Project Title:

Network Vulnerability Assessment for A More Secured Environment

Project Objective:

conduct a comprehensive vulnerability assessment of a simulated version of O-Enterprises' network environment using **Nmap** and **Nessus** to identify open ports, misconfigurations and known vulnerabilities. Provide actionable insights to improve the network's security posture.

Project Scope:

The task requires leveraging network scanning and vulnerability assessment tools and simulated real-world environment to help the client organization O-Enterprises identify and address security gaps effectively

Executive Summary:

- **Vulnerability Assessment ID:** CSA-SOC-MAY-2025-17
- **Assessment Risk Categories**: Critical/High/Medium/Low Risks

O – Enterprises noticed several discrepancies in its network environment possibly arising from misconfigurations and unpatched vulnerabilities from softwares and services in use. This gave rise to the need for a comprehensive vulnerability assessment using Nmap and Nessus to identify and mitigate these potential risks, improve overall network's security resilience and posture.

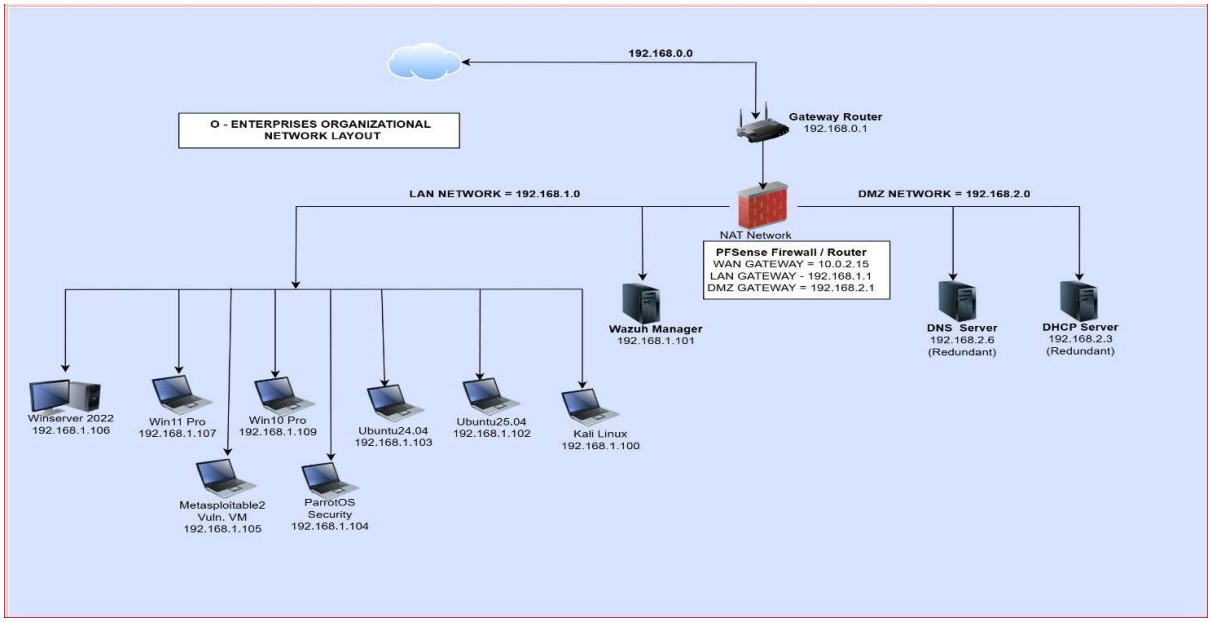
After setting studying the network environment, a thorough network scanning with Nmap was done. Several network ports were found to be open such Ports 21-FTP, 22-SSH, 80-HTTP, 443-HTTPS, 139/445-SMB and several others. Some of these ports are needed for day-to-day operations while some are not needed, left their current state due either misconfigurations or negligence.

Tenable-Nessus was also used to scan these hosts and the opened ports to determine the associated vulnerabilities and potential risk exposures. The identified risk categories ranged from critical to low and commensurate recommendations have been made to mitigate them before they are exploited by threat actors.

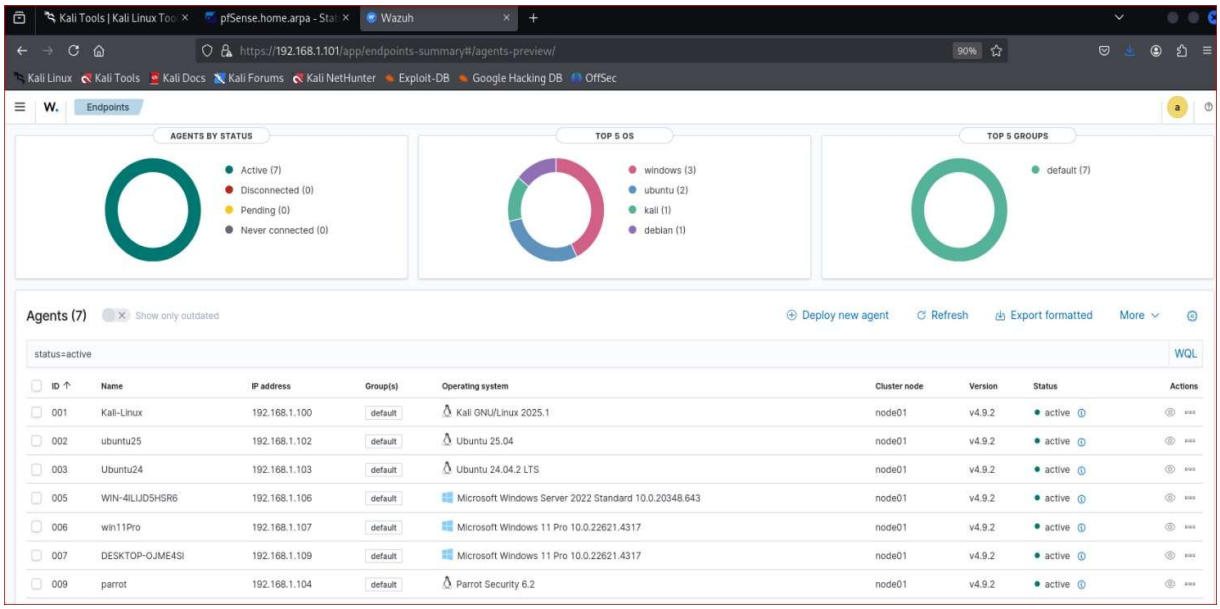
Set up of O-Enterprise network environment

The network landscape of O-Enterprise was setup in a virtual environment. Nmap and Nessus tools were installed and setup for the vulnerability assessment, tested and confirmed working in good condition. We had mix of Virtual Machine (VMs) running through the PFsense firewall and monitored on Wazuh dashboard and all were tested.

O-Enterprise Organizational network layout



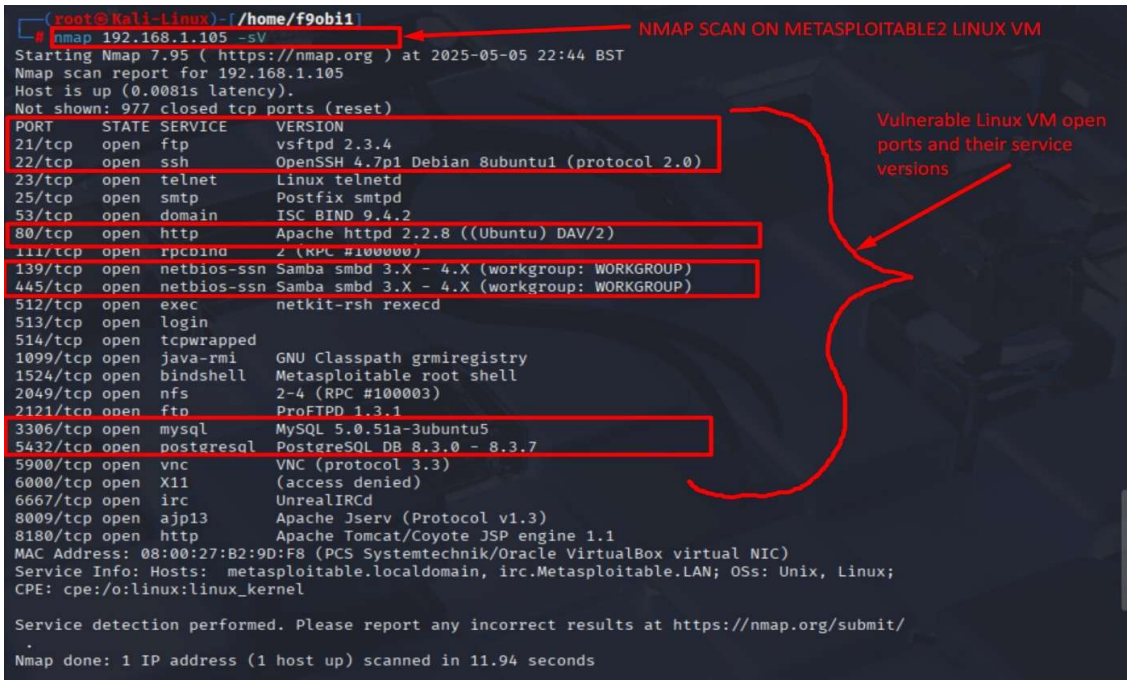
Wazuh server dashboard showing all the VMs in service

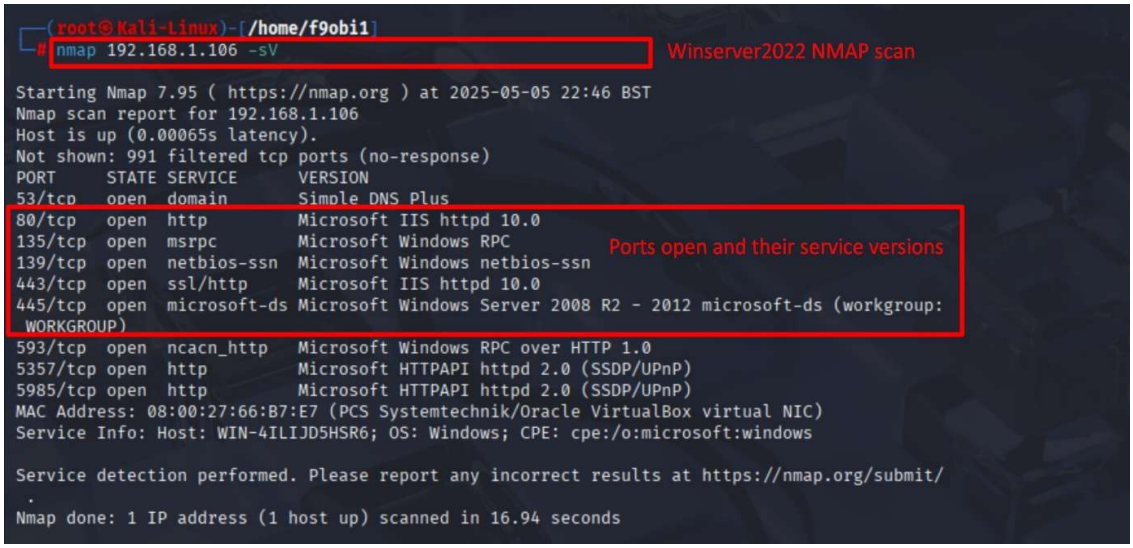


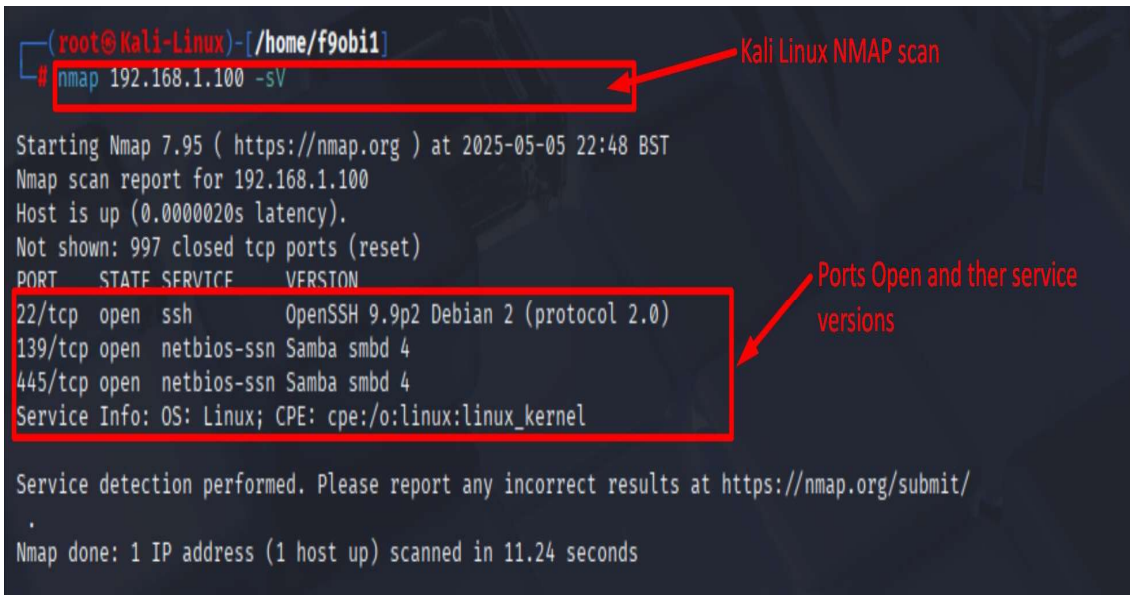
Wazuh Server vulnerability detection on the dashboard

Comprehensive VMs / network scanning Using Nmap

A comprehensive Nmap scan was done on the virtual machines to identify their open ports and corresponding network services. Kali-Linux machine was used for all scanning activities on the targeted machines. The VMs scanned were a vulnerable Linux (Metasploit2), Windows server 2022, Ubuntu Linux, windows 11 Pro and ParrotOS security including the Kali itself. Below are snapshots of some of the findings

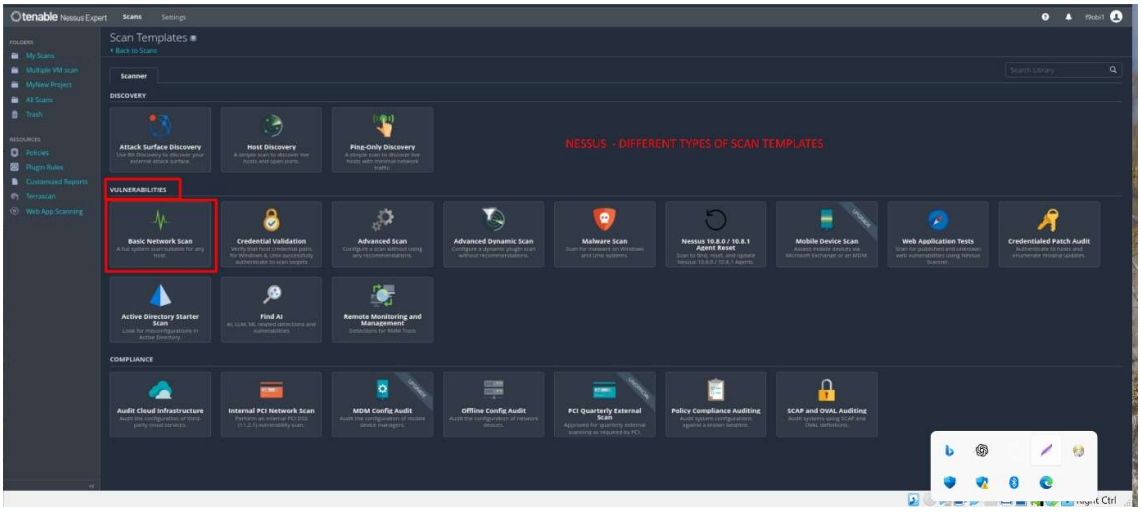


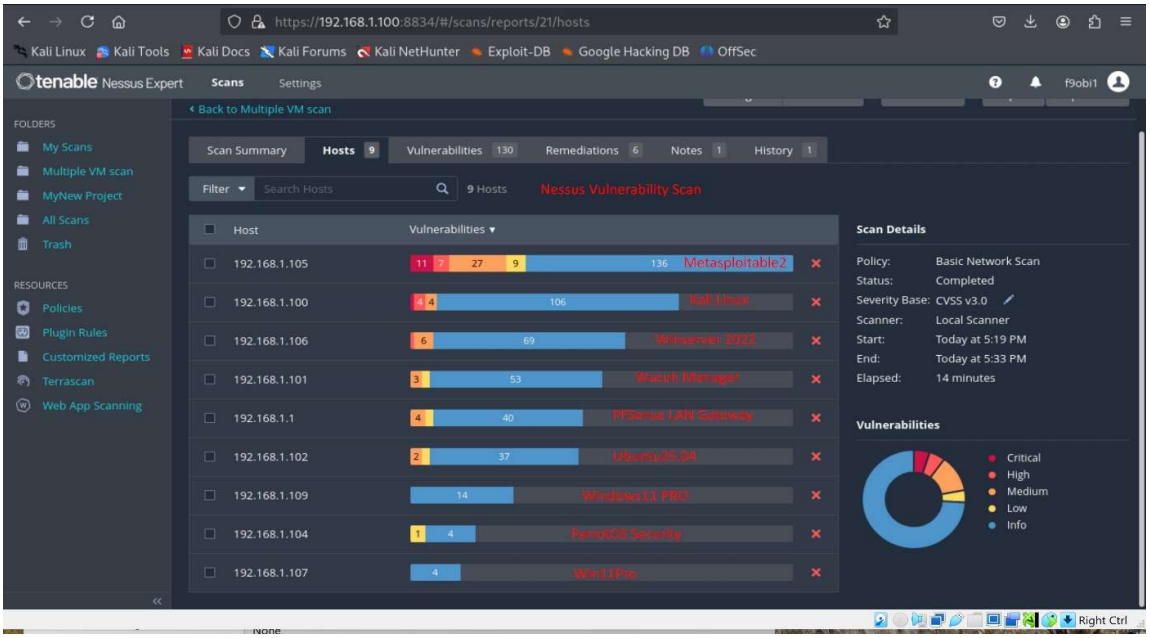

root@Kali-Linux)-[/home/f9obi1]
nmap 192.168.1.106 -sV
Winserver2022 NMAP scan
Starting Nmap 7.95 (https://nmap.org) at 2025-05-05 22:46 BST
Nmap scan report for 192.168.1.106
Host is up (0.00065s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
443/tcp open ssl/http Microsoft IIS httpd 10.0
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup:
WORKGROUP)
Ports open and their service versions
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:66:B7:E7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: WIN-4ILIJD5HSR6; 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 16.94 seconds


root@Kali-Linux)-[/home/f9obi1]
nmap 192.168.1.100 -sV
Kali Linux NMAP scan
Starting Nmap 7.95 (https://nmap.org) at 2025-05-05 22:48 BST
Nmap scan report for 192.168.1.100
Host is up (0.0000020s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.9p2 Debian 2 (protocol 2.0)
139/tcp open netbios-ssn Samba smbd 4
445/tcp open netbios-ssn Samba smbd 4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Ports Open and ther service versions
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 11.24 seconds

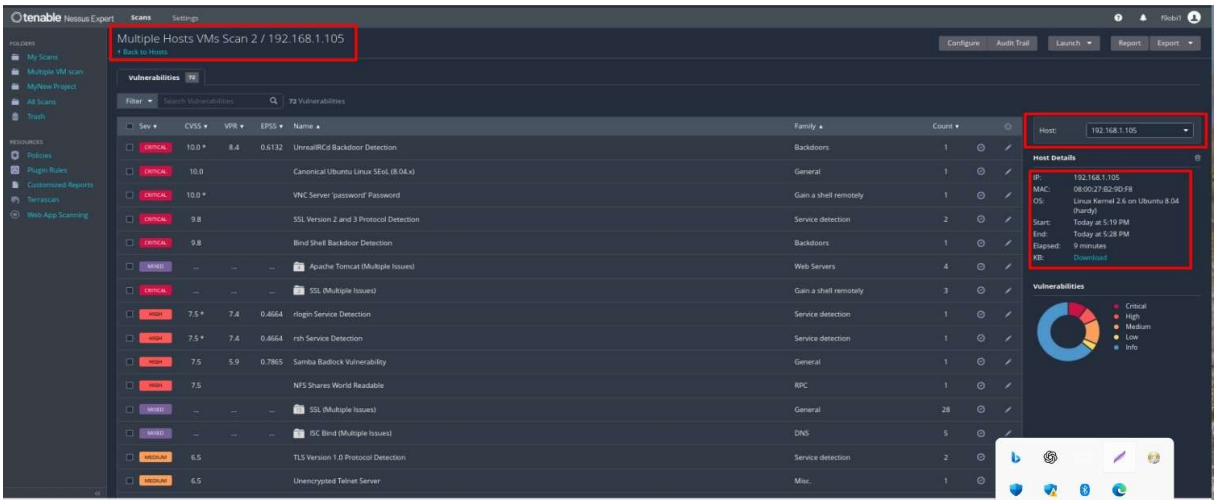
Comprehensive vulnerability scans using Nessus

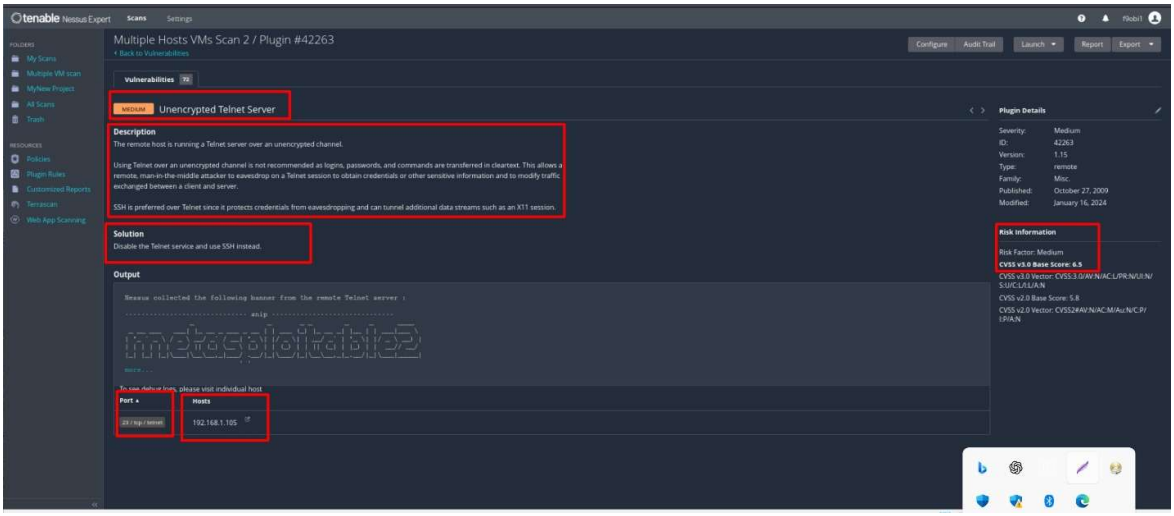
A comprehensive vulnerability scan was done on the targeted VMs and opened ports using the simple network scan template of the Nessus. Several results were obtained showing their vulnerabilities, issue descriptions, possible remediations, corresponding CVE & CVSS numbers. See some excerpts below;

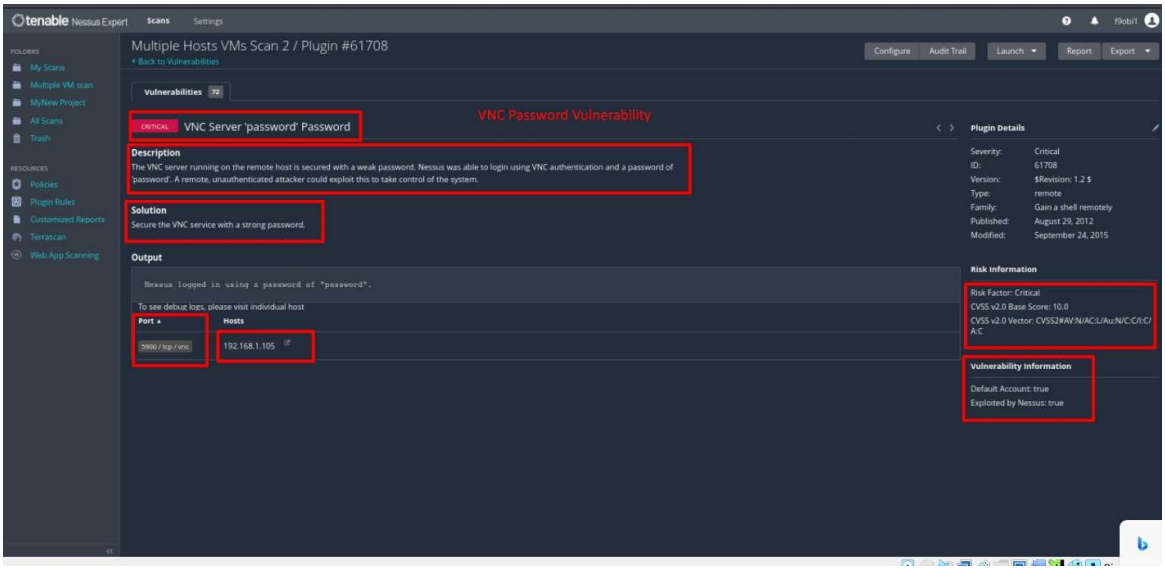


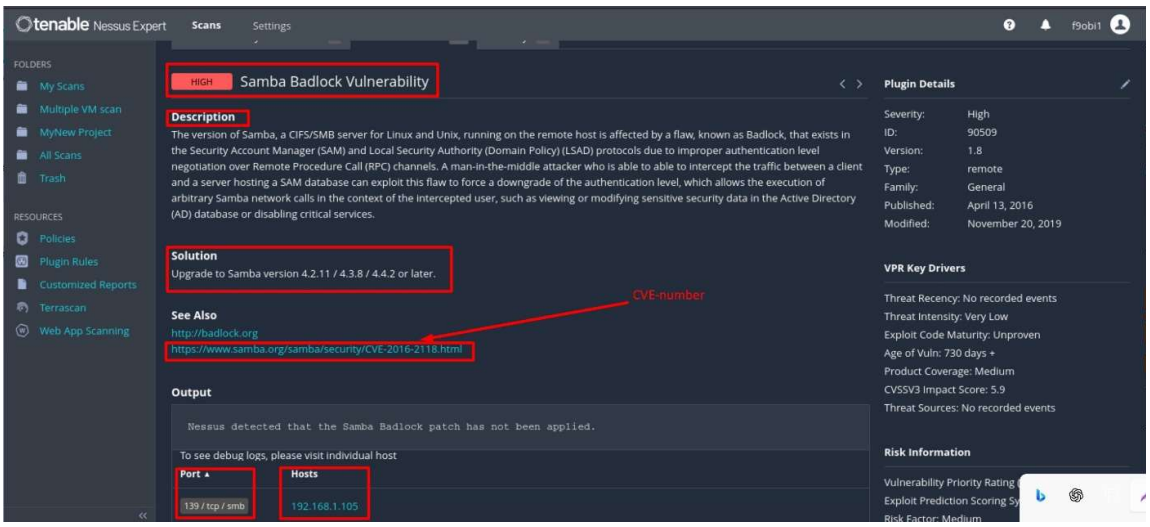


The ab



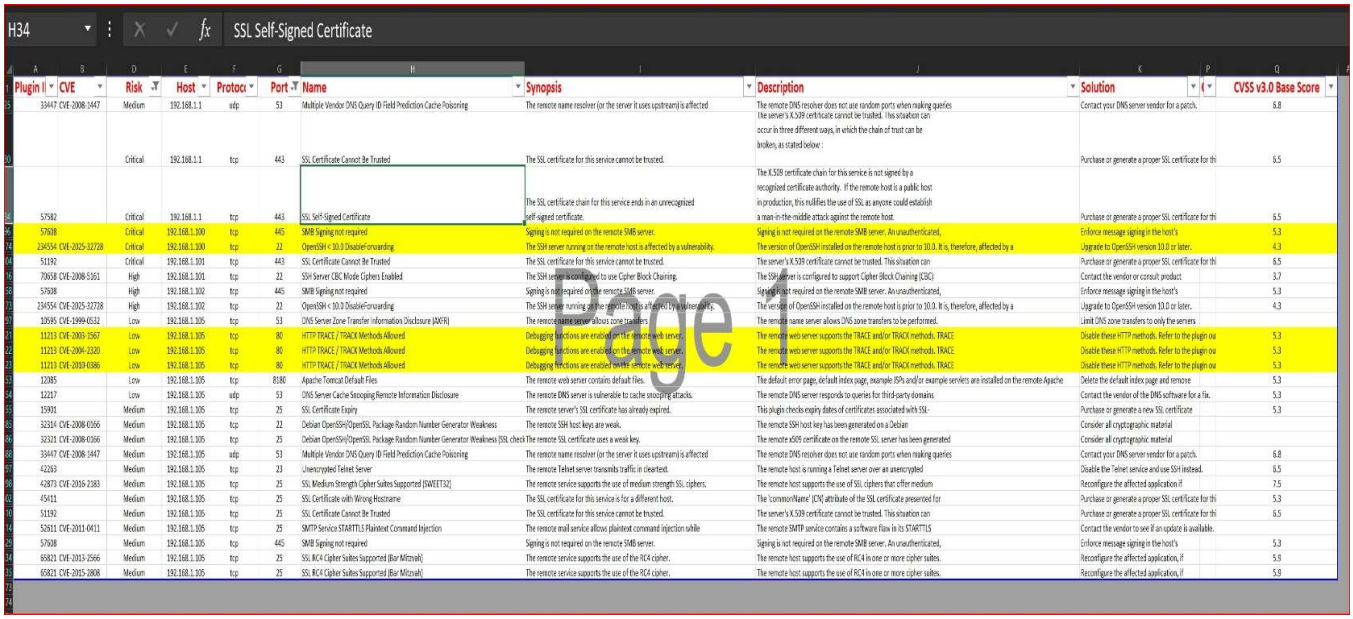

tenable Nessus Expert
Scans
Settings
Multiple Hosts VMs Scan 2 / Plugin #42263
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 72
MEDIUM
Unencrypted Telnet Server
Description
The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.
SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.
Solution
Disable the Telnet service and use SSH instead.
Output
Nessus collected the following banner from the remote Telnet server :
To see debug logs, please visit individual host
Port
Hosts
23 / tcp / telnet
192.168.1.105
Plugin Details
Severity: Medium
ID: 42263
Version: 1.15
Type: remote
Family: Misc.
Published: October 27, 2009
Modified: January 16, 2024
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v2.0 Base Score: 5.8


tenable Nessus Expert
Scans
Settings
Multiple Hosts VMs Scan 2 / Plugin #61708
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 72
VNC Password Vulnerability
CRITICAL
VNC Server 'password' Password
Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.
Solution
Secure the VNC service with a strong password.
Output
Nessus logged in using a password of "password".
To see debug logs, please visit individual host
Port
Hosts
5900 / tcp / vnc
192.168.1.105
Plugin Details
Severity: Critical
ID: 61708
Version: $Revision: 1.2 $
Type: remote
Family: Gain a shell remotely
Published: August 29, 2012
Modified: September 24, 2015
Risk Information
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
Vulnerability Information
Default Account: true
Exploited by Nessus: true

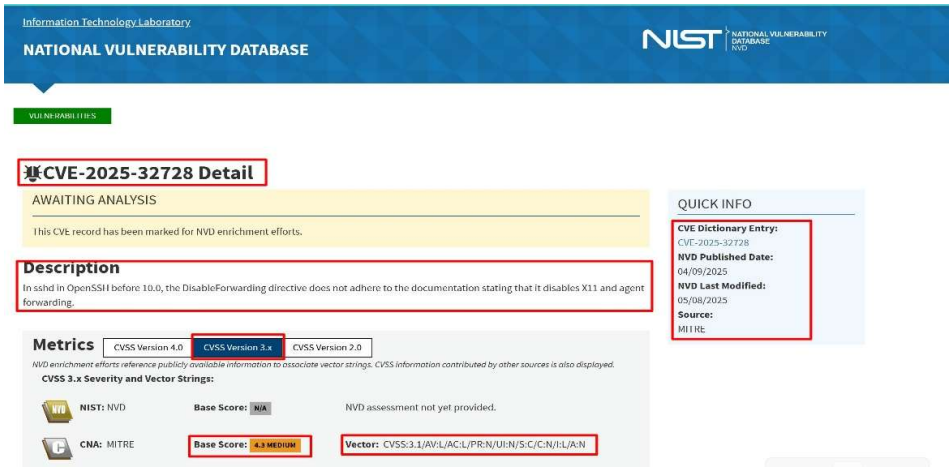

tenable Nessus Expert
Scans
Settings
HIGH
Samba Badlock Vulnerability
Description
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.
Solution
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
CVE-number
See Also
http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html
Output
Nessus detected that the Samba Badlock patch has not been applied.
To see debug logs, please visit individual host
Port
Hosts
139 / tcp / smb
192.168.1.105
Plugin Details
Severity: High
ID: 90509
Version: 1.8
Type: remote
Family: General
Published: April 13, 2016
Modified: November 20, 2019
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Medium
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events
Risk Information

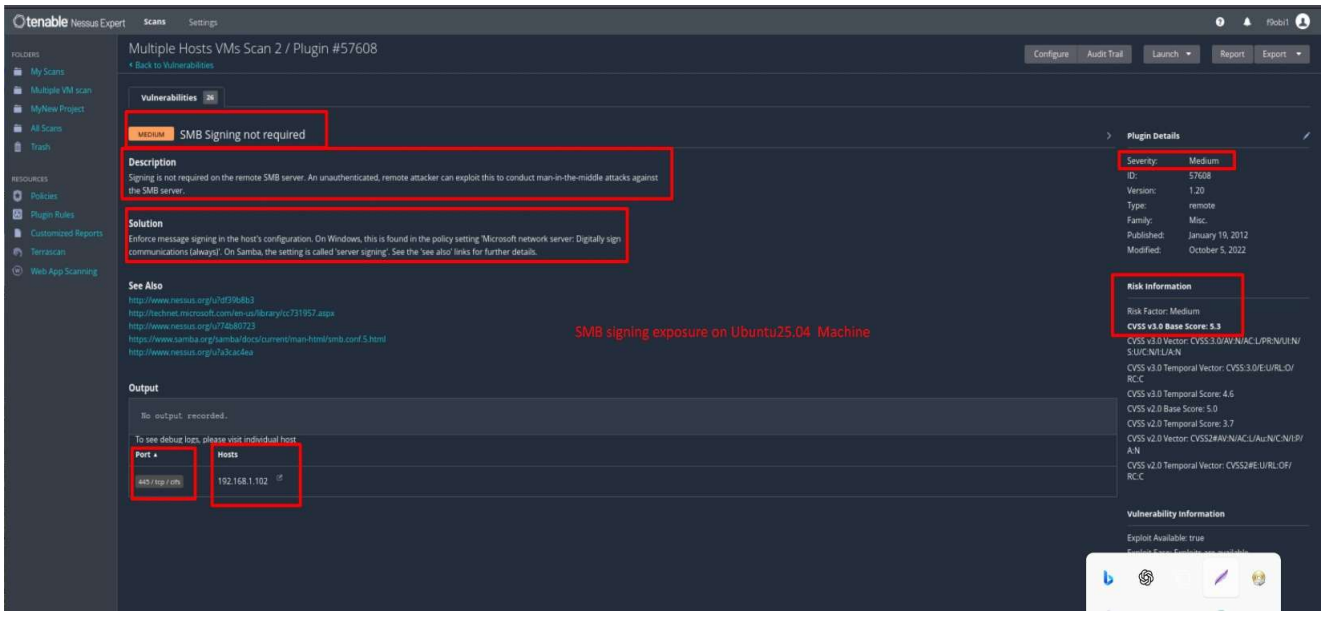
Validation of findings and correlation of results

The target hosts/open service ports rom Nmap scan are matched with scan results form the Nessus vulnerability scan. The correlations matched as shown in the MS Excel table below. Nessus was also able to generate the CVE/CVSS numbers, synopsis, descriptions and solutions -



Plugin I	CVE	Risk	Host	Protoc	Port	Name	Synopsis	Description	Solution	CVSS v3.0 Base Score
33447	CVE-2008-1447	Medium	192.168.1.1	udp	53	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	The remote name resolver (or the server it uses upstream) is affected	The remote DNS resolver does not use random ports when making queries	Contact your DNS server vendor for a patch.	6.8
		Critical	192.168.1.1	tcp	443	SSL Certificate Cannot Be Trusted	The SSL certificate for this service cannot be trusted.	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 :	Purchase or generate a proper SSL certificate for th	6.5
57582		Critical	192.168.1.1	tcp	443	SSL Self-Signed Certificate	The SSL certificate chain for this service ends in an unrecognized self-signed certificate.	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.	Purchase or generate a proper SSL certificate for th	6.5
57608		Critical	192.168.1.100	tcp	445	SMB Signing not required	Signing is not required on the remote SMB server.	Signing is not required on the remote SMB server. An unauthenticated,	Enforce message signing in the host's	5.3
234554	CVE-2025-32728	Critical	192.168.1.100	tcp	22	OpenSSH < 10.0 DisableForwarding	The SSH server running on the remote host is affected by a vulnerability.	The version of OpenSSH installed on the remote host is prior to 10.0. It is, therefore, affected by a	Upgrade to OpenSSH version 10.0 or later.	4.3
51192		Critical	192.168.1.101	tcp	443	SSL Certificate Cannot Be Trusted	The SSL certificate for this service cannot be trusted.	The server's X.509 certificate cannot be trusted. This situation can	Purchase or generate a proper SSL certificate for th	6.5
70658	CVE-2008-5161	High	192.168.1.101	tcp	22	SSH Server CBC Mode Ciphers Enabled	The SSH server is configured to use Cipher Block Chaining.	The SSH server is configured to support Cipher Block Chaining (CBC)	Contact the vendor or consult product	3.7
57608		High	192.168.1.102	tcp	445	SMB Signing not required	Signing is not required on the remote SMB server.	Signing is not required on the remote SMB server. An unauthenticated,	Enforce message signing in the host's	5.3
234554	CVE-2025-32728	High	192.168.1.102	tcp	22	OpenSSH < 10.0 DisableForwarding	The SSH server running on the remote host is affected by a vulnerability.	The version of OpenSSH installed on the remote host is prior to 10.0. It is, therefore, affected by a	Upgrade to OpenSSH version 10.0 or later.	4.3
10595	CVE-1999-0532	Low	192.168.1.105	tcp	53	DNS Server Zone Transfer Information Disclosure (AXFR)	The remote name server allows zone transfers	The remote name server allows DNS zone transfers to be performed.	Limit DNS zone transfers to only the servers	
11213	CVE-2003-1567	Low	192.168.1.105	tcp	80	HTTP TRACE / TRACK Methods Allowed	Debugging functions are enabled on the remote web server.	The remote web server supports the TRACE and/or TRACK methods. TRACE	Disable these HTTP methods. Refer to the plugin ou	5.3
11213	CVE-2004-2320	Low	192.168.1.105	tcp	80	HTTP TRACE / TRACK Methods Allowed	Debugging functions are enabled on the remote web server.	The remote web server supports the TRACE and/or TRACK methods. TRACE	Disable these HTTP methods. Refer to the plugin ou	5.3
11213	CVE-2010-0386	Low	192.168.1.105	tcp	80	HTTP TRACE / TRACK Methods Allowed	Debugging functions are enabled on the remote web server.	The remote web server supports the TRACE and/or TRACK methods. TRACE	Disable these HTTP methods. Refer to the plugin ou	5.3
12085		Low	192.168.1.105	tcp	8180	Apache Tomcat Default Files	The remote web server contains default files.	The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache	Delete the default index page and remove	5.3
12217		Low	192.168.1.105	udp	53	DNS Server Cache Snooping Remote Information Disclosure	The remote DNS server is vulnerable to cache snooping attacks.	The remote DNS server responds to queries for third-party domains	Contact the vendor of the DNS software for a fix.	5.3
15901		Medium	192.168.1.105	tcp	25	SSL Certificate Expiry	The remote server's SSL certificate has already expired.	This plugin checks expiry dates of certificates associated with SSL-	Purchase or generate a new SSL certificate	5.3
32314	CVE-2008-0166	Medium	192.168.1.105	tcp	22	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	The remote SSH host keys are weak.	The remote SSH host key has been generated on a Debian	Consider all cryptographic material	
32321	CVE-2008-0166	Medium	192.168.1.105	tcp	25	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check	The remote SSL certificate uses a weak key.	The remote x509 certificate on the remote SSL server has been generated	Consider all cryptographic material	
33447	CVE-2008-1447	Medium	192.168.1.105	udp	53	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	The remote name resolver (or the server it uses upstream) is affected	The remote DNS resolver does not use random ports when making queries	Contact your DNS server vendor for a patch.	6.8
42263		Medium	192.168.1.105	tcp	23	Unencrypted Telnet Server	The remote Telnet server transmits traffic in cleartext.	The remote host is running a Telnet server over an unencrypted	Disable the Telnet service and use SSH instead.	6.5
42873	CVE-2016-2183	Medium	192.168.1.105	tcp	25	SSL Medium Strength Cipher Suites Supported (SWEET32)	The remote service supports the use of medium strength SSL ciphers.	The remote host supports the use of SSL ciphers that offer medium	Reconfigure the affected application if	7.5
45411		Medium	192.168.1.105	tcp	25	SSL Certificate with Wrong Hostname	The SSL certificate for this service is for a different host.	The 'commonName' (CN) attribute of the SSL certificate presented for	Purchase or generate a proper SSL certificate for th	5.3
51192		Medium	192.168.1.105	tcp	25	SSL Certificate Cannot Be Trusted	The SSL certificate for this service cannot be trusted.	The server's X.509 certificate cannot be trusted. This situation can	Purchase or generate a proper SSL certificate for th	6.5
52611	CVE-2011-0411	Medium	192.168.1.105	tcp	25	SMTP Service STARTTLS Plaintext Command Injection	The remote mail service allows plaintext command injection while	The remote SMTP service contains a software flaw in its STARTTLS	Contact the vendor to see if an update is available.	
57608		Medium	192.168.1.105	tcp	445	SMB Signing not required	Signing is not required on the remote SMB server.	Signing is not required on the remote SMB server. An unauthenticated,	Enforce message signing in the host's	5.3
65821	CVE-2013-2566	Medium	192.168.1.105	tcp	25	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	The remote service supports the use of the RC4 cipher.	The remote host supports the use of RC4 in one or more cipher suites.	Reconfigure the affected application, if	5.9
65821	CVE-2015-2808	Medium	192.168.1.105	tcp	25	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	The remote service supports the use of the RC4 cipher.	The remote host supports the use of RC4 in one or more cipher suites.	Reconfigure the affected application, if	5.9





Remediations / Recommendations

The following are some of the recommendations mitigate / remediate identified vulnerabilities

- Implementation of all recommendations must be prioritized according to risk levels starting with critical, high, medium and low
- Host-IP 192.168.1.1:443 (PFsense firewall) SSL certificate cannot be trusted **– Critical risk.** The solution is to Purchase or generate a proper SSL certificate for this service.
- Host-IP 192.168.1.102:445 (Ubuntu25) **high risk.** 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. Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server. On Samba, the setting is called 'server signing'.
- CVE-2025-32728 on host-IP 192.168.1.100:22 **(Kali – medium risk)** is <version 10.0, disable forwarding. The version of OpenSSH installed on the remote host is prior to 10.0. It is, therefore, affected by a vulnerability. In sshd in OpenSSH the Disable Forwarding directive does not adhere to the documentation. Solution is to upgrade to OpenSSH version 10.0 or later.
- CVE-2010-0386 **Low risk** on host 192.168.1.105:80 (Metasploit Vulnerable Linux). The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. Disable these HTTP methods. Refer to the plugin output for more information.
- All identified vulnerabilities that borders on misconfigurations should be corrected immediately to prevent attackers from discovering and exploiting them anytime.
- All open network port services that are not in use/never used should be closed effective immediately
- The identified outdated services/unpatched applications (e.g. SSHD<10.0 & SSL cert.) should urgently be patched and updated to improve service resilience/ overall security posture
- All open action items /recommendations from past and present vulnerability assessment to tracked to closure to ensure effectiveness of risk management process and eliminate existing/potential exposures