Stage 2 Report - Nessus

Prepared by	**Dr.Sumaiya Thaseen,** **Associate Professor,** **School of Computer Engineering and Information Systems,** **Vellore Institute of Technology, Vellore,** **Tamil Nadu**

Overview of Nessus:-

Nessus is a popular proprietary vulnerability scanner developed by Tenable. This tool is mainly used for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources. The different types of scan which can performed on Nessus Essentials (free version which is limited to run 16 hosts). Figure 1 shows the dashboard of Nessus essentials

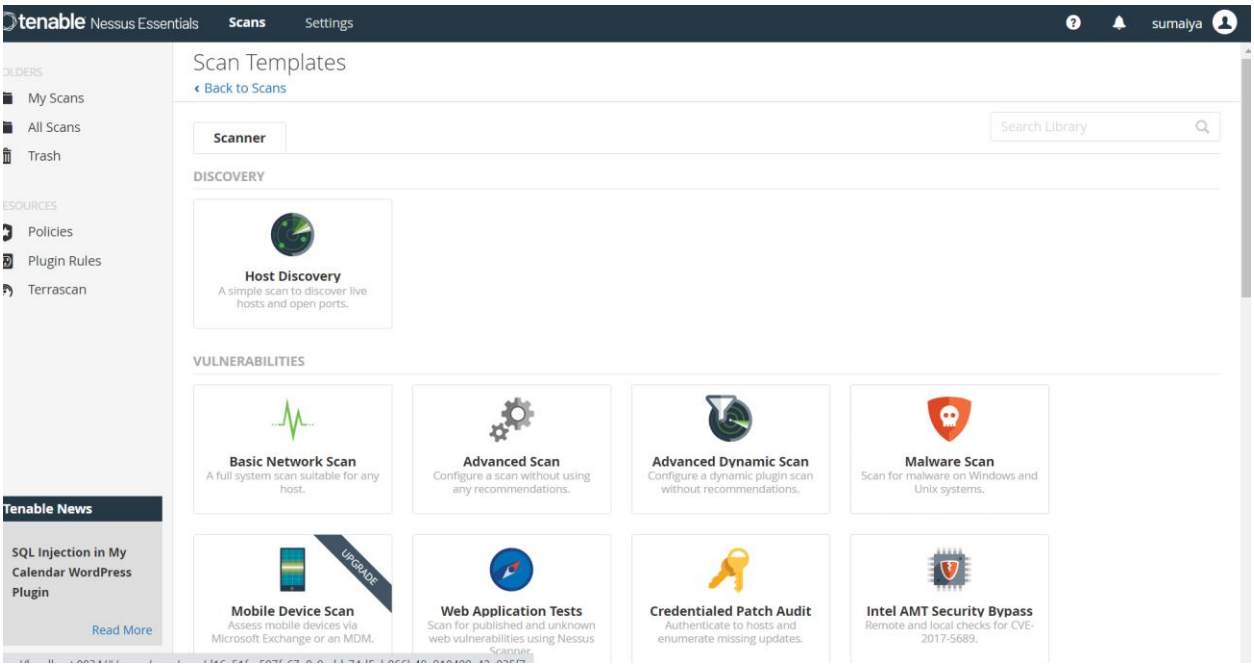

Figure 1: Nessus Dashboard

The major types of scan which can be executed on this version are

1. Basic Network Scan – A full system scan suitable for any host.
2. Advanced Scan – Configure a scan without using any recommendations.
3. Advanced Dynamic Scan – Configure a dynamic plugin scan without recommendations.
4. Malware Scan – Scan for malware on Windows and Unix systems.
5. Mobile Device Scan – Assess mobile devices via Microsoft Exchange or an MDM.
6. Web Application Tests – Scan for published and unknown web vulnerabilities.
7. Credential Patch Audit – Authenticate hosts and enumerate missing updates.
8. Intel AMT Security bypass – Remote and local checks for CVE-2017-5689
9. WannaCry Ransomware - Remote and local checks for MS17-010
10. Ripple20 Remote Scan – A remote scan to fingerprint hosts potentially running the Treck stack in the network.
11. Zerologon Remote Scan – A remote scan to detect Microsoft Netlogon Elevation of Privilege
12. Solorigate – Remote and local checks to detect Solarwinds Solorigate vulnerabilities.

13. ProxyLogon : MS Exchange – Remote and local checks to detect exchange vulnerabilities targeted by HAFNIUM.
14. PrintNightmare – Local checks to detect the PrintNightmare vulnerability in Windows Print Spooler.
15. Active Directory Starter Scan – Look for misconfigurations in Active Directory.
16. ContiLeaks – Detection of vulnerabilities revealed in the Contileaks chats.
17. Ransomware Ecosystem – Vulnerabilities used by ransomware groups and affiliates.
18. 2022 Threat Landscape Report – (LTR) – A scan to detect vulnerabilities featured in the End of Year Report.

Target website — demo.testfire.net

Target ip address:- 65.61.137.117

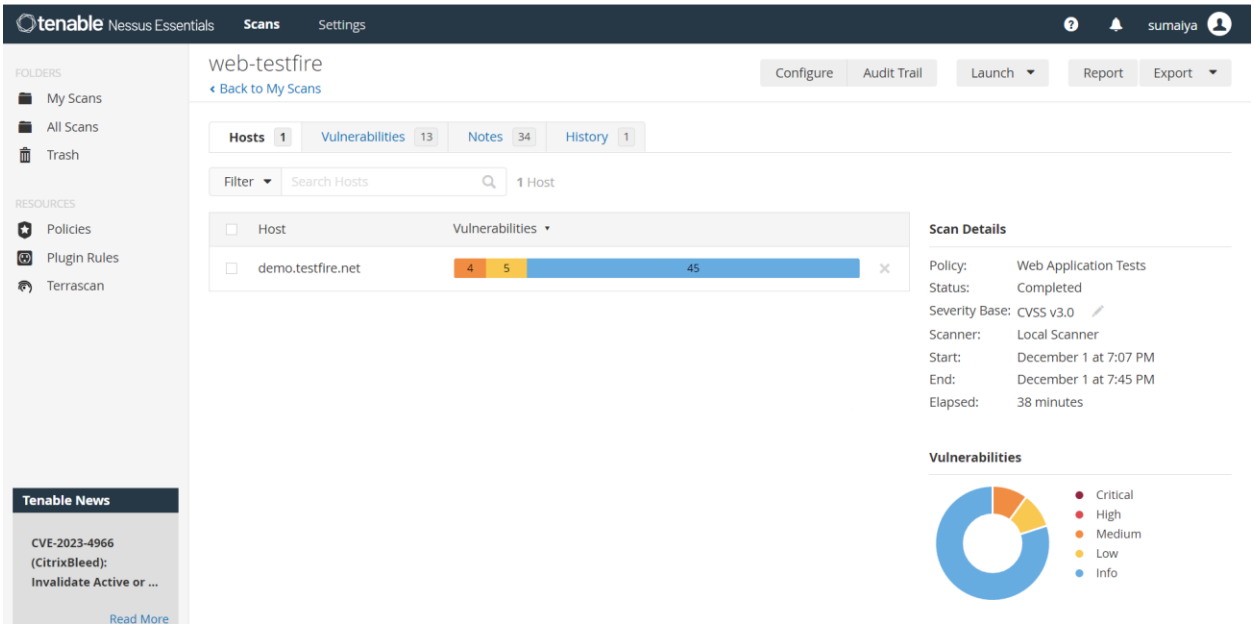

Figure 1: Snapshot of Nessus Dashboard with the host details.

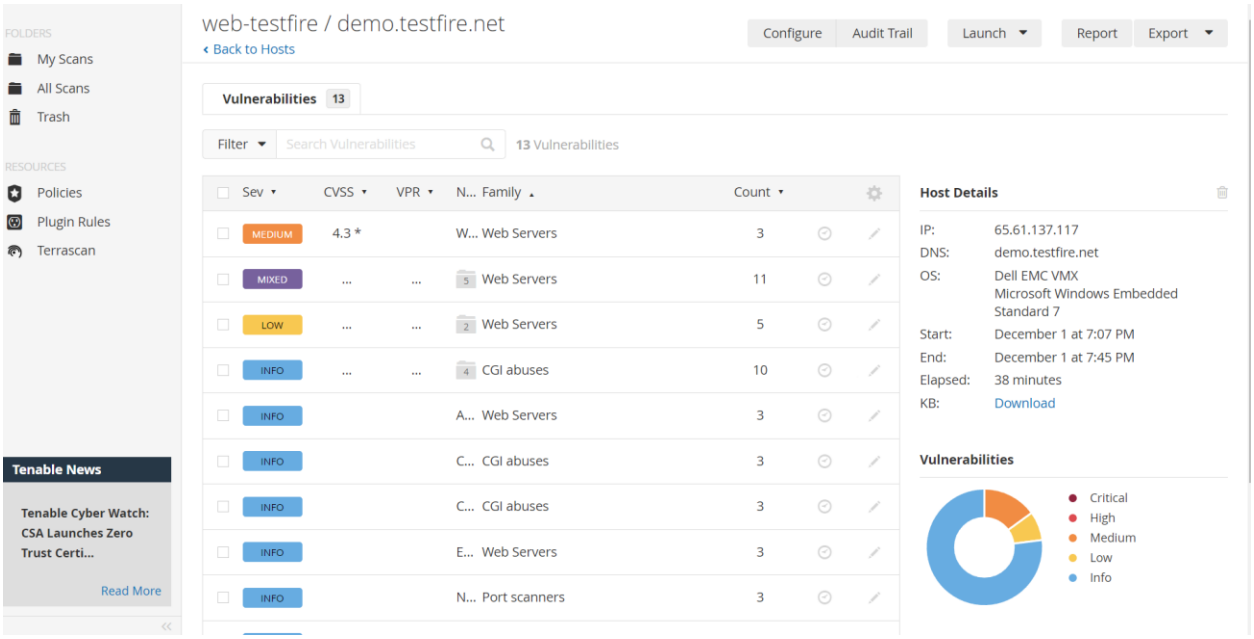

Figure 2: Snapshot of the Nessus Dashboard with Vulnerabilities listed on the website

List of vulnerability

s.no	Vulnerability name	Severity	plugins
1	Web Application Potentially Vulnerable to Clickjacking	**Medium**	85582
2	HSTS Missing From HTTPS Server (RFC 6797)	**Mixed**	142960
3	Web Server Transmits Cleartext Credentials	**Low**	26194

4	Web Server Allows Password Auto-Completion	**Low**	42057

REPORT:-

Vulnerability Name:-	Web Application Potentially Vulnerable to Clickjacking
Severity	Medium
Plugin	85582
Port	80 tcp
Description	The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts

	which sources can embed the protected resource.
Solution:-	Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.
Business Impact::-	This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

Vulnerability Name:-	HSTS Missing From HTTPS Server (RFC 6797)
Severity	Medium
Plugin	142960
Port	443 tcp
Description	The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-

	in-the-middle attacks, and weakens cookie-hijacking protections.
Solution:-	Configure the remote web server to use HSTS.
Business Impact::-	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. Impact: SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.s

Vulnerability Name:-	Web Server Transmits Cleartext Credentials
Severity	Low
Plugin	26194
Port	80 - tcp 8080 - tcp
Description	The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
Solution:-	Make sure that every sensitive form transmits content over HTTPS.
Business Impact::-	An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to

	get access to sensitive data like usernames or passwords

Vulnerability Name:-	Web Server Allows Password Auto-Completion
Severity	Low
Plugin	42057
Port	443 tcp 80 tcp 8080 tcp
Description	The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'. While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution:-	Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
Business Impact::-	If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application. The stored credentials can be captured by an attacker who gains control over the user's computer.

Best Practices and Customization:

Incorporating the best practices recommended for the Nessus Scanner and for vulnerability testing in general.

1. **Scan every device that touches your ecosystem.** Failing to do so may leave security gaps in some assets and expose all interconnected apps and devices to risk.
2. **Scan frequently**—because a large gap between scans leaves your systems open to new vulnerabilities that have cropped up in the ever-evolving threat landscape.
3. **Use credentialed scanning.** A credentialed scan is a vuln scan in which the scanning tool is provided with valid credentials, such as usernames and passwords, to access the target systems or devices. Credentialed scans yield more accurate results as testers can gain authorized access to internal systems and information.
4. **Assign owners to critical assets.** Articulate accountability for each device to a specific owner (try to pick someone who is affected if that device is compromised.) and make the owner responsible for keeping that device patched and secured.
5. **Prioritize the patching process.** Patch internet-facing devices for all discovered vulnerabilities, focusing first on assets with the highest risk levels.
6. **Document all scans and their results.** Run each **vulnerability scan** according to a management-approved schedule. Provide detailed reports, ensuring that they are actionable for technology teams as well as insightful for non-technical business teams, top management or stakeholders.
7. **Establish and implement a remediation process** based on the scan results and an in-depth study of the findings by experienced security teams or penetration testers. Categorize each vulnerability by its risk severity and the urgency to remediate, and estimate the required time for remediation.

References:

https://www.redlegg.com/blog/nessus-scanner-best-practices-for-common-issues