Tab 1

**SCHOOL OF CYBERSECURITY**

NAME: OBASI CHARLES CHIDOZIE

ID: VEPH/20B/CY053

TASK: TASK 20C (LESSON 20)

# 

# **Technical Cyber security Report**

# 

# **Analysis Using Nmap for a Networkscan on a target system’s IP address, incorporating the -sC, -sV, -vv, -sL, -sn, and -Pn options.**

# 

# 

# **By**

# **Cyber Security Personnel : OBASI CHARLES CHIDOZIE**

**Date : 09/04/2025**

**Stakeholders : Vephla Security Team**

**REPORT OUTLINE**

Outline of all pages within technical report

1. Executive Summary

* Brief overview of the entire report
* Key findings and recommendations

1. Background and purpose

* Scope/aim & Objectives of the report
* Objectives of tools used ( Nmap)

1. Methodology

* Step-by-step process followed
* Command-line options used (**-sC, -sV, -vv, -sL, -sn, and -Pn**)
* Tools configuration and execution

1. Findings and Analysis

* Behavioral Analysis
* Observations during scanning
* Risk and Impact Assessment
* Potential impacts on systems or networks

1. Recommendations

* Immediate Remediation Actions
* Mitigation Strategies

1. Conclusion

* Summary of findings

## 

## 

## 

## **1. Executive Summary**

* **Overview:**
  + The analysis with Nmap was conducted as part of an investigation to assess the behavior of a network to identify possible vulnerabilities and exploitations found during a routine security scan in the target systems network. The tool successfully provided insights into system modifications, network activity, and potential indicators of compromise, allowing the incident response team to take immediate action. The tool was used to scan the target system IP address and ports in the network utilizing Nmap with the **-sC, -sV, -vv, -sL, -sn, and -Pn**.
  + -sC command is to verify scripts running in the IP address if it pass through host and networks
  + -sV command checks for the version of service running through the ports.
  + -vv command gives a well detailed report on the IP address.
  + -sL command lists out all target hosts in the subnet without scanning.
  + -sn command disables port scanning
  + -Pn command disables host discovery.

* **Key Findings:**
  + The Nmap scan detected a total of 9 open ports along with services that delivered important security information regarding the target system flaws. The assessment revealed essential information about particular services along with their version and identities that might aid vulnerability assessments and proper threat detection.

## 

## **2. Background and Objectives**

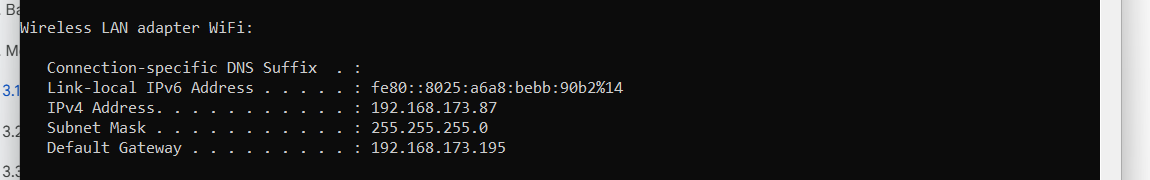
* **Project Context:**
  + The project aimed to assess the security posture of the network and to detect and identify vulnerabilities in the target system. Nmap was employed as a tool to scan the IP address and identify open ports in a network.
  + Determine service versions to match with known vulnerabilities.
  + Run default scripts to scan for possible vulnerabilities.
  + List out all target hosts in the subnet without scanning
  + Disable port scanning
* **Objective of the Tool Use:**
  + Nmap was utilized to detect and identify vulnerabilities in the target systems network. The tool was used to scan the target system IP address and ports in the target system network utilizing Nmap with the **-sC, -sV, -vv, -sL, -sn, and -Pn** options.

## **3. Methodology**

### **3.1 Tool Configuration**

* **Nmap Configuration:**
  + Open Nmap on your windows
  + Navigate to command prompt to get the IP address using the command> ipconfig
  + Go to the nmap and use the command **-sC, -sV, -vv, -sL, -sn, and -Pn** options to run nmap default service script,versions, and disable port.
* **Environment Configuration:**

**Target: Local IP address> 192.168.171.87**



### **3.2 Execution Process**

**Step-by-step Command executed**

* **Lunch the Nmap**
* Incorporating the Command Options below:  
  **-sC**: This command is to verify scripts running in the IP address if it passes through hosts and networks (basic vulnerability detection).  
  **-sV**: This Command checks for the version of service running through the ports.  
  **-vv**: This command gives a well detailed report on the IP address  
  **-sL**: This command lists out all target hosts in the subnet without scanning (hostnames).  
  **-sn**: This command is used to check Host discovery only (ping scan).  
  **-Pn**: This command disables host discovery (skip pinging)

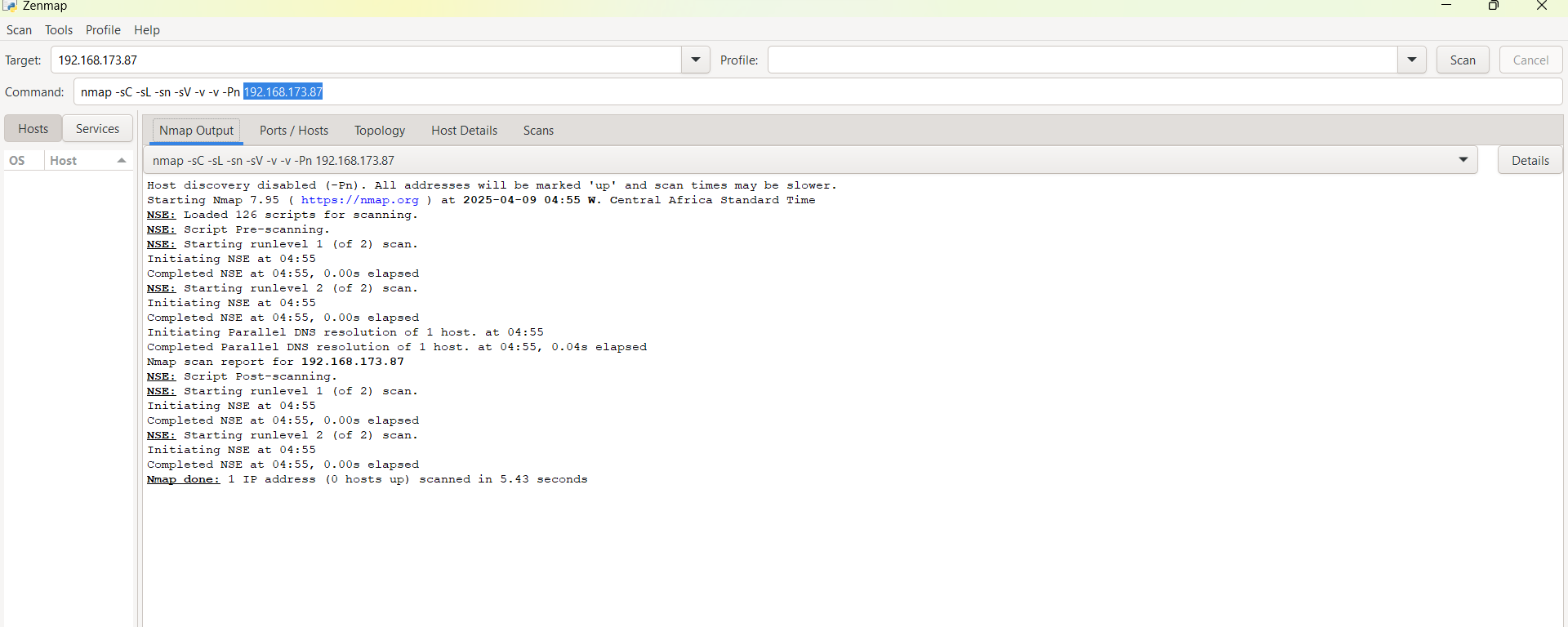
**Target ip address: 192.168.171.87**

Command execution:

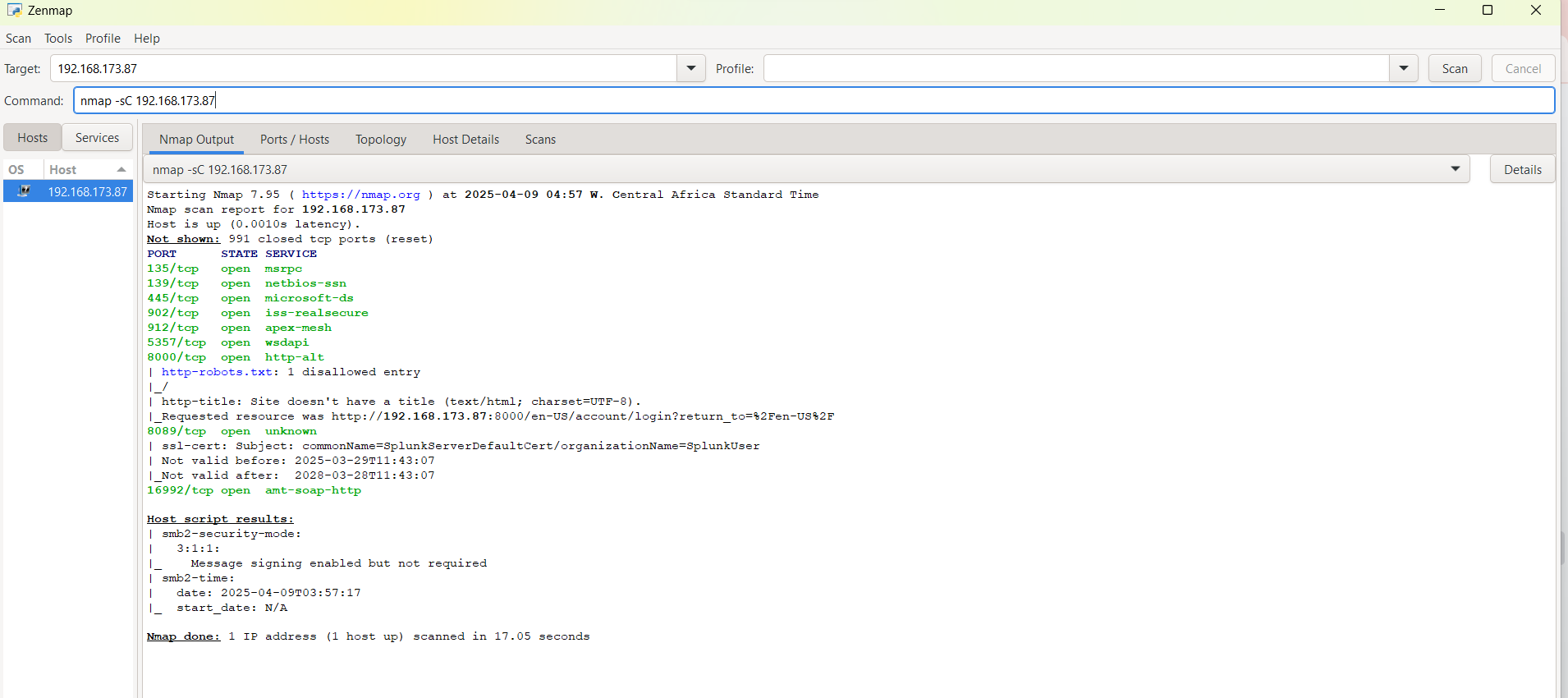
* Nmap **-sC -sV -vv -sL -sn -Pn** 192.168.171.87
* Nmap **-sC** 192.168.171.87
* Nmap **-sV** 192.168.171.87
* Nmap **-vv** 192.168.171.87
* Nmap **-sL** 192.168.171.87
* Nmap **-sn** 192.168.171.87
* Nmap **-Pn** 192.168.171.87

Each command was executed individually to analyze different aspects of the network and host.

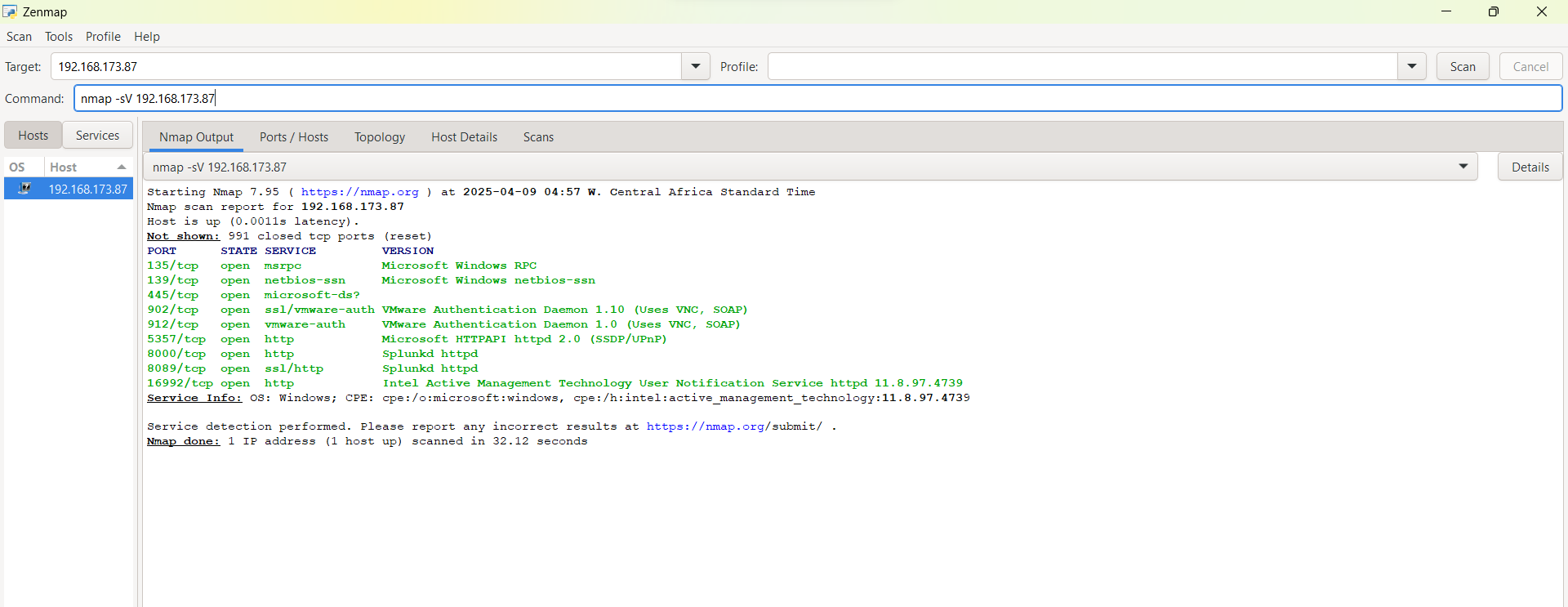
Nmap **-sC -sV -vv -sL -sn -Pn** 192.168.171.87

****

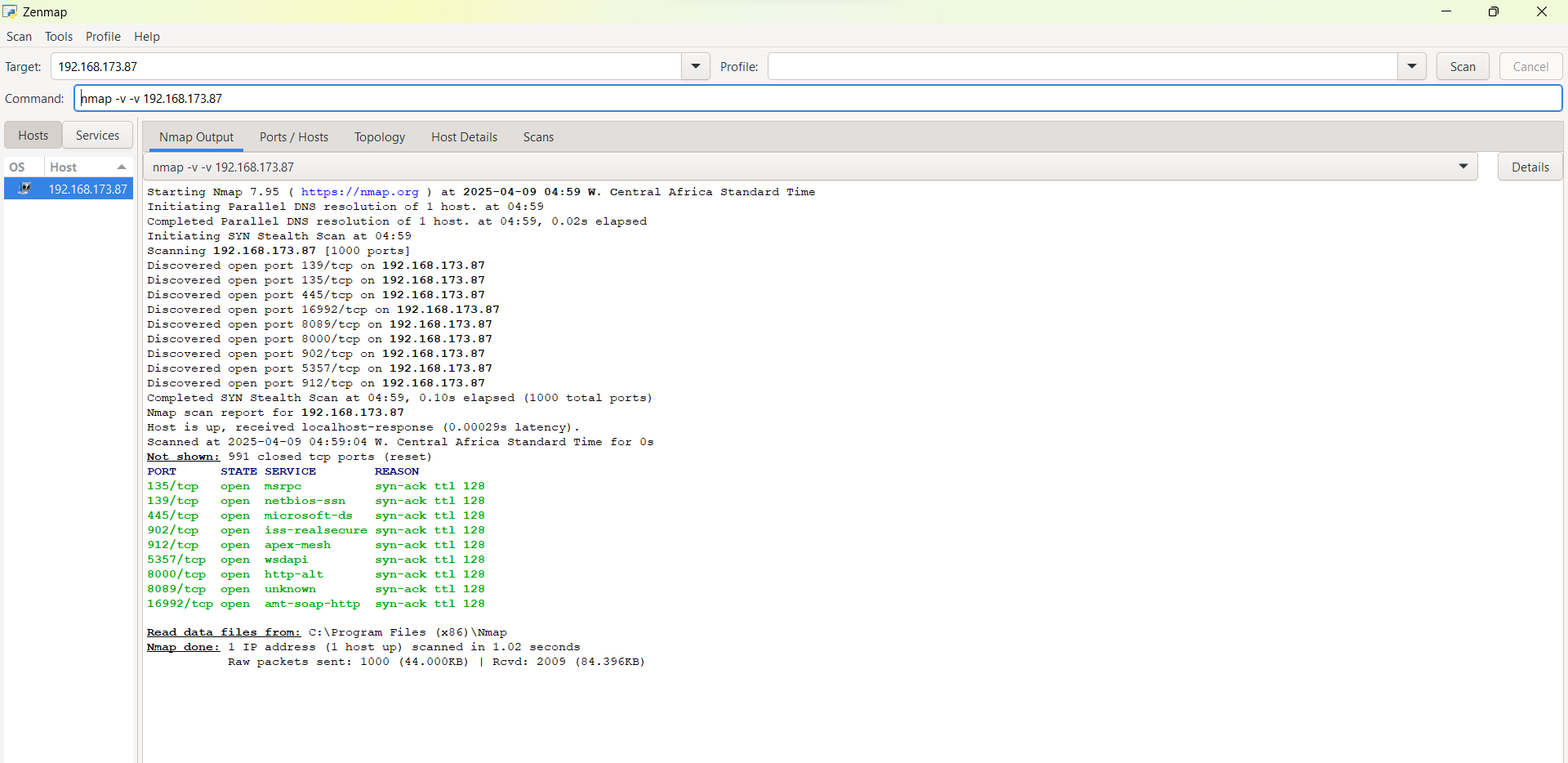
Nmap **-sC** 192.168.171.87



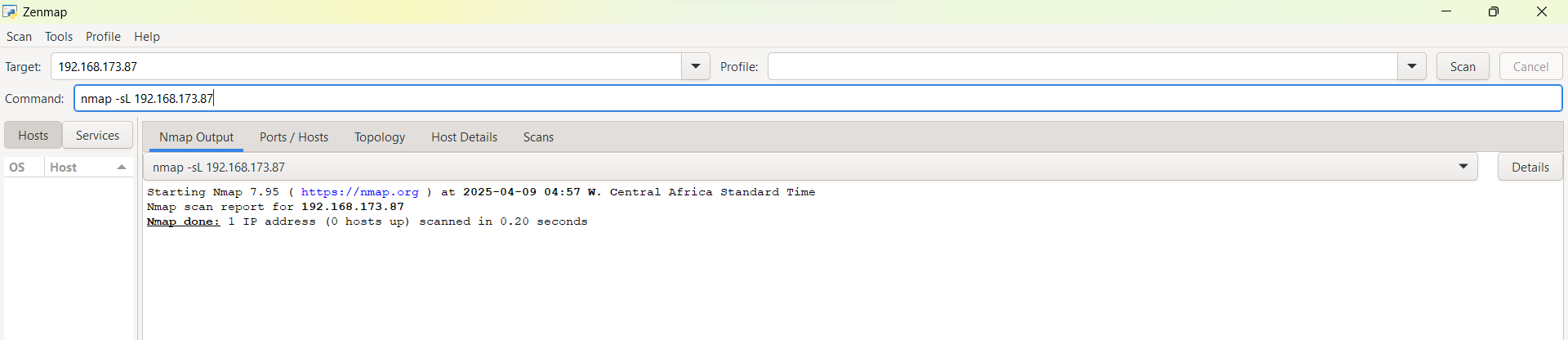
Nmap **-sV** 192.168.171.87



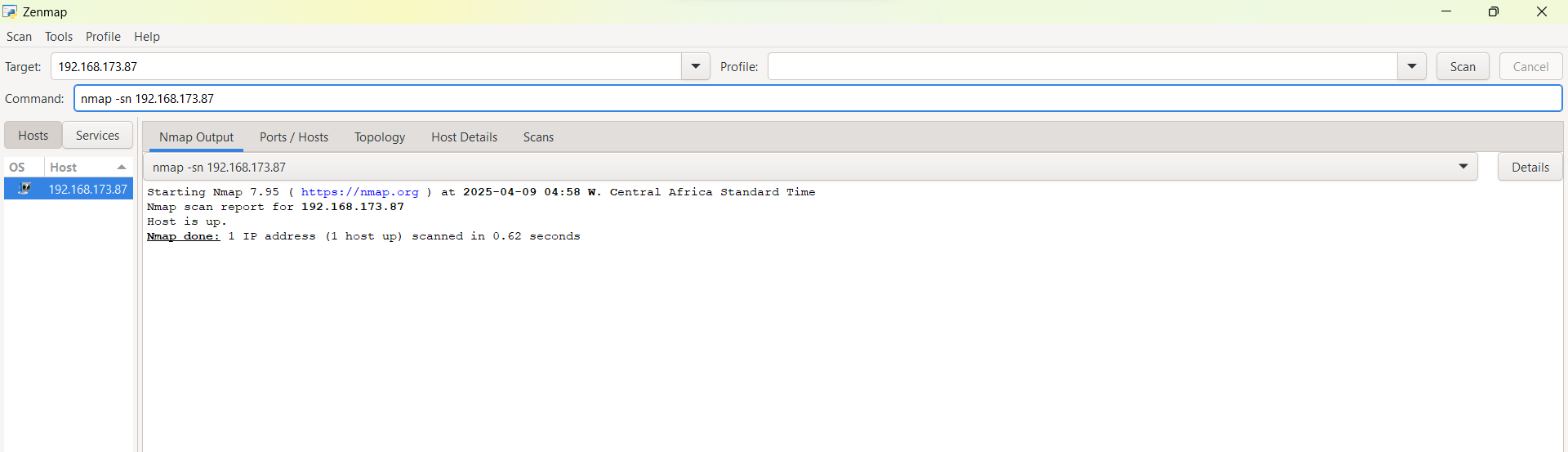
Nmap **-vv** 192.168.171.87



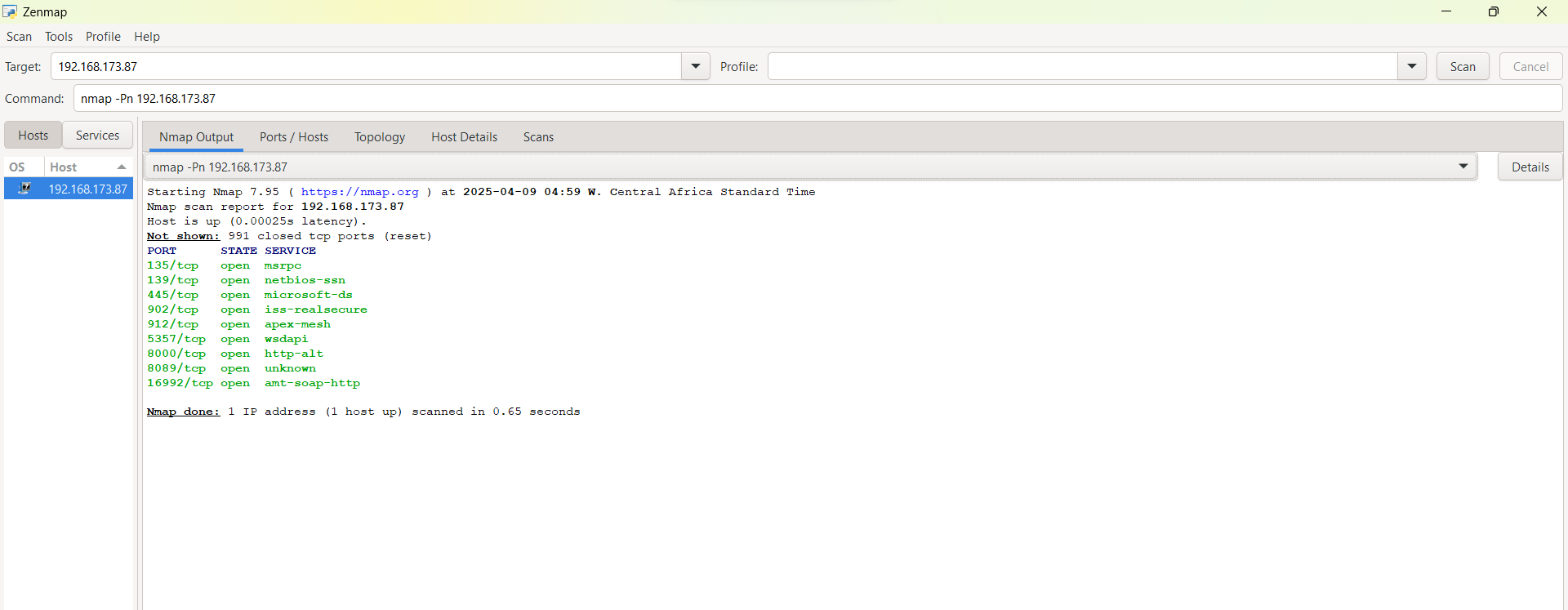
Nmap **-sL** 192.168.171.87



Nmap **-sn** 192.168.171.87



Nmap **-Pn** 192.168.171.87



### **3.3 Monitoring and Analysis:**

* **System Monitoring:**
* The scan revealed real-time system status including port availability and active services.
* Host detection and service enumeration were successful despite skipping ping-based host discovery.
* Nmap obtained TCP responses, indicating open ports and services.
* Scripts (-sC) scanned services for possible vulnerabilities, such as weak configurations in SMB or HTTP.
* **Network Monitoring:**
* Network behavior on the target system was observed through the open ports, some of which were http and ssl-enabled services.

## **4. Findings and Analysis**

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

* IP ADDRESS 192.168.171.87

PORT STATE SERVICE

135/tcp open msrpo

139/tcp open netbios-ssn

445/tcp open microsoft-ds?

902/tcp open ssl/vmware-auth

912/tcp open vmware-auth

5357/tcp open http

8000/tcp open http

8089/tcp open ssl/http

16992/tcp open http

**Include Image:** Screenshot of IOCs identified in the sandbox environment.

### 

### 

### **4.2 Behavioral Analysis:**

* The scan detected several services running over TCP.
* **Persistence Mechanisms:**No direct persistence mechanisms were observed.

### **4.3 Risk and Impact Assessment:**

* **Potential Impact:**  
  The presence of multiple open ports suggests a high risk of exploitation if these services are not secured. The VMware authentication ports may indicate exposed virtualization infrastructure, which can be exploited by attackers.
* System compromise, Denial of service(DoS), Unauthorized access to files and printers, Data exfiltration, Brute-force login attempts, exploitation, and tampering with security logs, hindering incident response.

## **5. Recommendations**

### **5.1 Immediate Remediation Actions:**

* Audit and validate the necessity of open ports and running services
* Restrict access to open ports to reduce risk of exploitation
* All systems operated through these ports should maintain absolute compliance with the latest critical security vulnerability updates.
* **Network Isolation:**
* Only approved networks and IP addresses should have permission to access ports 902 and 912 (VMware) and 8089 (Splunk).

### **5.2 Long-Term Mitigation:**

* **Security Measures:**
* Regular system security training should be done to teach analysts about security risks through the open ports and how to protect systems from malware and phishing attacks which can result in system compromise.
* Organizations should use Endpoint Detection and Response (EDR) solutions for their endpoints to gain sophisticated threat detection and response functionalities. The deployment of EDR solutions allows for the detection and blocking of potential attacks that would try to exploit these ports.
* **Monitoring and Detection Enhancements:**
* The implementation of Intrusion Detection Systems (IDS) to monitor suspicious activities should receive focus on these ports. The IDS needs to detect potential malicious events through excessive connection attempts, anomalous traffic patterns and exploitation attempts.
* Organizations should perform systematic vulnerability scans which determine and solve possible weaknesses within their system and applications infrastructure.
* Programs for port monitoring alongside extensive logging ensure the tracking of every interaction at these ports. Log analysis should begin with improper pattern detection and ongoing investigation into all irregular activities.

## **6. Conclusion**

* **Summary of Findings:**The scan indicated the target systems’ IP address 192.168.171.87 was active and running. A total of 9 ports were identified as open, with a total of 991 closed ports. Also running services such as MSRPC, netbios-ssn and microsoft-ds were identified. The scan identified several vulnerabilities such as open ports that could be exploited if not adequately secured.
* **Next Steps:**
* Conduct regular security audits and system checks.
* Confine open ports to specific segments.

## **Appendix: Additional Data**