# Project Report: Vulnerability Assessment and Penetration Testing

Done by: Sanjana Inchalmath

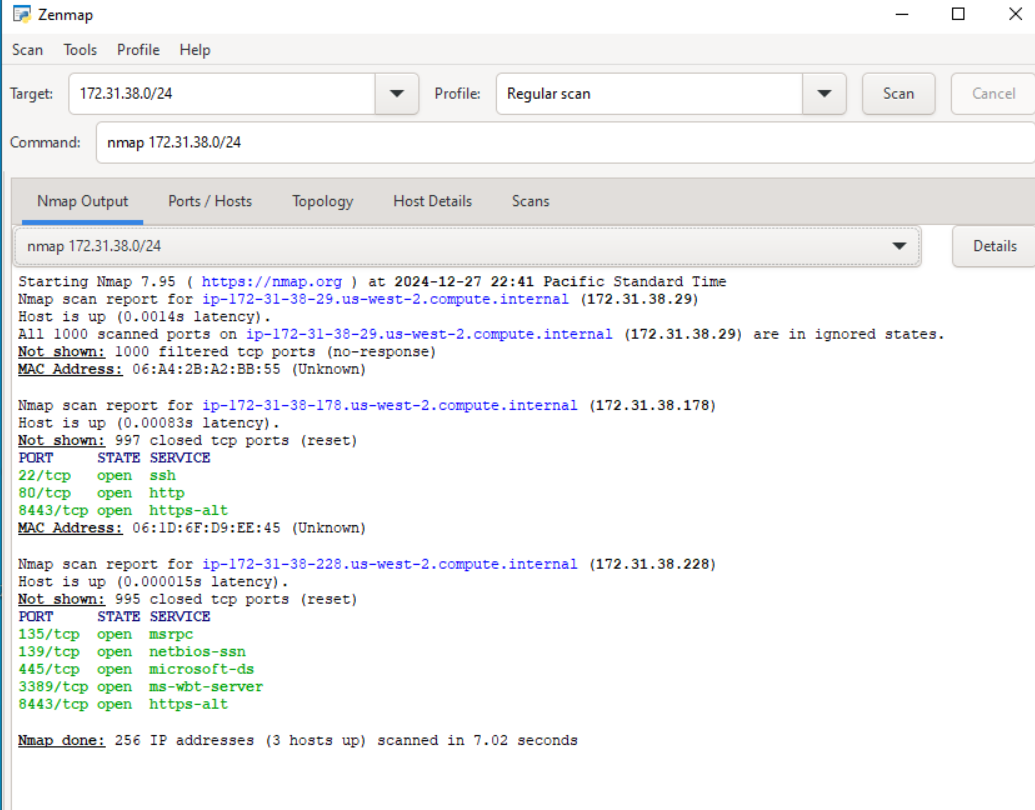
## Introduction

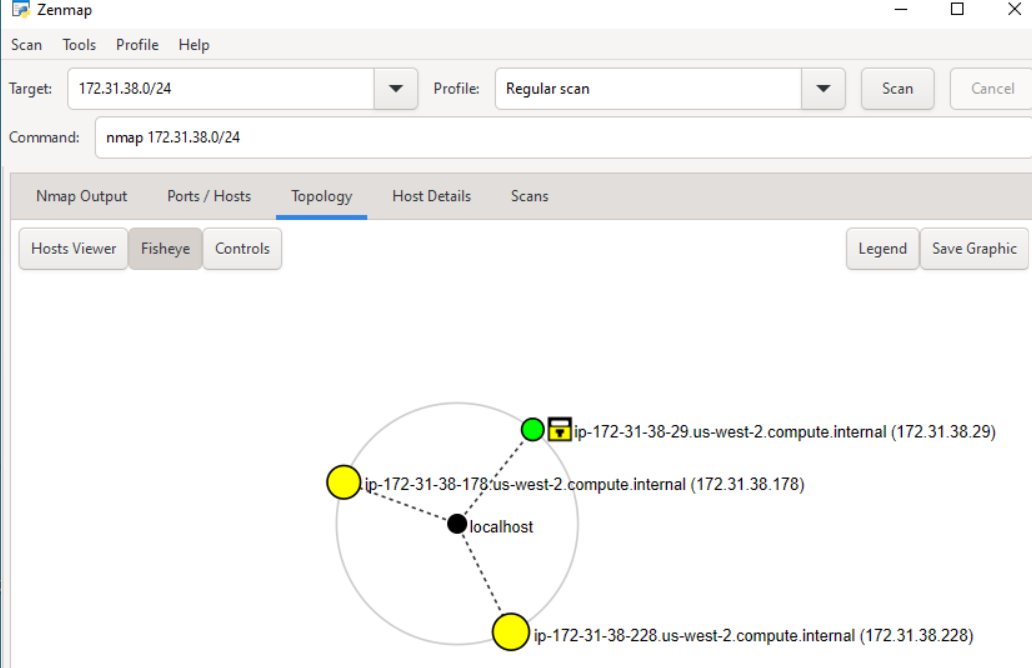
This document contains findings and actions performed during the Vulnerability Assessment (VA) and Penetration Testing (PT) of the Windows and Kali Linux systems. It includes commands, outputs, and screenshots to demonstrate the findings and exploitation evidence.

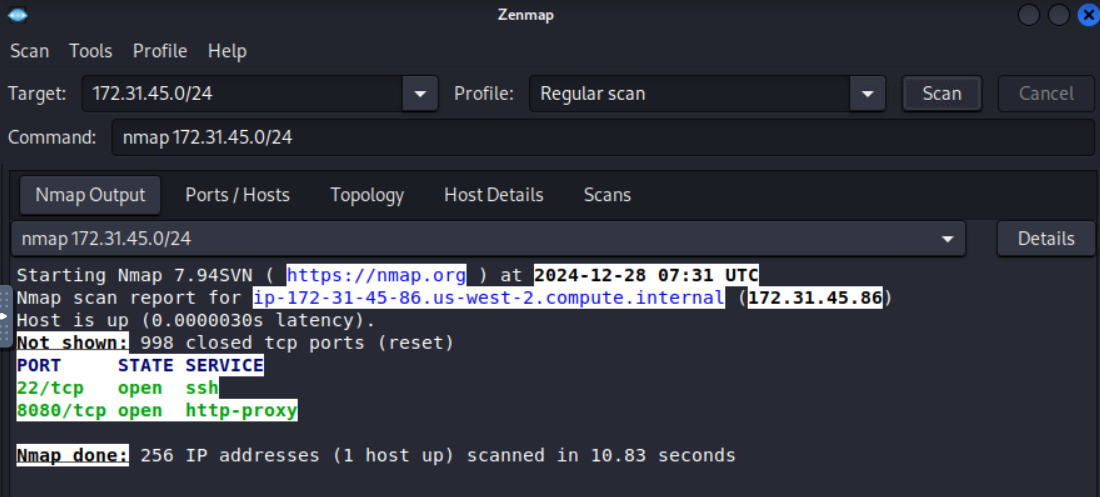
## Phase 1: Information Gathering and Reconnaissance

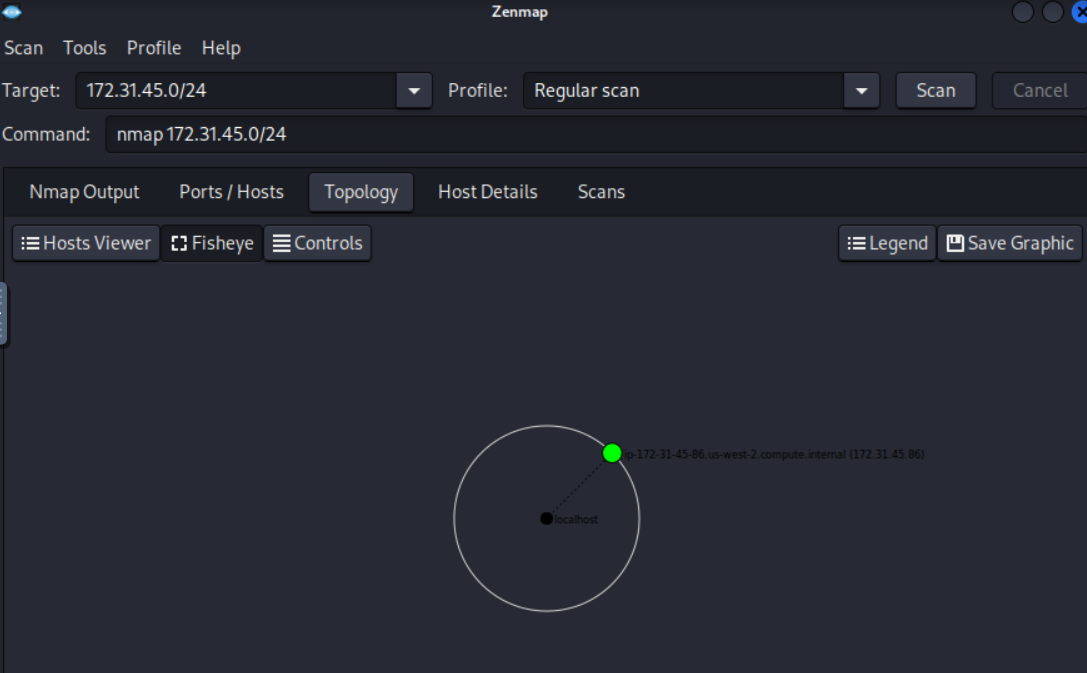
In this phase, information about the target systems was collected to identify potential entry points.

**Commands Executed**:  
1. Nmap Scan  
 - Identified two active systems:  
 - 172.31.38.228 (Windows 10)



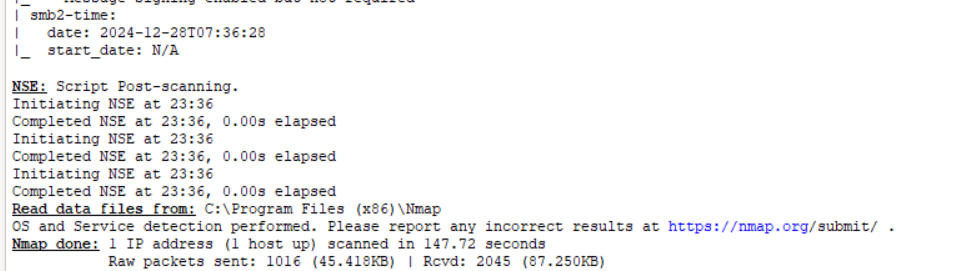
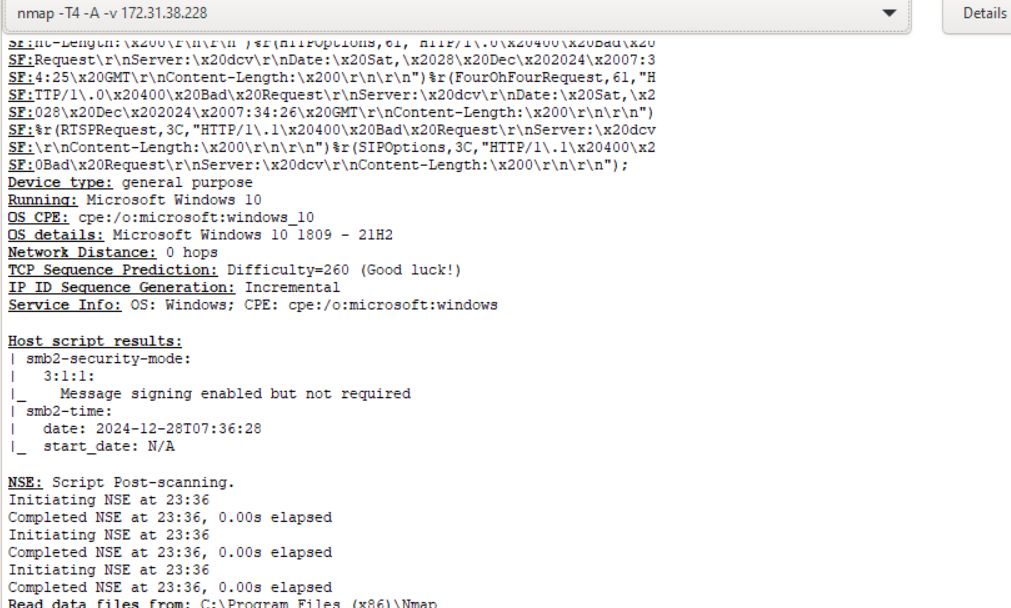
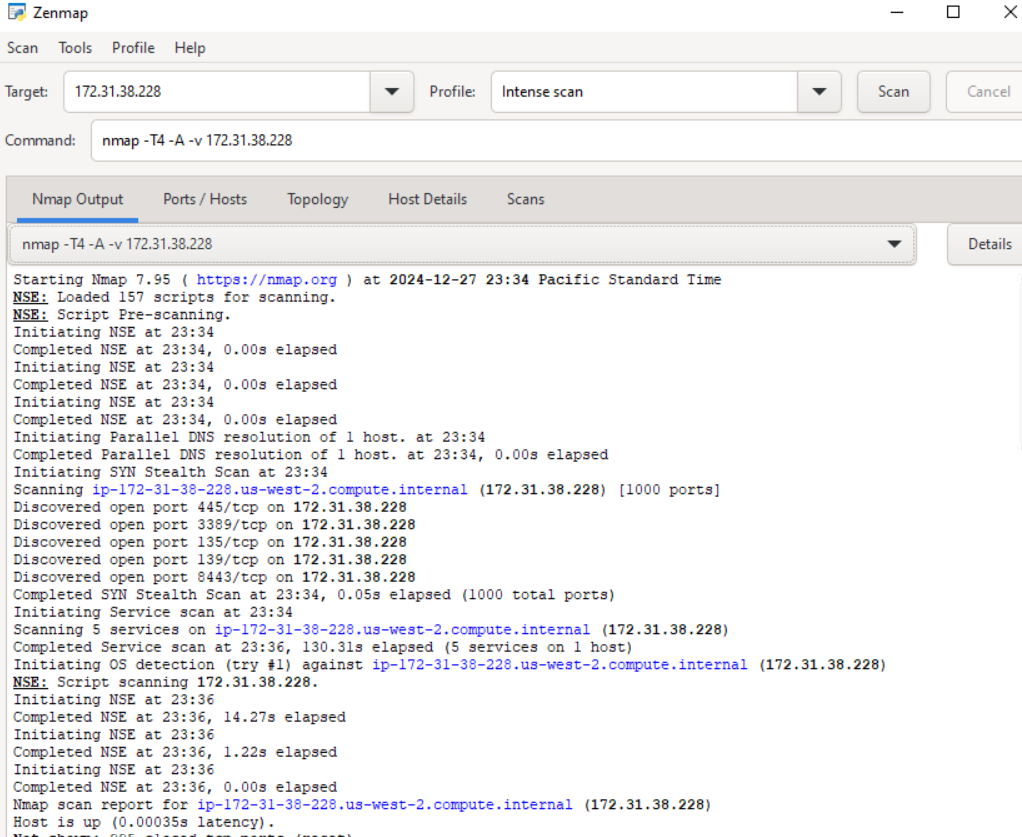


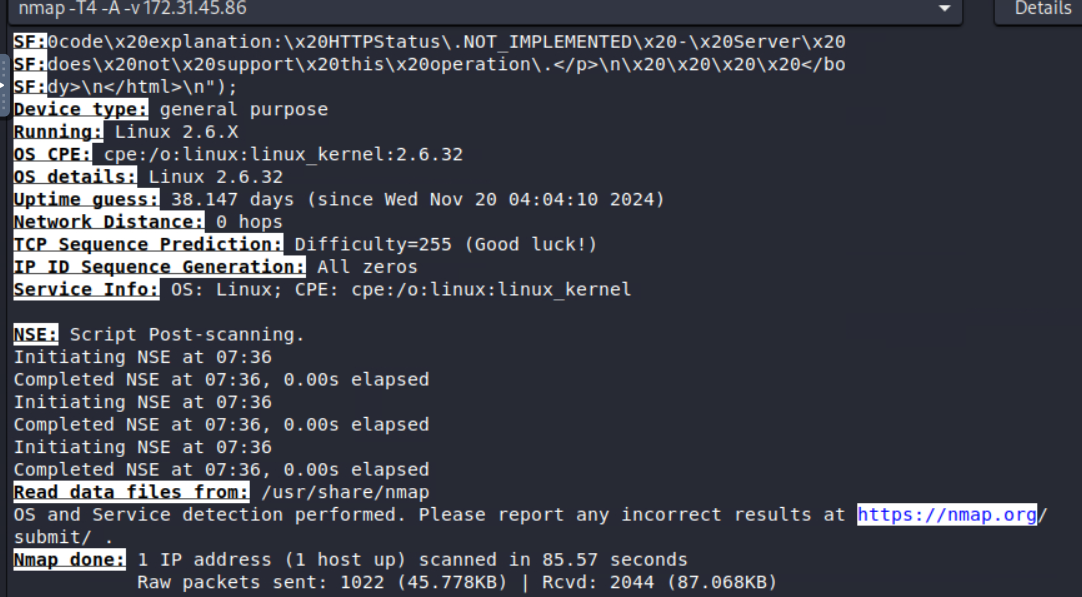
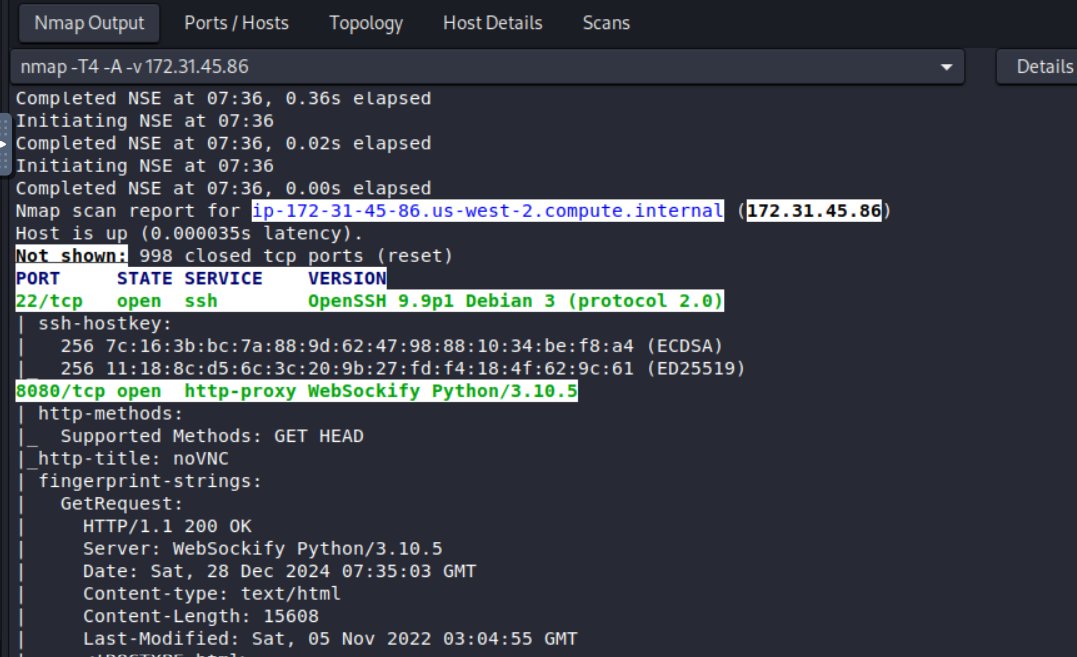
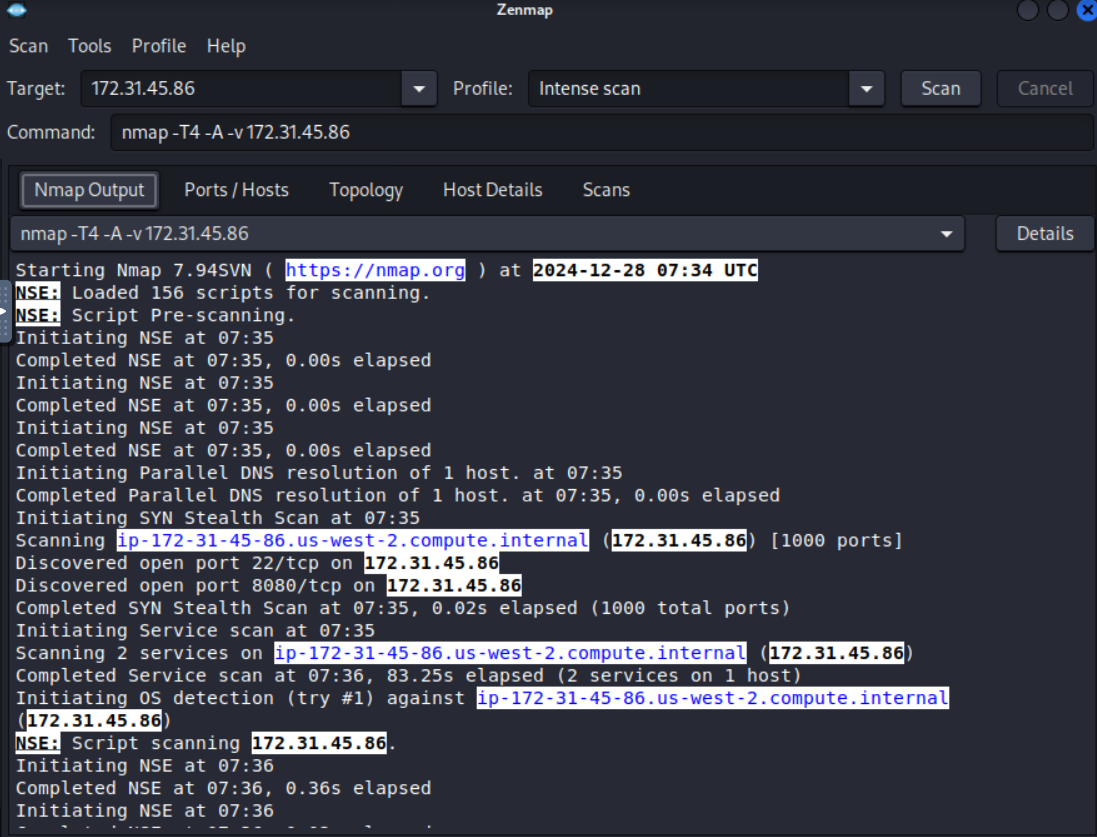
- 172.31.45.86 (Debian Linux) 

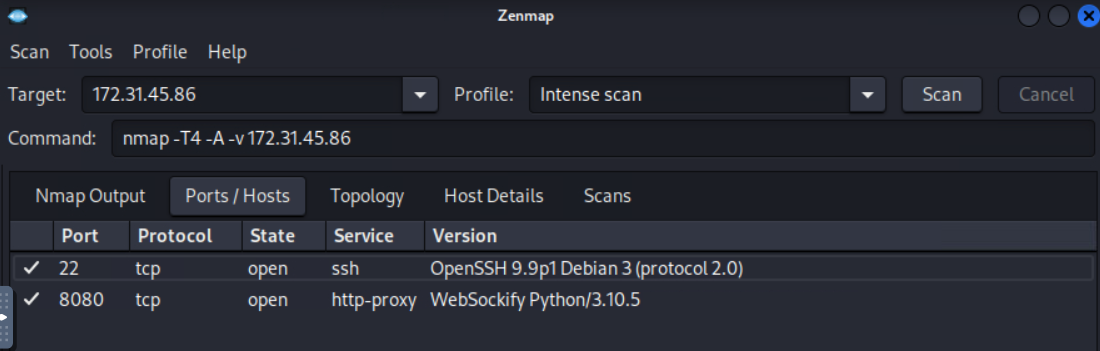


## Phase 2: Scanning and Enumeration

This phase involved identifying open ports and services on the target systems.

172.31.38.228 (Windows 10) 

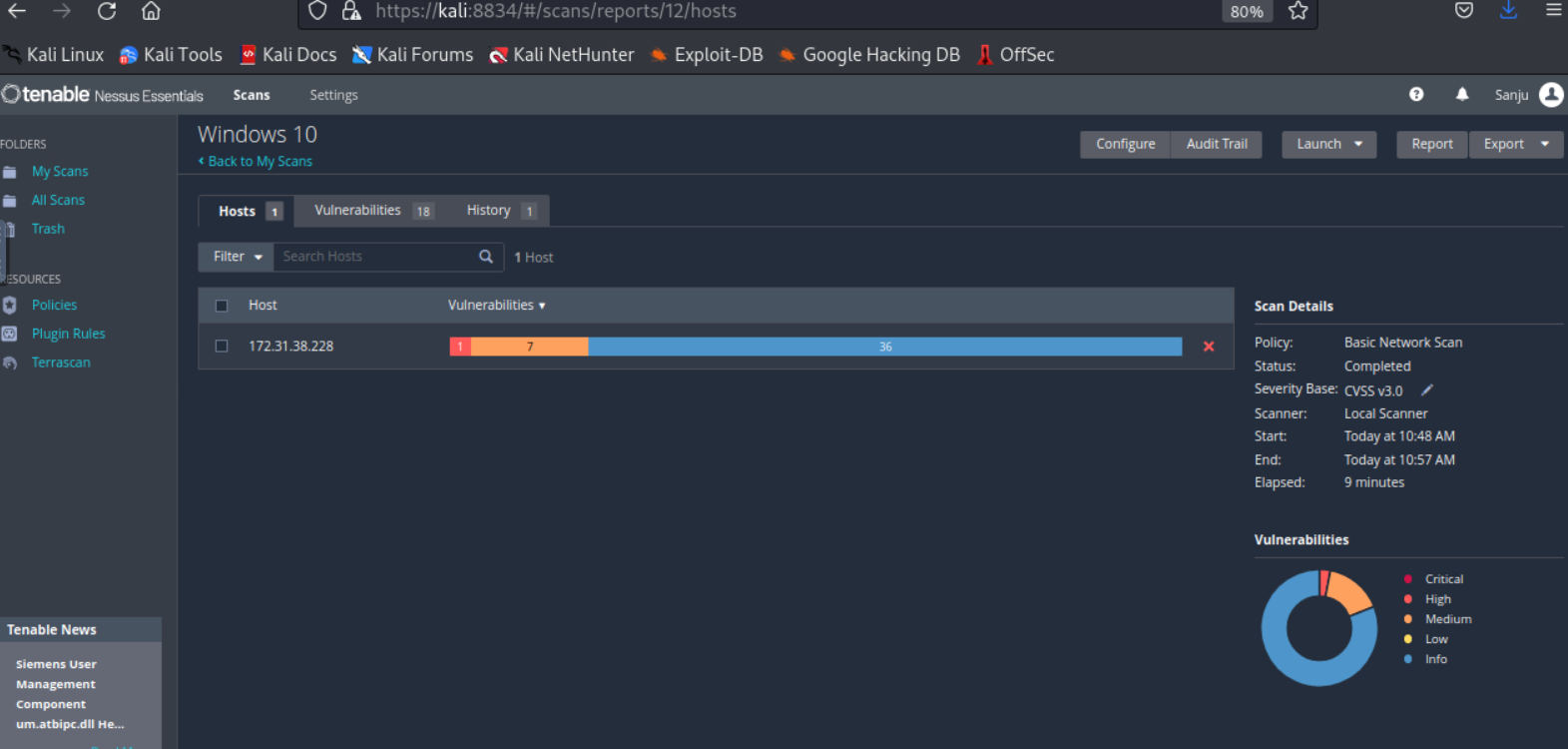
172.31.45.86 (Debian Linux)

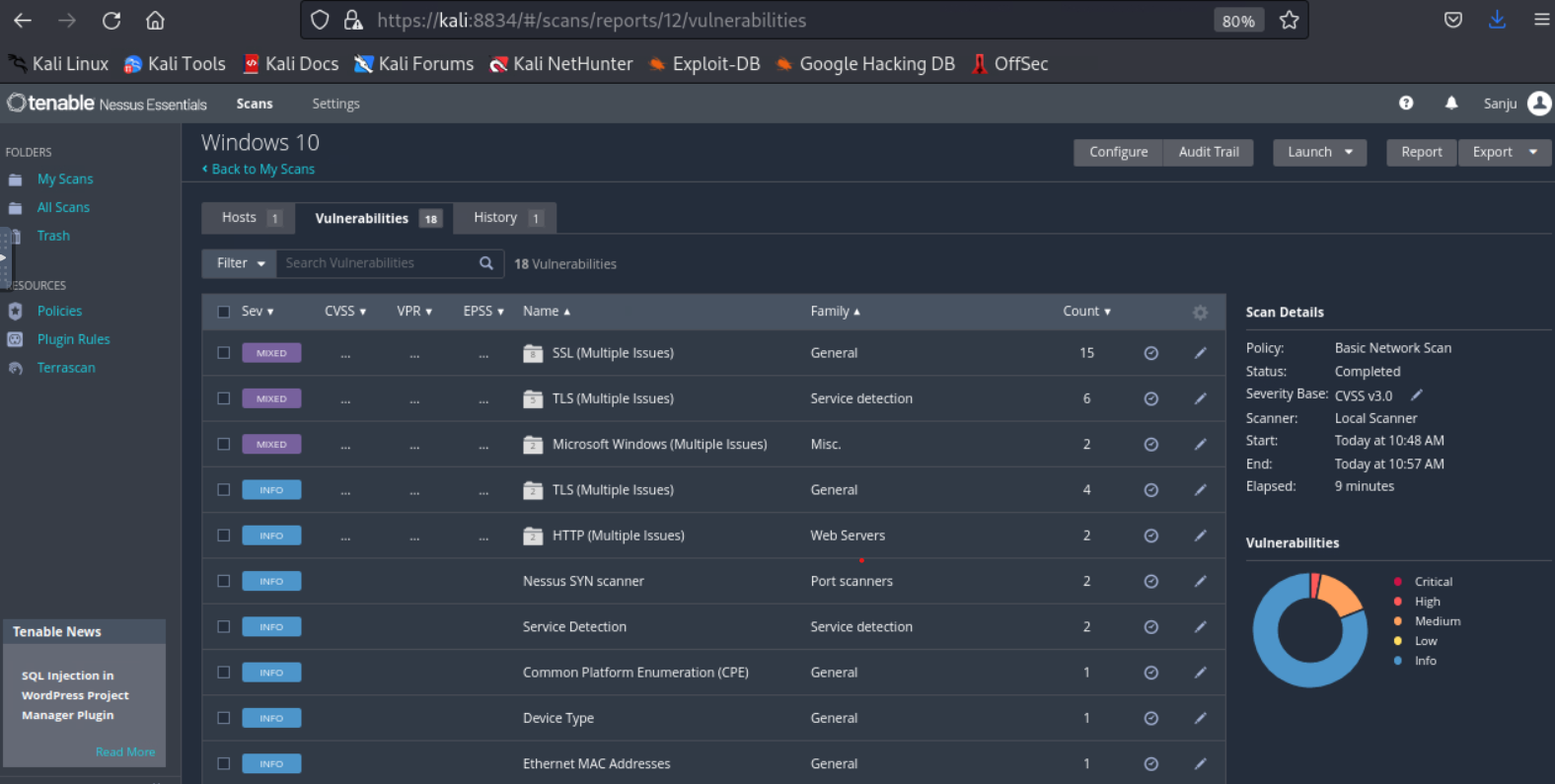


## Phase 3: Vulnerability Assessment

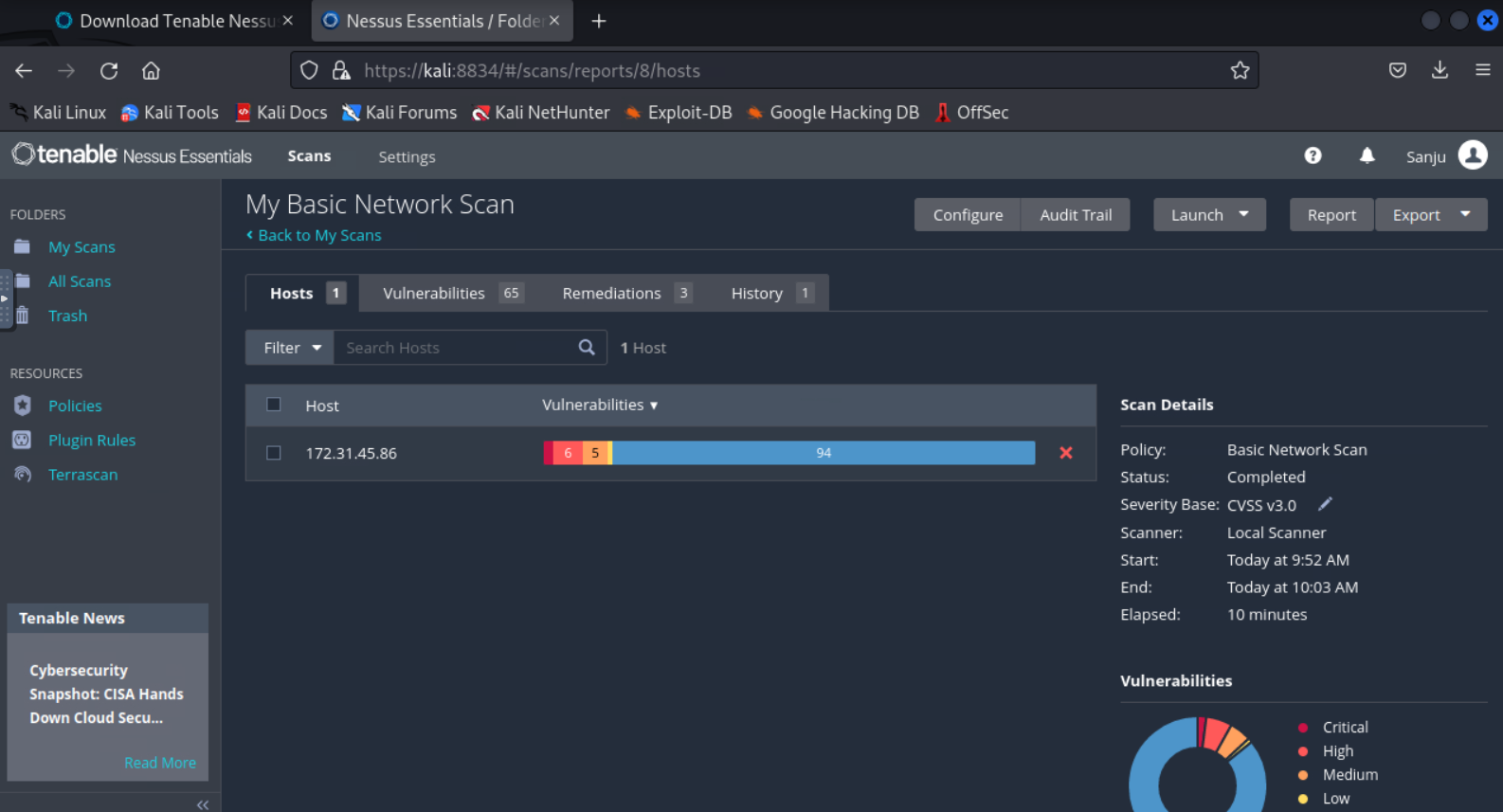
The identified systems were scanned for known vulnerabilities using automated tools. Nessus

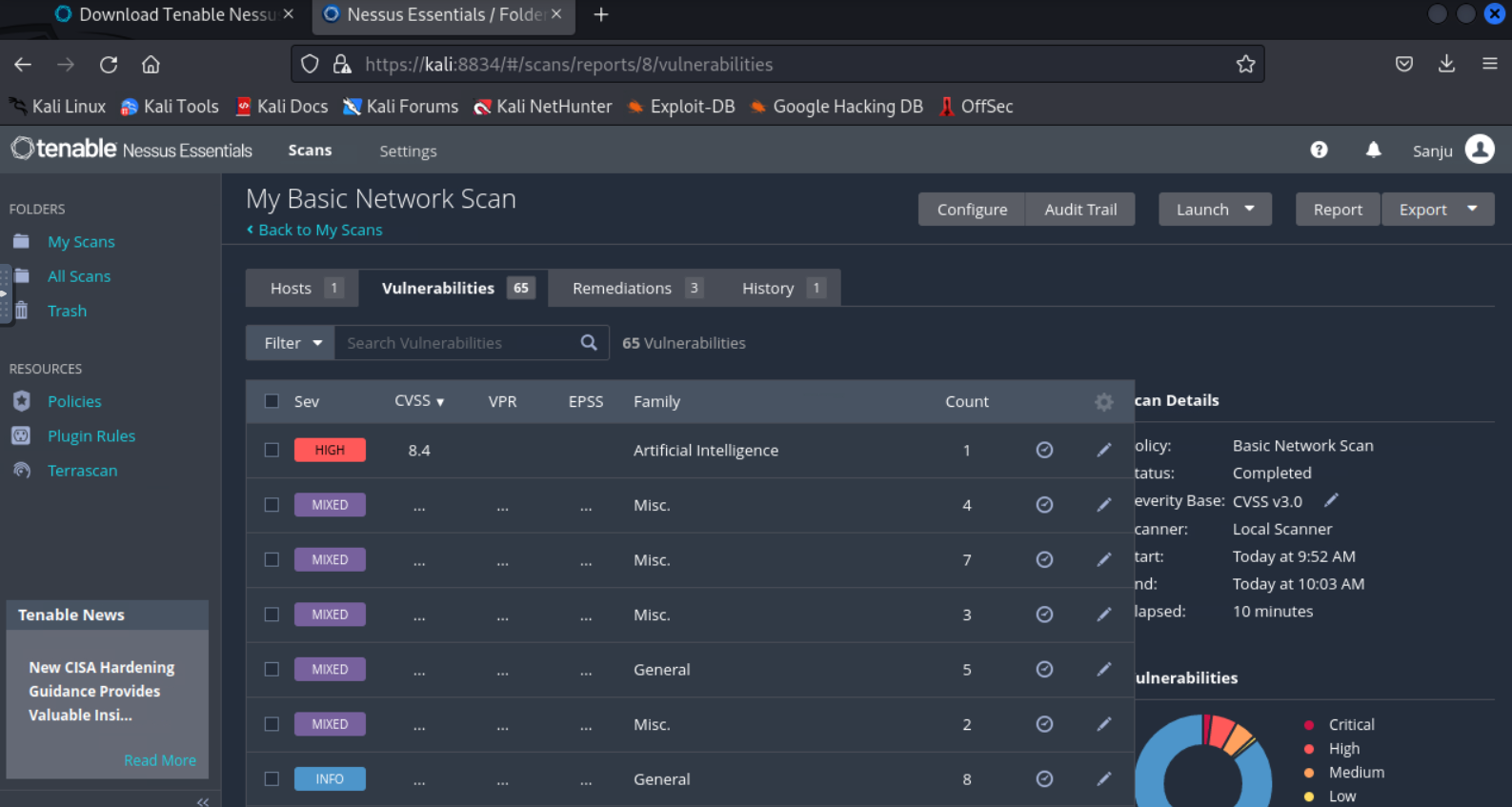
172.31.38.228 (Windows scan)

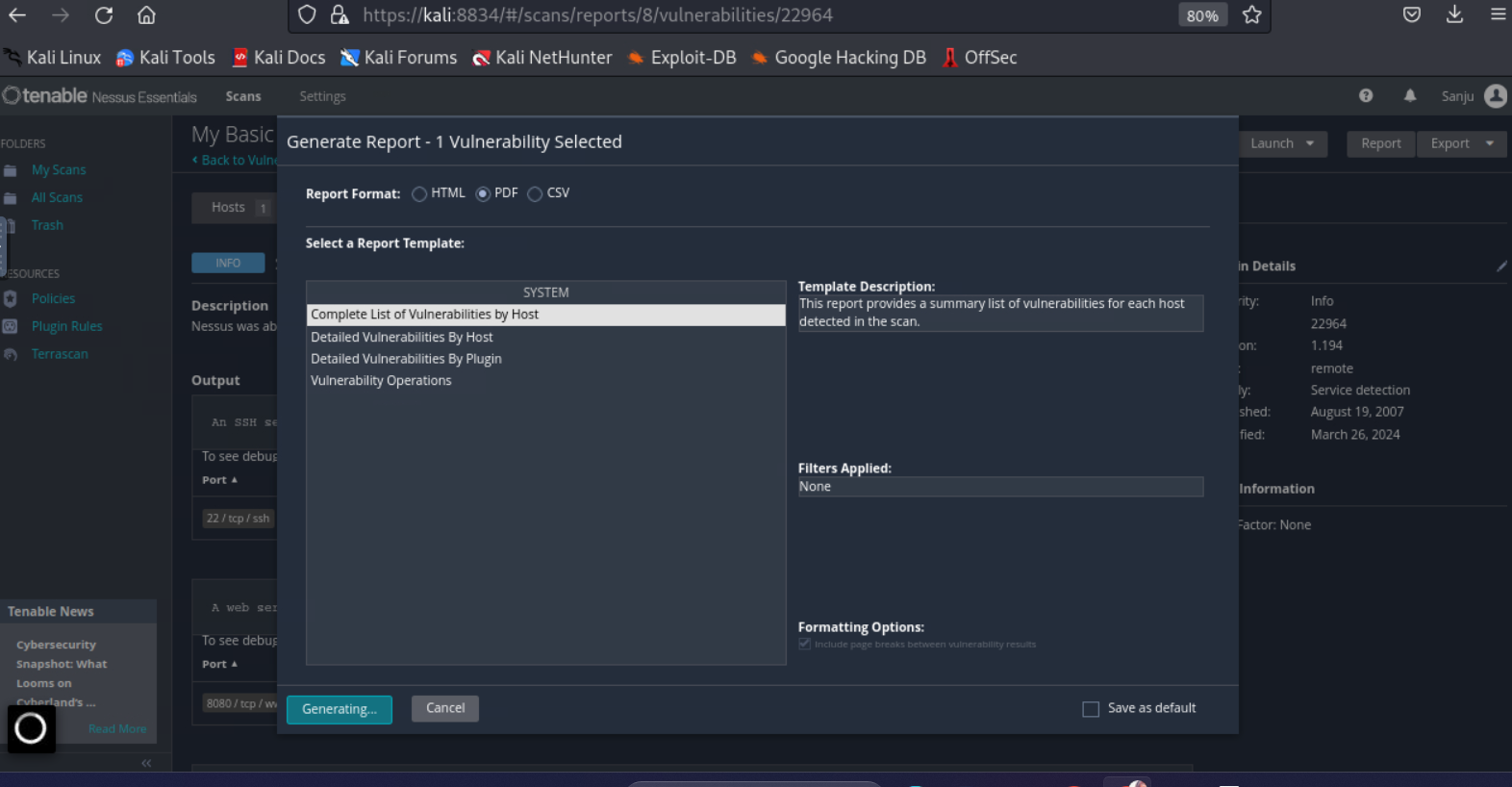




172.31.45.86 (Debian Linux scan)







|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Operating System** | **IP Address** | **Vulnerability Count \*** | **Risk Classification** | **Reference** | **Report** |
| Microsoft Windows 10 | 172.31.38.228 | 01 | Informational | 11219 | [Windows 10\_oiapxu.pdf](Windows%2010_oiapxu.pdf) |
| Debian Linux | 172.31.45.86 | 01 | Informational | 22964 | [My Basic Network Scan\_5nahjq.pdf](My%20Basic%20Network%20Scan_5nahjq.pdf) |

## Phase 5: Analysis and Reporting

The analysis highlights critical security gaps that require remediation.  
  
\*\*Key Risks:\*\*  
- Unauthorized access via SMB and Apache vulnerabilities.  
- Potential exploitation through weak configurations.  
  
\*\*Impact:\*\*  
- Loss of sensitive data.  
- Financial and reputational harm.  
  
\*\*Remediation Steps:\*\*  
1. Patch all vulnerabilities (e.g., SMBv1, Apache).  
2. Configure firewalls to restrict access to ports.  
3. Enforce strong password policies.

**Reports**

[My Basic Network Scan\_p6r3mz.pdf](My%20Basic%20Network%20Scan_p6r3mz.pdf)

[Windows 10\_09tuns.pdf](Windows%2010_09tuns.pdf)