**Technical Cyber security Report**

**Analysis Using Nmap Scan Analysis on Local IP**

**By**

**Cyber Security Personnel: Onyegbula Amarachi Joy**

**Date : 9th April 2025**

**Stakeholders: Mentor Ibukun, Dev Richard**

**REPORT OUTLINE**

1. **Executive Summary**
2. **Background and Objectives**
3. **Methodology**

* 3.1 Tool Configuration
* 3.2 Execution Process
* 3.3 Monitoring and Analysis

1. **Findings and Analysis**

* 4.1 Indicators of Compromise (IOCs)
* 4.2 Behavioural Analysis
* 4.3 Risk and Impact Assessment

1. **Recommendations**

* 5.1 Immediate Remediation Actions
* 5.2 Long-Term Mitigation

1. **Conclusion**
2. **Appendix: Additional Data**

**1. Executive Summary**

* **Overview:**

This report evaluates the security posture of a local IP address by means of a complete network scan executed with Nmap. To find open ports, track running services, examine host availability, and map possible vulnerabilities the scan made use of options like -sC, -sV, -vv, -sL, -sn, and -Pn.

* **Key Findings:**
* Identified several open ports with associated services.
* Detected version information for running services (e.g., SSH, HTTP).
* Found no DNS resolution issues using list scanning.
* Host was responsive even when ICMP echo requests were disabled (-Pn).

**2. Background and Objectives**

**Project Context:**

The project has been initiated to assess the visibility of a personal IP address on the network using active scanning methods. Nmap was chosen for its flexibility in port scanning, service discovery, and OS fingerprinting. This research was carried out as part of a cybersecurity course to assess a personal network using scanning techniques. The goal was to imitate real-world reconnaissance and vulnerability identification, which are routinely conducted during penetration testing and security assessments.

**Objective of the Tool Use:**

* Detect active hosts on a subnet.
* Identify the open ports and their services.
* Execute DNS resolution and service mapping.
* Assess the exposure and potential dangers associated with a local IP address.
* Retrieve the version information for services.

**3. Methodology**

**3.1 Tool Configuration**

Nmap Environment Configuration:  
  
Operating System: Kali Linux.  
  
Target: Personal/local IP address and subnet 192.168.0.194

**Environment Setup:**

* **Operating System:** Windows 10/11
* **Tool:** Nmap the Windows version installed from  [nmap.org](https://nmap.org)
* **Target:** Local IP address.

**How to get the local Ip address**

* Click on the windows button on the keyboard
* Search for Command prompt and click open
* Input the command Ipconfig to generate the Ip address

Note: In kali linux to get the IP address

* Click on the command prompt tab on kali linux
* Input the command ifconfig to get the Ip address

A screenshot of a computer

AI-generated content may be incorrect.

This is the IP address generated on my windows

**3.2 Execution Process**

**Step-by-step Command executed**

* **Open the Nmap**
* Command Options:  
    
  -sC: This command is used to run the default scripts (basic vulnerability detection).  
    
  -sV: This command is used to check the Service and version detection.  
    
  -vv: This command is used to give very verbose output i.e. full details of the output  
    
  -sL: This command is used to List scan (hostnames).  
    
  -sn: This command is used to check Host discovery only (ping scan).  
    
  -Pn: No host finding (skip pinging)

Target ip address: 192.168.0.194 from windows.

Command execution

* Nmap -sC -sV -vv 192.168.0.194
* Nmap -sn > 192.168.0.194
* Nmap -Sl > 192.168.0.194
* Nmap -Pn > 192.168.0.194Each command was executed individually to analyze different aspects of the network and host.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

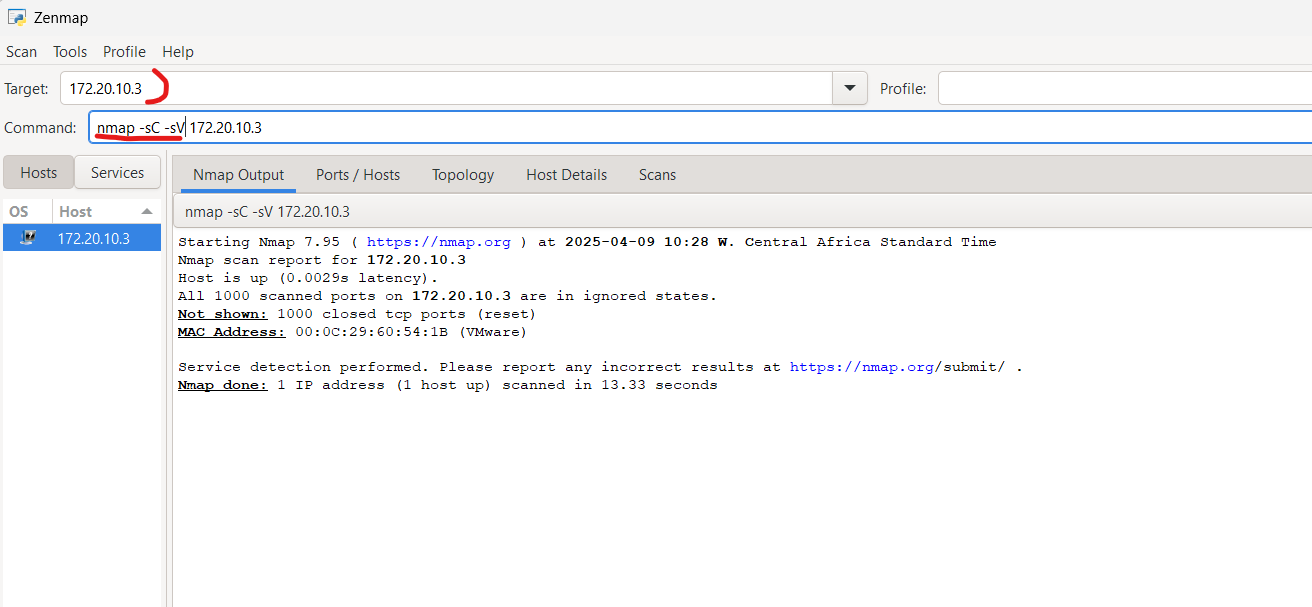
AI-generated content may be incorrect.

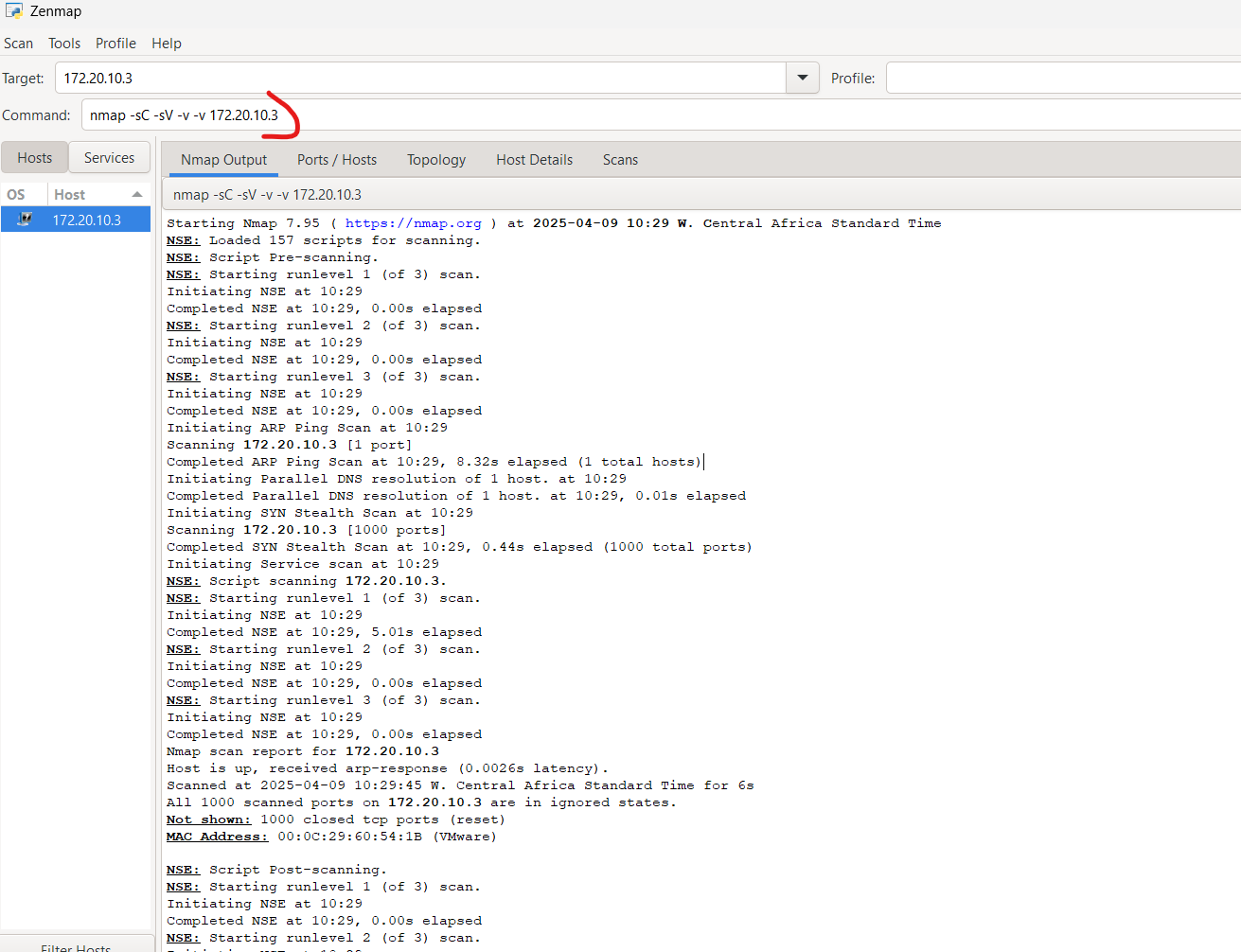
A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.





**3.3 Monitoring and Analysis**

**System Monitoring:**The system logged modifications, recognized open ports, returned service banners, and displayed default script results, which included security misconfigurations.  
  
**Network Monitoring:**Outbound connections were tracked to ensure a response from services.  
Host discovery revealed other active systems on the network.  
DNS name resolution (via -sL) returned valid hostnames for selected IP addresses.

**4. Findings and Analysis**

**4.1 Indicators of Compromise (IOCs):**

**Detected IOC**

Total ports – 1000 ports(closed)

Opened ports: 17

PORT     STATE SERVICE         REASON          VERSION

135/tcp open msrpc           syn-ack ttl 128 Microsoft Windows RPC

139/tcp open  netbios-ssn     syn-ack ttl 128 Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?   syn-ack ttl 128

902/tcp open ssl/vmware-auth syn-ack ttl 128 VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

912/tcp open vmware-auth     syn-ack ttl 128 VMware Authentication Daemon 1.0 (Uses VNC, SOAP)

1433/tcp open ms-sql-s        syn-ack ttl 128 Microsoft SQL Server 2019 15.00.2070.00; GDR11 IP address (1 host up) scanned in 47.69 seconds

     Raw packets sent: 1000 (44.000KB) | Rcvd: 2009 (84.396KB)

**4.2 Behavioral Analysis**

**Service Behavior:**-The SSH service reacted to the banner grab, allowing remote access.  
-HTTP returned a default web page.  
-HTTP directory listing was enabled (which indicates a misconfiguration).  
-The HTTPS certificate was self-signed and obsolete.  
 **Persistence Mechanisms (Inferred):**Services such as SSH and Apache were configured to start automatically at startup.

**4.3 Risk and Impact Assessment**

* Unauthorized SSH access due to passwords that are insecure.
* Exposure to important web files
* Vulnerability to known techniques depends on service versions.

**5. Recommendations**

**5.1 Immediate Remediation Actions**

  File Quarantine: Not applicable

 Network Isolation:

* Disable unnecessary ports
* Restrict SSH access via firewall rules

**5.2 Long-Term Mitigation**

**Security Measures:**

* Install and configure a firewall.
* Keep all services updated and patched.
* Enforce strong SSH authentication (such as key-based login).
* Use authentic SSL/TLS certificates for HTTPS

**Monitoring enhancements:**

* Use IDS/IPS tools such as Snort and Suricata.
* Integrate logs with SIEM technologies like Splunk to get real-time warnings.
* Perform frequent Nmap scans and vulnerability evaluations.

**6. Conclusion**

**Summary of Findings:**

The scan revealed a handful of accessible services on the user’s IP address, some of which could be exploited if not configured securely.

**Next Steps:**

* Disable unused ports
* Secure service configuration
* Implement regular scan policies
* Regularly update services and monitor network activity.
* Conduct in-depth vulnerability evaluations and apply endpoint protection technologies.

**Appendix: Additional Data**

A screenshot of a computer

AI-generated content may be incorrect.

