DIGITAL EMPOWERMENT NETWORK

INTERNSHIP REPORT

WEEK#01

PRESENTED BY ALIZA JAVED
CID DEN10161

CONTENTS

1. About The Company
2. Conducting Security Audits For A Network
3. Assets Inventory
4. Security Strengthening Measures
5. Scanning For Vulnerabilities
6. Compliance Management
7. Conclusion

ABOUT THE COMPANY

At Digital Empowerment Network, we are dedicated to empowering Pakistan's university students through a wide range of initiatives that foster leadership, academic growth, and technical expertise. By bridging the digital divide with workshops, coding camps, and hackathons, we equip students with essential skills to thrive in the modern workforce. Our commitment to education extends beyond the classroom, as we reinvest proceeds from our revenue-generating partnerships into impactful programs and charitable initiatives, providing resources and support to underserved communities. We believe in the power of education to create well-rounded individuals who can drive innovation and make a positive impact on society..

CONDUCTING SECURITY AUDITS FOR A NETWORK

1.Objective:

Perform comprehensive security audits for a network.

2.Description:

Evaluate the security posture of a network by identifying vulnerabilities and weaknesses provide recommendations to enhance security measures

3.Key Steps:

- Conducting a risk assessment and identifying potential threats.
- Using tools to scan for vulnerabilities.
- Reviewing security policies and procedures.
- Compiling a report with findings and recommendations.
- Presenting the audit results to stakeholders

ASSETS INVENTORY

Assets:

1. Mobile Phone:

   Specifications :

- Manufacturer: iPhone
- Model name: iPhone 11 pro
- Operating system: ios version 17.6.1
- Battery : 75%
- Storage : 256 GB

2. Laptop:

   Specifications :

- Manufacturer : HP
- Device name: Aliza
- Device model: HP EliteBook 840 G5
- Processor : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz   1.90 GHz
- RAM : 16GB
- Operating system : Windows 11 pro

3. Router:

   Specifications :

- Manufacturer: Huawei
- Model name: Huawei OptiXstar HG8141V5

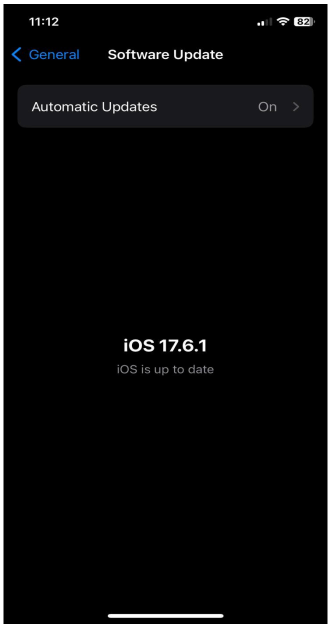
SECURITY STRENGTHENING MEASURES

Security strengthening refers to the process of enhancing the protective measures and protocols around systems and devices to defend against unauthorized access, data breaches, and various cyber threats. This involves implementing strategies such as updating software, enforcing strong access controls, and employing encryption to bolster the overall security posture. While security strengthening is crucial for safeguarding sensitive information and maintaining system integrity, it can introduce certain risks. These include potential disruptions during the implementation of new security measures, compatibility issues with existing systems, and the possibility of creating vulnerabilities if configurations are not managed properly. Additionally, overly stringent security controls may impact usability and productivity, requiring a balanced approach to ensure both robust protection and efficient operation.

The necessary steps that is taken to secure the devices are as below:

1. Keeping your software up to date:

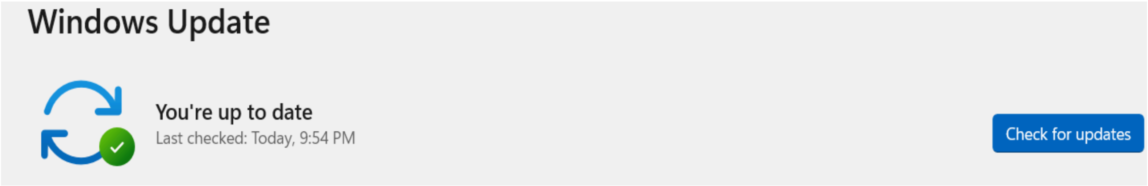
   Regular updates help protect your system from known vulnerabilities by applying patches and fixes provided by software developers. These updates can address security flaws, enhance functionality, and improve compatibility with other systems. Staying current with updates also reduces the risk of exploitation by cybercriminals who target outdated software with known vulnerabilities.



Automatic Updates On

iOS 17.6.1

iOS is up to date

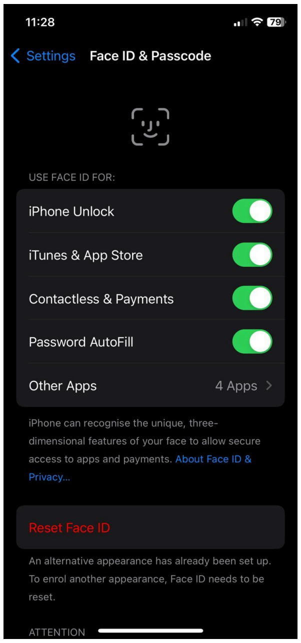


You're up to date

Last checked: Today, 9:54 PM

2. Keep your devices password protected:

Keeping your devices password protected is a fundamental practice in safeguarding sensitive information and ensuring privacy. Password protection serves as the first line of defense against unauthorized access to your devices, whether they are computers, smartphones, or tablets. By setting strong, unique passwords and using features like biometric authentication (fingerprints, facial recognition), you enhance the security of your devices and reduce the risk of data breaches or identity theft.



11:28 79

< Settings Face ID & Passcode

USE FACE ID FOR:

iPhone Unlock ●

iTunes & App Store ●

Contactless & Payments ●

Password AutoFill ●

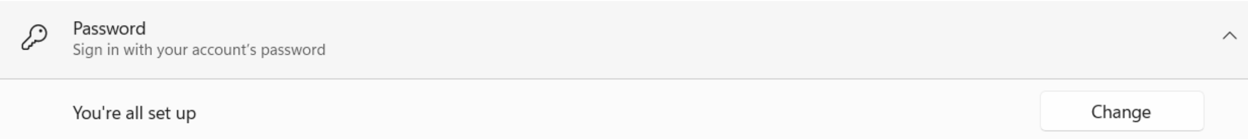
Other Apps 4 Apps >

iPhone can recognise the unique, three-dimensional features of your face to allow secure access to apps and payments. About Face ID & Privacy...

Reset Face ID

An alternative appearance has already been set up. To enrol another appearance, Face ID needs to be reset.

ATTENTION



Password

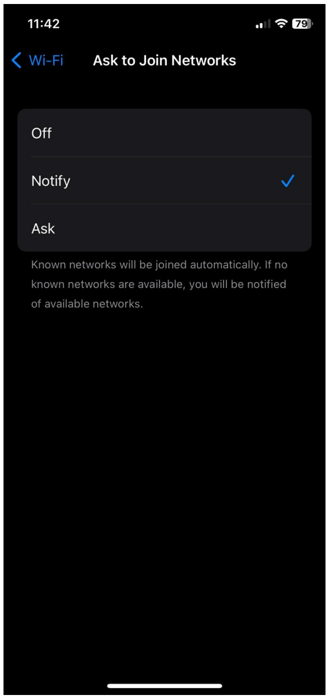
Sign in with your account's password

You're all set up

Change

3. Turn off Automatically wifi connection:

When automatic Wi-Fi connection is enabled, your device may connect to any available network without user intervention, which can expose it to insecure or malicious networks that could compromise data security or privacy.



Ask to Join Networks

Off

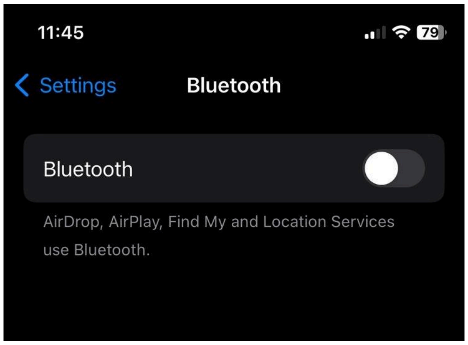
Notify ✓

Ask

Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.

4. Disable unnecessary ports and services:

   Ports and services are communication endpoints and functions that can be exploited by attackers if they are left open or active without necessity. By disabling those that are not in use, you minimize the attack surface available to potential intruders, reducing the risk of unauthorized access or exploitation.



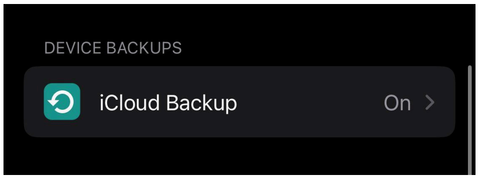
Bluetooth

Bluetooth ○

AirDrop, AirPlay, Find My and Location Services use Bluetooth.

5. Regular backups:

Regular backups are a vital component of a comprehensive data protection strategy, ensuring that critical information and system configurations are preserved and recoverable in the event of data loss, corruption, or system failure. By creating and maintaining up-to-date copies of your data, you can safeguard against various risks, including hardware failures, accidental deletions, ransomware attacks, and other unforeseen incidents.

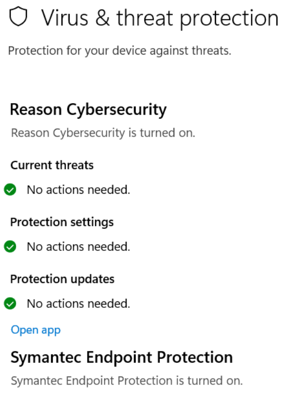


DEVICE BACKUPS

iCloud Backup On

6. Use Antivirus softwares:

Antivirus programs are designed to detect, quarantine, and remove harmful threats that could compromise your system's security, integrity, and performance. They provide real-time protection by scanning files, monitoring system activity, and detecting suspicious behavior to prevent infections and mitigate risks.



Virus & threat protection

Protection for your device against threats.

Reason Cybersecurity

Reason Cybersecurity is turned on.

Current threats

✓ No actions needed.

Protection settings

✓ No actions needed.

Protection updates

✓ No actions needed.

Open app

Symantec Endpoint Protection

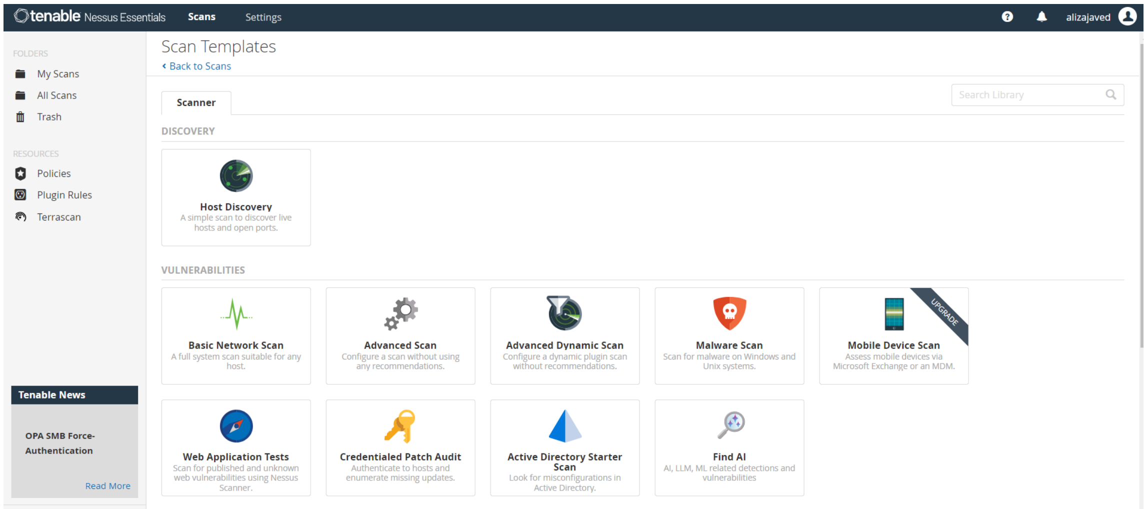
Symantec Endpoint Protection is turned on.

SCANNING FOR VULNERABILITIES

Nessus is widely used for host discovery and advanced vulnerability scanning because it offers a comprehensive and efficient way to identify security risks within a network. For host discovery, Nessus helps detect active devices on the network, providing a clear picture of the network's structure and identifying hosts that need to be scanned. Its advanced scanning capabilities go beyond basic vulnerability checks, performing in-depth assessments for known vulnerabilities, misconfigurations, and security loopholes across multiple platforms. Nessus can scan for a wide range of vulnerabilities, from outdated software to missing patches and potential exploits, making it a powerful tool for maintaining the security and integrity of a network.

Normal Scan:

- Open nessus in your machine and open “new scan”.



Host Discovery
A simple scan to discover live hosts and open ports.

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

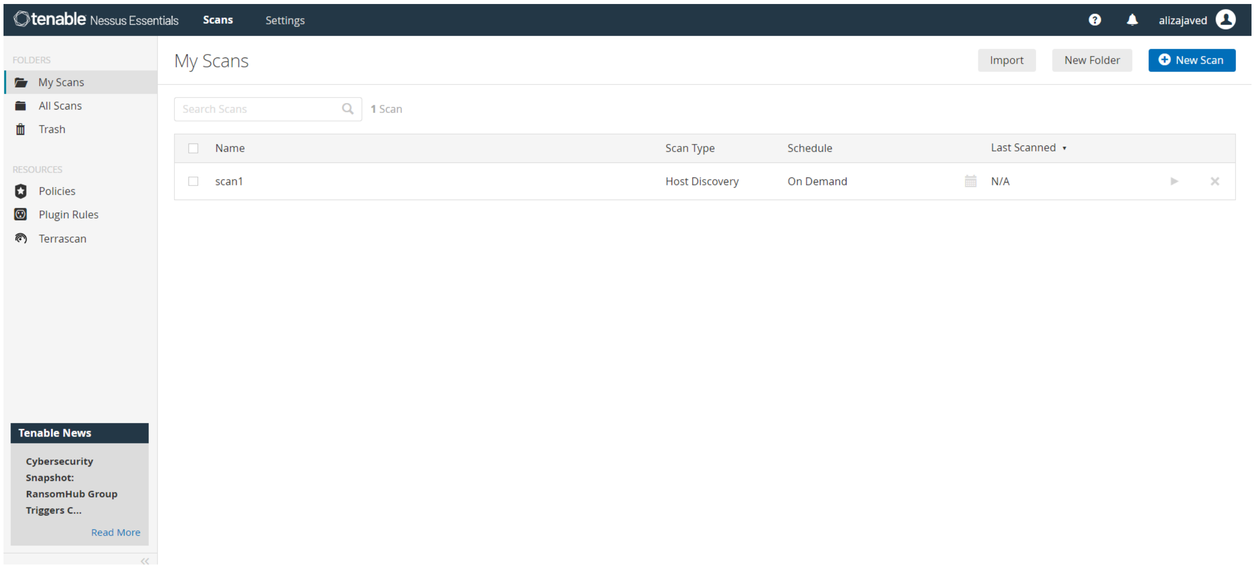
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Find AI
AI, LLM, ML related detections and vulnerabilities

- Select “host discovery“ , add the details of the scan and save the details.

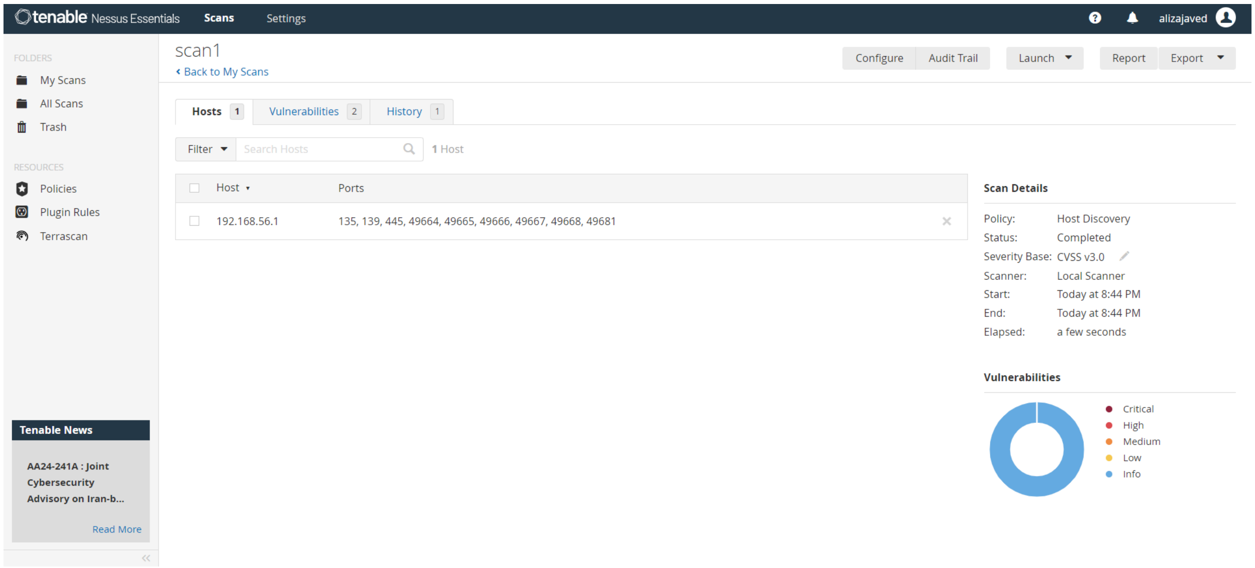


My Scans

1 Scan

Name	Scan Type	Schedule	Last Scanned
scan1	Host Discovery	On Demand	N/A

- Start the scan and after completion, click at the ip tab.



scan1

1 Host

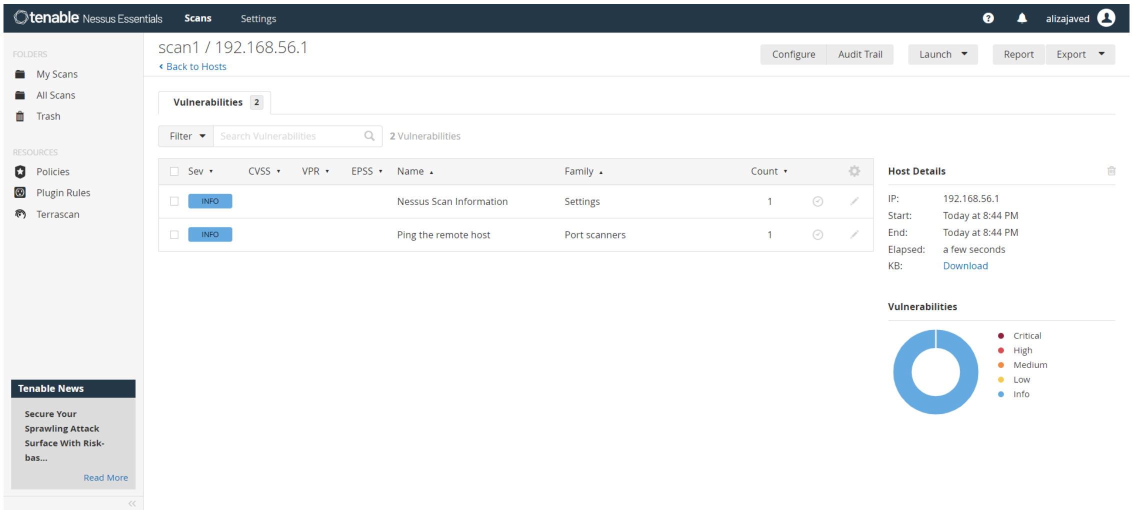
Host	Ports
192.168.56.1	135, 139, 445, 49664, 49665, 49666, 49667, 49668, 49681

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:44 PM
End: Today at 8:44 PM
Elapsed: a few seconds

Vulnerabilities

- Explore both the tabs and check the “scan detail” section.



scan1 / 192.168.56.1

‹ Back to Hosts

2 Vulnerabilities

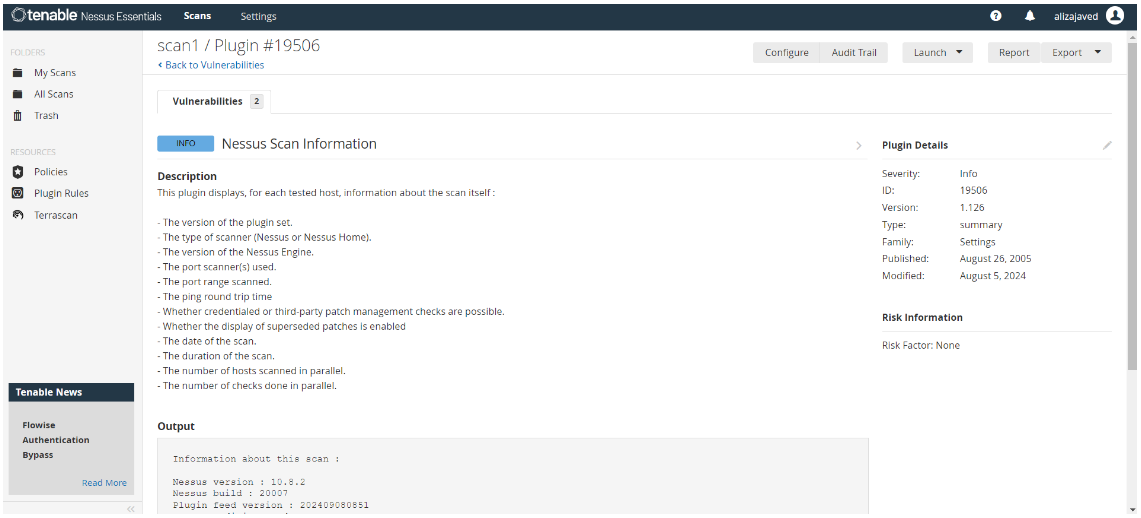
Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Nessus Scan Information	Settings	1
INFO				Ping the remote host	Port scanners	1

Host Details

IP:	192.168.56.1
Start:	Today at 8:44 PM
End:	Today at 8:44 PM
Elapsed:	a few seconds
KB:	Download

Vulnerabilities

- Explore deeply into each tab.



scan1 / Plugin #19506

‹ Back to Vulnerabilities

INFO Nessus Scan Information

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Output

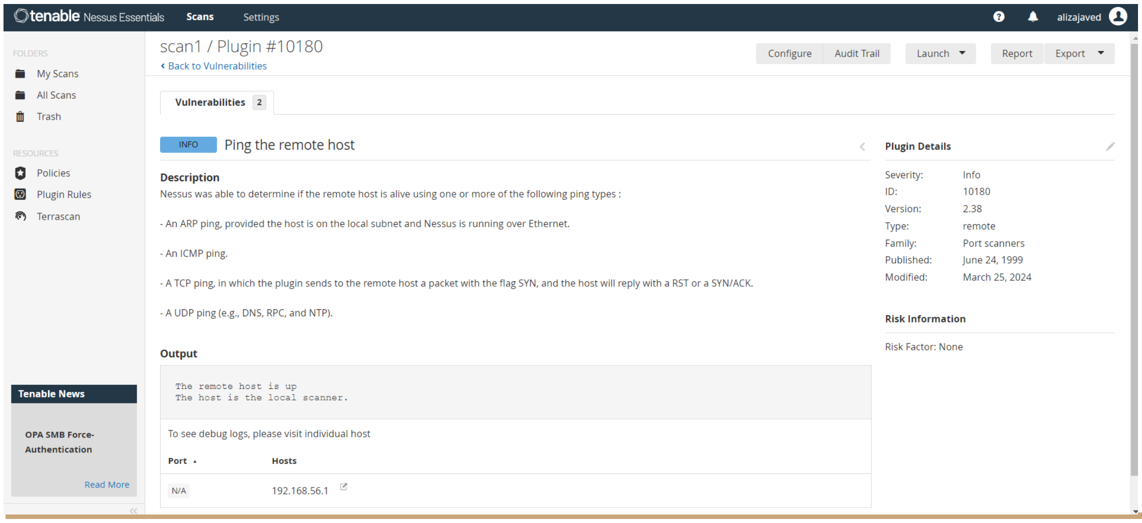
```
Information about this scan :

Nessus version : 10.8.2
Nessus build : 20007
Plugin feed version : 202409080851
```

Plugin Details

Severity:	Info
ID:	19506
Version:	1.126
Type:	summary
Family:	Settings
Published:	August 26, 2005
Modified:	August 5, 2024

Risk Information

Risk Factor: None



scan1 / Plugin #10180

‹ Back to Vulnerabilities

INFO Ping the remote host

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Output

```
The remote host is up
The host is the local scanner.
```

To see debug logs, please visit individual host

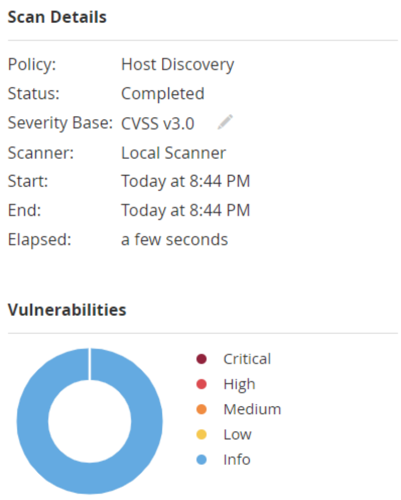
Port	Hosts
N/A	192.168.56.1

Plugin Details

Severity:	Info
ID:	10180
Version:	2.38
Type:	remote
Family:	Port scanners
Published:	June 24, 1999
Modified:	March 25, 2024

Risk Information

Risk Factor: None

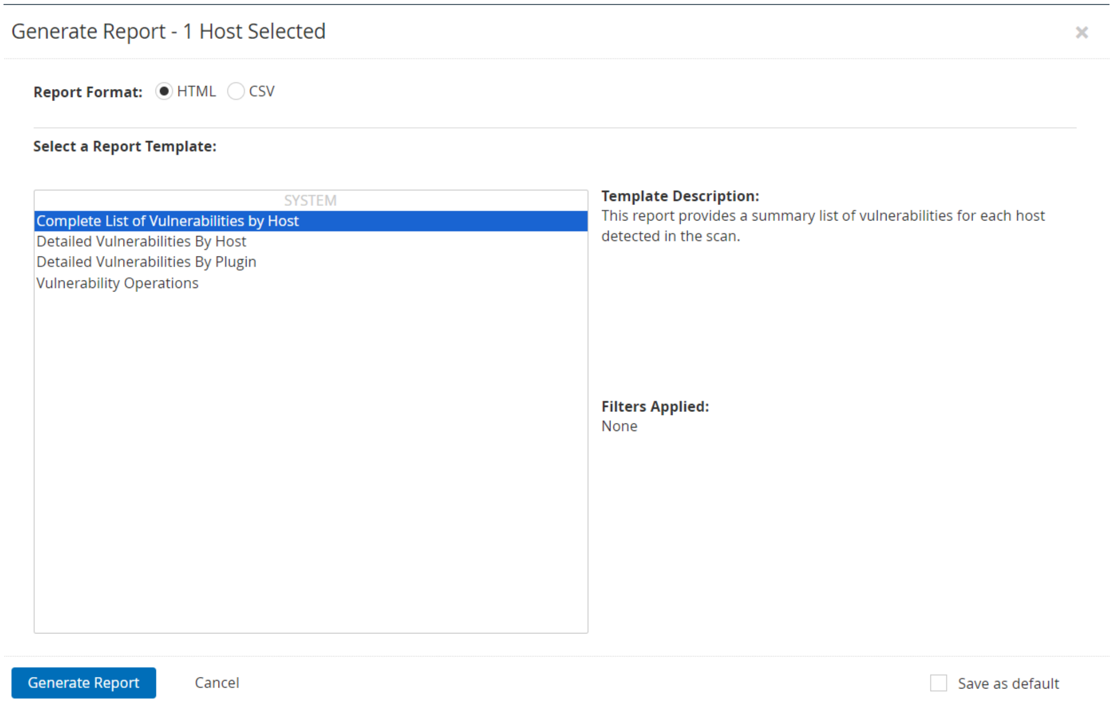


Scan Details

Policy:	Host Discovery
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:44 PM
End:	Today at 8:44 PM
Elapsed:	a few seconds

Vulnerabilities

- Now generate the report.



Generate Report - 1 Host Selected

Report Format: ● HTML ○ CSV

Select a Report Template:

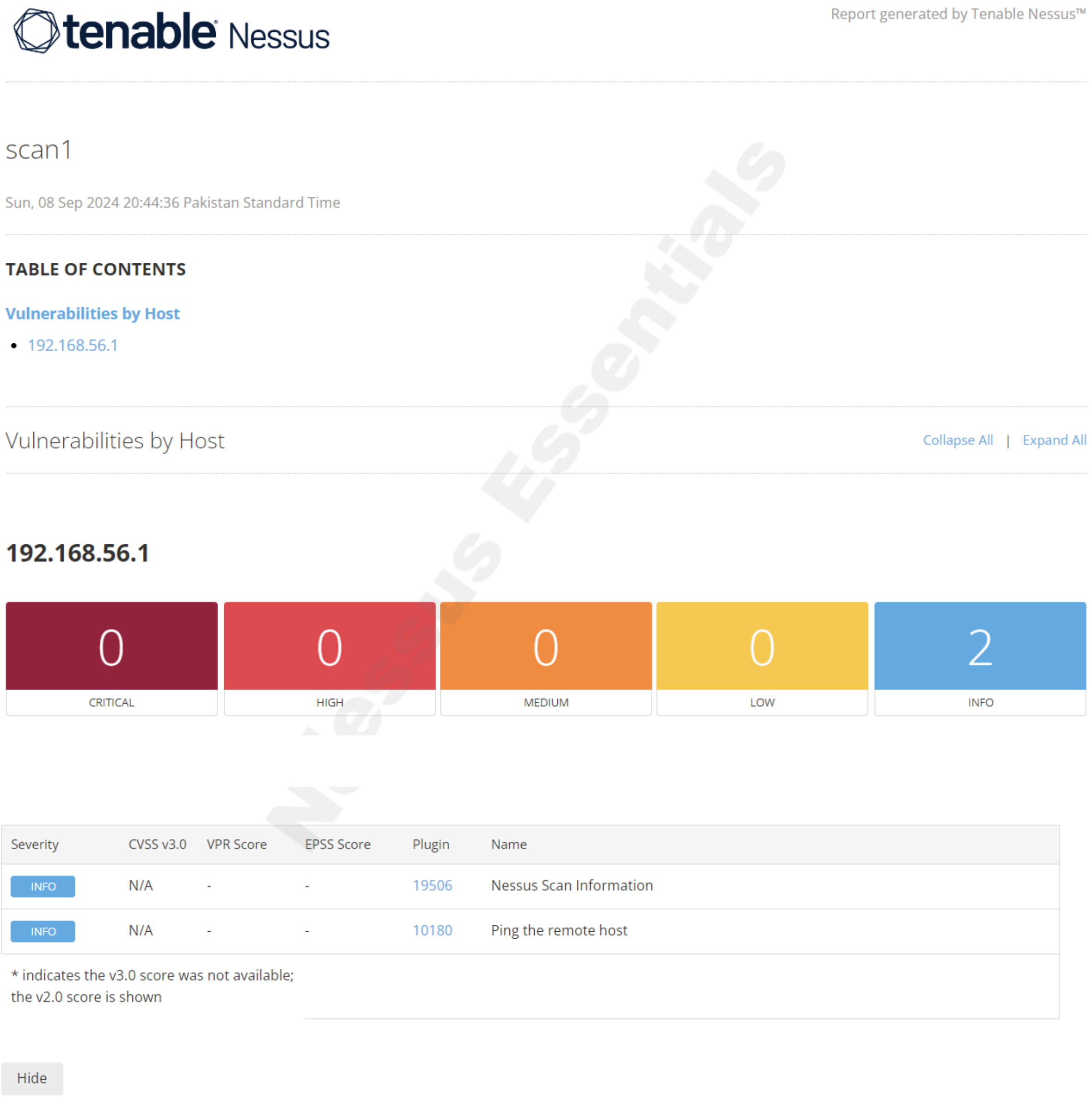
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Generate Report
Cancel
□ Save as default

- The report shows the following details.



Report generated by Tenable Nessus™

scan1

Sun, 08 Sep 2024 20:44:36 Pakistan Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.56.1

Vulnerabilities by Host

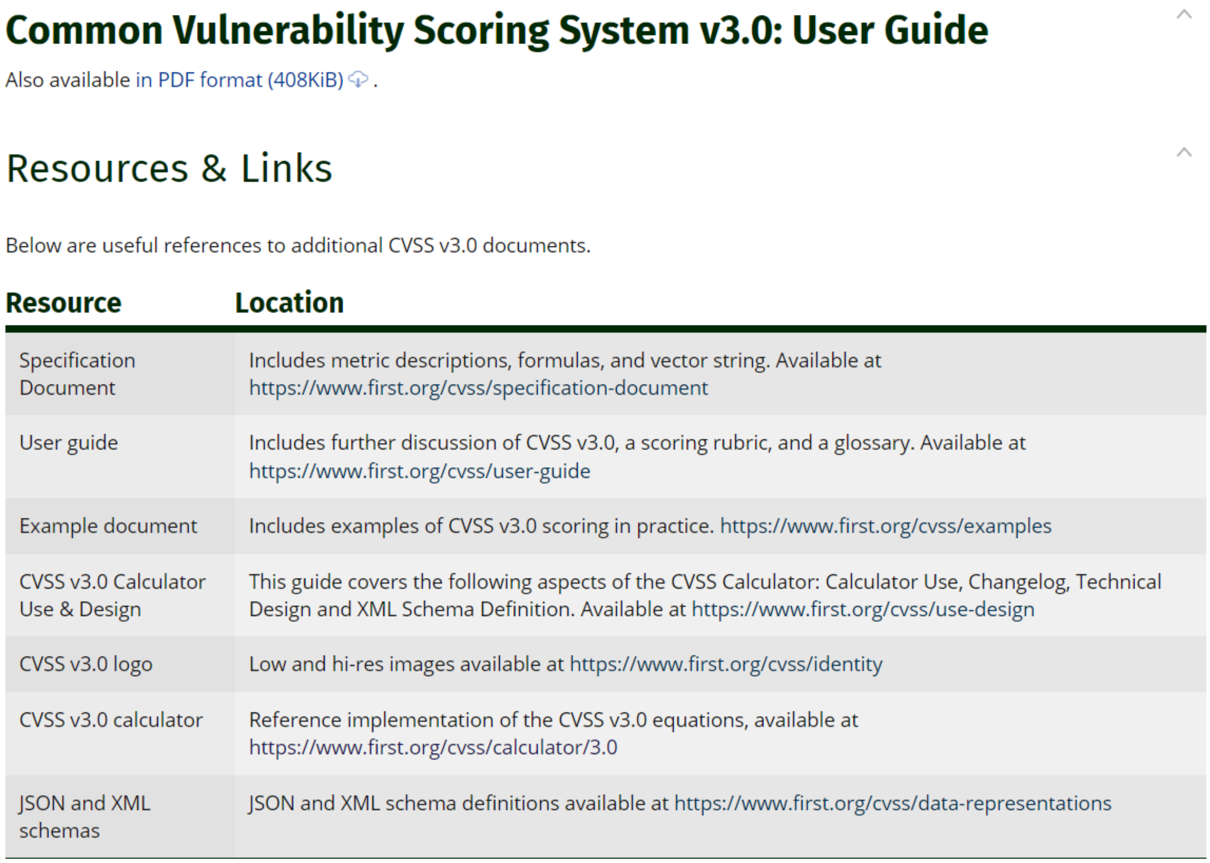
192.168.56.1

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10180	Ping the remote host

* indicates the v3.0 score was not available; the v2.0 score is shown

- The scan details show the severity base : CVSS v 3.0



Common Vulnerability Scoring System v3.0: User Guide

Also available in PDF format (408KiB) .

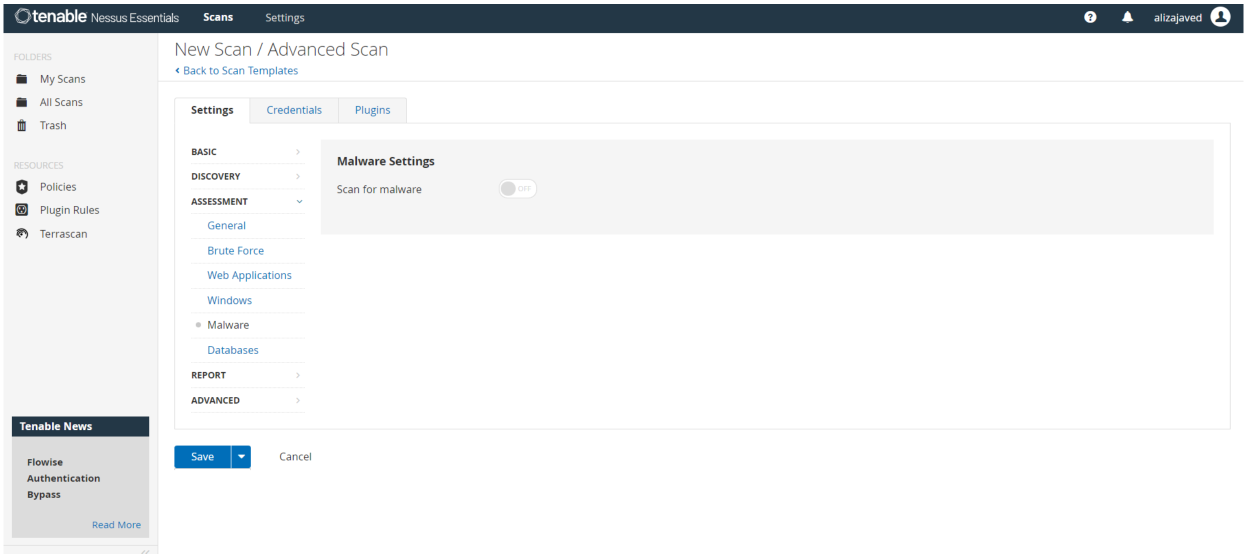
Resources & Links

Below are useful references to additional CVSS v3.0 documents.

Resource	Location
Specification Document	Includes metric descriptions, formulas, and vector string. Available at https://www.first.org/cvss/specification-document
User guide	Includes further discussion of CVSS v3.0, a scoring rubric, and a glossary. Available at https://www.first.org/cvss/user-guide
Example document	Includes examples of CVSS v3.0 scoring in practice. https://www.first.org/cvss/examples
CVSS v3.0 Calculator Use & Design	This guide covers the following aspects of the CVSS Calculator: Calculator Use, Changelog, Technical Design and XML Schema Definition. Available at https://www.first.org/cvss/use-design
CVSS v3.0 logo	Low and hi-res images available at https://www.first.org/cvss/identity
CVSS v3.0 calculator	Reference implementation of the CVSS v3.0 equations, available at https://www.first.org/cvss/calculator/3.0
JSON and XML schemas	JSON and XML schema definitions available at https://www.first.org/cvss/data-representations

Advance scan:

- Select the advance scan in the new scan option to deeply scan for the vulnerability in the network.



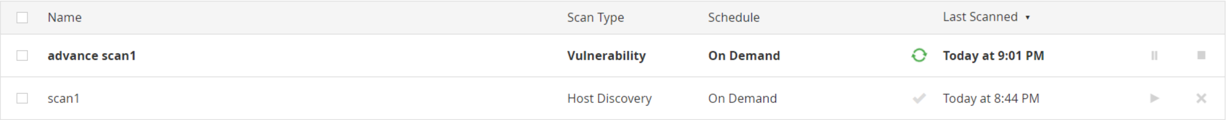
New Scan / Advanced Scan

‹ Back to Scan Templates

Malware Settings

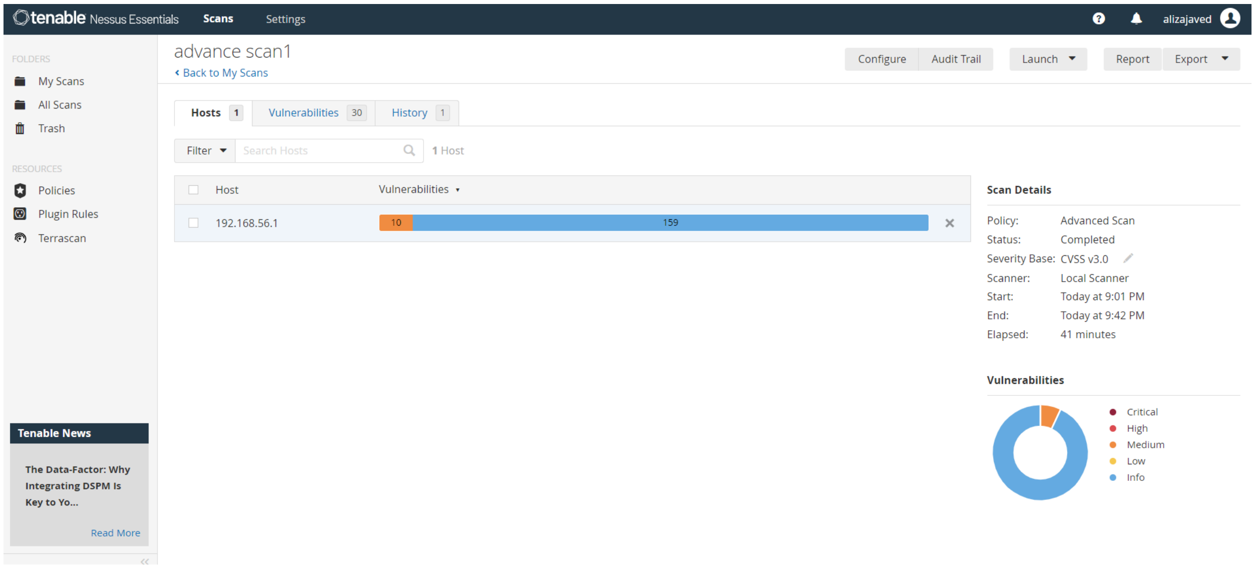
Scan for malware: OFF

- Add and save the details of the scan and start the scan.



□	Name	Scan Type	Schedule		Last Scanned ▾		
□	**advance scan1**	**Vulnerability**	**On Demand**	⟳	**Today at 9:01 PM**	⏸	■
□	scan1	Host Discovery	On Demand	✓	Today at 8:44 PM	▶	✕

- After completing the scan, open the tab.



advance scan1

‹ Back to My Scans

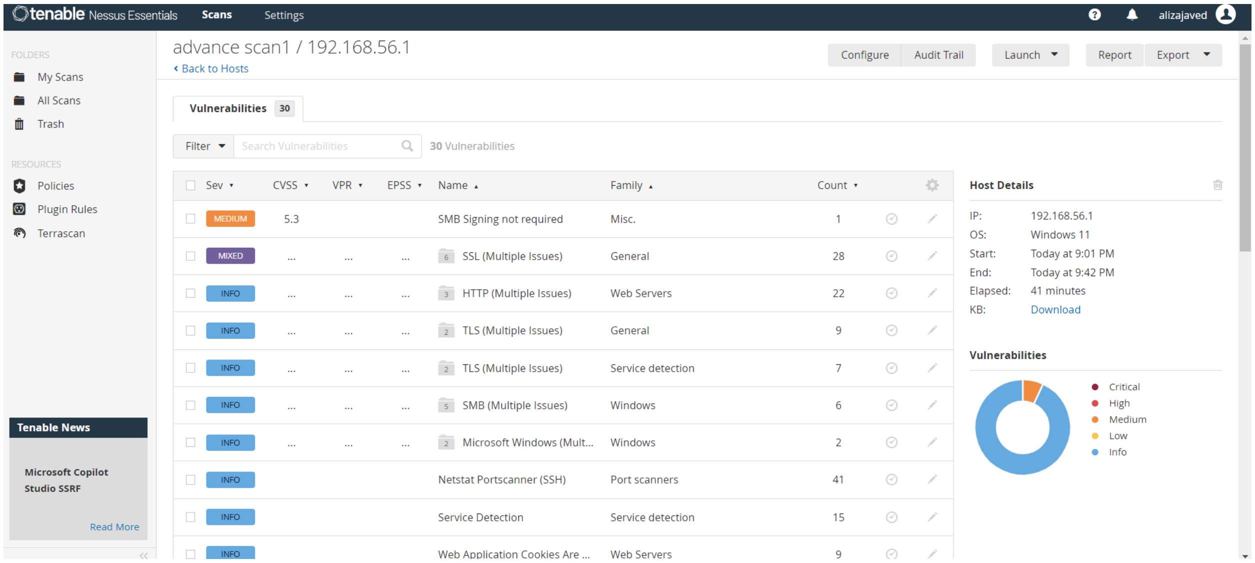
□	Host	Vulnerabilities ▾
□	192.168.56.1	10 159

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:01 PM
End: Today at 9:42 PM
Elapsed: 41 minutes

Vulnerabilities

- The scan shows the following details.



advance scan1 / 192.168.56.1

‹ Back to Hosts

Vulnerabilities 30

30 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	6 SSL (Multiple Issues)	General	28
INFO	...	...	...	3 HTTP (Multiple Issues)	Web Servers	22
INFO	...	...	...	2 TLS (Multiple Issues)	General	9
INFO	...	...	...	2 TLS (Multiple Issues)	Service detection	7
INFO	...	...	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	...	...	2 Microsoft Windows (Mult...	Windows	2
INFO				Netstat Portscanner (SSH)	Port scanners	41
INFO				Service Detection	Service detection	15
INFO				Web Application Cookies Are ...	Web Servers	9

Host Details

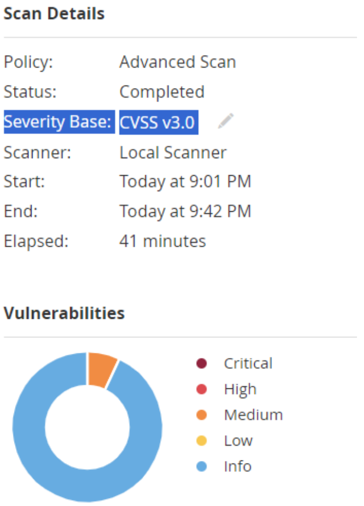
IP:	192.168.56.1
OS:	Windows 11
Start:	Today at 9:01 PM
End:	Today at 9:42 PM
Elapsed:	41 minutes
KB:	Download

Vulnerabilities

Tenable News

Microsoft Copilot Studio SSRF

Read More

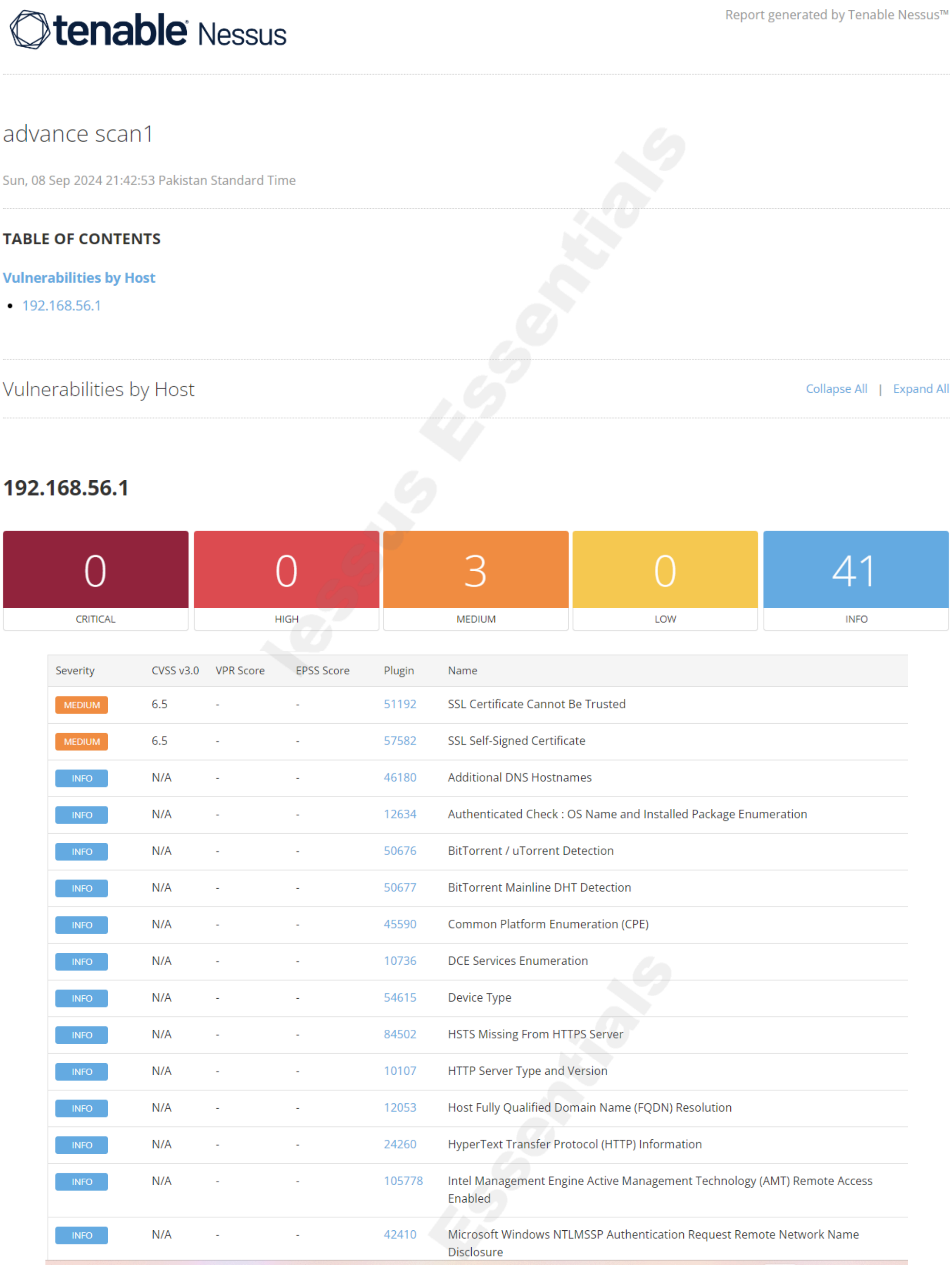


Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:01 PM
End:	Today at 9:42 PM
Elapsed:	41 minutes

Vulnerabilities

- Explore each tab in detail and generate the report.



tenable Nessus

Report generated by Tenable Nessus™

advance scan1

Sun, 08 Sep 2024 21:42:53 Pakistan Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

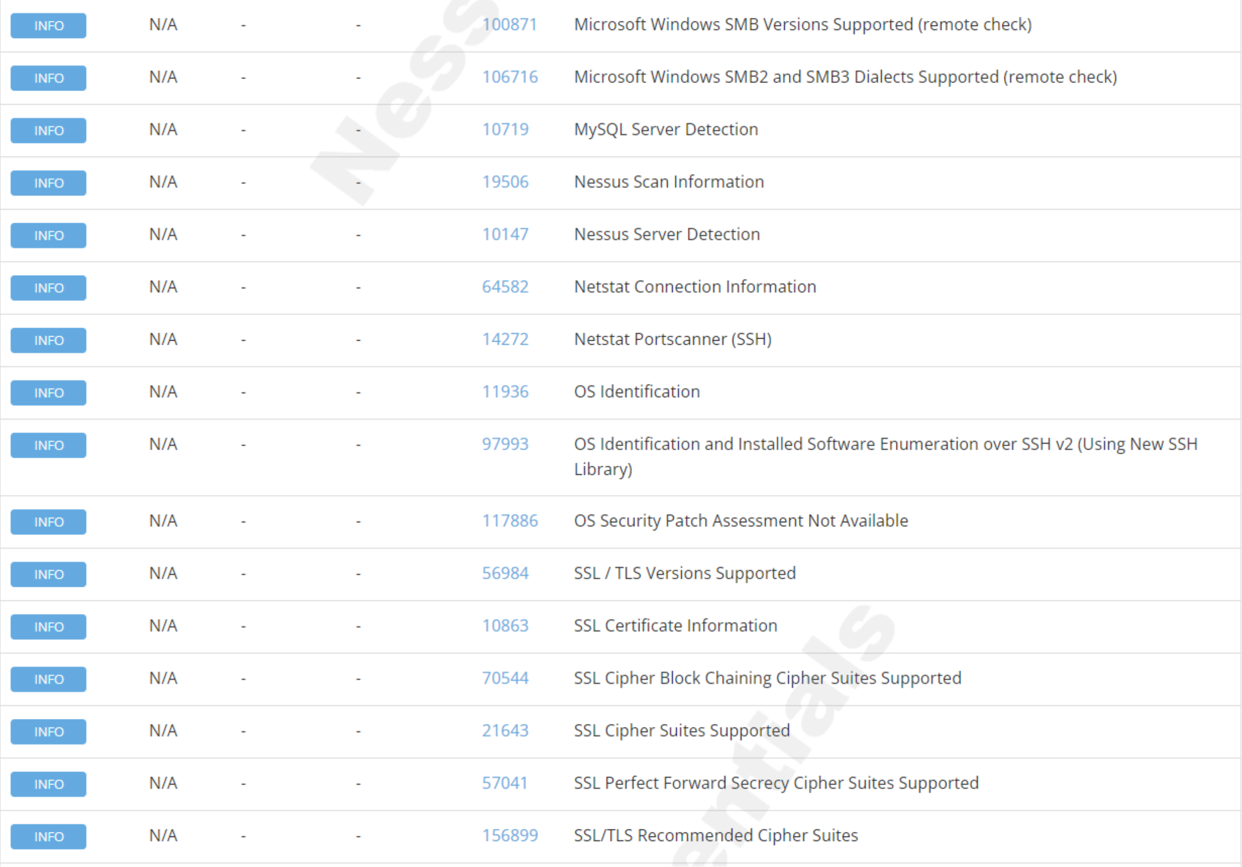
- 192.168.56.1

Vulnerabilities by Host

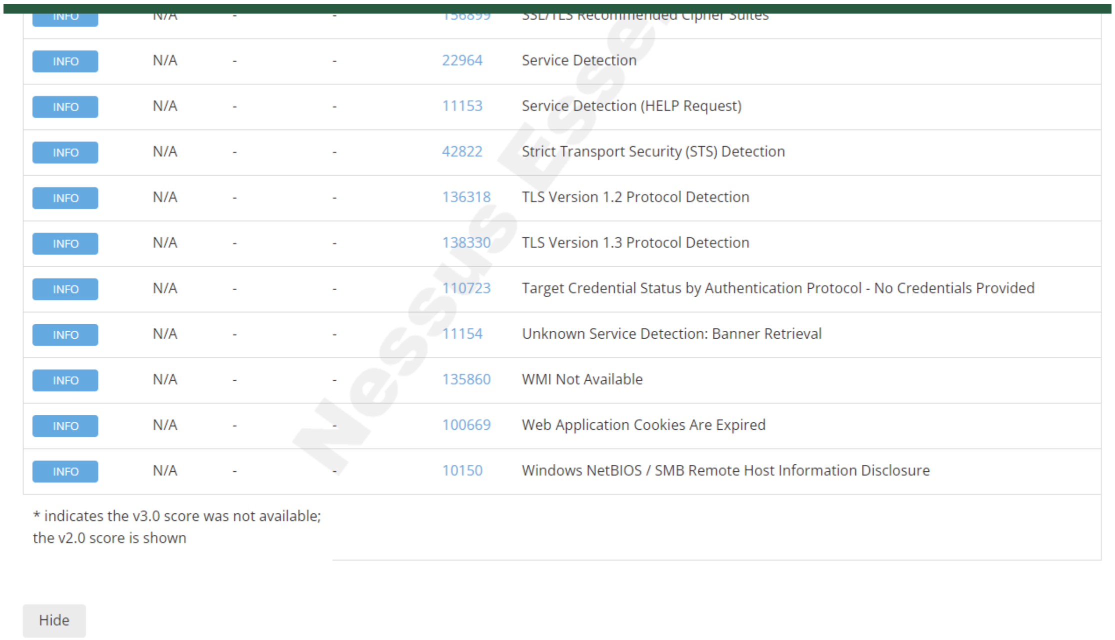
192.168.56.1

0	0	3	0	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
INFO	N/A	-	-	46180	Additional DNS Hostnames
INFO	N/A	-	-	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	-	-	50676	BitTorrent / uTorrent Detection
INFO	N/A	-	-	50677	BitTorrent Mainline DHT Detection
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	105778	Intel Management Engine Active Management Technology (AMT) Remote Access Enabled
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure



INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	10719	MySQL Server Detection
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10147	Nessus Server Detection
INFO	N/A	-	-	64582	Netstat Connection Information
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites



INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available;
the v2.0 score is shown

COMPLIANCE MANAGEMENT

Compliance management ensures that an organization's information security practices meet the ISO/IEC 27001:2013 standards. This process involves establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The goal is to safeguard information assets and ensure the organization meets regulatory and business requirements.

Steps to Achieve Compliance

1. **Initial Gap Analysis:** Conduct a gap analysis to compare the current information security practices with ISO/IEC 27001:2013 standards.
2. **Develop an Action Plan:** Based on the gap analysis, create a detailed action plan to address any deficiencies and implement the necessary controls.
3. **Training and Awareness:** Provide training and raise awareness among staff regarding information security policies, procedures, and their responsibilities in ensuring compliance.
4. **Document Management:** Maintain and control all ISMS documentation to ensure it is up-to-date and accessible to relevant personnel.
5. **Incident Management:** Establish a process for detecting, reporting, and responding to information security incidents promptly.
6. **Supplier Management:** Ensure third-party suppliers comply with the organization's information security requirements, as part of the overall ISMS.
7. **Certification Audit:** Undergo a certification audit by an accredited certification body to achieve ISO/IEC 27001:2013 certification, confirming compliance with the standards.

CONCLUSION

This report presents a thorough security audit conducted on a network, focusing on identifying and mitigating potential vulnerabilities. The process began with evaluating the network's structure and inventorying assets, followed by implementing key security improvements such as enforcing strong password policies, establishing account protection mechanisms, and ensuring timely software updates. Advanced vulnerability scanning techniques were used to detect weaknesses, and compliance measures were aligned with recognized security standards to enhance the network's resilience. The recommendations provided will help strengthen the security framework and safeguard the network from emerging threats.