

Report Submission

To



Task 3: Vulnerability Scanning with Nessus Essentials

NAME	YASH JAVIYA
Submission to	Elevated Labs

Task Objective

To gain hands-on experience in identifying security vulnerabilities on a local Linux system using widely adopted vulnerability assessment tool: **Nessus Essentials**. This exercise helps in understanding the vulnerability scanning process, CVSS scoring, mitigation strategies, and practical security assessment reporting.

Tools Used

Tool	Description
Nessus Essentials	A free-tier vulnerability scanner developed by Tenable. Used globally for professional vulnerability assessments.

Test Environment Configuration

Component	Details
Operating System	Kali Linux (Rolling) – Debian-based distribution with Linux kernel 6.12.25-amd64
Host Type	Virtual Machine (VMware detected via MAC: 00:0c:29:30:8a:91)
Target IP (IPv4)	127.0.0.1 (localhost — scanned by Nessus)
Loopback IP	127.0.0.1
Docker Interface	docker0 – 172.17.0.1 detected as a bridge interface
MAC Address	00:0c:29:30:8a:91 (VMware Virtual Adapter)
Hostname	kali (detected by Nessus)
Network Interfaces	lo, eth0, docker0
Running Services	Apache HTTP Server, SSH, Docker containers, Nessus daemon (port 8834)
Installed Software	Apache 2.4.63, Node.js 20.11.0, Log4j (1.x and 2.x), Python Tornado, Trivy, ClamAV
Firewall Status	UFW not actively detected (presumed disabled or not interfering with scans)
NAT/Bridged Mode	Likely Bridged or NAT mode (VM uses local loopback and host-only networking)

Vulnerability Scanning with Nessus Essentials

About Nessus Essentials

Nessus is a vulnerability scanner developed by Tenable. Its Essentials version is free for up to 16 IP addresses, making it ideal for labs and students.

Step-by-Step Process

1. Download and Install

Wget <https://www.tenable.com/downloads/api/v1/public/pages/nessus/downloads/<nessus-deb-package>>

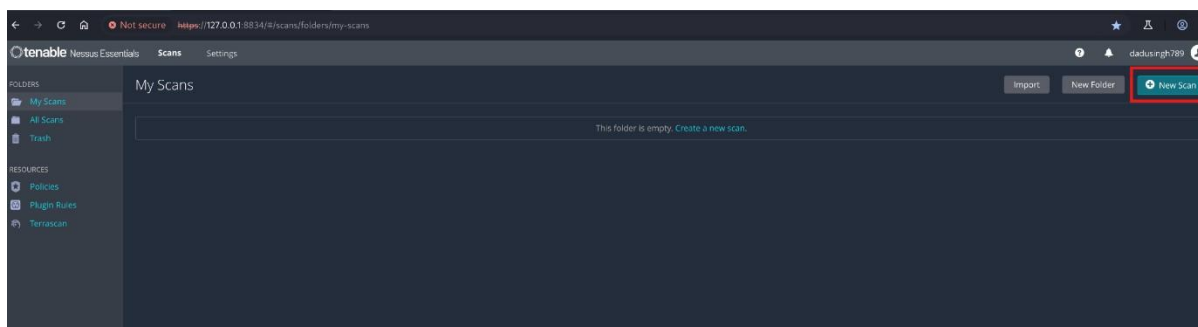
```
sudo dpkg -i <Nessus-deb-package>
```

```
sudo systemctl start nessusd
```

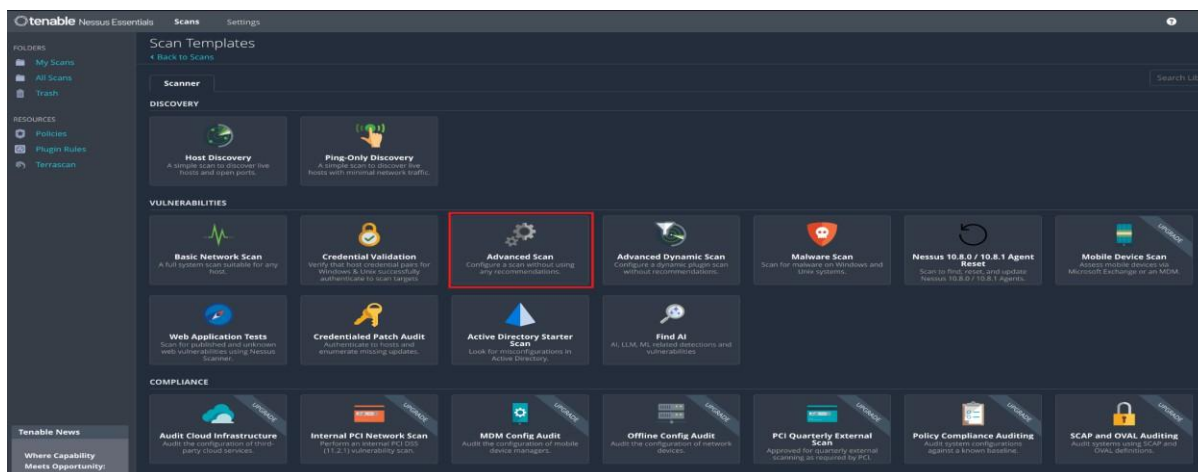
2. Setup via Web Interface

- URL: <https://localhost:8834>
- Choose **Nessus Essentials**
- Register for free activation code at Tenable
- Create local admin user
- Plugin download begins (~25 mins)

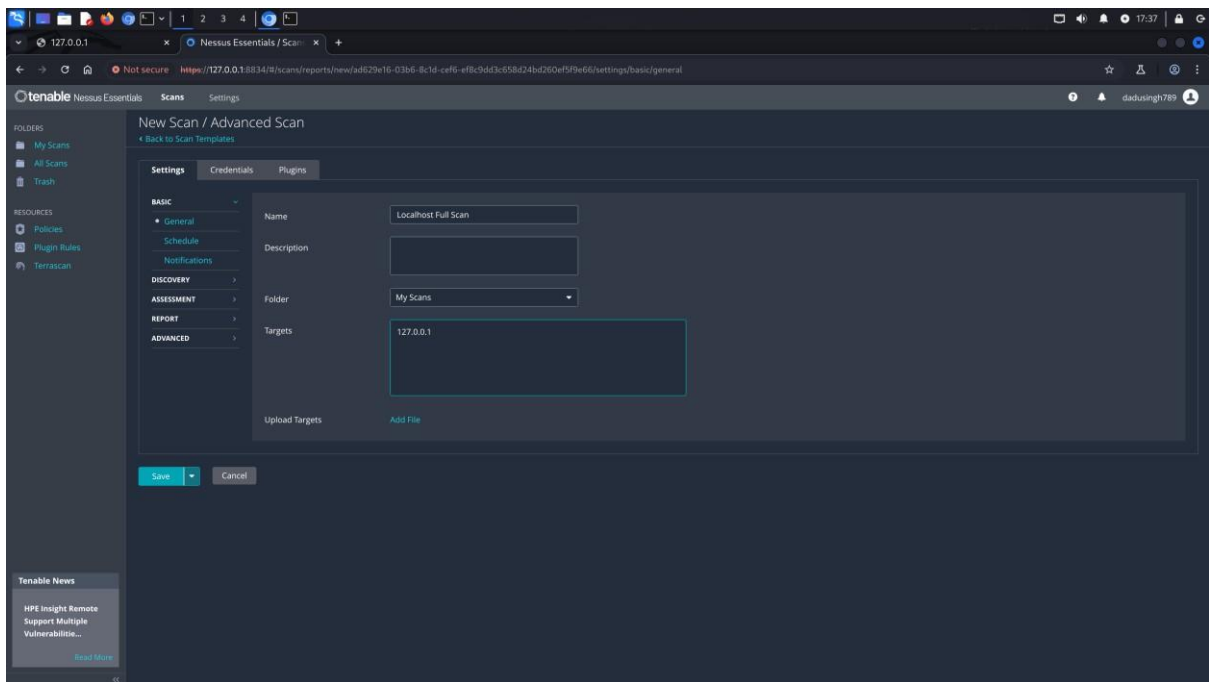
3. New Scan Creation



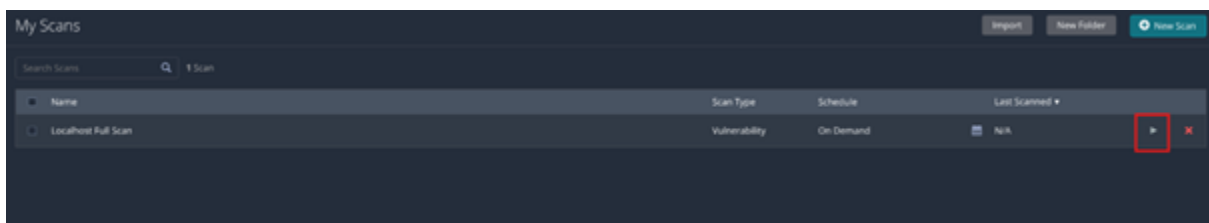
- Go to **Scans** → **New Scan** → **Advance Scan**



- Name: Localhost Full Scan
- Target: 127.0.0.1
- Save



- Launch Scan
 - From the scan list, click the **play (▶)** icon next to your scan
 - Nessus will begin scanning



Step 4: Review Scan Results



1. Click the scan after it's finished
2. View:

- **Summary (number of vulnerabilities)**
- **Details (CVE, affected software, risk levels)**
- **Nessus recommendations**

Localhost Full Scan

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 70 Remediations 3 History 1

Filter Search Vulnerabilities 70 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
High	8.4			Pandas DataFrame.query Code Injection (Unpatched)	Artificial Intelligence	1
Mixed				Nodejs Node.js (Multiple Issues)	Misc.	7
Mixed				Apache Log4j (Multiple Issues)	Misc.	4
Mixed				Tornadoweb Tornado (Multiple Issues)	Misc.	2
Mixed				SSL (Multiple Issues)	General	5
Info				SSH (Multiple Issues)	General	6
Info				Apache HTTP Server (Multiple Issues)	Web Servers	2
Info				Docker (Multiple Issues)	Service detection	2
Info				HTTP (Multiple Issues)	Web Servers	2
Info				TLS (Multiple Issues)	Service detection	2
Info				PostgreSQL Client/Server Installed (Linux)	Databases	2
Info				Service Detection	Service detection	2
Info				A/LLM Software Report	Artificial Intelligence	1
Info				Aqua Security Trivy Installed (Linux / Unix)	Misc.	1
Info				ClamAV Installed (Linux)	Misc.	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:40 PM
End: Today at 5:48 PM
Elapsed: 8 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Localhost Full Scan

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 70 Remediations 3 History 1

Search Actions 3 Actions

Action	Vulns	Hosts
Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple Vulnerabilities (Wednesday, May 14, 2025 Security Releases): Upgrade to Node.js version 20.19.2 / 22.15.1 / 23.11.1 / 24.0.2 or later.	20	1
Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104): Upgrade to Apache Log4j version 2.16.0 or later since 1.x is end of life. Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.	1	1
Python Library Tornado 6.5.0 DoS: Upgrade to Tornado version 6.5.0 or later.	0	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:40 PM
End: Today at 5:48 PM
Elapsed: 8 minutes

Step 5: Document Critical Vulnerabilities

- **Focus on Critical and High severity issues**
- **Note:**
 - **CVE**
 - **Affected software**
 - **Fix/patch URL**
 - **Risk description**

Localhost Full Scan / Plugin #213084

[Back to Vulnerabilities](#)

Hosts 1

Vulnerabilities 70

Remediations 3

History 1

HIGH

Pandas DataFrame.query Code Injection (Unpatched)

<

>

Plugin Details

Description

The version of the Pandas library installed on the remote host has an unpatched exposure. It is, therefore, affected by a code injection vulnerability in the pandas.DataFrame.query function. The function is intended to allow querying the columns of a DataFrame using a boolean expression. A malicious attacker can construct a malicious query to bypass input validation mechanisms and trigger a code injection vulnerability which can lead to command execution if the code passes untrusted input into self.eval().

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

This vulnerability is currently not fixed. Fix the code manually or monitor new releases for a fix.

See Also

<https://huntr.com/bounties/a48baae1-4652-4d6c-a179-3132c1c41a8d>
<http://www.nessus.org/u/d0bbeef33>
<http://www.nessus.org/u/7f63005e>

Output

These vulnerabilities remain unfixed and exist in the following locations:

Path: /usr/lib/python3/dist-packages/pandas-2.2.3-dfsg.egg-info

Version: 2.2.3

To see debug logs, please visit individual host

Port	Hosts
N/A	127.0.0.1

Severity: High

ID: 213084

Version: 1.4

Type: local

Family: Artificial Intelligence

Published: December 17, 2024

Modified: February 20, 2025

Risk Information

Risk Factor: High

CVSS v3.0 Base Score: 8.4

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

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:Q/RC:C

CVSS v3.0 Temporal Score: 7.3

CVSS v2.0 Base Score: 7.2

CVSS v2.0 Temporal Score: 5.3

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

CVSS v2.0 Temporal Vector: CVSS2@E:U/RL:Q/RC:C

Vulnerability Information

CPE: rpe:/s:pandas-dev:pandas

Exploit Available: true

Exploit Ease: Exploits are available

Vulnerability Pub Date: December 3, 2024

Reference Information

Nessus Scan Summary:

Scan Target: 127.0.0.1 (Kali

Linux) Scanner: Tenable Nessus

Essentials

OS Detected: Linux Kernel 6.12.25-amd64

Severity	Count
Critical	3
High	5
Medium	2
Low	0
Info	79

Key Critical & High Vulnerabilities

1. Apache Log4j 1.x Multiple Vulnerabilities

- CVE IDs: [CVE-2019-17571](#), [CVE-2020-9488](#), [CVE-2022-23302](#), [CVE-2022-23305](#), [CVE-2022-23307](#)
- Severity: High / Critical
- CVSS v3 Base Score: 9.8–10.0
- Impact: Remote Code Execution (RCE), SMTP MITM, unpatched use
- Recommendation: Upgrade to Log4j $\geq 2.17.1$, remove JMSAppender
- Path: /usr/share/javasnoop/lib/log4j-1.2.16.jar

2. Node.js Multiple Vulnerabilities

- Version Detected: 20.11.0
- CVEs: [CVE-2024-22019](#), [CVE-2024-21892](#), [CVE-2025-23167](#), [CVE-2024-27983](#)
- Severity: Critical / High
- Impact: DoS, Memory Leak, Path Traversal, Request Smuggling
- Recommendation: Upgrade to Node.js $\geq 20.19.2$
- Path: /usr/lib/python3/dist-packages/playwright/driver/node

3. Apache Log4j JMSAppender RCE

- CVE: [CVE-2021-4104](#)
- Severity: Medium
- Impact: RCE when JMSAppender enabled
- Recommendation: Upgrade Log4j and remove JMSAppender

- **Path:** /usr/share/javasnoop/lib/log4j-1.2.16.jar

4. SSL Certificate Cannot Be Trusted

- **Port Affected:** 8834
- **Impact:** Self-signed cert not trusted
- **Severity:** Medium
- **Fix:** Replace with CA-issued SSL certificate

5. Python Tornado DoS Vulnerability

- **CVE:** [CVE-2025-47287](#)
- **Version:** 6.4.2
- **Severity:** High
- **Impact:** Log flooding via malformed input
- **Fix:** Upgrade to Tornado $\geq 6.5.0$

Detected Installed Components

Software	Version
Apache HTTP Server	2.4.63
Log4j (multiple)	1.2.16, 2.17.1, 2.19.0, 2.24.3
Node.js	20.11.0
Tornado (Python)	6.4.2
Docker	Installed
Trivy	0.62.1
ClamAV	1.4.2
Containerd	1.7.24

Network Information (Enumerated by Nessus)

Interface	Address	Description
eth0	192.168.10.128	Main Kali adapter
docker0	172.17.0.1	Docker bridge
lo	127.0.0.1	Loopback interface
Hostname	kali	Local VM
MAC	00:0c:29:30:8a:91	VMware virtual adapter

Recommendations Summary

Action	Recommendation
Patch Log4j	Upgrade and remove all instances of Log4j 1.x
Patch Node.js	Upgrade to Node.js $\geq 20.19.2$
Fix SSL	Use certificates signed by a trusted CA
Audit Docker	Review insecure Dockerfiles and exposed ports
Upgrade Tornado	Use Tornado $\geq 6.5.0$ to fix DoS issue
Harden Access	Disable unused services and limit remote exposure

Next Steps

1. Apply patches and updates
2. Regenerate SSL certificates
3. Harden firewall and limit exposed services
4. Re-run vulnerability scans to confirm remediation
5. Maintain updated documentation and compliance logs