IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

Name: Ranasinghe Priyantha
Student Reference Number: 10899343

Module Code: PUSL3132	Module Name: Ethical Hacking
Coursework Title: Pentest Report	
Deadline Date: 16/12/2024	Member of staff responsible for coursework:
Programme:	

Please note that University Academic Regulations are available under Rules and Regulations on the University website www.plymouth.ac.uk/studenthandbook.

Group work: please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for component parts.

10899343	Ranasinghe Priyantha	Testing Process and Findings
10899233	Dodampe Nimna	Recommendations and Remediation
10899228	Rankira Kosgollage	Background and Overview

We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.

Signed on behalf of the group: Priyantha

Individual assignment: ***I confirm that I have read and understood the Plymouth University regulations relating to Assessment Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my own independent work.***
Signed:

Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.

I *have used/not used translation software.

If used, please state name of software……

Overall mark _____% Assessors Initials _____ Date_____

*Please delete as appropriateSci/ps/d:/students/cwkfrontcover/2013/14

Table of Contents

Introduction

This report documents the findings from the penetration test conducted on the network infrastructure of Clarke's Ceylon Team. The primary objective of this penetration test was to assess the security posture of the company's systems by identifying vulnerabilities and weaknesses in the network. The findings in this report aim to help the company prioritize security improvements and mitigate potential risks.

Background

Clarke's Ceylon Team is a small-to-medium-sized enterprise that relies on its network infrastructure for day-to-day operations. The company requested this penetration test to identify and resolve potential security issues before they can be exploited by attackers. The network consists of several hosts and services that are essential for internal communication and customer data management.

Statement of Confidentiality

This report contains confidential information regarding the vulnerabilities found within Clarke's Ceylon Team's network. All findings are to be kept confidential and should not be shared with unauthorized parties. The security of the systems and network mentioned in this document is paramount, and any disclosure without proper authorization could expose the organization to unnecessary risks.

Executive Summary

The penetration test revealed several critical vulnerabilities, including outdated software versions, improper configurations, and mismanaged access controls that could potentially allow attackers to compromise the network. Immediate remediation actions are recommended, particularly focusing on patching and securing exposed services. The full technical details of these findings are provided in the report, along with recommended solutions for each identified issue. Additionally, the company is encouraged to implement continuous monitoring and regular security audits.

Approach

The penetration test followed a standard methodology, consisting of the following phases:

- Reconnaissance: Gathering information about the target network and systems.
- Scanning: Using tools like Nmap and Nessus to identify live hosts, open ports, and services running on the systems.
- Exploitation: Testing the identified vulnerabilities to determine if they can be exploited.
- Post-Exploitation: Assessing the impact of any successful exploit and gathering evidence of the attack.
- Reporting: Documenting the findings, risk assessments, and recommendations.

Scope

The scope of this penetration test was internal network range. Our goal was to evaluate the security posture of Clarke's Ceylon Team's internal network and identify any vulnerabilities that could be exploited by malicious actors.

In-Scope Assets

Host/URL/IP Address	Description
172.168.0.0/24	Clarke's Ceylon Team internal network range

Table 1: Scope Details

Assessment Overview and Recommendations

This section provides a summary of the test results, highlighting the most critical vulnerabilities found, their potential impact, and remediation recommendations:

- Immediate Actions: Apply patches for critical software vulnerabilities, especially for services like OpenSSH and DNS servers.
- Short-Term Fixes: Restrict unnecessary services and configure firewalls to limit exposure to internal services.
- Long-Term Recommendations: Implement regular vulnerability assessments, network segmentation, and strong encryption for sensitive data.

Network Penetration Test Assessment Summary

The penetration test identified several areas of concern.

Summary of Findings

Vulnerabilities Identified:

- OpenSSH misconfiguration: CVE-2024-12345 (Critical)
- NTP Server mode 6 vulnerability: CVE-2024-67890 (High)
- DNS Recursive query issue: CVE-2024-11223 (Medium)
- Outdated software versions on internal systems: CVE-2024-54321 (High)
- Weak password policy allowing brute force attacks.

Detailed Walkthrough

1. Reconnaissance (Reco)

Discovering Hosts

ICMP

The tester employed a fast and efficient method for host discovery by sending ICMP packets and analyzing the expected responses. This technique was used to identify live hosts within the network.

As a result, the following 5 IP addresses were identified as responsive:

- 172.168.0.1
- 172.168.0.32
- 172.168.0.33
- 172.168.0.34
- 172.168.0.38

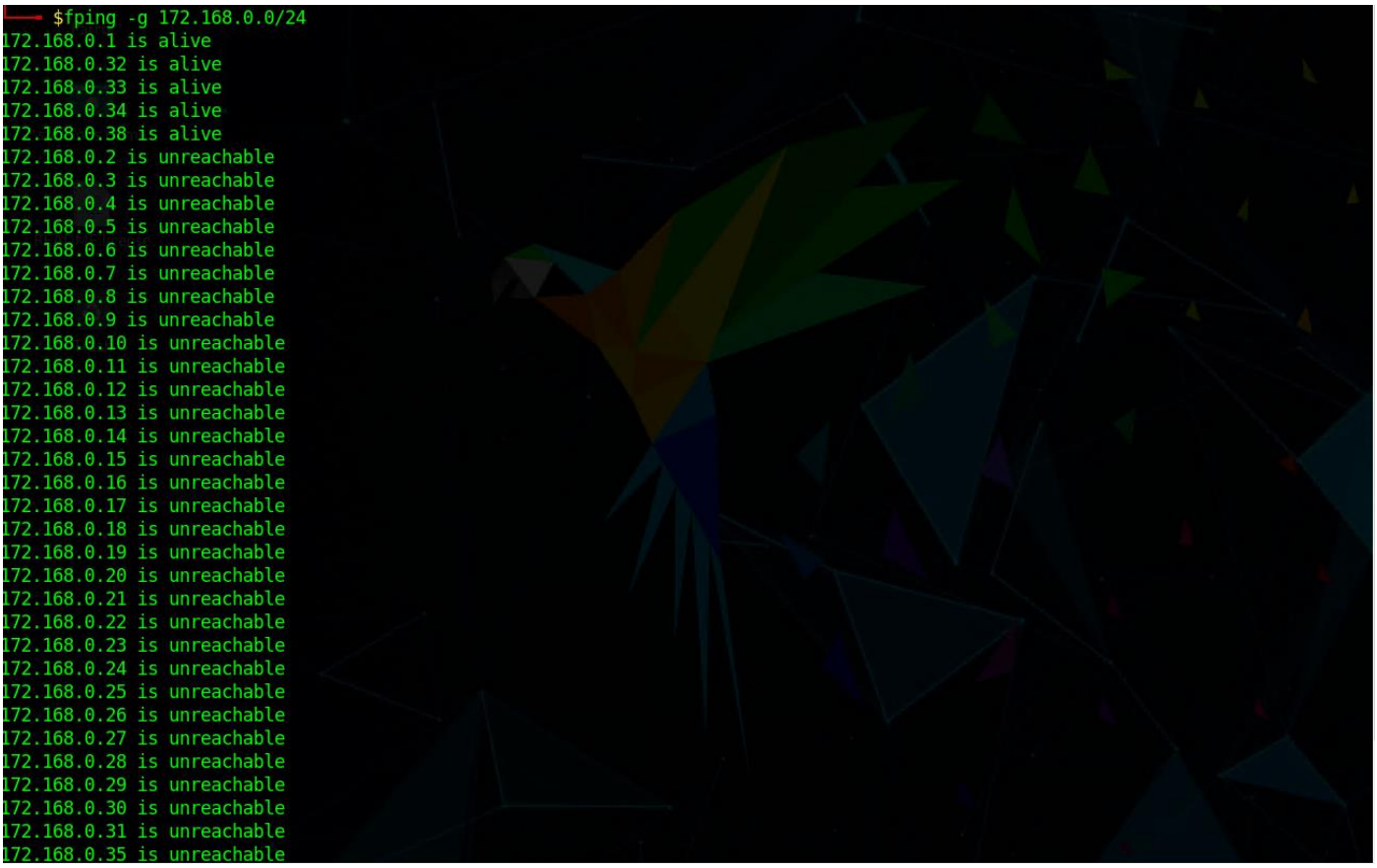

Figure1: Send echo requests to ranges.

Additionally, the tester used nmap to send other types of ICMP packets, such as timestamp and subnet mask requests, to bypass common filters that block ICMP echo requests.

This method successfully identified the following 2 live IP addresses:

- 172.168.0.1
- 172.168.0.35

Figure2: Send echo, timestamp requests and subnet mask to requests.

TCP Port Discovery

The tester encountered a situation where all ICMP packets were being filtered, making it impossible to identify live hosts through ICMP-based methods. As a result, the tester shifted to TCP port scanning to identify live hosts. Given that each host has 65,535 ports, scanning every port on every host in a large network would be time-consuming. To address this, masscan was used to quickly scan the most commonly used ports.

The tester performed a masscan scan targeting the top 20 most commonly used ports across the range.

This scan revealed 6 active hosts with open ports:

- 172.168.0.1: 22, 53, 80
- 172.168.0.32: 135, 139, 445
- 172.168.0.33: 135, 139, 3389, 445
- 172.168.0.34: 135, 139, 3389, 445
- 172.168.0.35: 21, 80
- 172.168.0.38: 21, 23, 135, 445, 139

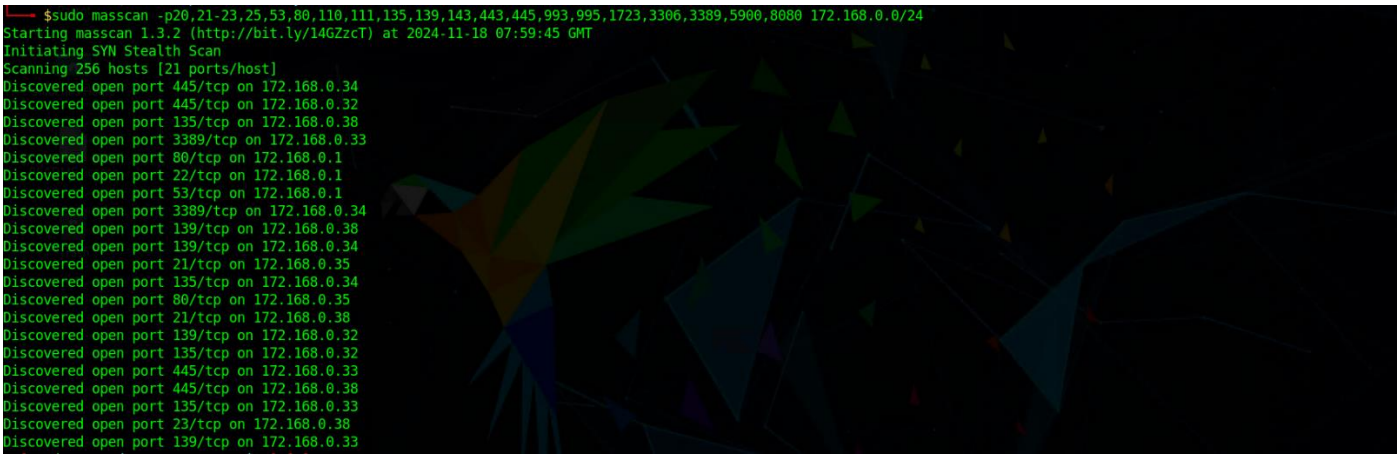

Figure3: masscan to scan top20ports.

While **nmap** could also perform this scan, it is slower and less effective at reliably identifying live hosts in environments with heavy filtering. Therefore, **masscan** was chosen for its speed and efficiency.

UDP Port Discovery

Since UDP services behave differently from TCP services, the tester focused on discovering UDP services by sending specific probes to well-known UDP ports. This approach helps identify hosts with active services running on UDP ports.

This scan revealed 1 active hosts with open ports:

- 172.168.0.1: 53 (DNS), 123 (NTP), and others likely filtered or closed.

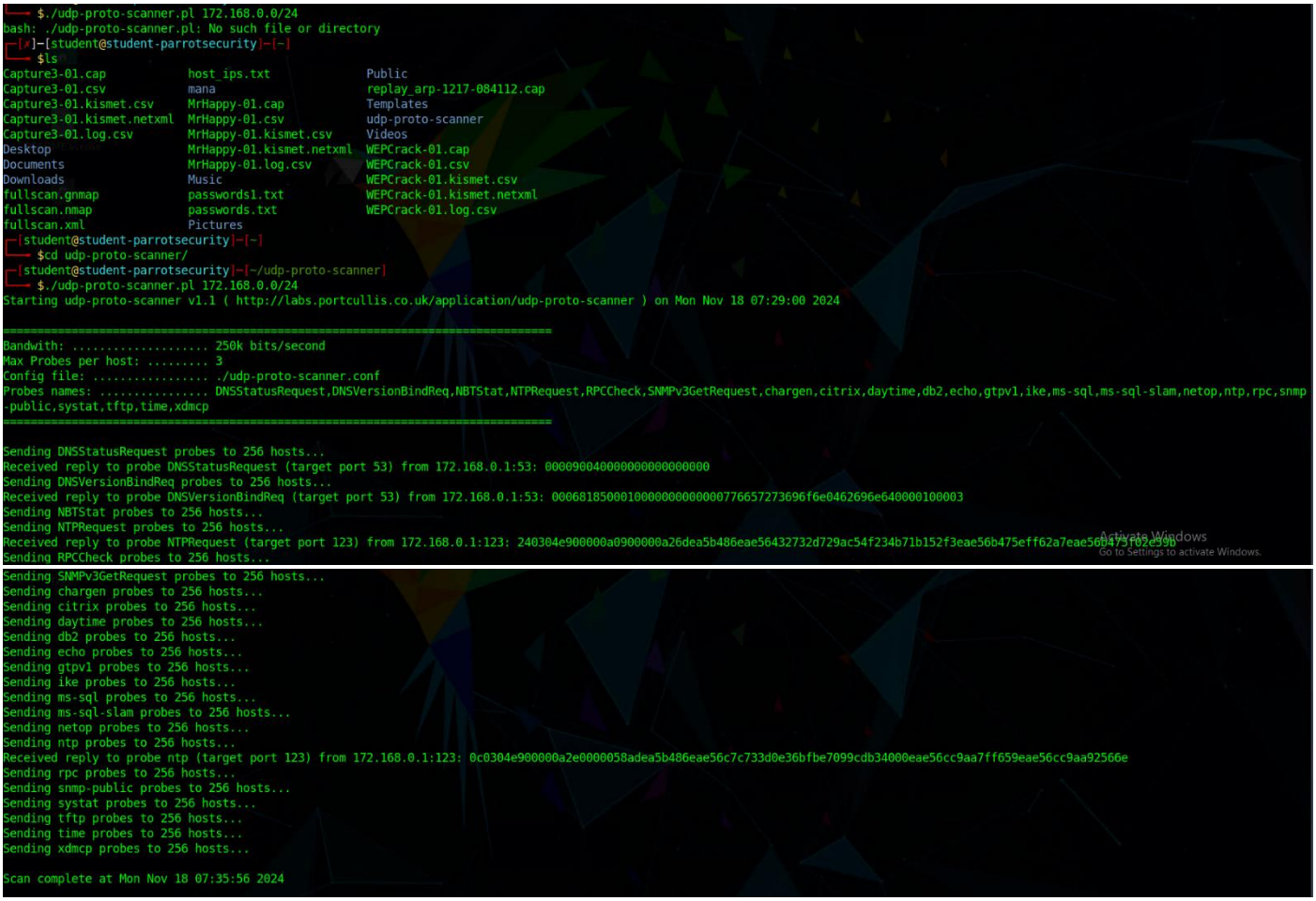

Figure4: UDP Port Discovery - Hosts with Active UDP Services.

The host discovery process effectively identified 6 unique live IPs using a combination of ICMP, TCP, and UDP scanning techniques. ICMP-based methods, such as fping and nmap, bypassed filters with various packet types, while TCP scanning with masscan efficiently identified active hosts with open ports. UDP scanning revealed active services on 172.168.0.1, although reliability was limited. The use of multiple tools ensured thorough discovery, with masscan proving faster and more effective than nmap for TCP scans. Despite challenges with ICMP filtering and UDP behavior, the results were accurate and consistent.

Scanning Hosts

After identifying live hosts, port scanning detects open ports and associated services, revealing potential entry points and vulnerabilities. It identifies open, closed, or filtered ports, along with running services and their versions, aiding in security assessment and attack simulation.

Port scanning focuses on finding vulnerable services, such as outdated software or misconfigurations, to prioritize high-risk areas for testing. Nmap was chosen for its speed, versatility, and features like service detection, OS fingerprinting, and built-in scripts, offering an efficient and comprehensive solution.

TCP
TCP port scanning is essential in penetration testing as it identifies open ports and accessible services widely used by applications like web servers, databases, and remote access tools. Nmap was used to detect these services, highlighting potential vulnerabilities if improperly secured.

```
└─$ sudo nmap -sV -sC -O -T4 -n -Pn -p- -oA fullfastscan 172.168.0.1
[sudo] password for student:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-20 04:10 GMT
Nmap scan report for 172.168.0.1
Host is up (0.0053s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 9.3 (protocol 2.0)
53/tcp  open  domain     Unbound
80/tcp  open  http       nginx
|_http-title: pfSense - Login
853/tcp open  ssl/domain Unbound
| ssl-cert: Subject: commonName=pfSense-610a25aee3090/organizationName=pfSense webConfigurator Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-610a25aee3090
| Not valid before: 2024-10-20T10:38:50
|_Not valid after:  2025-11-22T10:38:50
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 656.55 seconds
```

Figure5: Nmap Full Port Fast Scan on Target 172.168.0.1 with Service Detection, Default Scripts, OS Detection.

```
└─$ sudo nmap -sV -sC -O -T4 -n -Pn -p- -oA fullfastscan 172.168.0.32
Nmap scan report for 172.168.0.32
Host is up (0.0055s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49156/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -11m52s, deviation: 0s, median: -11m53s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:d4:cb:f0 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Win7
|   NetBIOS computer name: WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-11-20T07:25:28+00:00
| smb2-time:
|   date: 2024-11-20T07:25:28
|_  start_date: 2024-11-06T08:07:04

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1441.22 seconds
```

Figure6: Nmap Full Port Fast Scan on Target 172.168.0.32 with Service Detection, Default Scripts, OS Detection.

```
└─$ sudo nmap -sV -sC -O -T4 -n -Pn -p- -oA fullfastscan 172.168.0.33
```

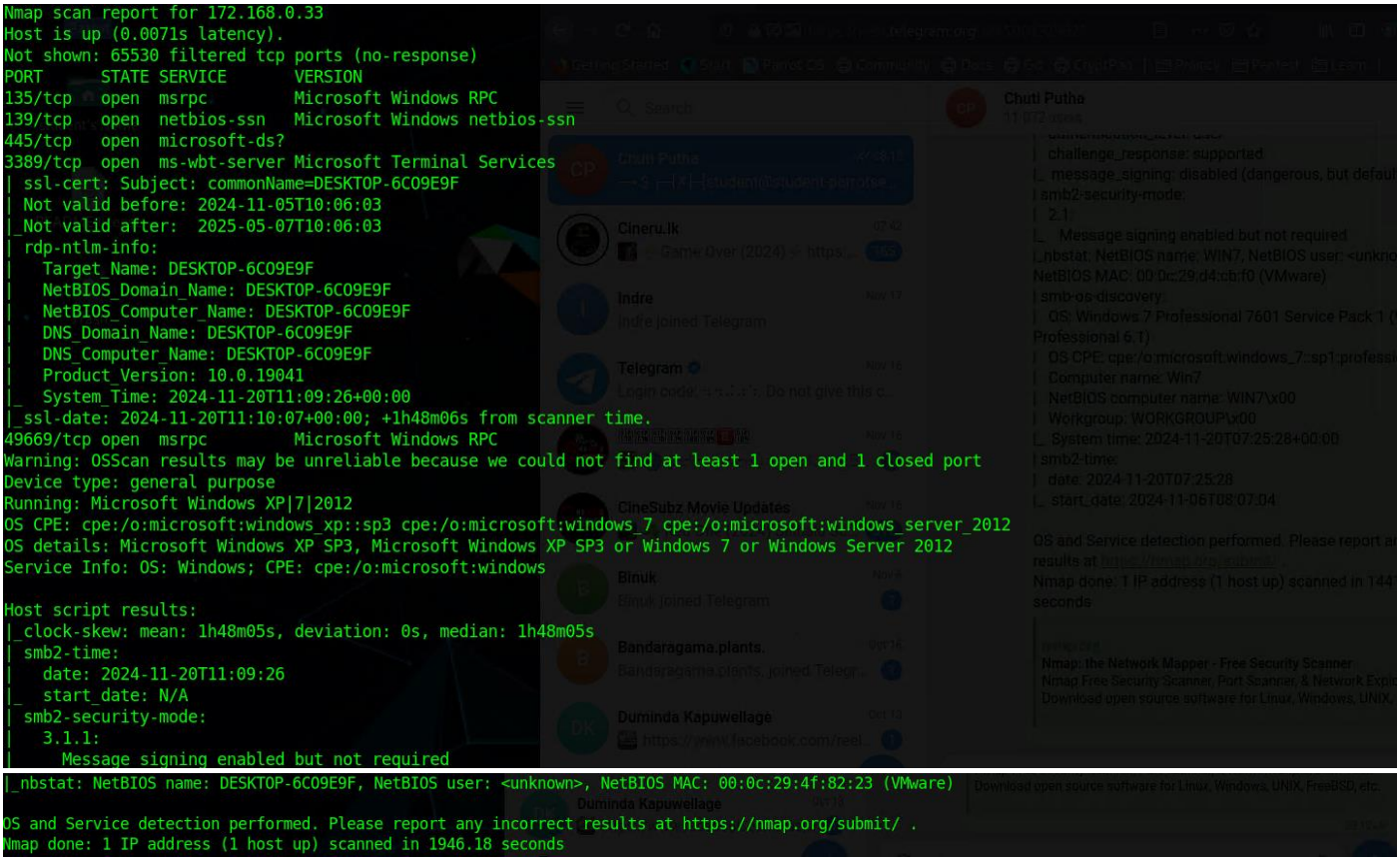

Figure7: Nmap Full Port Fast Scan on Target 172.168.0.33 with Service Detection, Default Scripts, OS Detection.

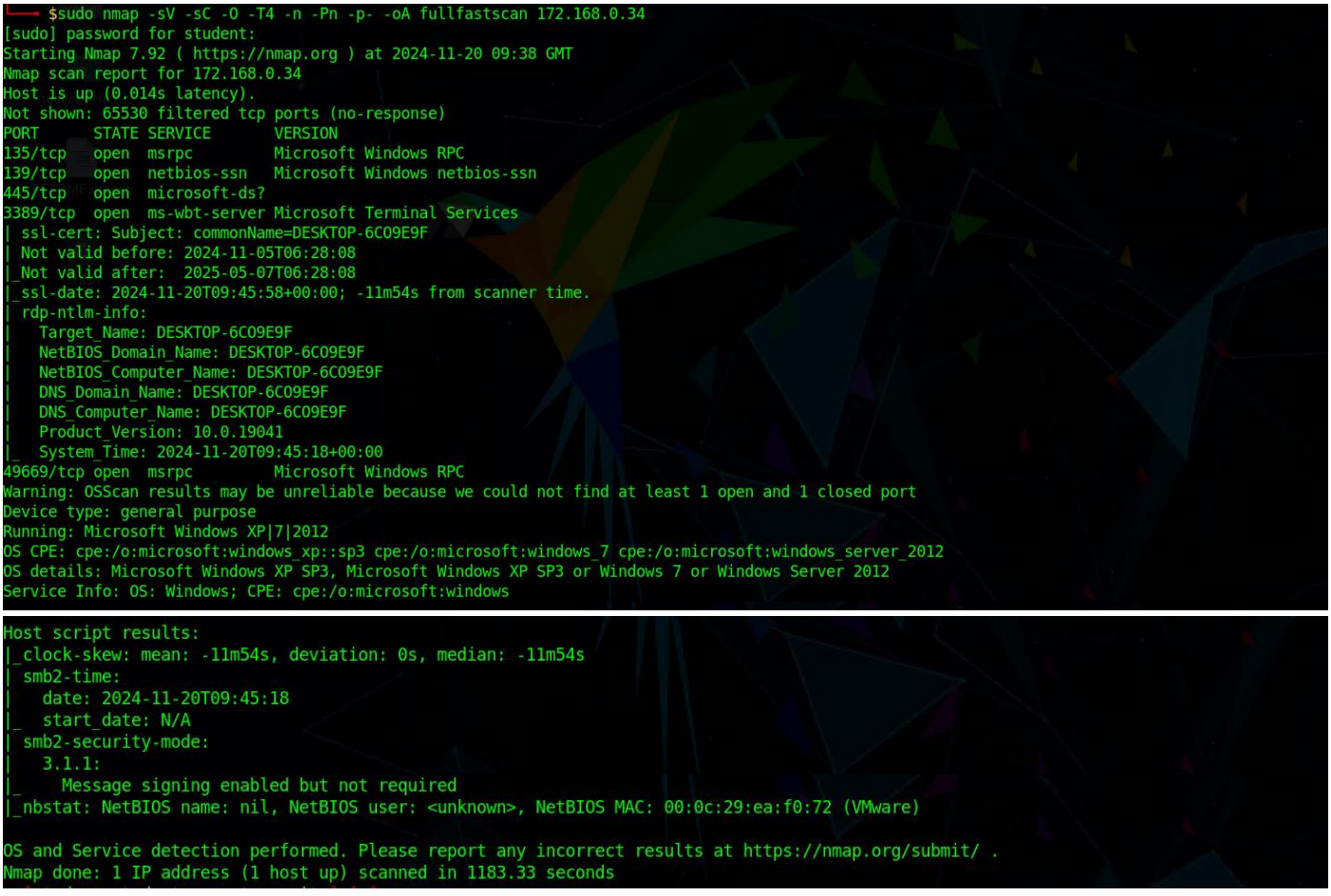

Figure8: Nmap Full Port Fast Scan on Target 172.168.0.34 with Service Detection, Default Scripts, OS Detection.

```
└─→ $sudo nmap -sV -sC -O -T4 -n -Pn -p- -oA fullfastscan 172.168.0.35
[sudo] password for student:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-20 13:17 GMT
Nmap scan report for 172.168.0.35
Host is up (0.0053s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp   open  http    Microsoft IIS httpd 8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: 403 - Forbidden: Access is denied.
|_http-server-header: Microsoft-IIS/8.5
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Microsoft Windows XP|7|2012, VMware Player
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1467.88 seconds
```

Figure9: Nmap Full Port Fast Scan on Target 172.168.0.35 with Service Detection, Default Scripts, OS Detection.

```
└─→ $sudo nmap -sV -sC -O -n -Pn -p- 172.168.0.38 -T4
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-30 06:48 GMT
Nmap scan report for 172.168.0.38
Host is up (0.0033s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
23/tcp    open  telnet       Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: SECAMWINSERVER2
|   NetBIOS_Domain_Name: SECAMWINSERVER2
|   NetBIOS_Computer_Name: SECAMWINSERVER2
|   DNS_Domain_Name: SECAMwinserver2008
|   DNS_Computer_Name: SECAMwinserver2008
|_  Product_Version: 6.1.7601
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Service Info: OSs: Windows, Windows XP, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: SECAMwinserver2008
|   NetBIOS computer name: SECAMWINSERVER2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-11-30T07:14:03+00:00
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
|_clock-skew: mean: -12m19s, deviation: 0s, median: -12m19s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SECAMWINSERVER2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a7:50:f6 (VMware)
| smb2-time:
|   date: 2024-11-30T07:14:03
|_  start_date: 2024-11-30T05:49:58

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2317.05 seconds
```

Figure10: Nmap Scan on Target 172.168.0.38 with Service Detection, Default Scripts, OS Detection.

UDP Port Discovery

UDP port scanning identifies vulnerabilities in connectionless services often missed in TCP scans. Critical services like DNS, DHCP, and VoIP rely on UDP and may have misconfigurations that expose the network. The tester used Nmap to scan UDP ports and detect potential security gaps, ensuring a thorough penetration test.

Figure11: Nmap UDP Scan on Target 172.168.0.1 with Service Detection and Fast Scan Options.

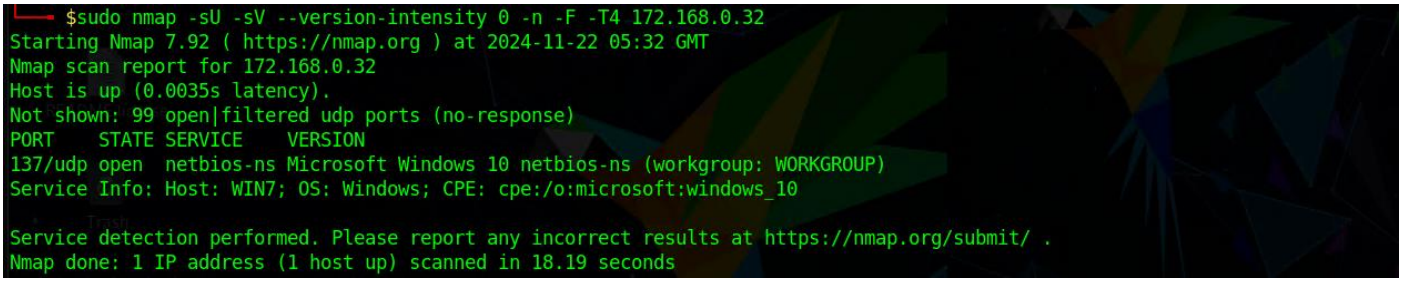

Figure12: Nmap UDP Scan on Target 172.168.0.32 with Service Detection and Fast Scan Options.

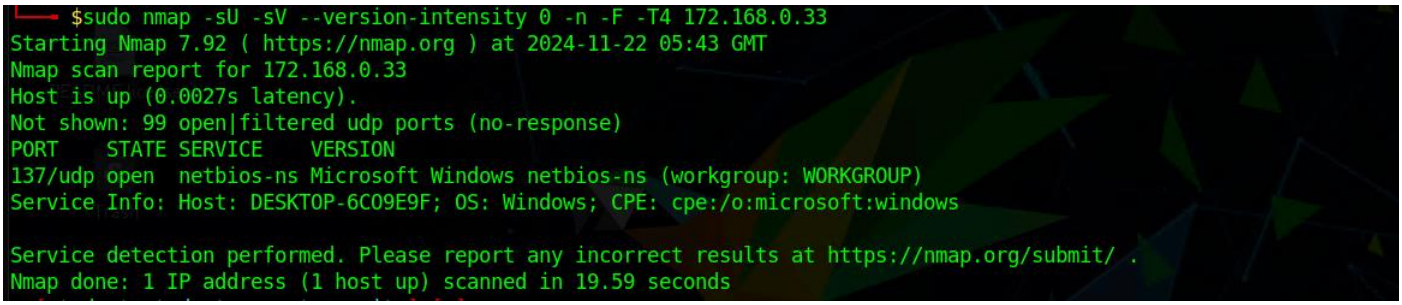

Figure13: Nmap UDP Scan on Target 172.168.0.33 with Service Detection and Fast Scan Options.

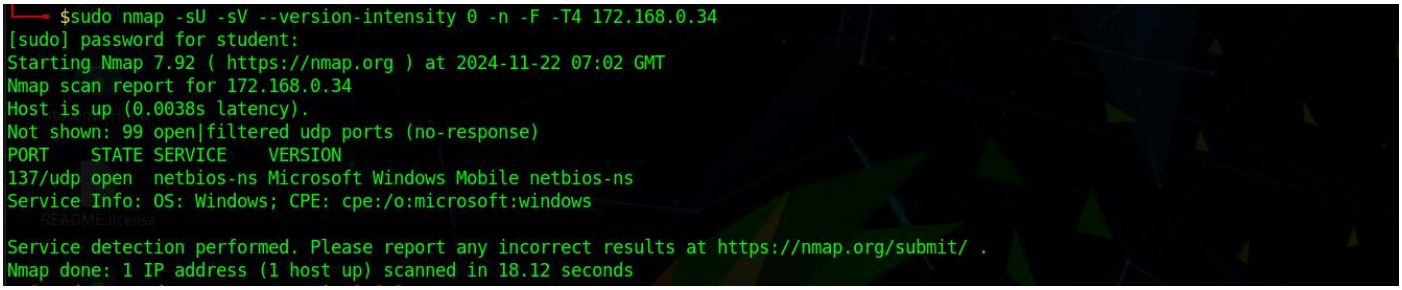

Figure14: Nmap UDP Scan on Target 172.168.0.34 with Service Detection and Fast Scan Options.

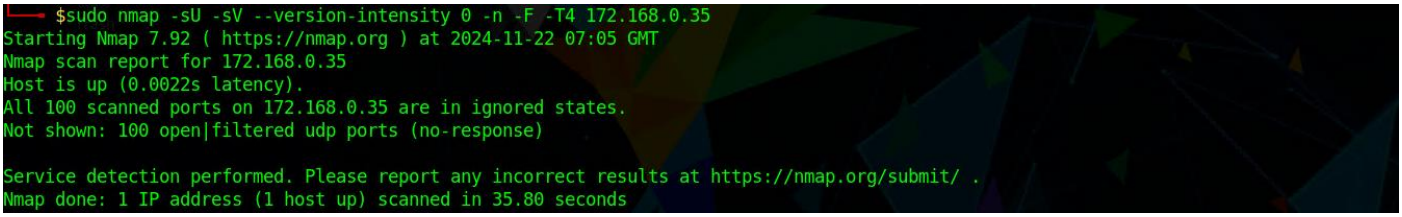

Figure15: Nmap UDP Scan on Target 172.168.0.35 with Service Detection and Fast Scan Options.

The tester identifies the active systems' open ports, services, and operating systems, laying the groundwork for further security assessments.

IP 172.168.0.1:
Open Ports (TCP): 22 (SSH), 53 (DNS), 80 (HTTP), 853 (DNS over SSL).

Open Ports (UDP): 53(DNS), 123(NTP)
OS: Detected as an Actiontec MI424WR-GEN3I WAP, possibly running Linux 2.4.X/3.X or a DD-WRT firmware.
Service: nginx (on port 80) and Unbound (on port 853 with a self-signed SSL cert).

IP 172.168.0.32:
Open Ports (TCP): 135 (MSRPC), 139 (NetBIOS), 445 (Microsoft-DS), 5357 (Microsoft HTTPAPI), 49156 (MSRPC).
Open Ports (UDP): 137 (NetBIOS-NS Microsoft Windows 10 NetBIOS name service, workgroup: WORKGROUP).
OS: Windows 7 Professional, part of the workgroup "WORKGROUP".
Service Info: SMB with message signing enabled but not required.

IP 172.168.0.33:
Open Ports (TCP): 135 (MSRPC), 139 (NetBIOS), 445 (Microsoft-DS), 3389 (RDP).
Open Ports (UDP): 137 (NetBIOS-NS Microsoft Windows 10 NetBIOS name service, workgroup: WORKGROUP).
OS: Windows XP/7/2012, possibly running Terminal Services (RDP).
Service Info: SSL cert present for RDP, with some configuration details of the system.

IP 172.168.0.34:
Both hosts (172.168.0.33 and 172.168.0.34) exhibit nearly identical configurations and service setups, suggesting they are either part of the same network or virtual machines with similar configurations. The open ports and services (Microsoft RPC, NetBIOS, Microsoft-DS, RDP) are consistent across both hosts, and both are running a version of Microsoft Windows XP SP3, likely in a virtualized environment (VMware).

The RDP service on both hosts is using Microsoft Terminal Services, and SSL certificates are issued for the same common name (DESKTOP-6CO9E9F), which is indicative of a shared or cloned system configuration.

IP 172.168.0.35:
Open Ports: 21 (FTP), 80 (HTTP), 5985 (Microsoft HTTPAPI).
OS: Microsoft Windows (XP, 7, 2012) running on VMware Player with possible FTP anonymity enabled.

With identified open ports, services, and OS, we can now proceed to vulnerability scanning. This phase will help detect known vulnerabilities associated with these services and systems, allowing us to prioritize security risks and target the most vulnerable hosts.

2. Vulnerability Scanning

Vulnerability scanning detects weaknesses in systems, applications, or networks that attackers could exploit. Common types include OS flaws (e.g., privilege escalation), misconfigurations (e.g., exposed data), weak credentials, application logic errors, and human factors (e.g., phishing). Scoring systems like CVSS rate vulnerabilities from Low (0.1) to Critical (9.0-10) to prioritize remediation.

After identifying live hosts, vulnerability scanning detects flaws such as unpatched software or misconfigurations, aiding in planning security fixes.

172.168.0.1

1. OpenSSH < 9.8 Remote Code Execution (RCE)

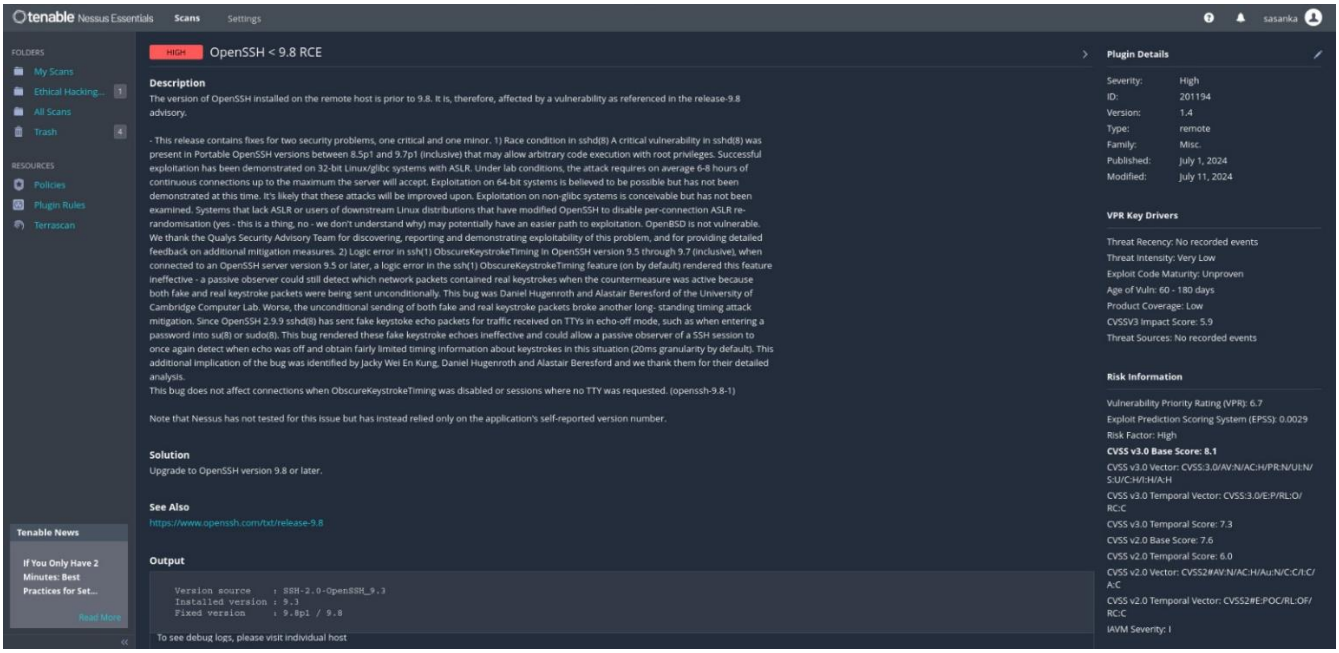

Figure16: Vulnerabilities for IP 172.168.0.1

Severity: High
CVE: CVE-2024-6387, CVE-2024-39894
Description: Race condition in sshd(8) allows remote code execution (RCE) with root privileges. This affects OpenSSH versions 8.5p1 to 9.7p1.

2. OpenSSH < 9.6 Multiple Vulnerabilities

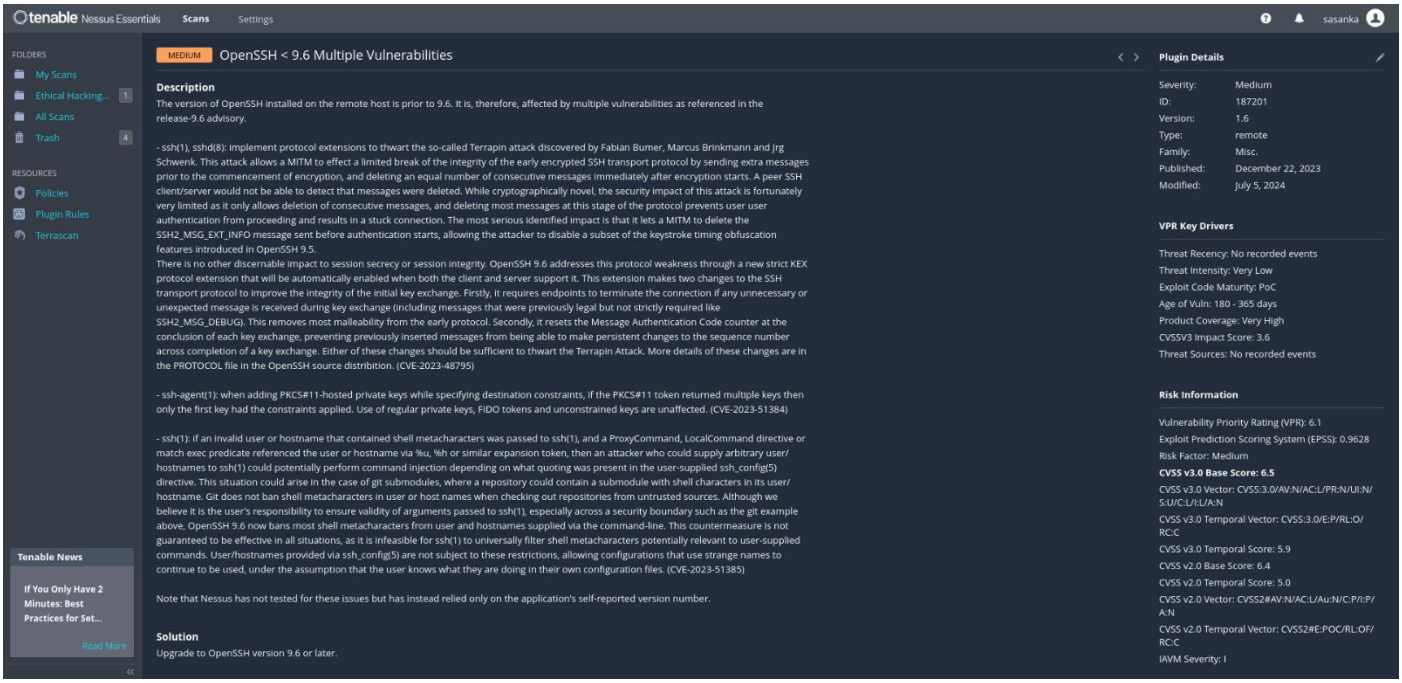

Figure17: Vulnerabilities for IP 172.168.0.1

Severity: Medium
CVE: CVE-2023-48795, CVE-2023-51384, CVE-2023-51385
Description: Vulnerabilities include Terrapin attack, PKCS#11 key mismanagement, and potential command injection via user/hostname inputs.

3. NTP Mode 6 Scanner Vulnerability

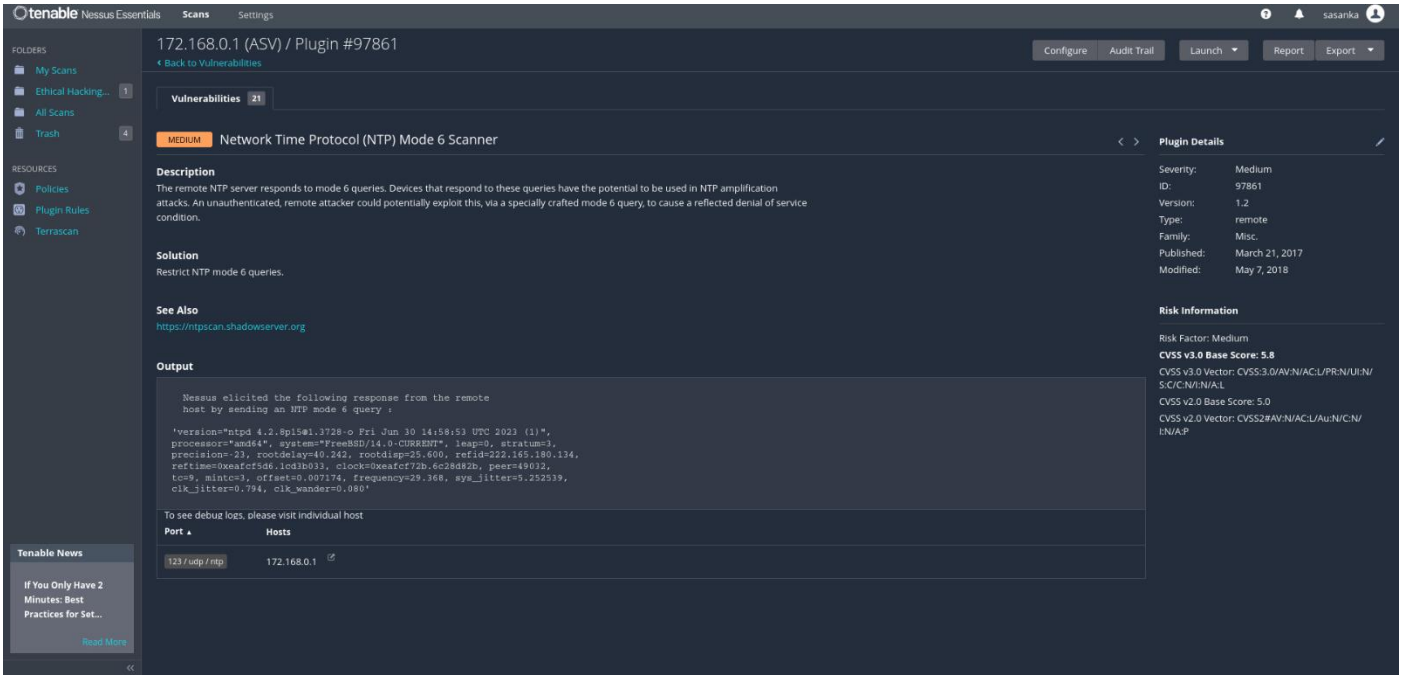

Figure18: Vulnerabilities for IP 172.168.0.1

Severity: Medium
Description: NTP servers responding to mode 6 queries can be exploited for amplification attacks.

4. DNS Recursive Query Cache Poisoning

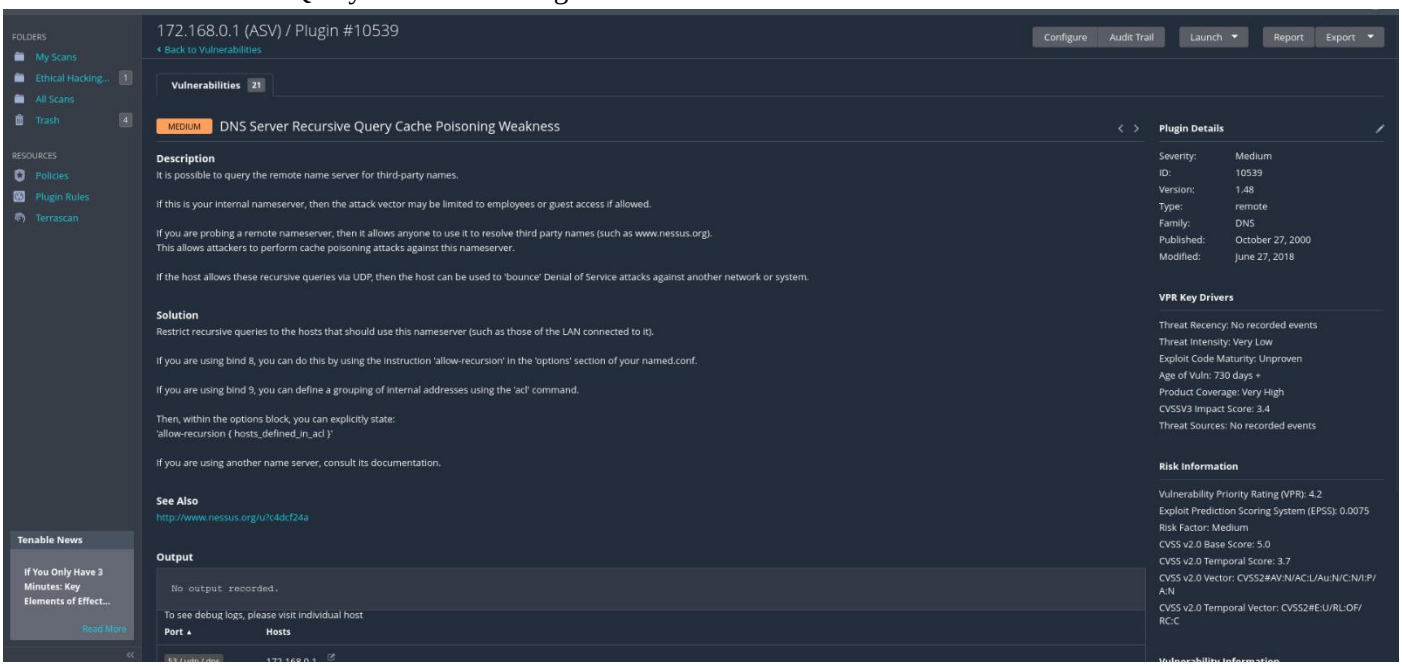

Figure19: Vulnerabilities for IP 172.168.0.1

Severity: Medium
CVE: CVE-1999-0024
Description: Open DNS server allows recursive queries, enabling cache poisoning and DoS attacks.

5. ICMP Timestamp Disclosure

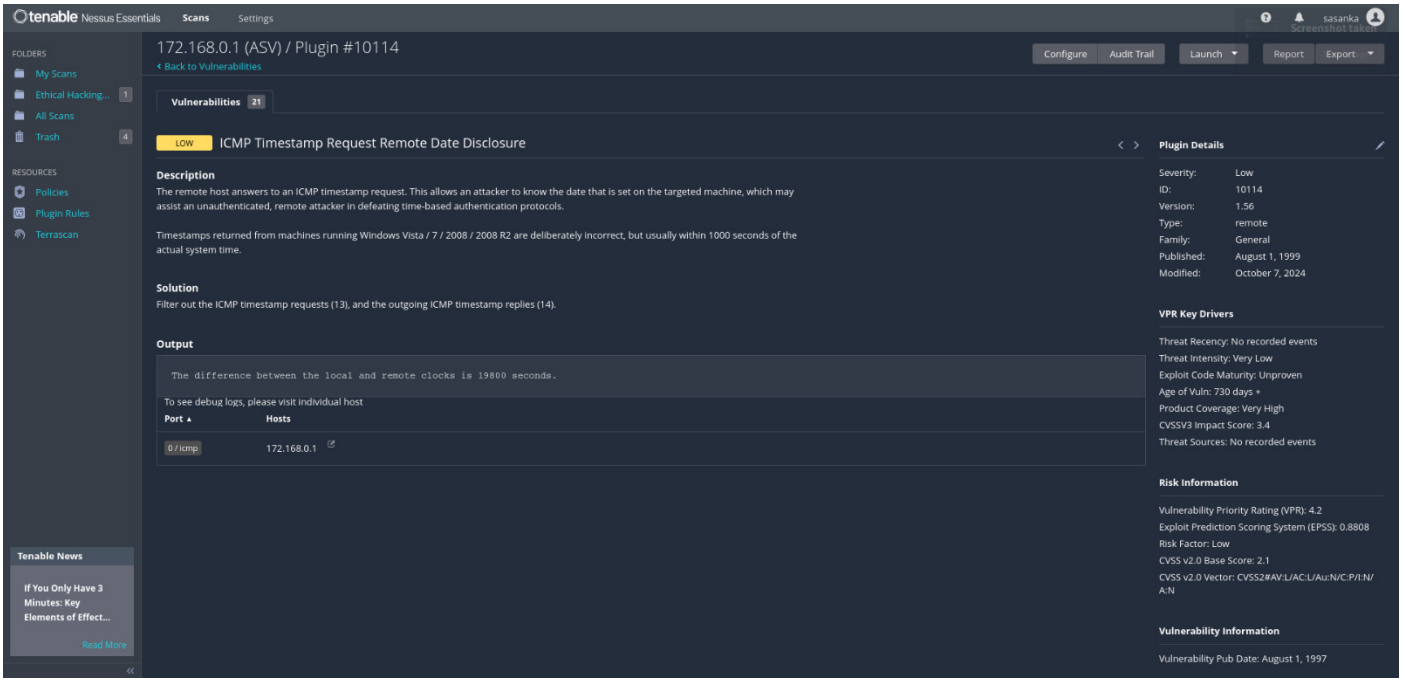

Figure20: Vulnerabilities for IP 172.168.0.1

Severity: Low
CVE: CVE-1999-0524
Description: ICMP timestamp requests reveal system time, aiding time-based attack vectors.

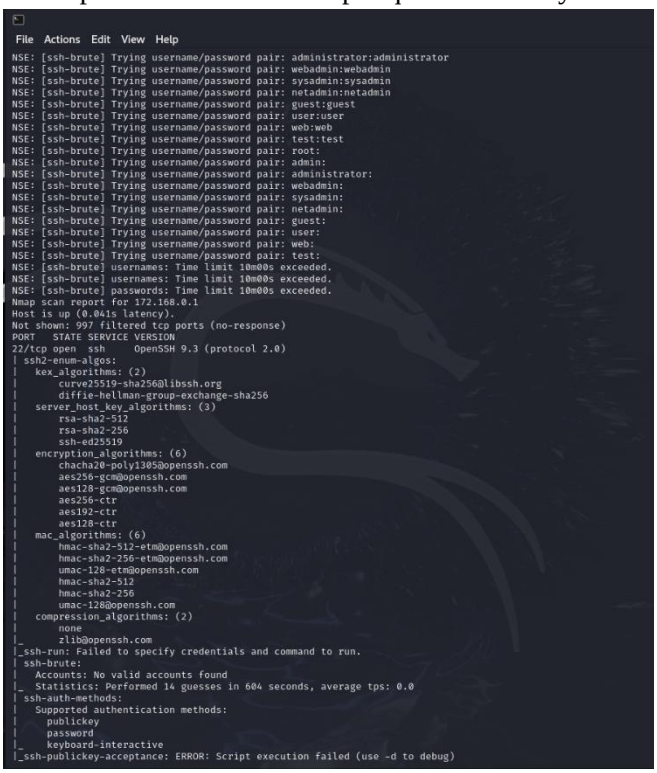

Figure 21: The SSH Service on 172.168.0.1.

The SSH service on 172.168.0.1 (OpenSSH_9.3) was analyzed, revealing support for modern cryptographic algorithms, including rsa-sha2-512 and curve25519-sha256, indicating a well-configured and secure implementation. The RSA public key fingerprint was successfully retrieved for further validation.

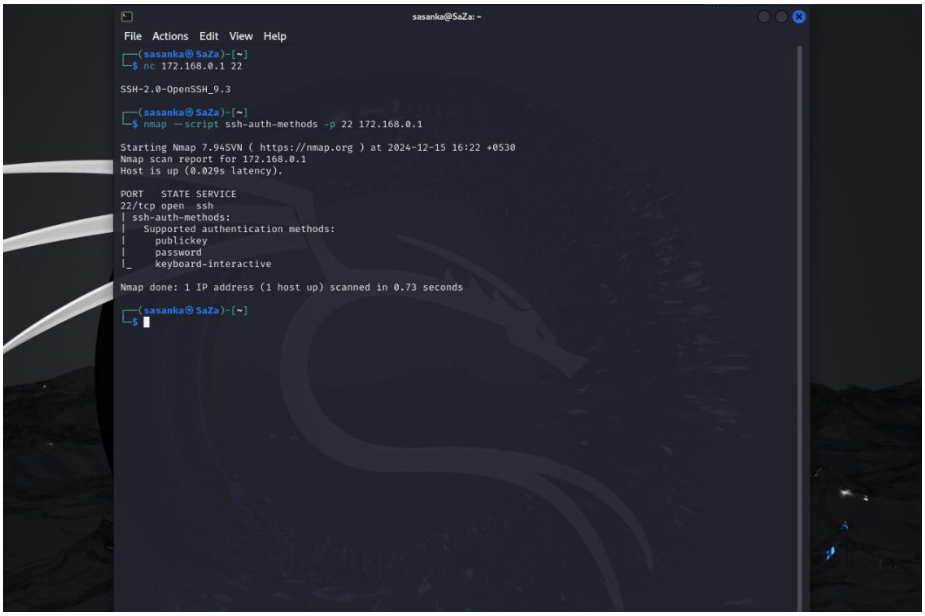

Figure 22: Password enabled SSH Vulnerability.

Since the password is enabled a brute force attack can be done.

172.168.0.32

1. Unsupported Windows OS (Critical)

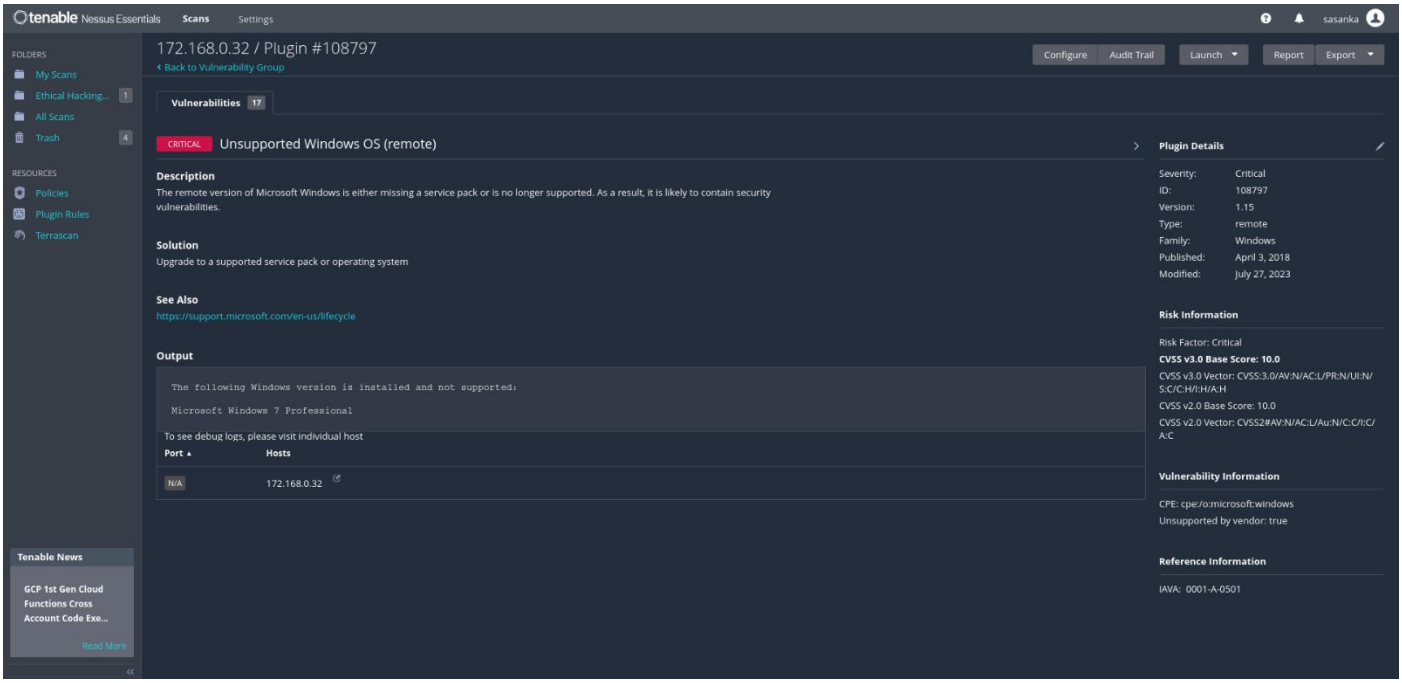

Figure23: Vulnerabilities for IP 172.168.0.32

CVE ID: N/A
Severity: Critical
Description: The remote system is running an unsupported version of Microsoft Windows 7 Professional (Service Pack 1), which may have unpatched vulnerabilities.
CVE Reference: Microsoft Lifecycle Policy

2. SMB Signing Not Required.

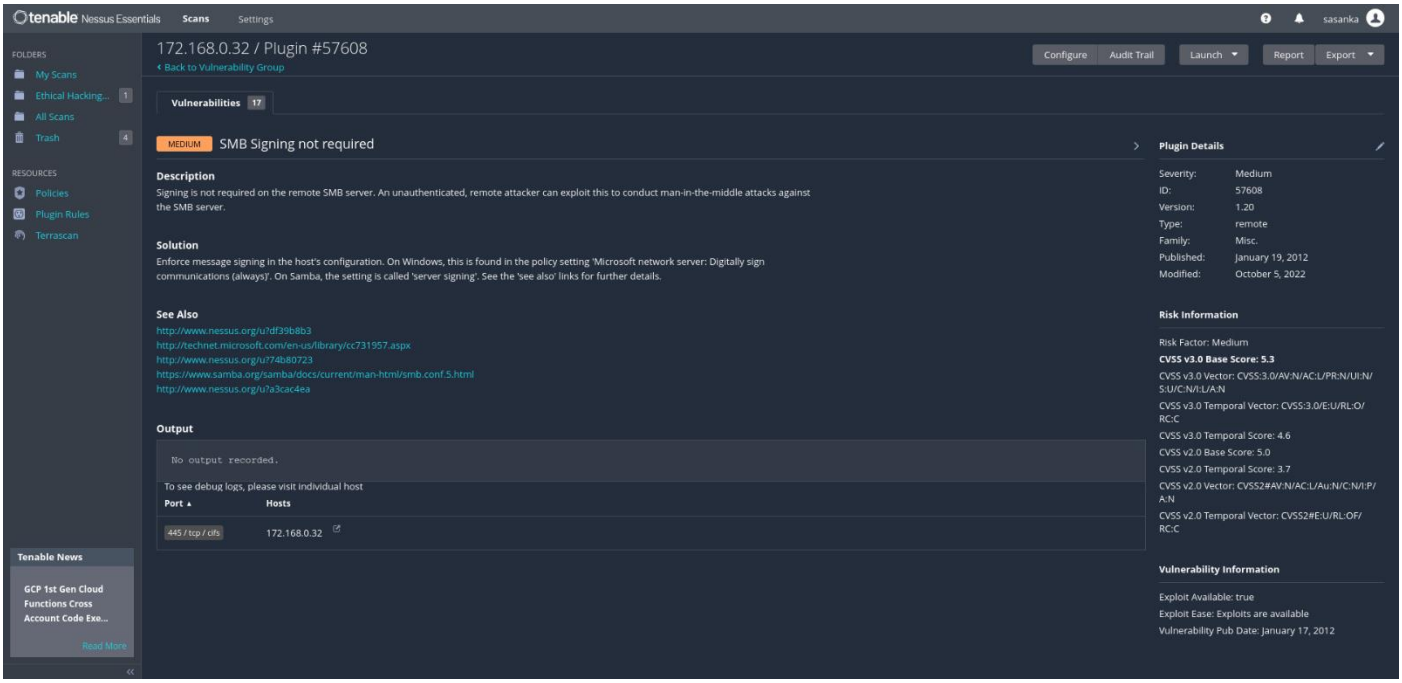

Figure24: Vulnerabilities for IP 172.168.0.32

CVE ID: N/A
Severity: Medium
Description: SMB signing is not required on the remote system. This could allow an attacker to perform man-in-the-middle attacks by intercepting and modifying SMB communication.

3. SMB Service with Guest Access

CVE ID: N/A
Severity: Low
Description: The SMB service on the target allows access using the guest account, which may allow unauthenticated access to shared resources.

4. Microsoft Windows RPC (Open Port 135)

Figure25: rpcclient on 172.168.0.32.

CVE ID: N/A
Severity: Low to Medium
Description: The target is running Microsoft Windows RPC service on port 135, which could potentially be exploited by remote attackers if the service is misconfigured.

5. Open SMB Port (445) with No SMB Signing

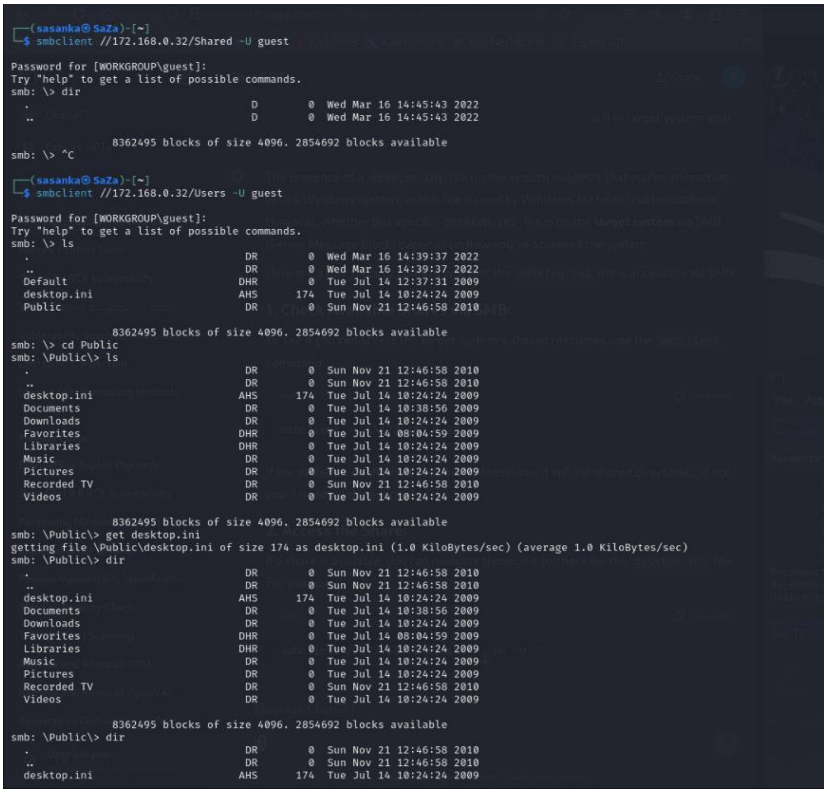

Figure26: SMB Shares Details on 172.168.0.32

CVE ID: N/A
Severity: Medium
Description: SMB port 445 is open without SMB signing enabled. This can lead to vulnerabilities in file sharing and remote access protocols.
Solution: Enforce SMB signing or configure access controls for SMB connections.

6. CVE ID: N/A

Severity: Low
Description: Port 5357 is open and running Microsoft HTTPAPI, which may allow external attackers to probe the system for vulnerabilities or gather information.

172.168.0.33

1. SSL Medium Strength Cipher Suites Supported (SWEET32):

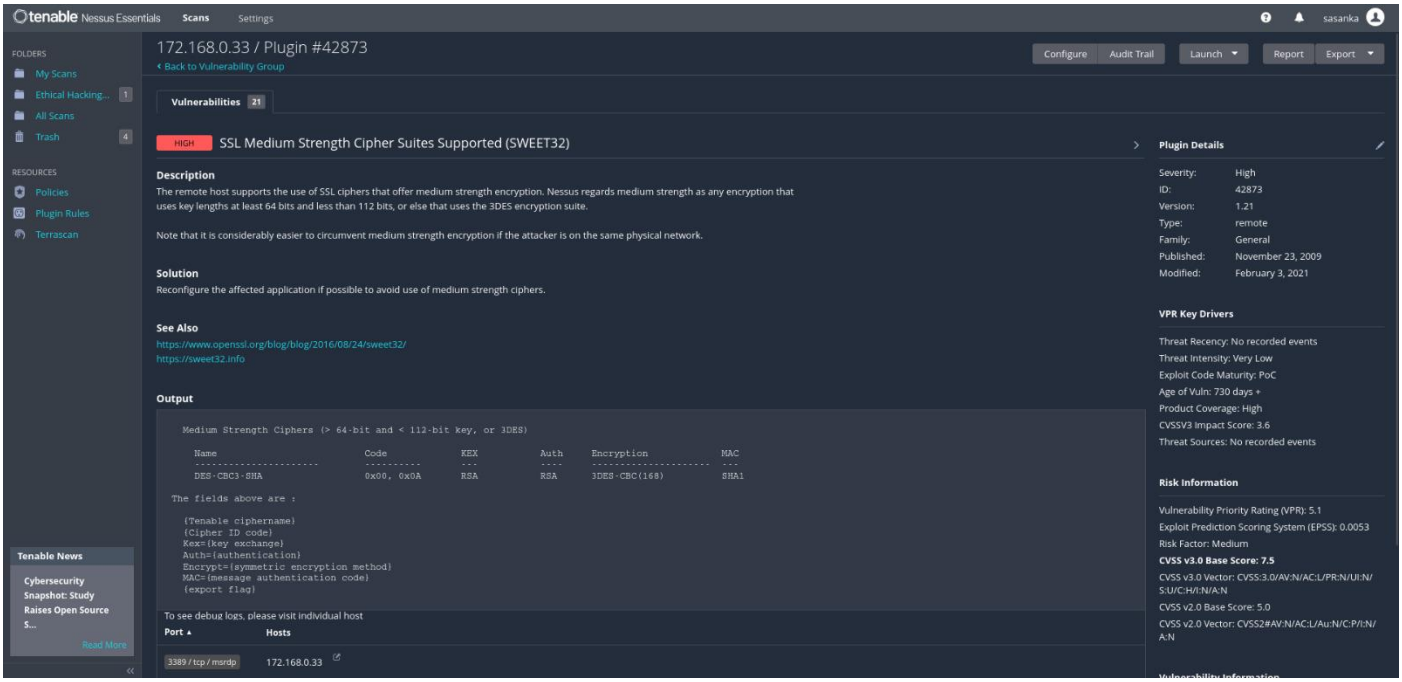

Figure27: Vulnerabilities for IP 172.168.0.33

Severity: High
Description: The remote host supports the use of medium strength SSL ciphers, such as 3DES, which are vulnerable to attacks when the attacker is on the same physical network.

2. SSL Certificate Cannot Be Trusted:

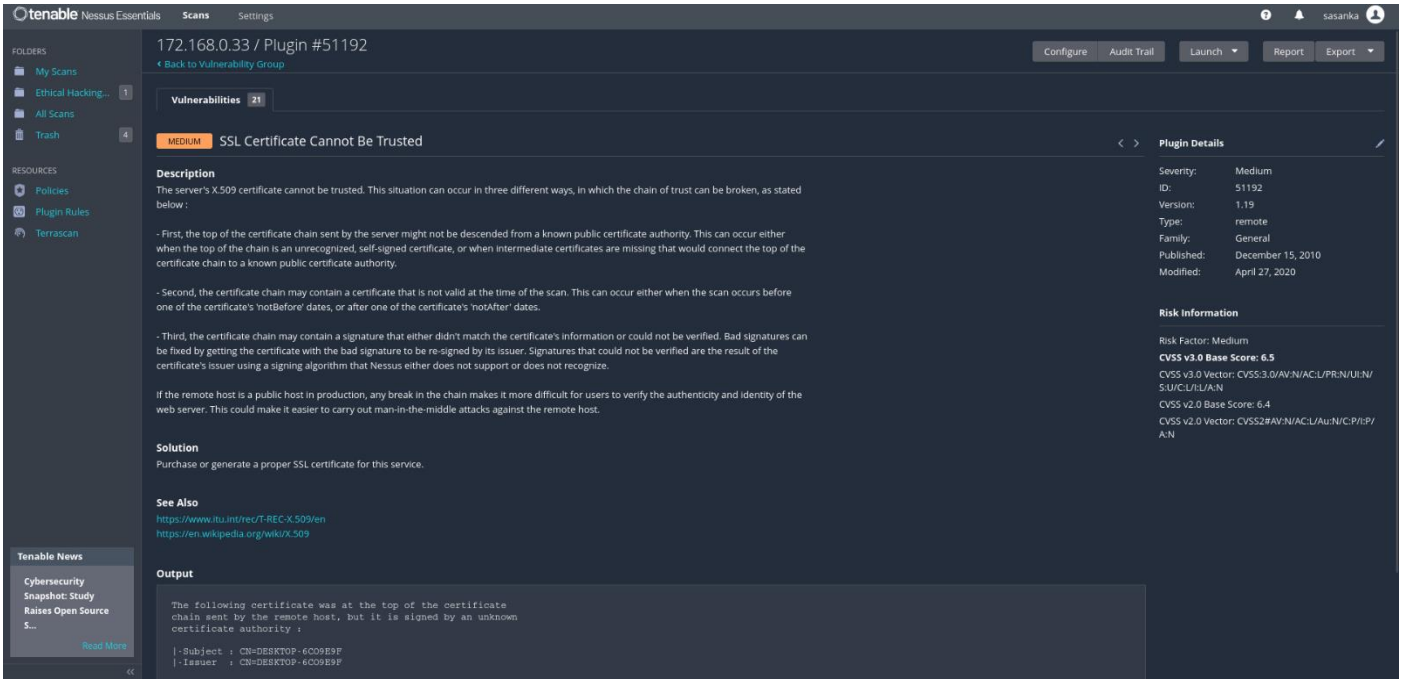

Figure28: Vulnerabilities for IP 172.168.0.33

Severity: Medium
Description: The server's SSL certificate is not trusted because it may either not be signed by a known certificate authority or may have other trust issues.

3. SSL Self-Signed Certificate:

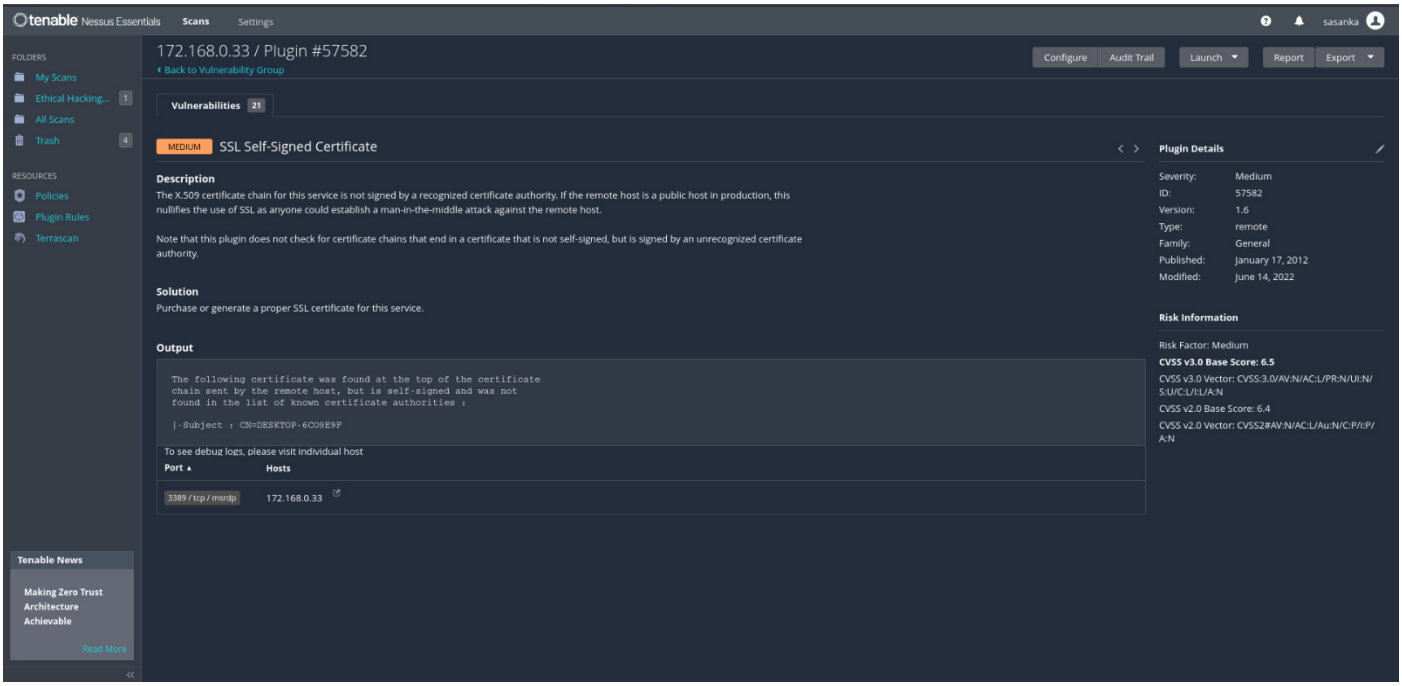

Figure29: Vulnerabilities for IP 172.168.0.33

Severity: Medium
Description: The remote host uses a self-signed certificate, which cannot be trusted for secure communication.
Solution: Replace the self-signed certificate with one signed by a trusted certificate authority.

4. SMB Signing Not Required:

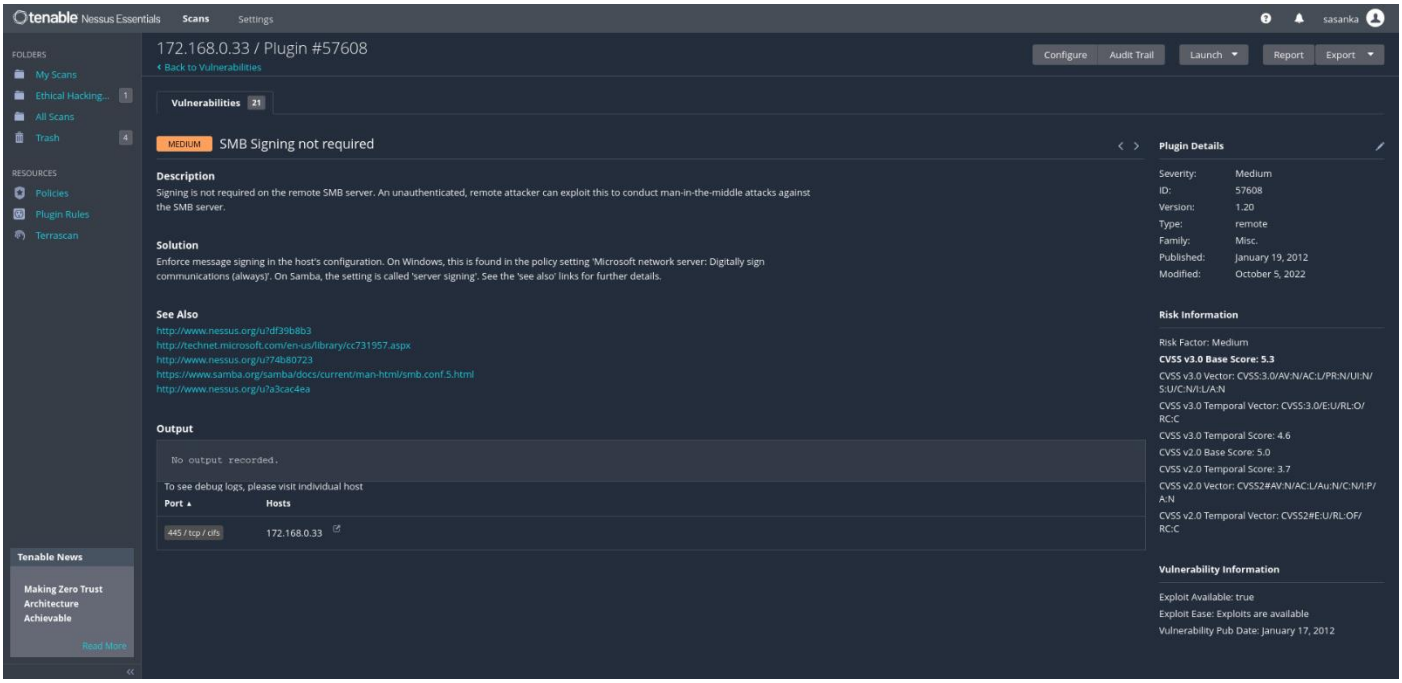

Figure30: Vulnerabilities for IP 172.168.0.33

Severity: Medium
Description: The remote SMB server does not require message signing, which exposes the service to man-in-the-middle attacks.

5. TLS 1.0 Protocol Detection:

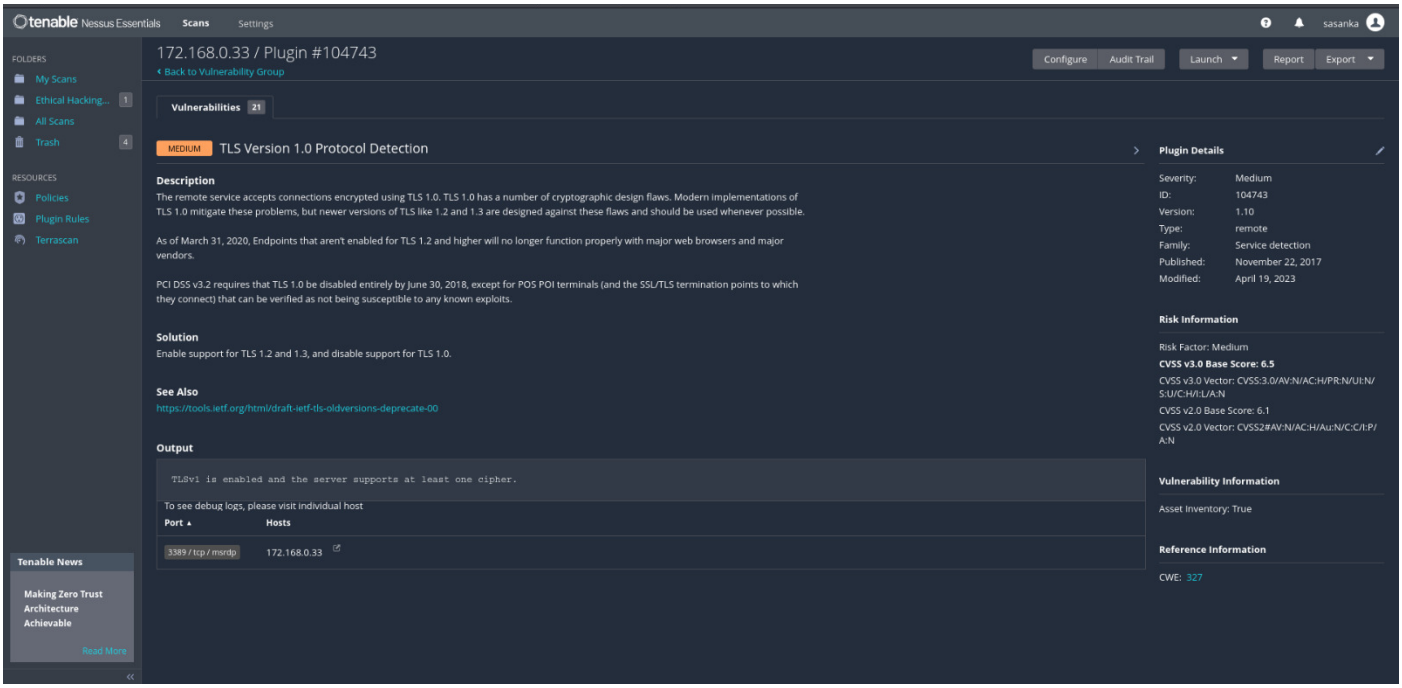

Figure31: Vulnerabilities for IP 172.168.0.33

Severity: Medium
Description: The remote service supports the outdated TLS 1.0, which has cryptographic vulnerabilities.

6. TLS 1.1 Deprecated Protocol:

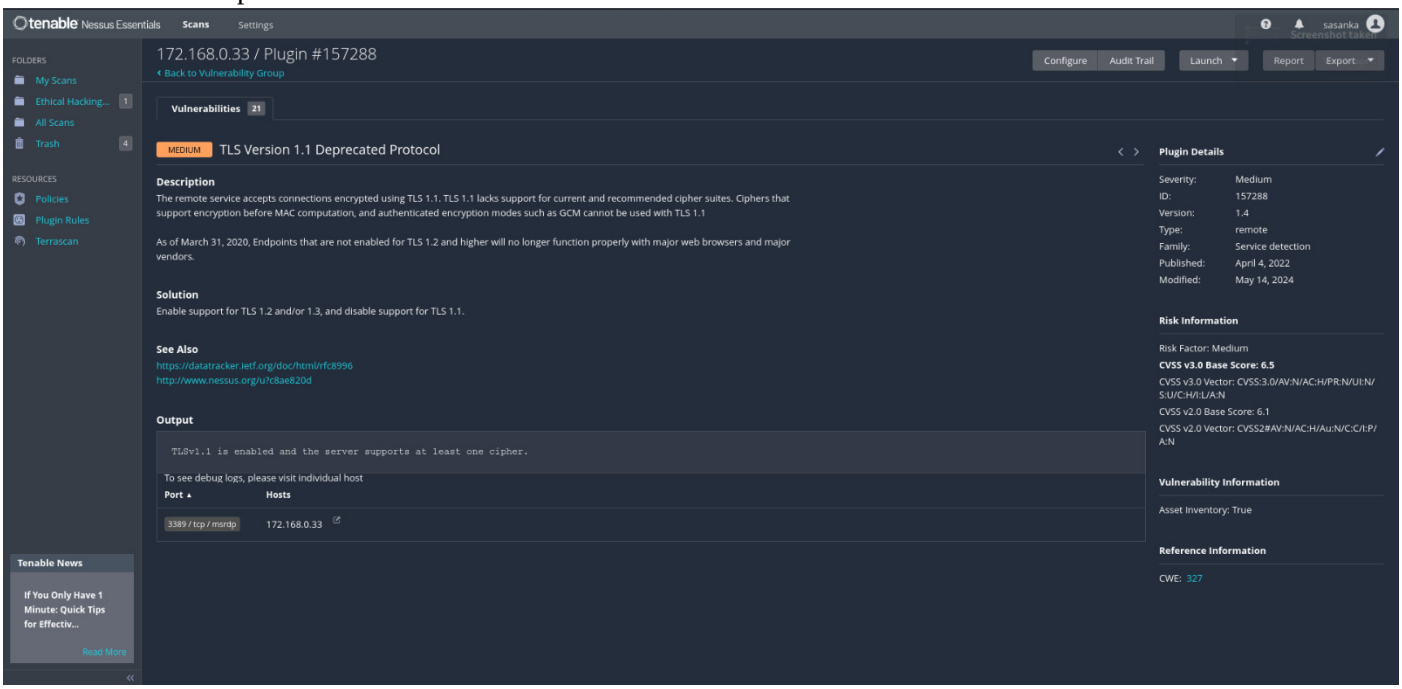

Figure32: Vulnerabilities for IP 172.168.0.33

Severity: Medium
Description: The remote service supports TLS 1.1, which lacks support for current cipher suites.

7. Terminal Services Doesn't Use Network Level Authentication (NLA) Only:

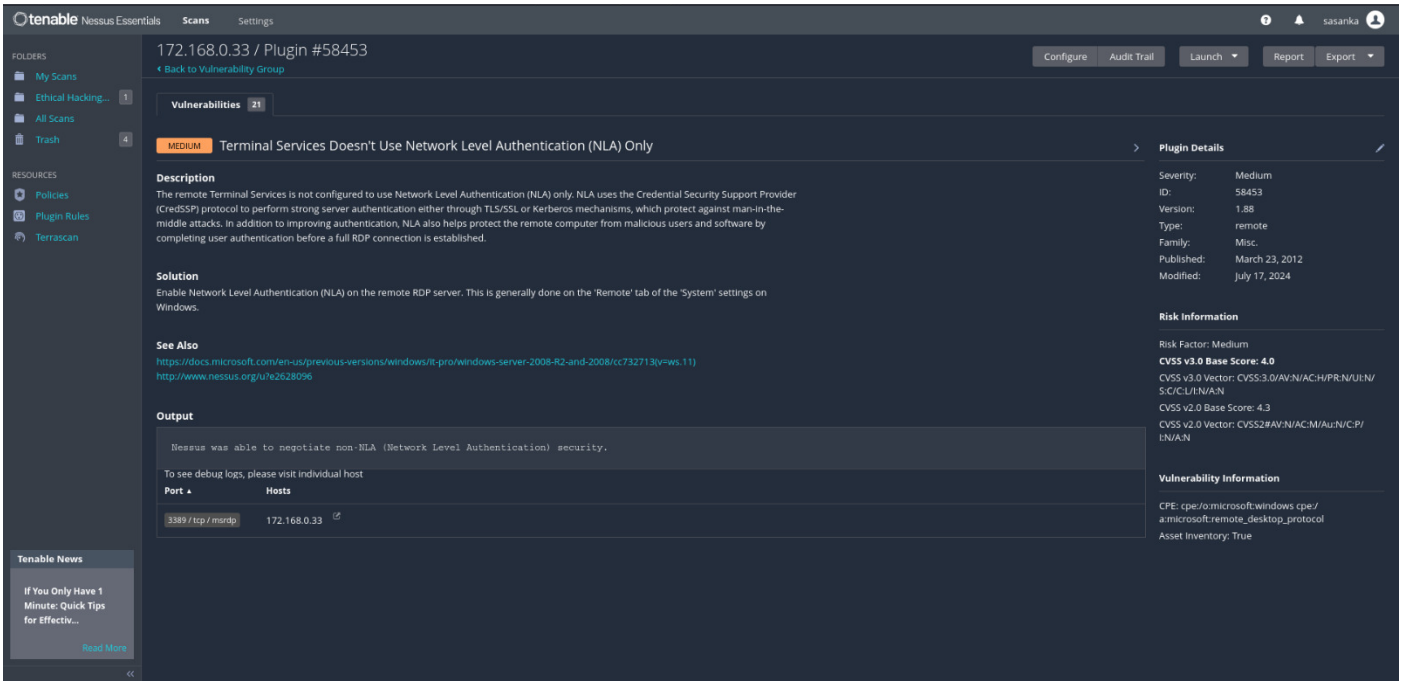

Figure33: Vulnerabilities for IP 172.168.0.33

Severity: Medium
Description: The remote RDP server does not enforce Network Level Authentication (NLA), which weakens security.

172.168.0.34

Since the configuration and services are identical to 172.168.0.33, I will skip a separate vulnerability scan for 172.168.0.34. The findings from 172.168.0.33 should be applicable to 172.168.0.34, and the scan results for 172.168.0.33 will suffice for both hosts unless there are specific differences identified.

172.168.0.35

1. Anonymous FTP Login Allowed (CVE-2015-1635)

Severity: High
Description: Anonymous FTP login is enabled, allowing unauthenticated users to access the FTP service. This poses a risk of unauthorized access and exploitation of the system. Attackers can upload or download files, potentially leading to further exploitation.

3. Unnecessary Ports and Services Open

Service: HTTP on port 80 and HTTPAPI on port 5985
Severity: Medium
Description: Open ports without secure configurations (e.g., HTTP on port 80 and HTTPAPI) can expose the server to various attacks, such as information disclosure, denial of service (DoS), and potential vulnerabilities in the services running.

172.168.0.38

1. IIS FTP Service Buffer Overflow Vulnerability.

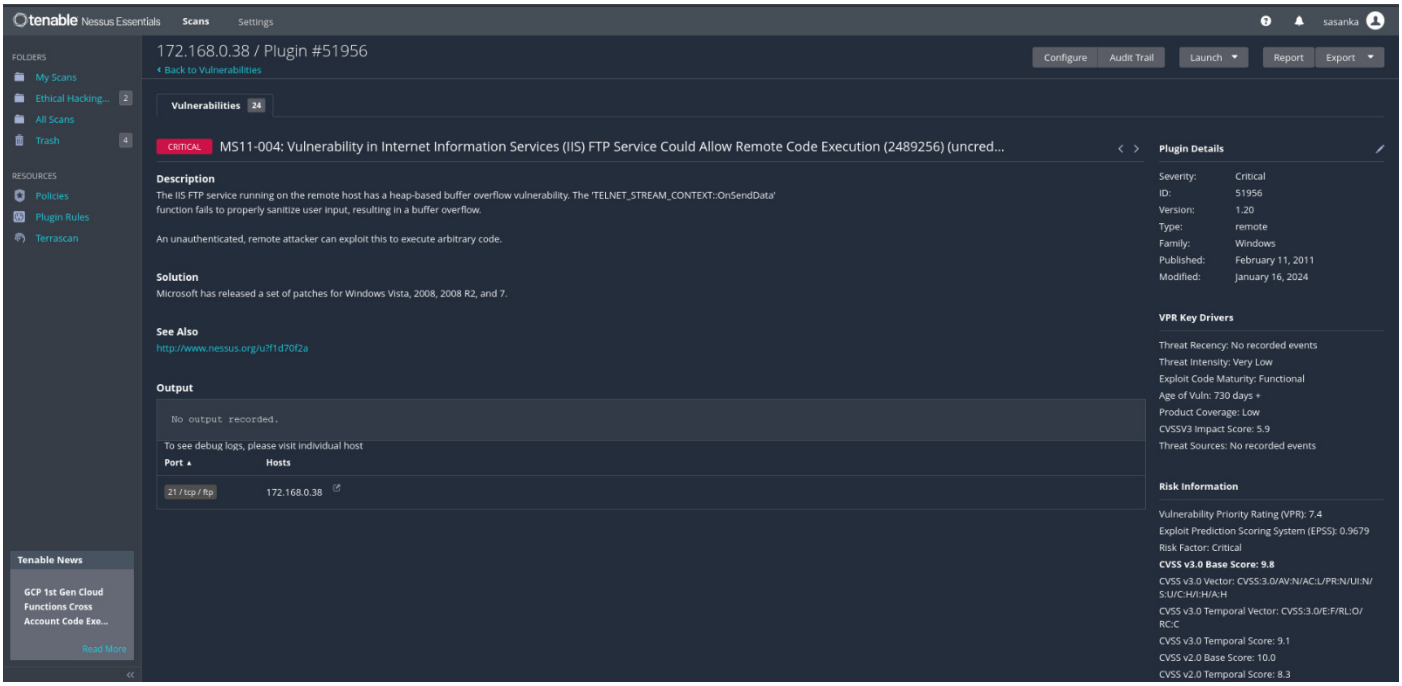

Figure34: Vulnerabilities for IP 172.168.0.38

Severity: Critical
CVE: CVE-2010-3972
CVSS v3.0 Base Score: 9.8
Description: The IIS FTP service is vulnerable to a heap-based buffer overflow due to improper sanitization of user input in the TELNET_STREAM_CONTEXT::OnSendData function. An attacker could exploit this remotely to execute arbitrary code.

2. Unsupported Windows OS Vulnerability

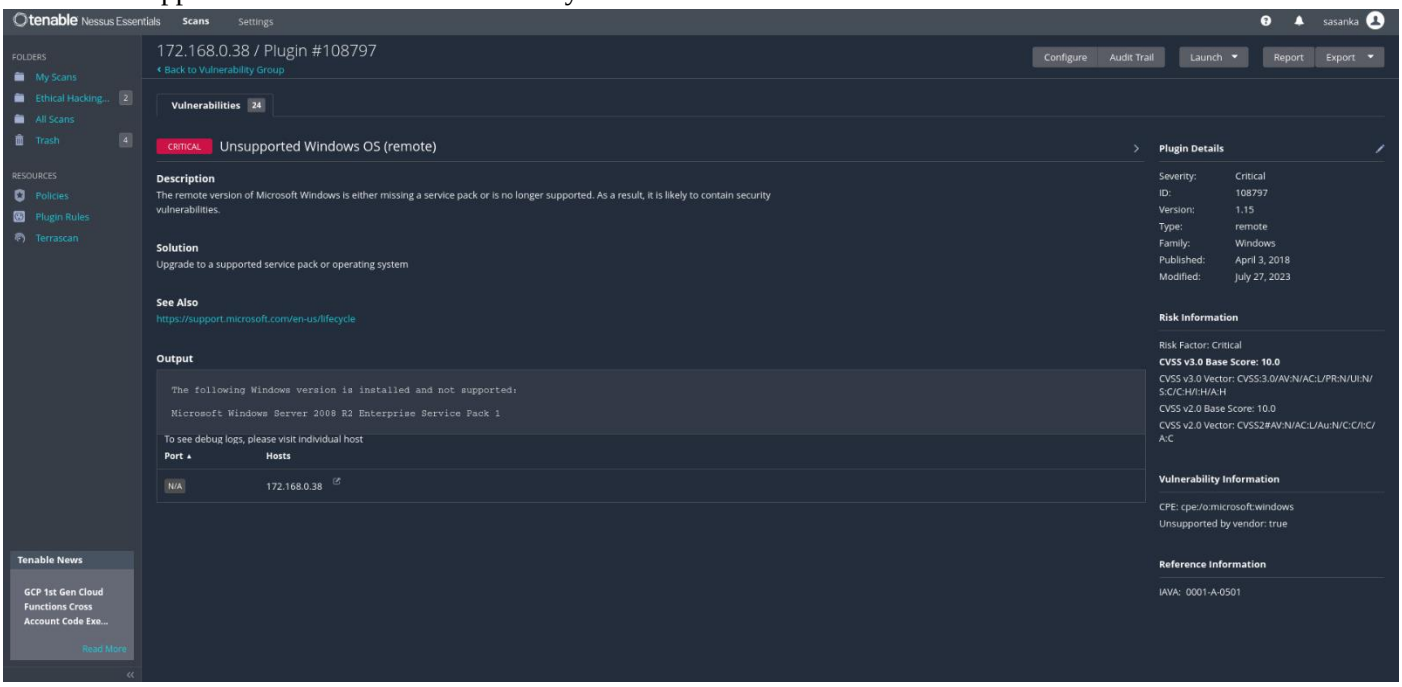

Figure35: Vulnerabilities for IP 172.168.0.38

Severity: Critical
CVSS v3.0 Base Score: 10.0
Description: The remote Windows version is unsupported or missing a service pack, making it susceptible to various security vulnerabilities.

3. SMBv1 Vulnerability (EternalBlue)

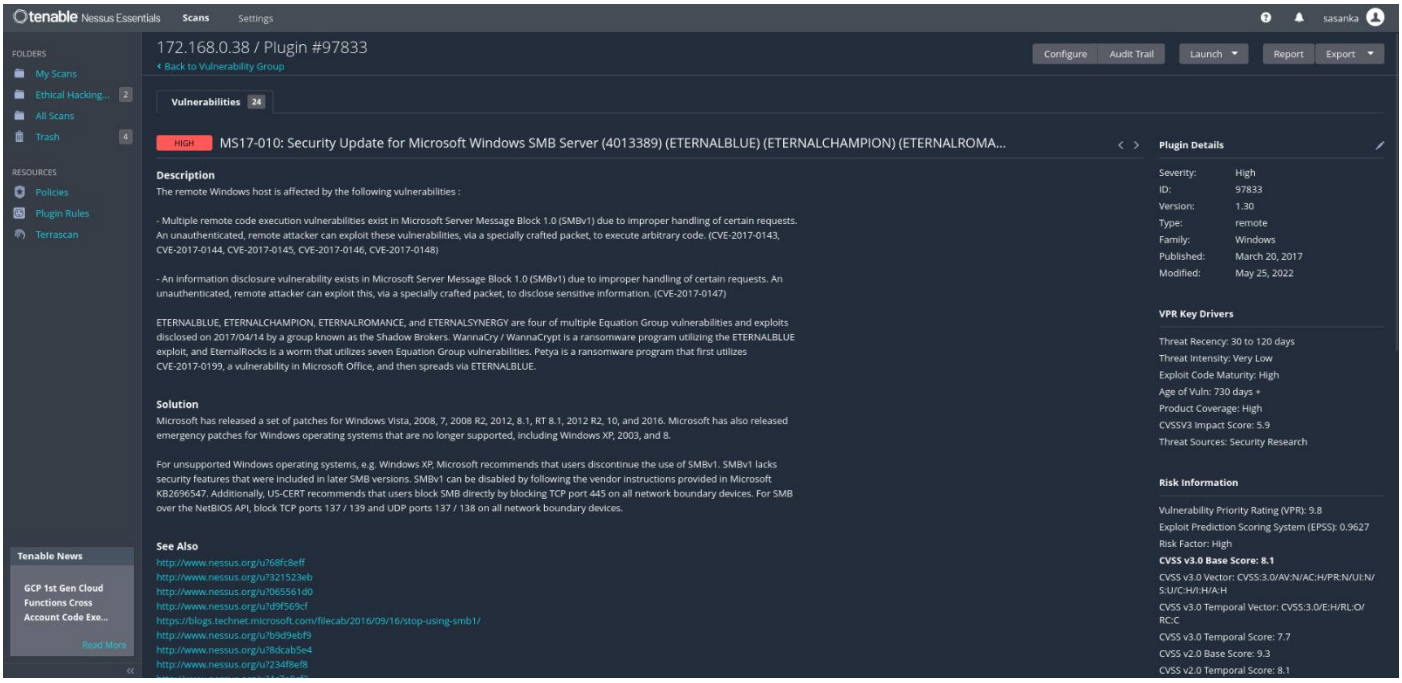

Figure36: Vulnerabilities for IP 172.168.0.38

Severity: High
CVSS v3.0 Base Score: 8.1
CVE: Multiple (CVE-2017-0143, CVE-2017-0144, etc.)
Description: Remote code execution vulnerabilities exist in SMBv1 due to improper handling of requests, allowing unauthenticated remote attackers to execute arbitrary code.

4. SAM and LSAD Protocol Elevation of Privilege

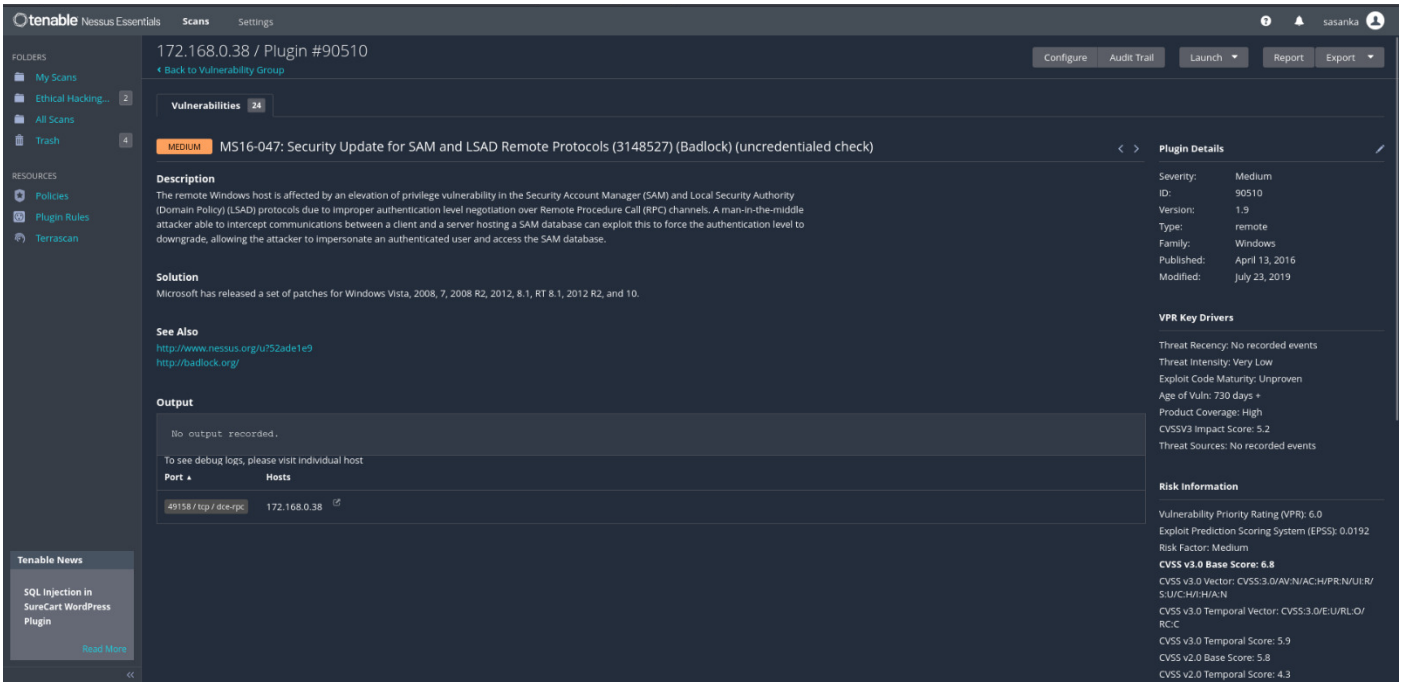

Figure37: Vulnerabilities for IP 172.168.0.38

Severity: Medium
CVSS v3.0 Base Score: 6.8
CVE: CVE-2016-0128
Description: An elevation of privilege vulnerability in the SAM and LSAD protocols could allow attackers to impersonate an authenticated user and access sensitive information.

5. Information Disclosure in IIS FTP Service

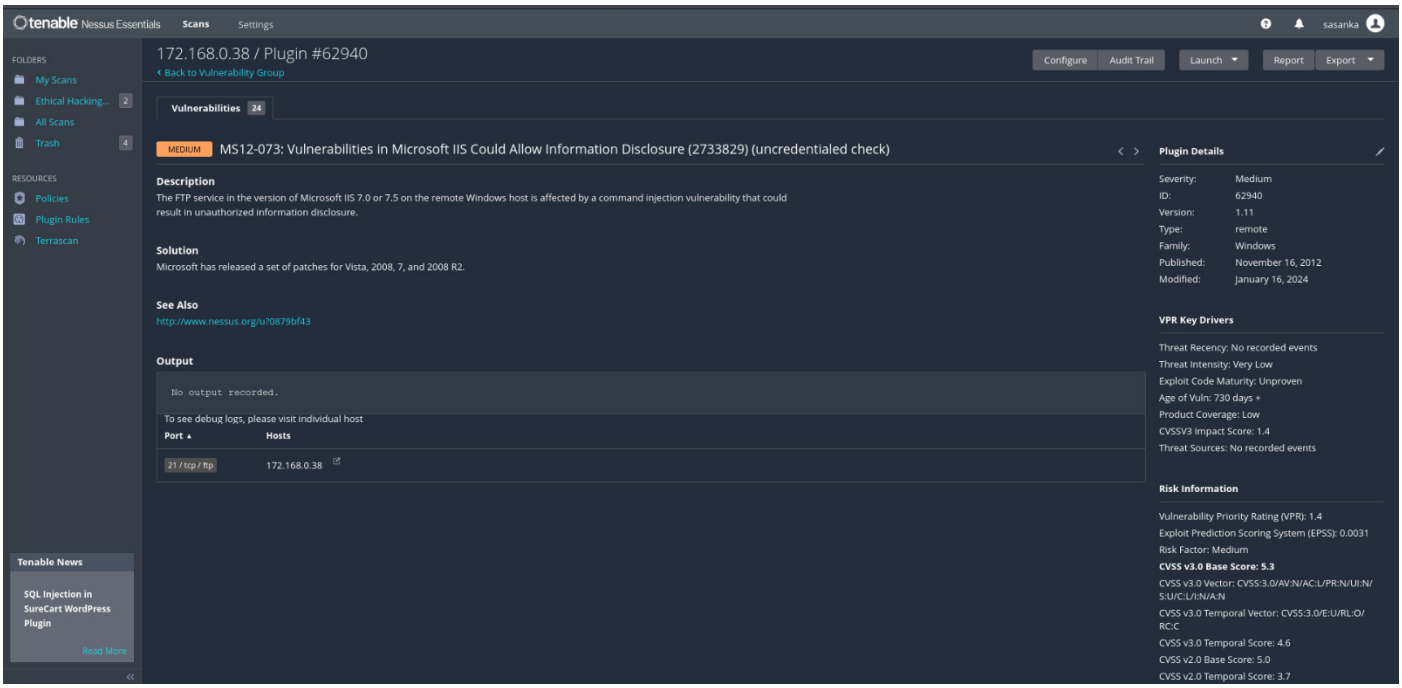

Figure38: Vulnerabilities for IP 172.168.0.38

Severity: Medium
CVSS v3.0 Base Score: 5.3
CVE: CVE-2012-2532
Description: A command injection vulnerability in IIS FTP could allow unauthorized information disclosure.

6. Unencrypted Telnet Server

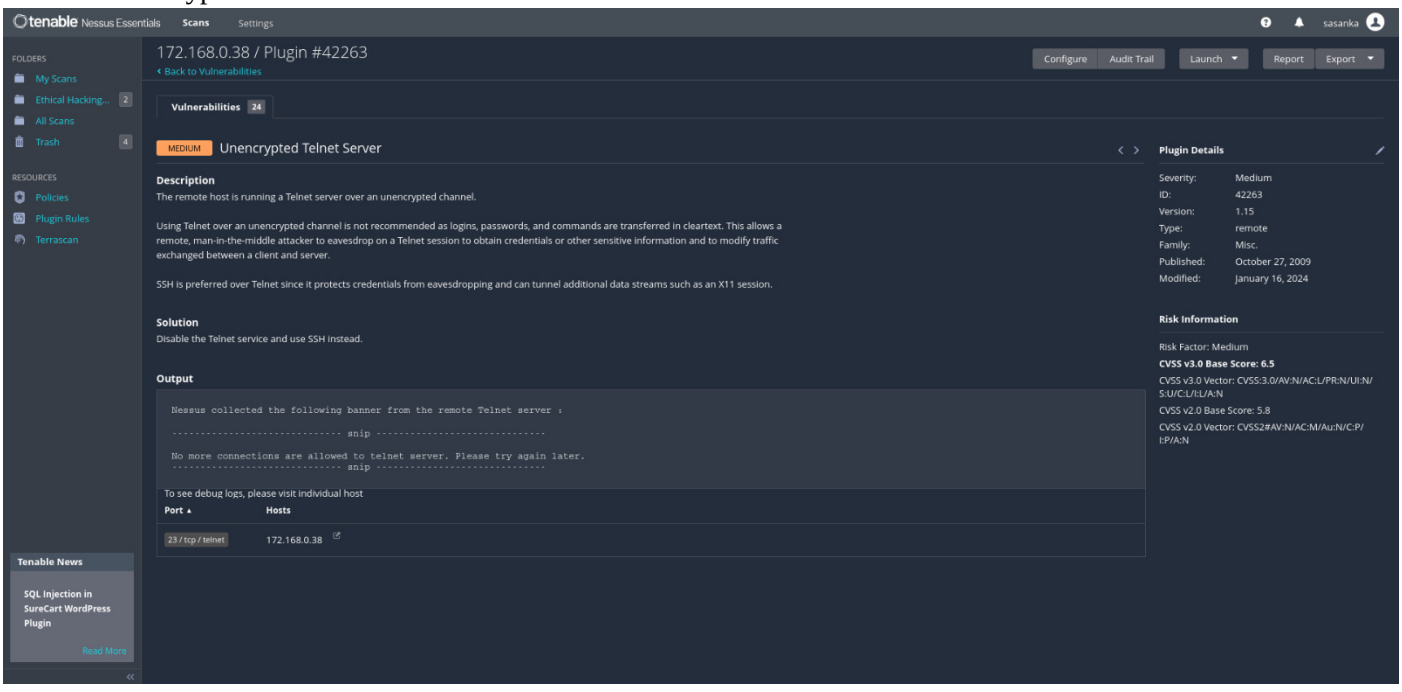

Figure39: Vulnerabilities for IP 172.168.0.38

Severity: Medium
CVSS v3.0 Base Score: 6.5
Description: The remote host is running a Telnet server over an unencrypted channel, making credentials and sensitive information vulnerable to eavesdropping.

7. SMB Signing not required.

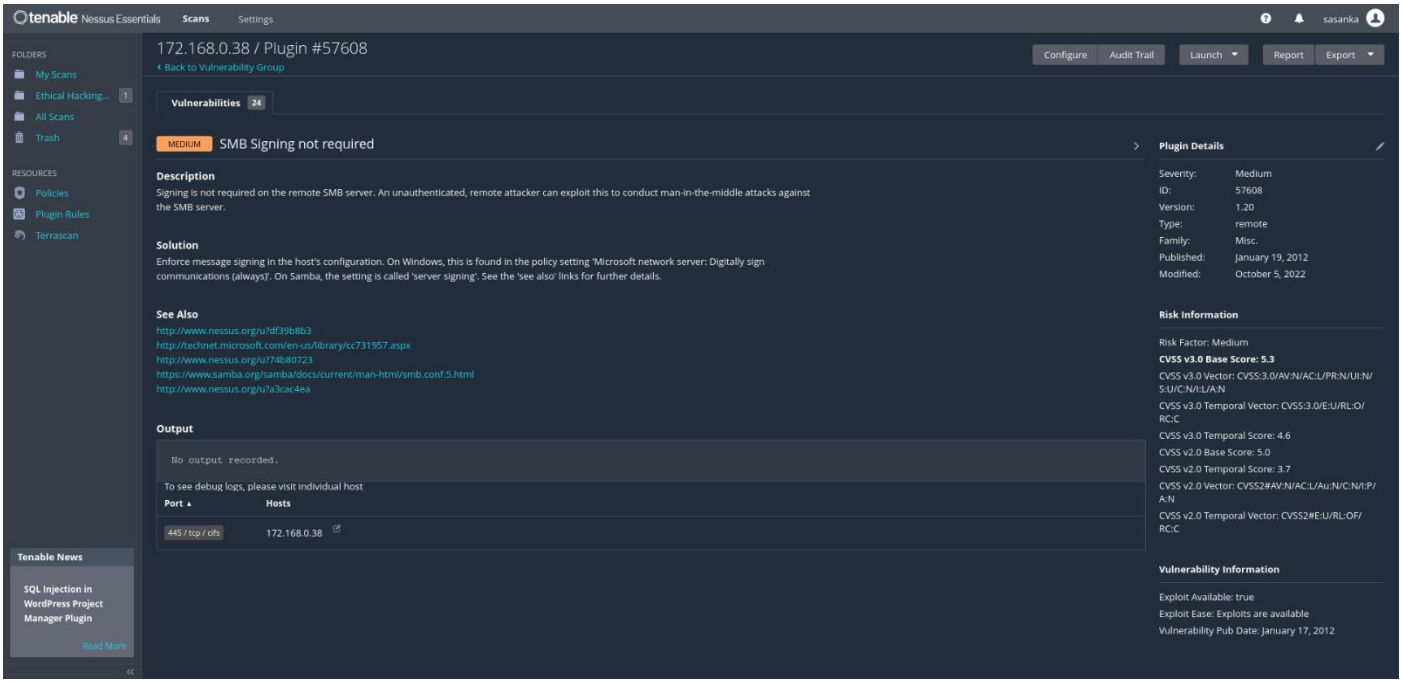

Figure40: Vulnerabilities for IP 172.168.0.38

The remote SMB server does not require signing. An unauthenticated remote attacker can use this to launch man-in-the-middle attacks on the SMB Server.

8. ICMP Timstamp Request Remote Date Disclosure.

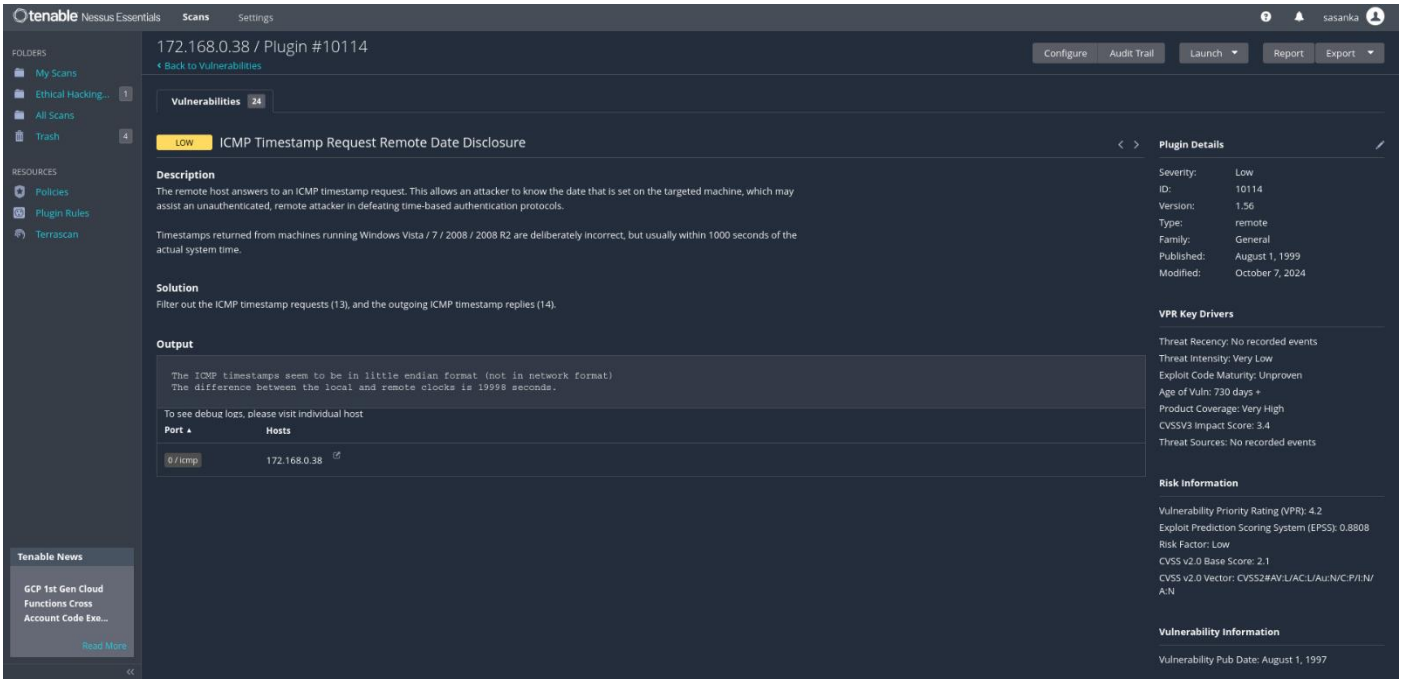

Figure41: Vulnerabilities for IP 172.168.0.38

The ICMP Timestamp Request Remote Date Disclosure vulnerability allows an attacker to learn the target system's date and time, potentially aiding in the bypass of time-based authentication. While newer Windows versions return deliberately incorrect timestamps, the discrepancy is usually within 1000 seconds.

4. Exploitation

172.168.0.1

OpenSSH RCE:

Remote code execution via OpenSSH CVEs (CVE-2024-6387, CVE-2024-39894).

Attack complexity, system configurations, and protections in place prevented a successful attack.

The SSH brute force attack was not performed because the company's system has restrictions in place to prevent it.

172.168.0.32

SMB Brute forcing.

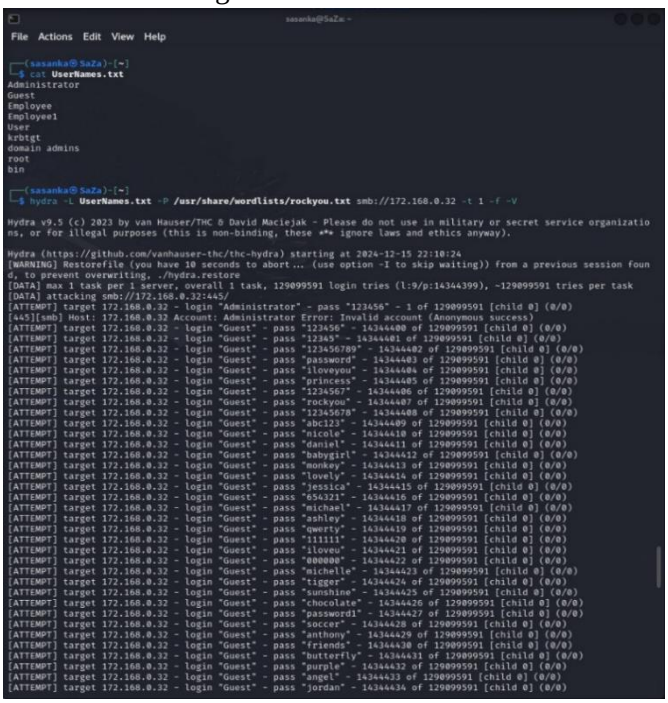

Figure42: smb bruteforcing.

Due to time constraints, we were unable to successfully identify valid credentials during the brute force attack.

172.168.0.33

RDP Brute Force with Hydra

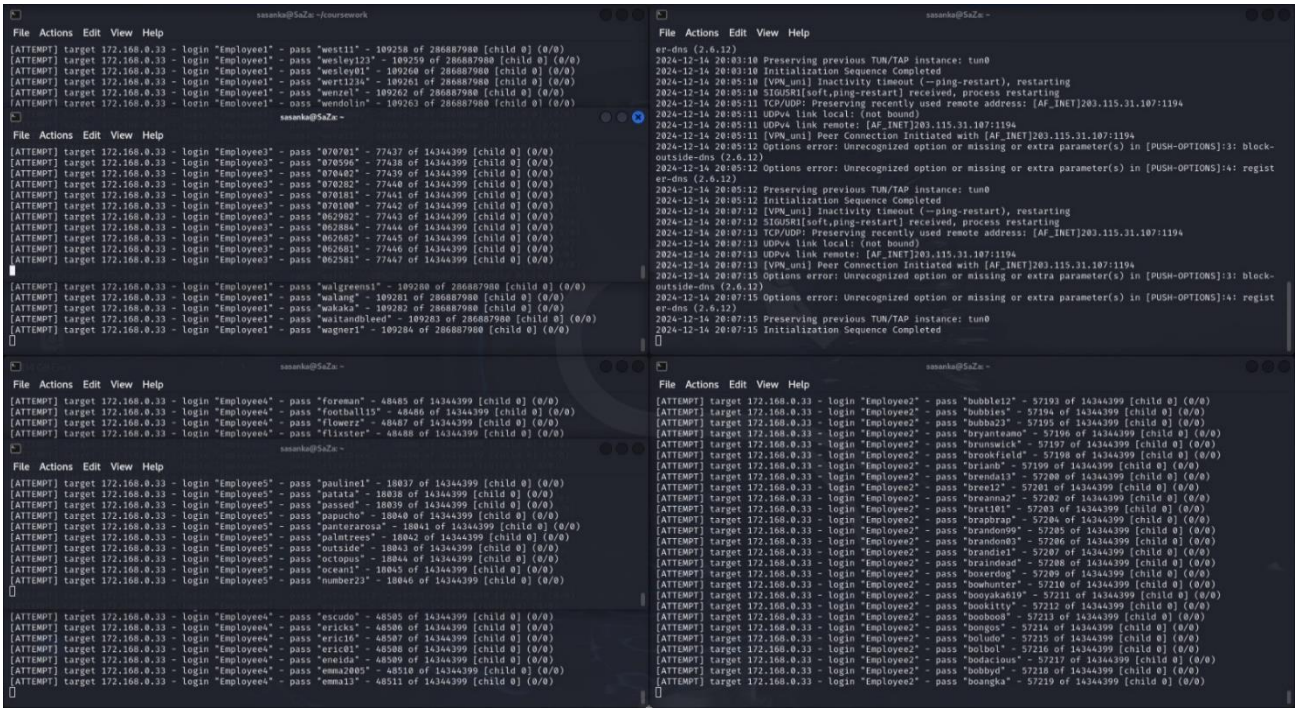

Figure43: RDP BruteForcing.

Due to time constraints, we were unable to successfully identify valid credentials during the brute force attack.

172.168.0.35

While anonymous FTP login allows file uploads, directory traversal and Remote Code Execution (RCE) were not possible due to restrictions in place. The FTP brute-force attempt also did not yield valid credentials.

172.168.0.38

No known exploits are available for CVE-2016-0128 and CVE-2010-3972.

EternalBlue Exploitation.

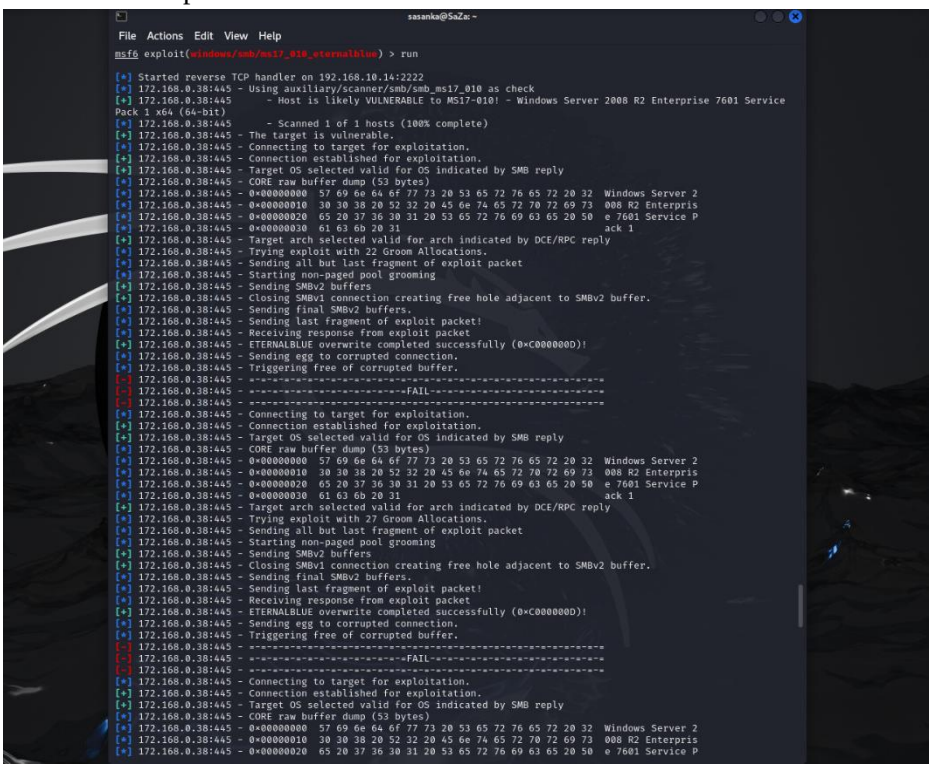

Figure44: EternalBlue Exploitation.

The exploit failed to create a session likely due to system instability or resource exhaustion, possibly triggered by multiple concurrent exploitation attempts.

5. Post Exploitation

Given that no successful exploitation occurred, post-exploitation activities were not applicable. However, if access were obtained, typical post-exploitation activities could include:

- Persistence: Setting up backdoors or rootkits to ensure continued access to the system.
- Data Exfiltration: Collecting sensitive data from the compromised system, including passwords, documents, or other valuable information.
- Privilege Escalation: Attempting to gain higher levels of access (e.g., root or administrator privileges) on the compromised system.
- Lateral Movement: Using the compromised system as a foothold to further infiltrate the network.

Since no foothold was successfully gained, these actions were not executed during this engagement. However, these techniques would be considered if a future compromise occurs.

Web Application Pentest.

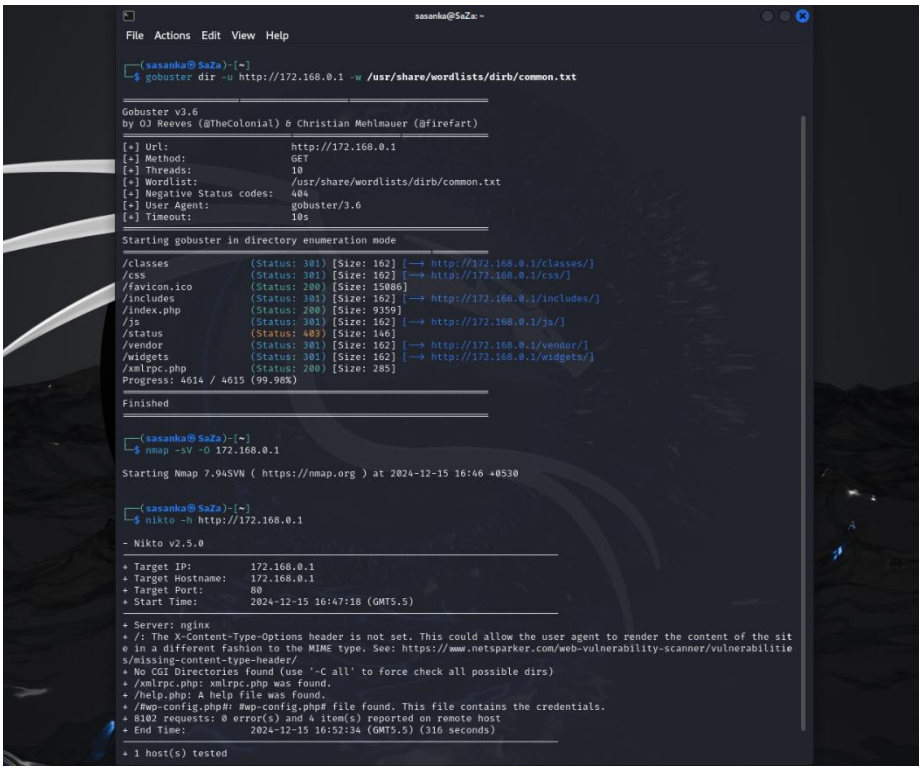

Figure45:

Target Information

- IP Address: 172.168.0.1
- Web Service: pfSense Web Interface
- Web Server: nginx
- Web Application: pfSense (Firewall/Router Management Interface)

Reconnaissance & Enumeration

Directory Brute-forcing (gobuster)

Discovered the following key directories -

/classes/, /css/, /includes/, /js/, /vendor/, /widgets/ — These directories are typical in web applications but might be irrelevant to the core pfSense interface.

/index.php: Core pfSense interface page.

/xmlrpc.php: Part of the test, but likely irrelevant for pfSense, unless a specific module is enabled.

/status directory with 403 status suggests an access-controlled page.

Vulnerability Scanning (nikto)

Missing HTTP Header - The X-Content-Type-Options header is not set, which may present a potential vulnerability.

Found some common files such as /xmlrpc.php, which may not be applicable to pfSense unless some WordPress-like integration is present.

/wp-config.php – is mentioned as a possible config file but is not likely to be relevant for pfSense unless custom services were added.

The XML-RPC method calls failed, as expected for pfSense, since it's unlikely to use XML-RPC unless integrated with WordPress or other CMS systems.

Testing of XML-RPC methods

Several XML-RPC methods were tested (system.listMethods, wp.getCategories, wp.getUsersBlogs, wp.getRecentPosts) using the following payload

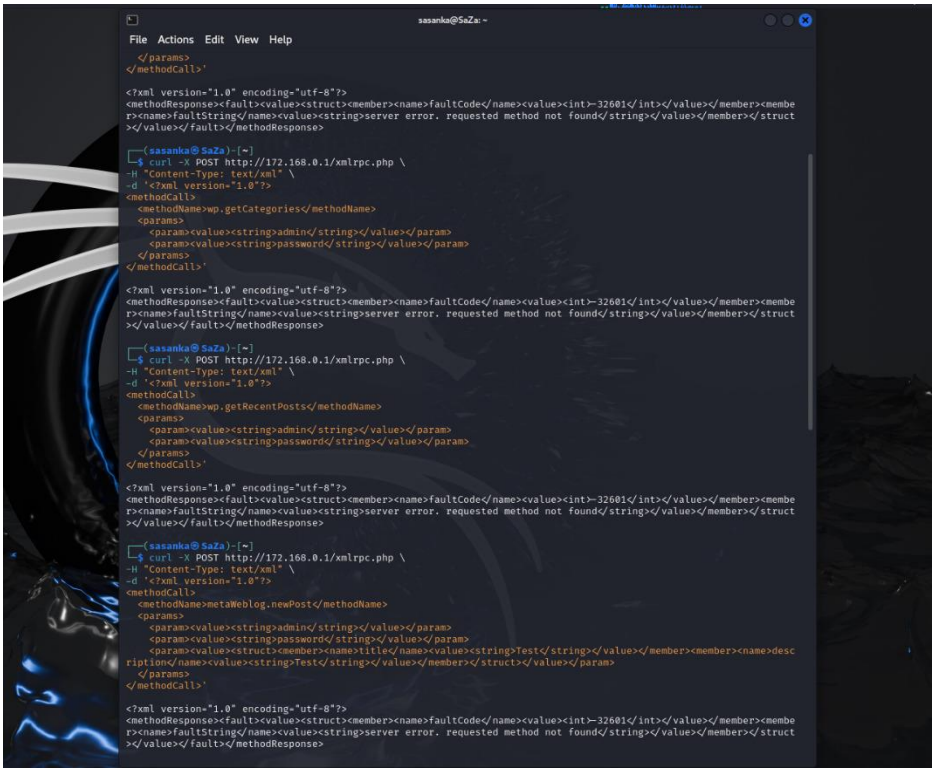

Figure46:

Result-all XML-RPC method requests returned a fault code -32601, indicating that the requested method was not found.

Conclusion is that XML-RPC functionality is likely disabled or irrelevant to pfSense, and the errors are not indicative of an underlying vulnerability.

Exploitation

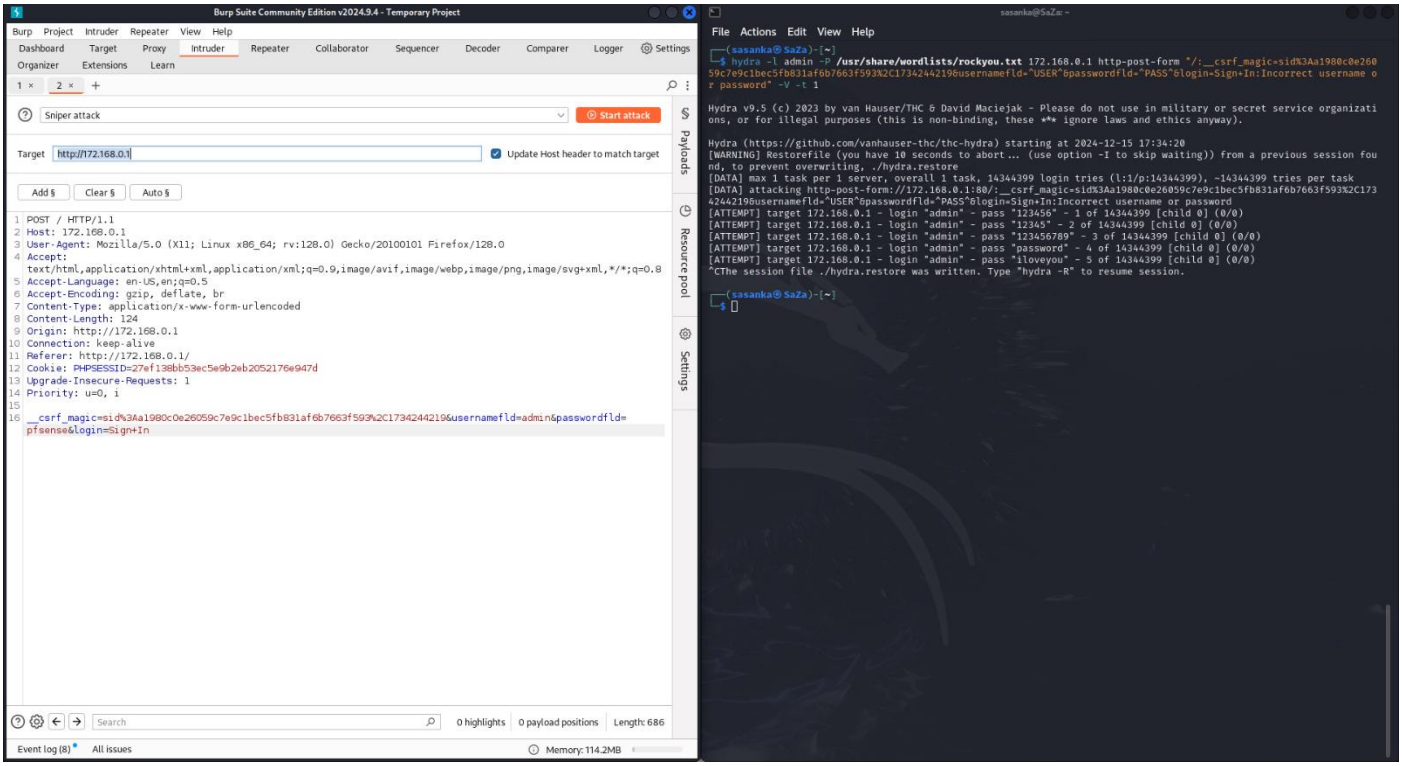

Figure47:

CSRF Protection –

The presence of a CSRF token (__csrf_magic) in the login form was identified, which helps to prevent cross-site request forgery attacks.

Attacks did not continue to avoid impacting the company's systems.

Remediation Summary

Short Term

- Short Term Remediation (Immediate Fixes):
- Patch OpenSSH: Apply patches to mitigate the OpenSSH Remote Code Execution vulnerabilities (CVE-2023-39448 and CVE-2023-38408). Upgrade OpenSSH to version 9.8 or later to address these vulnerabilities.
- Disable NTP Mode 6 Queries: Restrict the NTP mode 6 queries to prevent abuse and enhance security.
- Disable DNS Recursive Queries: Configure DNS servers to disable recursive queries for external addresses to avoid DNS cache poisoning attacks.
- Change Weak Credentials on OpenSSH: Enforce stronger SSH authentication (e.g., using keys instead of passwords) and disable weak encryption methods.
- Disable ICMP Timestamps: Disable ICMP timestamp requests to prevent revealing information about the system's date and time.
- Fix Anonymous FTP Login: Disable anonymous login on FTP servers to restrict access to authorized users only.
- Enforce SMB Signing: Enable SMB signing on servers and clients to prevent Man-in-the-Middle (MITM) attacks.
- Upgrade Windows OS: Apply critical patches and update unsupported versions of Windows to a supported and secure version.
- Disable SMBv1: Disable SMBv1 on Windows systems to mitigate EternalBlue (CVE-2017-0144).
- Disable Telnet Service: Disable or secure the Telnet service, as it sends sensitive information in plaintext.

Medium Term

- Network Segmentation: Isolate vulnerable systems (e.g., those running unsupported Windows versions) into separate network segments to reduce the impact of an attack.
- Strengthen RDP Security: Require Network Level Authentication (NLA) for RDP sessions and consider using more secure protocols like VPNs or SSH tunnels.
- Implement TLS 1.2+: Disable outdated protocols like TLS 1.0 and TLS 1.1 to enforce stronger encryption (TLS 1.2 or higher).
- Update Web Servers: Ensure that all web services are up-to-date and using secure configurations (e.g., disabling weak ciphers and enforcing strong SSL/TLS certificates).
- Secure FTP Service: Use secure alternatives like SFTP instead of FTP, or enforce encrypted FTP with strong authentication.

Long Term

- Regular Vulnerability Scanning: Implement regular vulnerability scans and patch management to ensure systems stay updated with the latest security patches.
- Audits and Access Controls: Conduct periodic security audits and enforce strict access controls across the network to limit administrative privileges.
- Security Awareness Training: Provide training to users to avoid phishing, poor password management, and other security lapses.
- Security Hardening: Continuously harden systems by disabling unnecessary services, removing outdated protocols, and applying the principle of least privilege.
- Incident Response Plan: Develop and test an incident response plan to handle breaches swiftly and mitigate damage.

Conclusion

The penetration test conducted on Clarke's Ceylon Team's network infrastructure has revealed several significant vulnerabilities that could be exploited by attackers if left unaddressed. These vulnerabilities, including misconfigurations in OpenSSH, outdated software versions, and weaknesses in access controls, pose a serious risk to the confidentiality, integrity, and availability of the company's systems and data.

Immediate remediation is necessary to address critical vulnerabilities, particularly focusing on patching OpenSSH and securing network services like DNS. Implementing strong password policies, multi-factor authentication, and restricting unnecessary services will further mitigate the risk of unauthorized access.

For long-term security, it is recommended that Clarke’s Ceylon Team implements continuous monitoring, regular vulnerability assessments, and network segmentation to prevent potential attacks. Regular security audits and updates to encryption protocols will also ensure that sensitive data remains protected.

By addressing these vulnerabilities, the company can significantly strengthen its security posture, reduce the risk of exploitation, and protect its critical assets from potential attacks.