DEN

DIGITAL EMPOWERMENT NETWORK

INTERNSHIP REPORT

WEEK # 1

M. USAMA SHAHBAZ

CONTENTS

ABOUT THE COMPANY

Nessus is a widely-used vulnerability assessment tool developed by Tenable, Inc. It helps organizations identify and manage security vulnerabilities in their network infrastructure. Here's a quick overview of what Nessus does:

1. **Vulnerability Scanning**: Nessus scans networked systems to identify potential vulnerabilities, such as missing patches, misconfigurations, or insecure services.
2. **Comprehensive Reporting**: After scanning, Nessus provides detailed reports on identified vulnerabilities, including their severity, potential impact, and recommended remediation steps.
3. **Customizable Scanning**: Users can configure scans to focus on specific areas or systems, schedule regular scans, and apply different scan policies to meet their needs.
4. **Compliance Checks**: Nessus can assess systems against various compliance standards (e.g., PCI DSS, HIPAA) to help ensure adherence to regulatory requirements.
5. **Risk Management**: By identifying vulnerabilities, Nessus helps organizations prioritize and address security risks based on their potential impact and exploitability.

Nessus is often used by security professionals and IT administrators to enhance the security posture of their networks and systems. It offers both a free version (Nessus Essentials) with limited features and a paid version (Nessus Professional) with more advanced capabilities.

CONDUCTING SECURITY AUDITS FOR A NETWORK

- Objective:

  Perform Comprehensive Security Audits for A Network.

- Description:

  Evaluate The Security Posture of a Network by Identifying Vulnerabilites and Weakness provide Recommendations to Enhance Security Measure
- Key Steps:

  Conducting a Risk Assessment and Identifying Potential Threats.
  Using Tool to scan vulnerabilities.
  Reviewing Security Polices and Procedure.
  Compiling a Report with Finding and Recommendations.
  Presenting The Audit to Stakeholders.

ASSETS INVENTORY

1. Laptop:

   Manufacture: DELL

   Device Model: DELL Latitude | E6530

   Processor: Intel Core i5-3350U CPU

   OS: Window 10

2. Router

   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.

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.

3. Disable unnecessary ports and services:

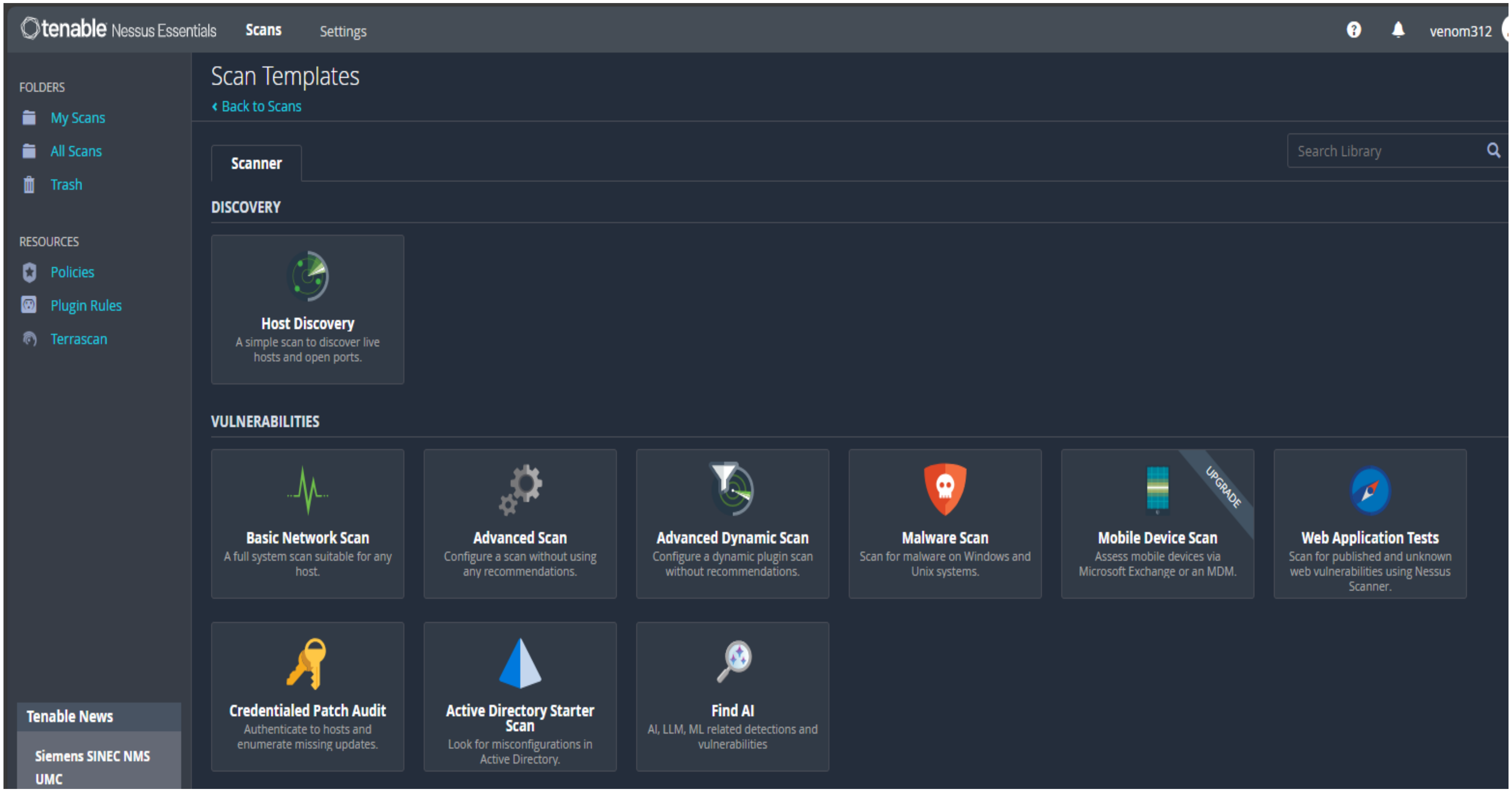
Ports and services are communication endpoints and functions that can be exploited by attackers if they are left open or active without necessity. By disabling those that are not in use, you minimize the attack surface available to potential intruders, reducing the risk of unauthorized access or exploitation.

4. 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.
5. Use Antivirus software’s:
   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.

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.

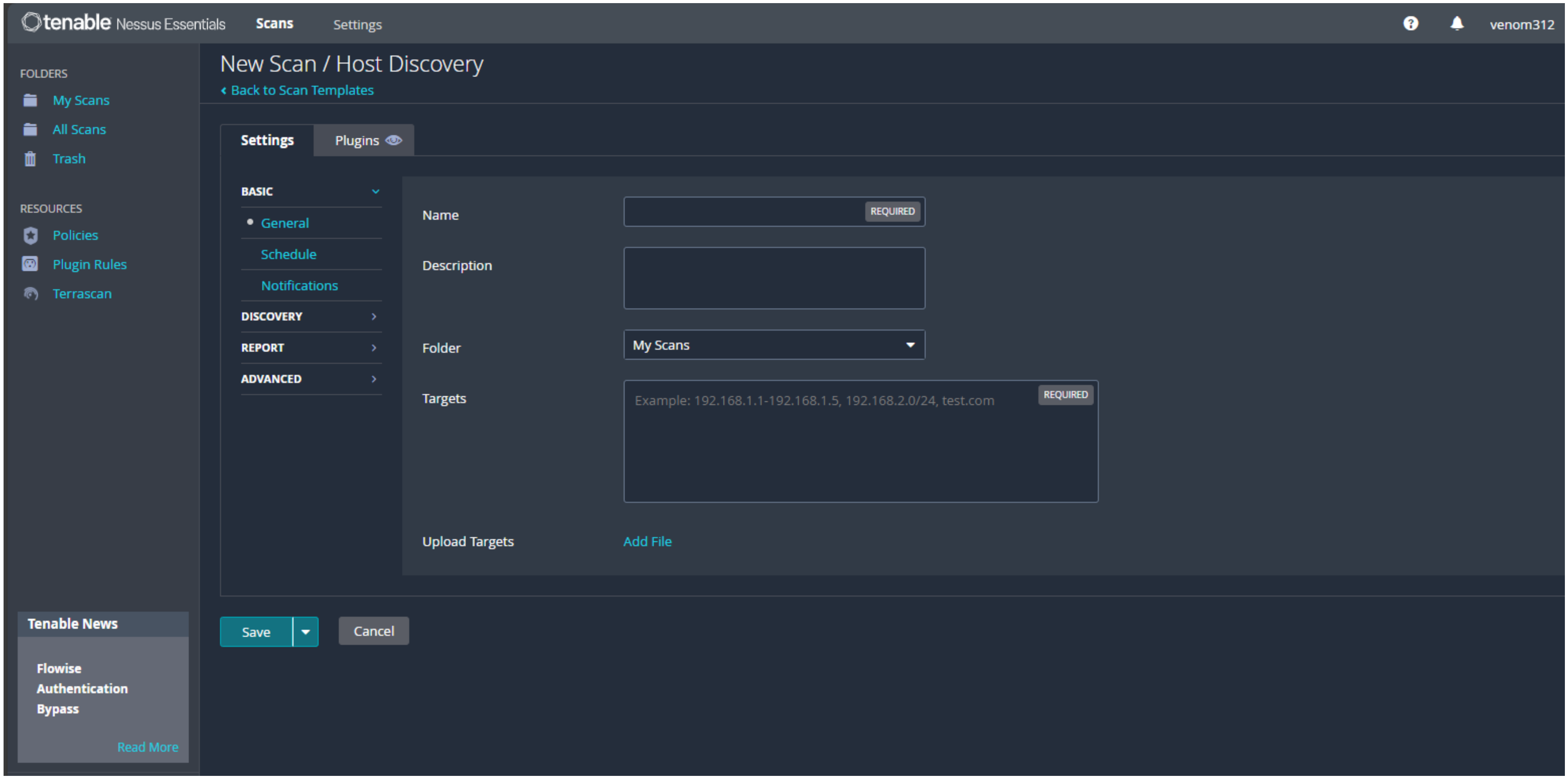
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

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.



New Scan / Host Discovery

‹ Back to Scan Templates

Name: REQUIRED

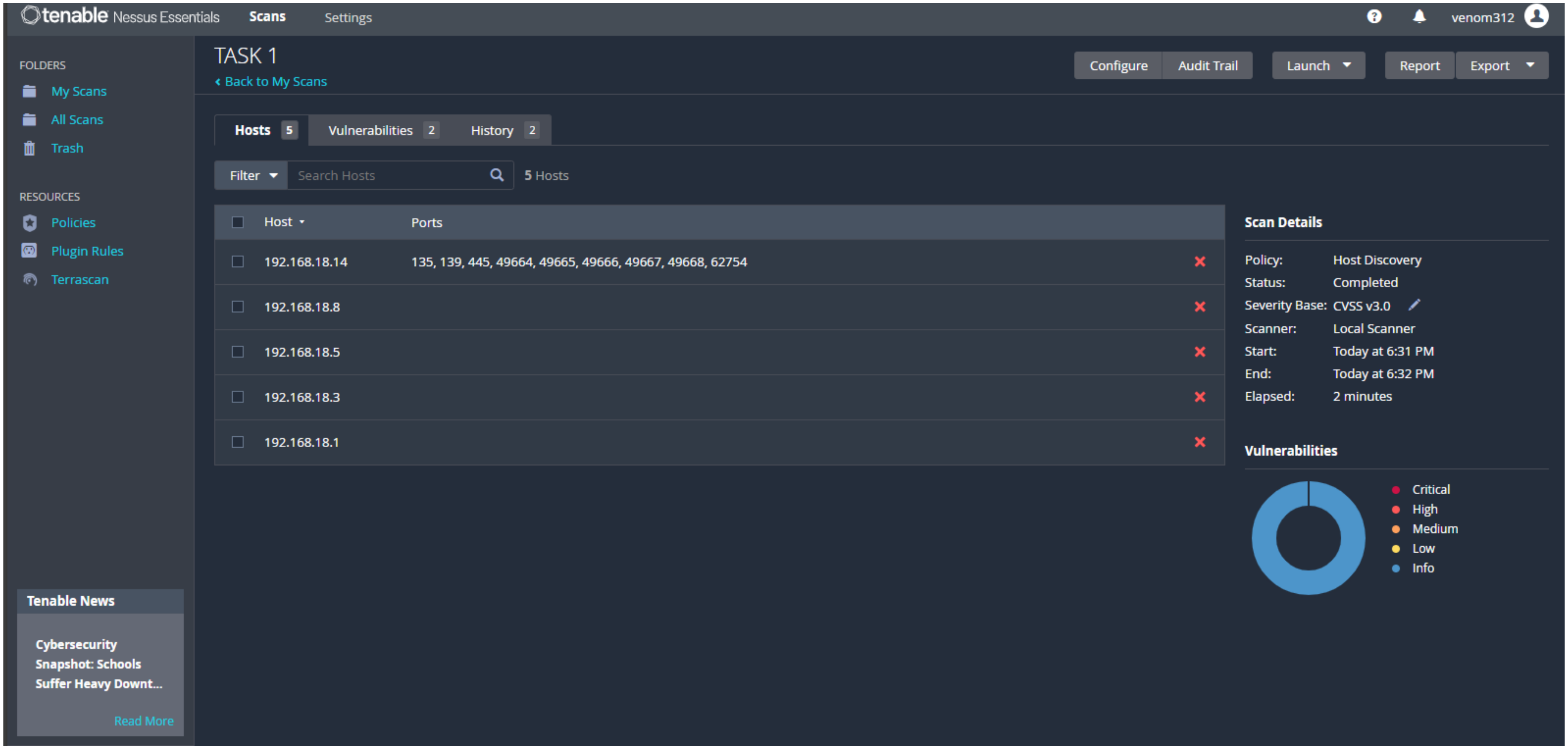
Description:

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED

Upload Targets: Add File

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



TASK 1

‹ Back to My Scans

5 Hosts

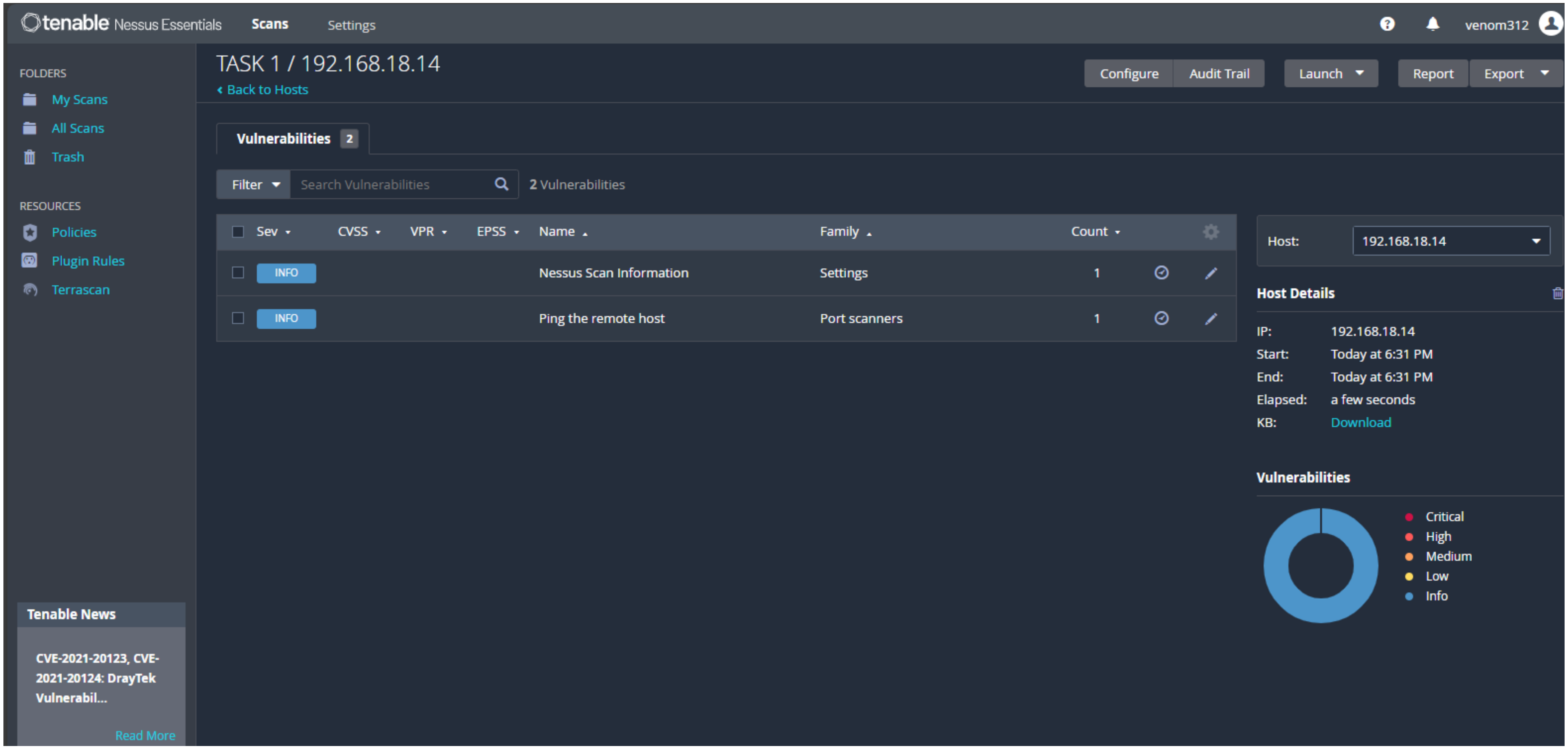
Host	Ports
192.168.18.14	135, 139, 445, 49664, 49665, 49666, 49667, 49668, 62754
192.168.18.8	
192.168.18.5	
192.168.18.3	
192.168.18.1	

Scan Details

Policy:	Host Discovery
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:31 PM
End:	Today at 6:32 PM
Elapsed:	2 minutes

Vulnerabilities

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



TASK 1 / 192.168.18.14

2 Vulnerabilities

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

Host: 192.168.18.14

Host Details

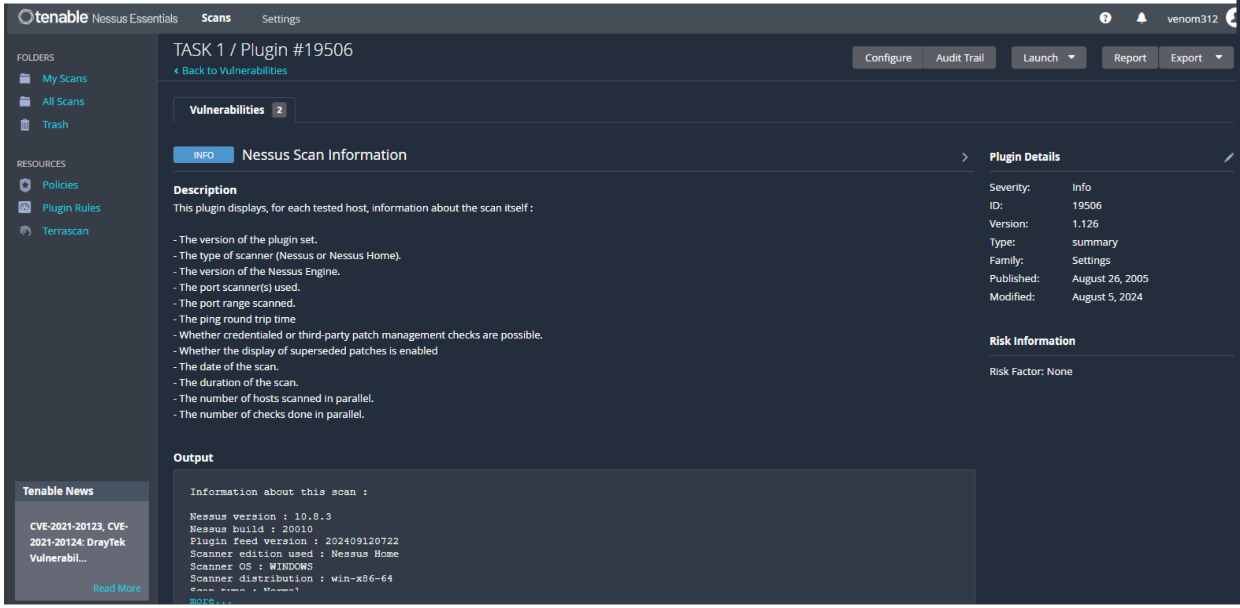
IP:	192.168.18.14
Start:	Today at 6:31 PM
End:	Today at 6:31 PM
Elapsed:	a few seconds
KB:	Download

Vulnerabilities

Tenable News

CVE-2021-20123, CVE-2021-20124: DrayTek Vulnerabil...

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



TASK 1 / Plugin #19506

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 : 10.8.3
Nessus build : 20010
Plugin feed version : 202409120722
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
more...
```

Plugin Details

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

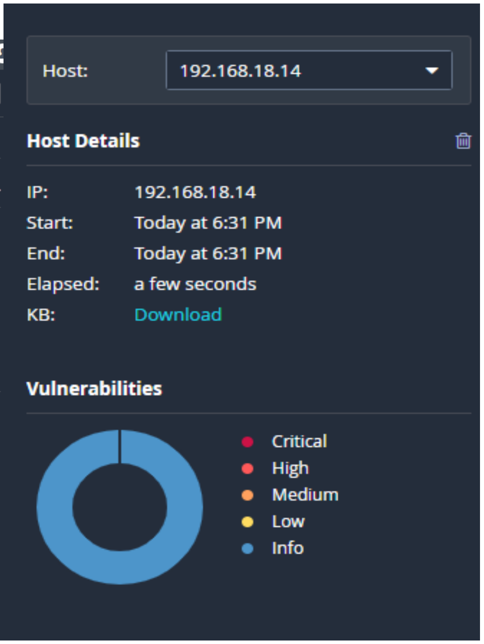
Risk Information

Risk Factor: None

Tenable News

CVE-2021-20123, CVE-2021-20124: DrayTek Vulnerabil...

Read More



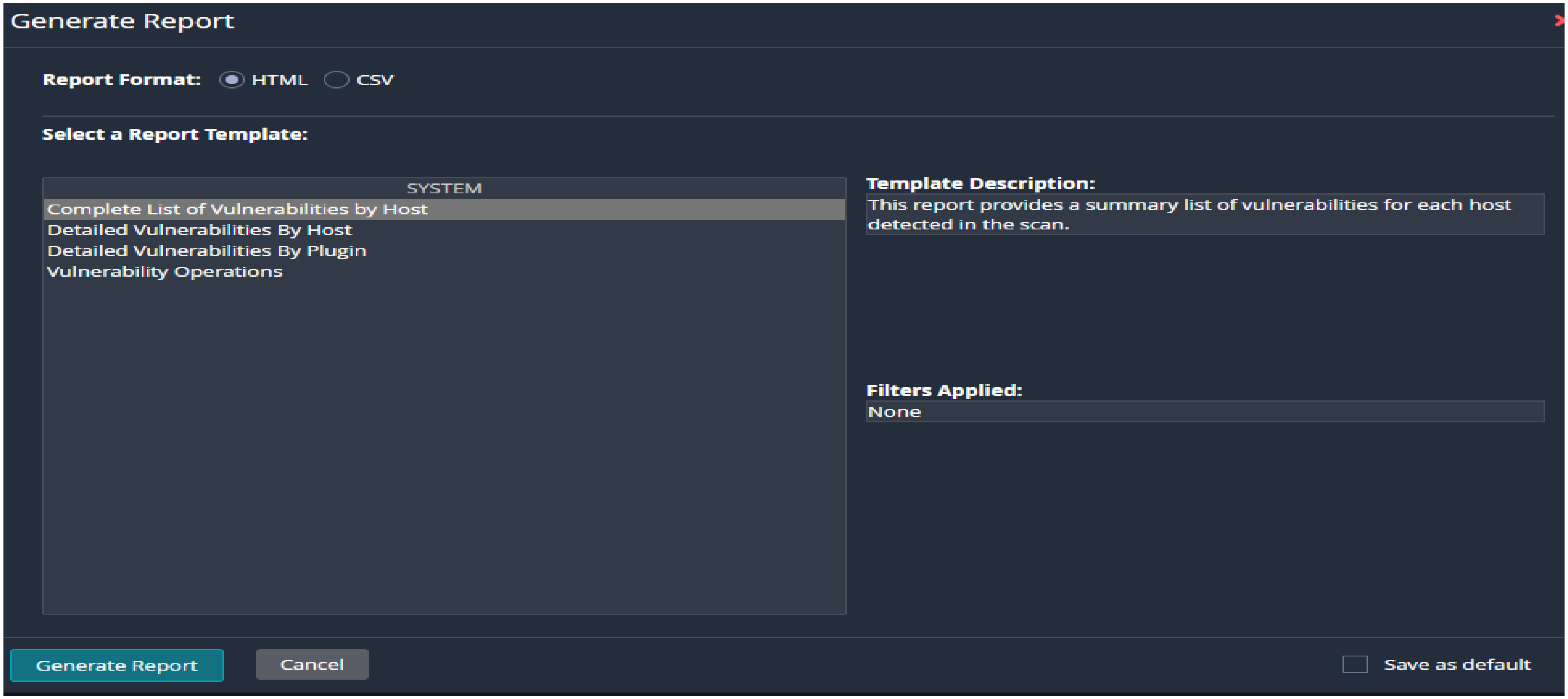
Host: 192.168.18.14

Host Details

IP: 192.168.18.14
Start: Today at 6:31 PM
End: Today at 6:31 PM
Elapsed: a few seconds
KB: Download

Vulnerabilities

Now Export the File



Generate Report

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

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