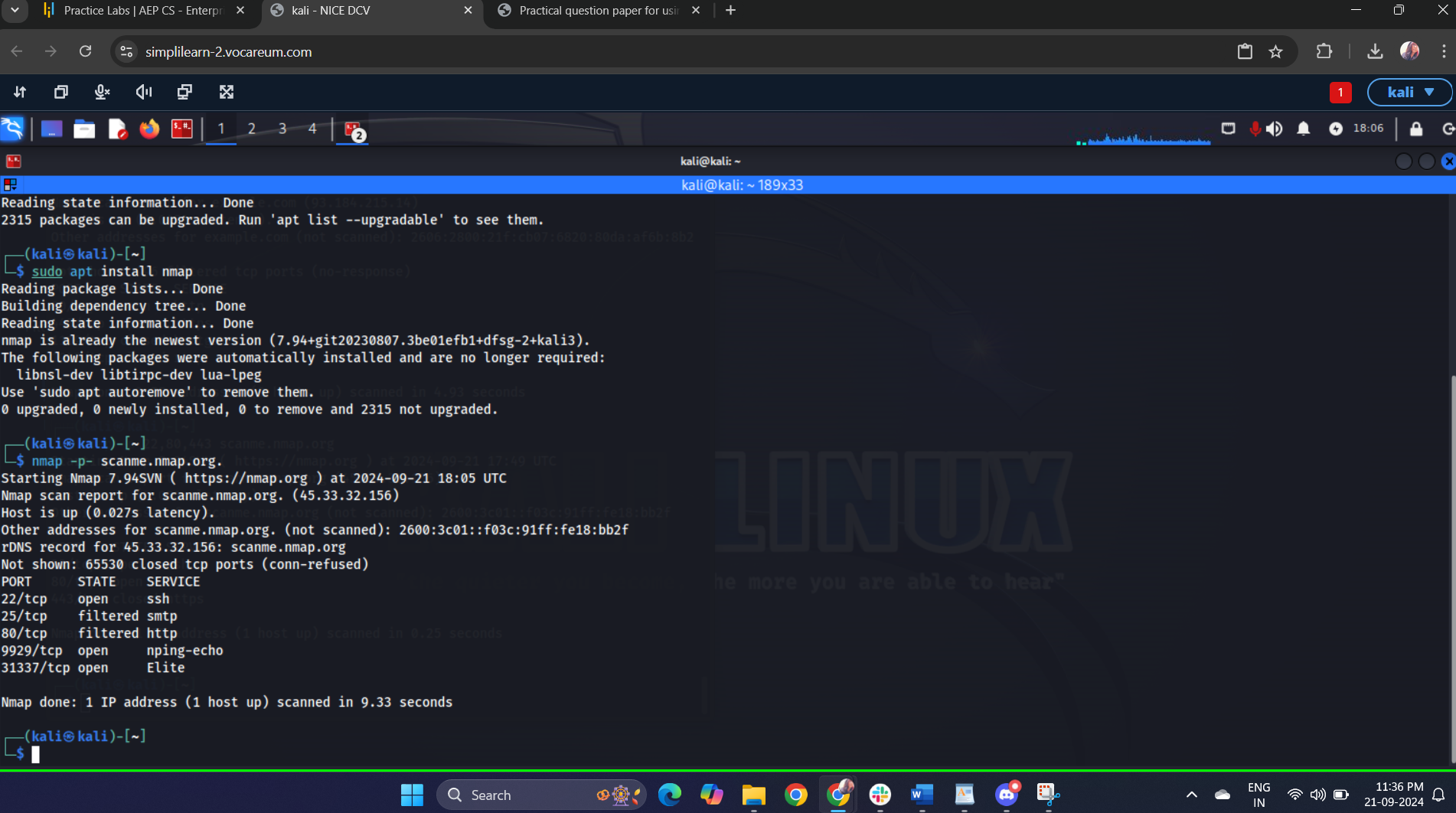
Email id.: sanjanainchalmath@gmail.com

Machine: Kali Linux

**Task 1**

**Command used**: nmap -p- scanme.nmap.org.

**Output Generated:**



**Conclusion:**

The host ‘**scanme.nmap.org**’ has several open ports that provide various services:

1) SSH (port 22) allows for secure remote access.

2) HTTP (port 80) indicates a web server presence.

3) Nping- Echo (port 9929) is part of network testing utilities.

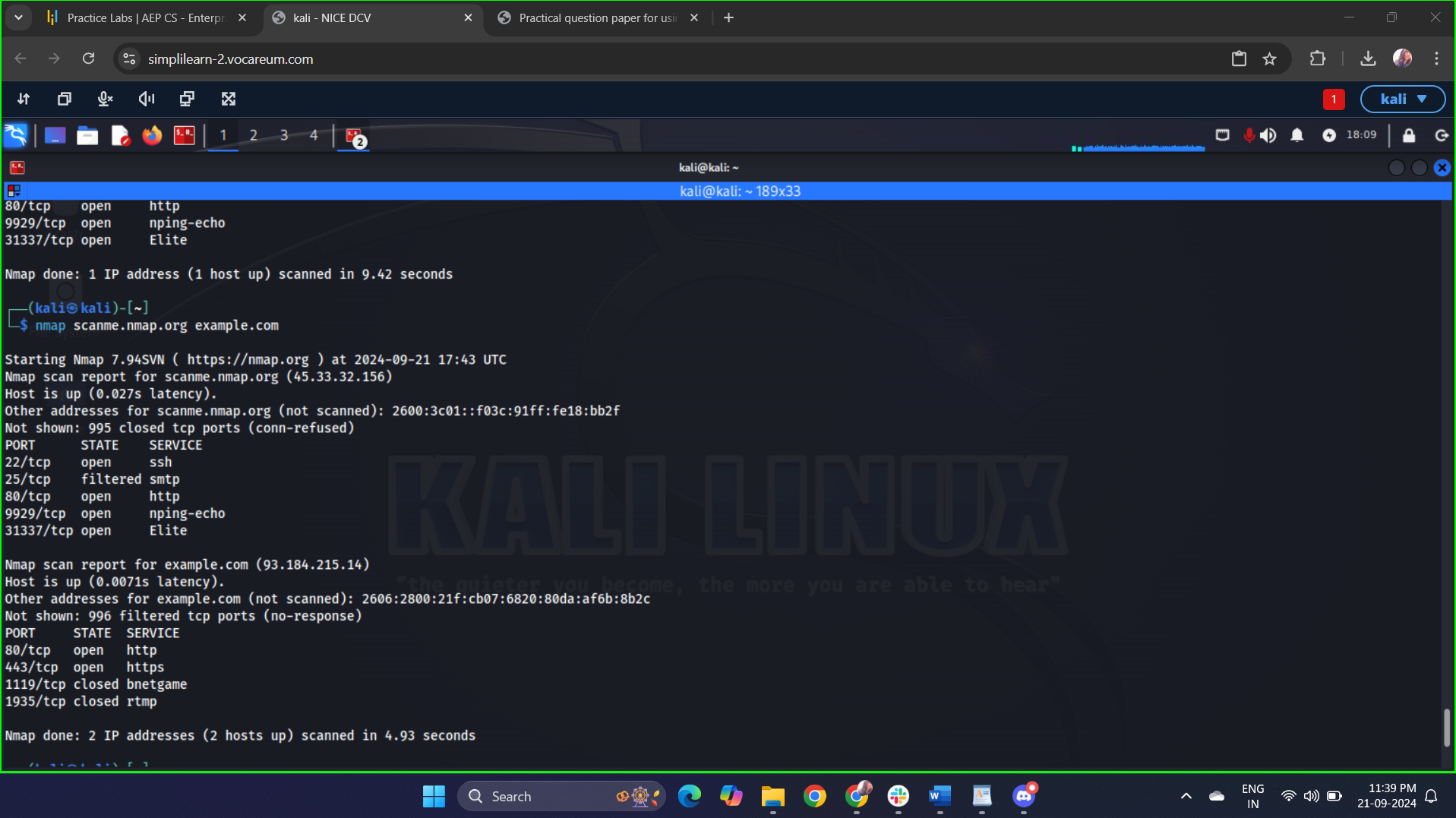
4) Elite (port 31337) might be a demonstration service for educational purposes.

5) SMTP (port 25) is filtered, indicating that access to this port is restricted, possibly for security reasons.

**Task 2**

**Command used**: nmap scanme.nmap.org. example.com

**Output Generated:**



**Conclusion:**

Scan Results:

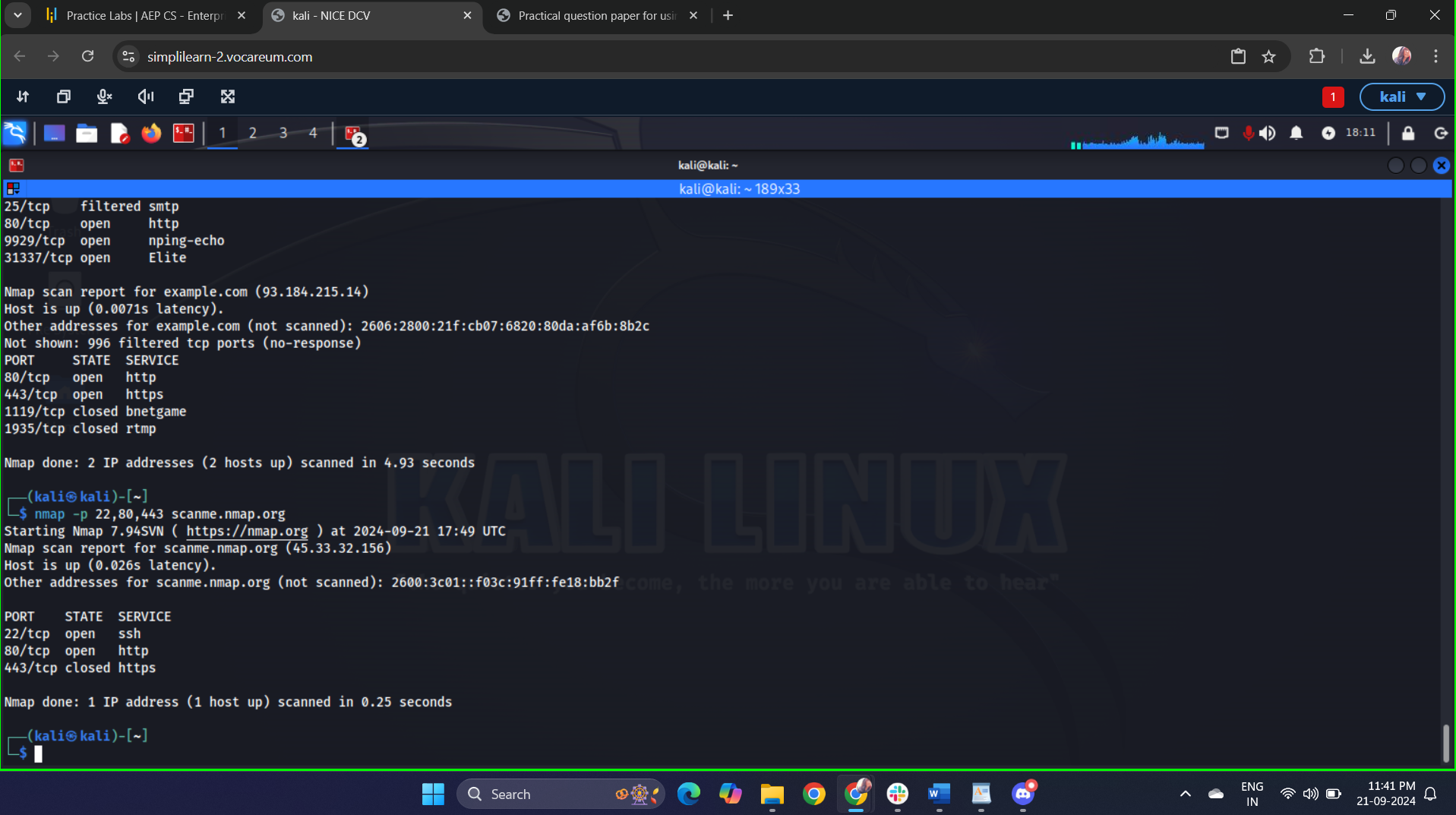
* scanme.nmap.org:
  + Open Ports: (e.g., 22/tcp, 80/tcp)
* example.com:
  + Open Ports: (e.g., 80/tcp, 443/tcp)
* **scanme.nmap.org** has the following open ports: 22 (SSH), 80 (HTTP).
* **Nping- Echo (port 9929)** is part of network testing utilities.
* **Elite (port 31337)** might be a demonstration service for educational purposes.
* **example.com** has the following open ports: 80 (HTTP), 443(HTTPS)
* **80/tcp (HTTP)**: This indicates that the server is running a web service.
* **443/tcp (HTTPS)**: this indicates that example.com is providing a secure web service.
* **Implication**: using HTTPS is essential for securing sensitive data, especially for login forms or payment transactions.

This information can be useful for assessing potential vulnerabilities or for network management tasks.

**Task 3**

**Command used**: nmap -p 22,80,443 scanme.nmap.org

**Output Generated:**



**Conclusion:**

Host Status:

* The host scanme.nmap.org is up and responsive, which is indicated by the latency time.

Specific Port Status:

* 22/tcp (SSH): Open
  + This port is used for secure shell access. Being open means that remote connections to the server via SSH are allowed.
* 80/tcp (HTTP): Open
  + This port is used for standard web traffic. Its status indicates that a web server is running and accessible via unsecured HTTP.
* 443/tcp (HTTPS): Closed
* This means the server is not configured to accept HTTPS connections, possibly indicating that it does not support secure web traffic.
* **Port 22 (SSH)**: Open – The server is accepting SSH connections, which is standard for remote management.
* **Port 80 (HTTP)**: Open – The server is serving web traffic over HTTP, indicating a web application is accessible without encryption.
* **Port 443 (HTTPS)**: Closed – No secure web service is available on this port.

**Task 4**

**Command used**: nmap 192.168.1.1-20

**Output Generated:**



**Conclusion:**

The reason for all the hosts down.

* The devices are indeed powered off or disconnected.
* There is a configuration issue in the network.
* Firewall settings are preventing Nmap from detecting hosts.

**Task 5**

**Command used**: sudo nmap -A -sV -O scanme.nmap.org

**Output Generated:**





**Conclusion:**

**Host Status**:

* The host scanme.nmap.org is up, indicated by the response time.

**Open Ports and Services**:

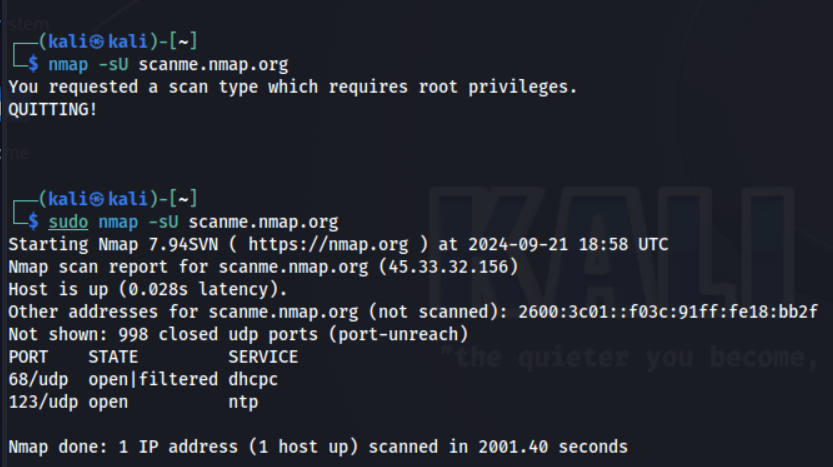
* **Port 22 (SSH)**:
  + State: Open
  + Version: OpenSSH 6.6.1p1(ubuntu)
* **Port 80 (HTTP)**:
  + State: Open
  + Aggressive OS guesses: Linux 2.6.32

**Task 6**

**Command used**: nmap -sU scanme.nmap.org

Sudo nmap -sU scanme.nmap.org

**Output Generated:**



**Conclusion:**

**Open UDP Ports**:

* **Port 68/udp (DHCP Client)**:
  + This port is used by DHCP clients to receive configuration parameters from DHCP servers. An open status typically indicates that the host is set up to receive DHCP offers.
* **Port 123/udp (NTP)**:
  + This port is used by the Network Time Protocol (NTP) for time synchronization between devices. An open status means that the host is likely running an NTP service.

**Task 7**

**Command used**: sudo nmap -O scanme.nmap.org

**Output Generated:**

****

**Conclusion:**

**Host**: scanme.nmap.org is reachable.

**Open Ports**:

* **Port 22**: SSH service (ensure strong authentication and access controls).
* **Port 80**: HTTP service (ensure web applications are secured).
* **Port 9929**: nping-echo (part of network testing utilities).
* **Port 31337**: Potentially sensitive (monitor and secure)

**Task 8**

**Command used**: nmap -sV scanme.nmap.org

**Output Generated:**

****

**Conclusion:**

**Host**: scanme.nmap.org is reachable.

**Open Ports**:

* **Port 22**: OpenSSH 6.6 (protocol 2.0) - ensure strong authentication methods.
* **Port 80**: Apache HTTPD 2.4.7 (Ubuntu) - keep web server software updated to prevent vulnerabilities.
* **Port 9929**: nping echo - part of network testing utilities.
* **Port 31337**: Elite service - potential security risk, monitor closely.

**Task 9**

**Command used**: nmap scanme.nmap.org –script vuln

**Output Generated:**





**Conclusion:**

**Host Status**:

* The host scanme.nmap.org is reachable.

**Open Ports and Services**:

* **Port 22 (SSH)**: OpenSSH 7.4 (protocol 2.0)
* **Port 80 (HTTP)**: Apache HTTPD 2.4.18 (Ubuntu)

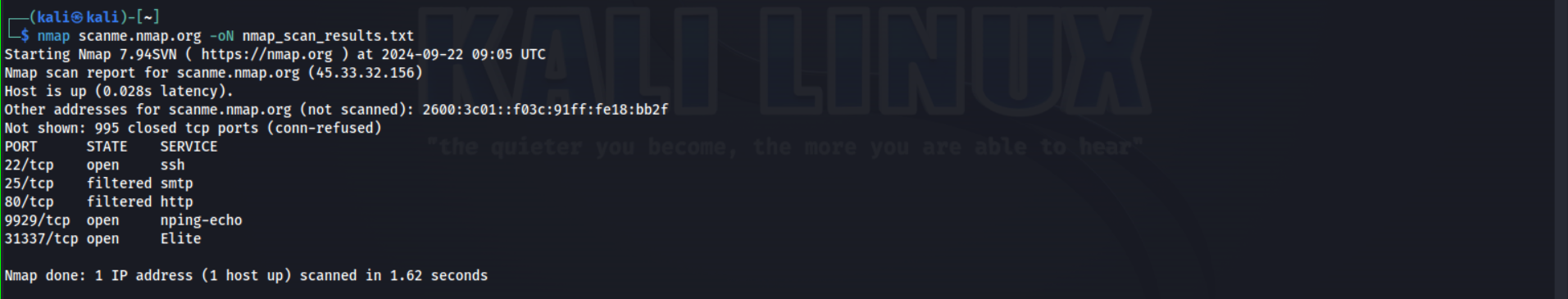
**Vulnerability Findings**:

**Slowloris DOS Attack- likely vulnerable**

**Task 10**

**Command used**: nmap scanme.nmap.org -oN nmap\_scan\_results.txt

**Output Generated:**



**Conclusion:**

nmap: This is the command to invoke the Nmap tool.

scanme.nmap.org: This is the target host you want to scan.

-oN nmap\_scan\_results.txt: This option tells Nmap to output the scan results in a normal format to a file named nmap\_scan\_results.txt.

<nmap_scan_results.txt>

**1. What is the difference between TCP and UDP port scanning?**

- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) port scanning are two types of network scanning techniques used to identify open ports and services running on a target system.

**TCP Port Scanning**: TCP port scanning involves sending TCP packets to a target system to determine which ports are open and listening. Here's how it works:

1. Sender sends a TCP SYN (synchronize) packet to the target system.

2. If the port is open, the target system responds with a SYN-ACK (synchronize-acknowledgment) packet.

3. The sender responds with an ACK (acknowledgment) packet, completing the three-way handshake.

4. If the port is closed, the target system responds with a RST (reset) packet.

Types of TCP scans:

1. Full Connect Scan (TCP SYN scan)

2. Half-Open Scan (TCP SYN scan without completing the handshake)

3. FIN Scan

4. Xmas Scan

5. Null Scan

**UDP Port Scanning:** UDP port scanning involves sending UDP packets to a target system to determine which ports are open and listening. Here's how it works:

1. Sender sends a UDP packet to the target system.

2. If the port is open, the target system may respond with an ICMP (Internet Control Message Protocol) "Port Unreachable" error message (Type 3, Code 3).

3. If the port is closed, the target system responds with an ICMP "Port Unreachable" error message (Type 3, Code 3).

4. Some services may respond with a UDP packet, indicating an open port.TCP vs. UDP Port Scanning:

When to use each:

1. TCP scanning: For services that use TCP, such as HTTP, FTP, SSH.

2. UDP scanning: For services that use UDP, such as DNS, DHCP, SNMP.

The port scanning can be used for malicious purposes, such as reconnaissance for potential attacks. It's essential to use port scanning responsibly and with permission from the target system's owner.

**2. How does Nmap determine the operating system running on a target host?**

- Nmap, a popular network scanning tool, uses various techniques to determine the operating system (OS) running on target hosts. Here's a breakdown of the methods Nmap employs:

**TCP/IP Fingerprinting**: Nmap sends a series of TCP and ICMP packets to the target host, analyzing the responses to identify unique characteristics, such as:

1. TCP Initial Sequence Number (ISN) behavior

2. TCP options (e.g., window scaling, timestamp)

3. TCP flags (e.g., SYN, ACK, RST)

4. ICMP error messages (e.g., TTL exceeded, port unreachable)

5. IP ID and IP header fields

**OS Detection Techniques**

Nmap uses the following techniques to determine the OS:

1. TCP ISN analysis: Examines the ISN increment and behavior.

2. TCP options analysis: Checks for specific options and their ordering.

3. TCP timestamp analysis: Examines the timestamp option.

4. IP ID analysis: Analyzes the IP ID field behavior.

5. ICMP analysis: Examines ICMP error messages and behavior.

6. Port scanning: Identifies open ports and services, which can indicate OS-specific characteristics.

7. DNS query analysis: Analyzes DNS query responses.

**Nmap OS Detection Phases**

Nmap's OS detection process involves two phases:

Phase 1: Probe scanning

1. Send TCP and ICMP probes to gather information.

2. Analyze responses to determine potential OS matches.

Phase 2: OS classification

1. Compare gathered information with Nmap's OS database.

2. Assign a confidence level to each potential OS match.

3. Select the most likely OS match based on confidence levels.

Nmap OS Database

Nmap maintains an extensive database of known OS fingerprints, which is regularly updated. This database contains information on various OS versions, including:

1. Windows

2. Linux

3. macOS

4. FreeBSD

5. Solaris

6. AIX

7. HP-UX

8. Others

**3. Why is it important to perform a vulnerability scan on target hosts?**

-Performing vulnerability scans on target hosts is crucial for identifying and addressing potential security weaknesses. Here are reasons why:

Benefits:

1. Identifies known vulnerabilities: Scans detect known vulnerabilities, allowing for timely patching and remediation.

2. Reduces attack surface: Vulnerability scans help eliminate exposure to potential attacks.

3. Enhances security posture: Regular scans ensure ongoing security monitoring and improvement.

4. Compliance: Meets regulatory requirements (e.g., PCI DSS, HIPAA).

5. Risk assessment: Informs risk management decisions.

6. Prioritization: Helps focus remediation efforts on critical vulnerabilities.

7. Cost-effective: Proactive vulnerability management saves resources.

Types of Vulnerabilities Detected:

1. Unpatched software

2. Misconfigured systems

3. Default passwords

4. SQL injection flaws

5. Cross-site scripting (XSS)

6. Buffer overflow vulnerabilities

7. Authentication weaknesses

Vulnerability Scan Types:

1. Network-based scans (e.g., Nmap, Nessus)

2. Host-based scans (e.g., OS-specific tools)

3. Web application scans (e.g., OWASP ZAP)

4. Database scans

5. Wireless network scans

Performing vulnerability scans is essential for maintaining robust security and protecting against potential threats.

**4. What are the potential risks associated with aggressive scanning?**

-Aggressive scanning can pose several potential risks:

Network and System Risks:

1. System crashes or instability

2. Network congestion or slowdown

3. Overwhelming logging and monitoring systems

4. Resource exhaustion (CPU, memory, bandwidth)

5. Disruption of critical services or applications

6. Data corruption or loss

Security Risks:

1. Triggering intrusion detection/prevention systems (IDS/IPS)

2. Alerting malicious actors to scanning activity

3. Potential exploitation of scanned vulnerabilities

4. Increased likelihood of false positives/negatives

5. Unintentional disclosure of sensitive information

Compliance and Regulatory Risks:

1. Violation of organization's security policies

2. Non-compliance with regulatory requirements (e.g., PCI DSS)

3. Potential legal liabilities

Reputation and Relationship Risks:

1. Damage to organization's reputation

2. Strained relationships with network/service providers

3. Potential loss of business or revenue

Other Risks:

1. Unintended scanning of sensitive areas (e.g., military, government)

2. Scanning of unauthorized networks or systems

3. Inadvertent participation in distributed denial-of-service (DDoS) attacks

Aggressive Scanning Techniques:

1. Fast scanning (high packet send rate)

2. Multiple simultaneous scans

3. Deep packet inspection

4. SYN flood scanning

5. UDP bombing

Best Practices:

1. Conduct scanning with clear objectives

2. Choose appropriate scanning tools and techniques

3. Configure scanning parameters carefully

4. Monitor and analyze scan results

5. Document scanning activities and results

To minimize risks, it's essential to adopt responsible scanning practices, ensure proper authorization, and consider potential consequences.

**5. How can Nmap scan results be useful for network administrators in securing their networks?**

**-**Nmap scan results provide valuable information for network administrators to secure their networks. Here's how:

Identify:

1. Open ports and services: Detect potential entry points for attackers.

2. Operating systems and devices: Identify OS versions, device types, and potential vulnerabilities.

3. Network layout and topology: Understand network structure, including subnets, VLANs, and routing.

Vulnerability Management:

1. Detect known vulnerabilities: Identify exploitable flaws in software and services.

2. Prioritize remediation: Focus on critical vulnerabilities and patch or mitigate accordingly.

3. Monitor for changes: Regular scans detect new vulnerabilities and track remediation progress.

Security Configuration:

1. Identify misconfigured systems: Detect deviations from secure configuration standards.

2. Optimize firewall rules: Refine rules based on scan results to ensure only necessary ports are open.

3. Enhance access control: Restrict access to sensitive areas and services.

Compliance and Auditing:

1. Meet regulatory requirements: Use Nmap to demonstrate compliance with standards like PCI DSS, HIPAA.

2. Conduct regular audits: Verify security controls and identify areas for improvement.

Incident Response:

1. Detect unauthorized devices: Identify unknown devices connected to the network.

2. Investigate suspicious activity: Analyze scan results to identify potential security breaches.

3. Contain and respond: Use scan results to inform incident response strategies.

Network Optimization:

1. Improve network segmentation: Segment networks based on scan results to reduce attack surfaces.

2. Optimize network performance: Identify bandwidth-hungry services and optimize network configuration.

3. Streamline network services: Remove unnecessary services and protocols.

Nmap Output Formats:

1. XML: Easily parseable for automation and integration.

2. CSV: Importable into spreadsheets for analysis.

3. Text: Human-readable for quick review.

Integration with Other Tools:

1. Vulnerability scanners (e.g., Nessus, OpenVAS)

2. Incident response platforms (e.g., Splunk, ELK)

3. Configuration management tools (e.g., Ansible, Puppet)

Best Practices:

1. Regularly schedule scans

2. Use Nmap scripts for customized scanning

3. Integrate Nmap with other security tools

4. Analyze and act on scan results

5. Document scanning activities and results

By leveraging Nmap scan results, network administrators can:

1. Strengthen network security

2. Improve compliance

3. Optimize network performance

4. Enhance incident response

5. Reduce risk