Penetration Test Workshop (CSE3157)

Finding Vulnerabilities with nessus

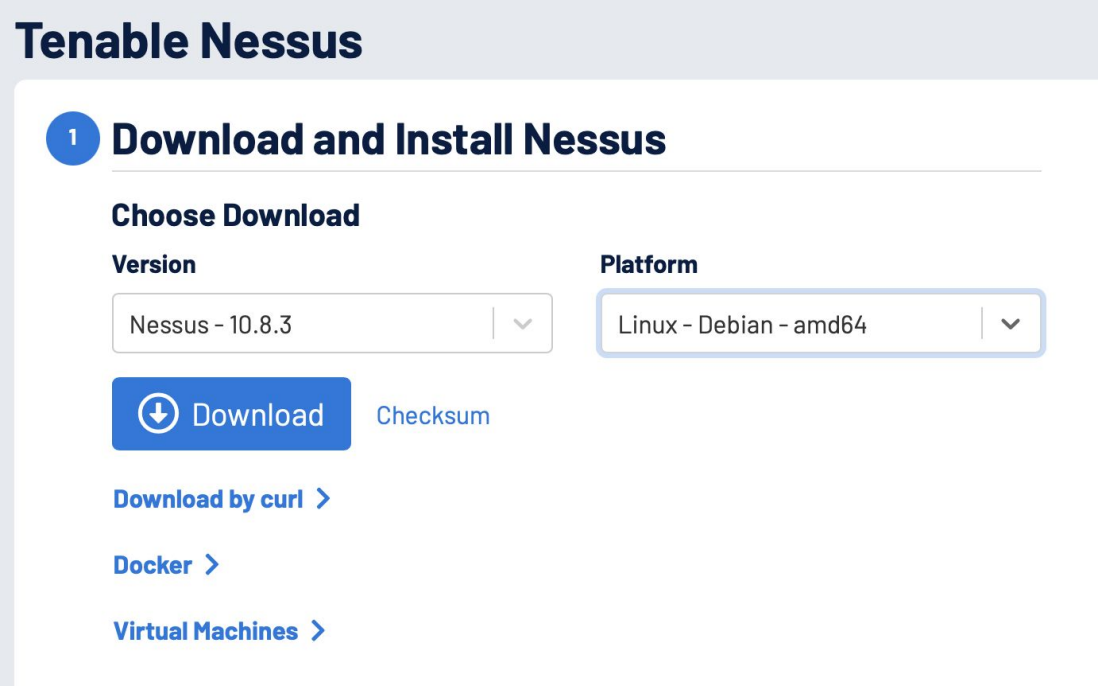
Dr. Rourab Paul

Computer Science Department, SOA University

Download

Download Link

Select version and platform, for your case it should be Linux Debian-amd64 because kali in debian based linux and you have amd processor



Installation and Open

Install

sudo su dpkg -i <nessus_package_name>.deb

open

/bin/systemctl/ start nessusd.service

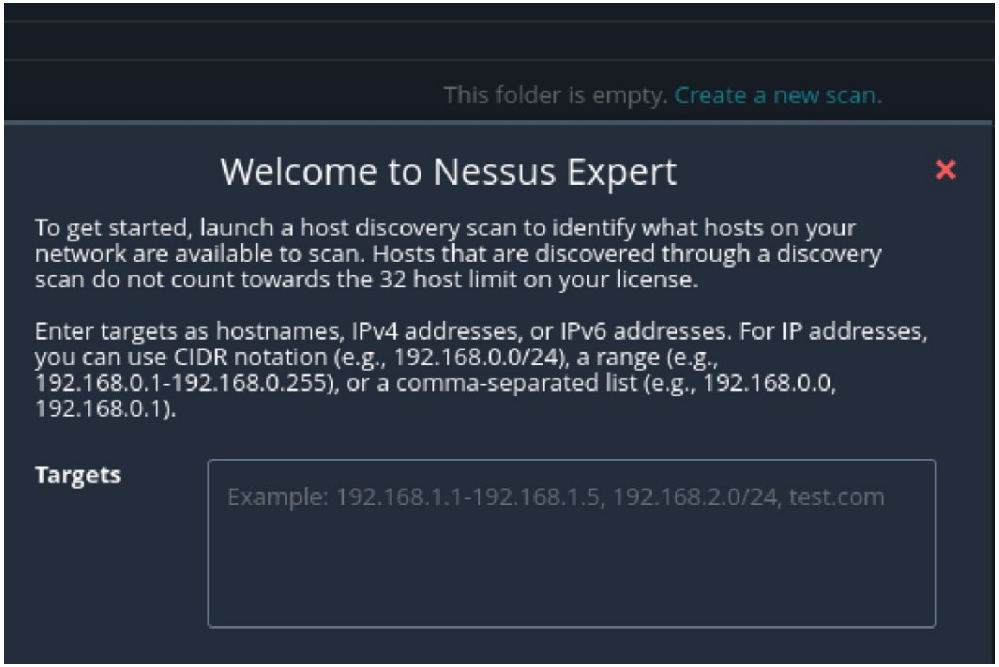
Account Configuration:

Offline

trial version for 7 days

Configure Nessus

- After successful login go to ‘settings’.
- Select ‘update plugins’.
- Click ‘save’.
- Wait until plugins are downloaded. Once the plugin download is done, you should get below message.



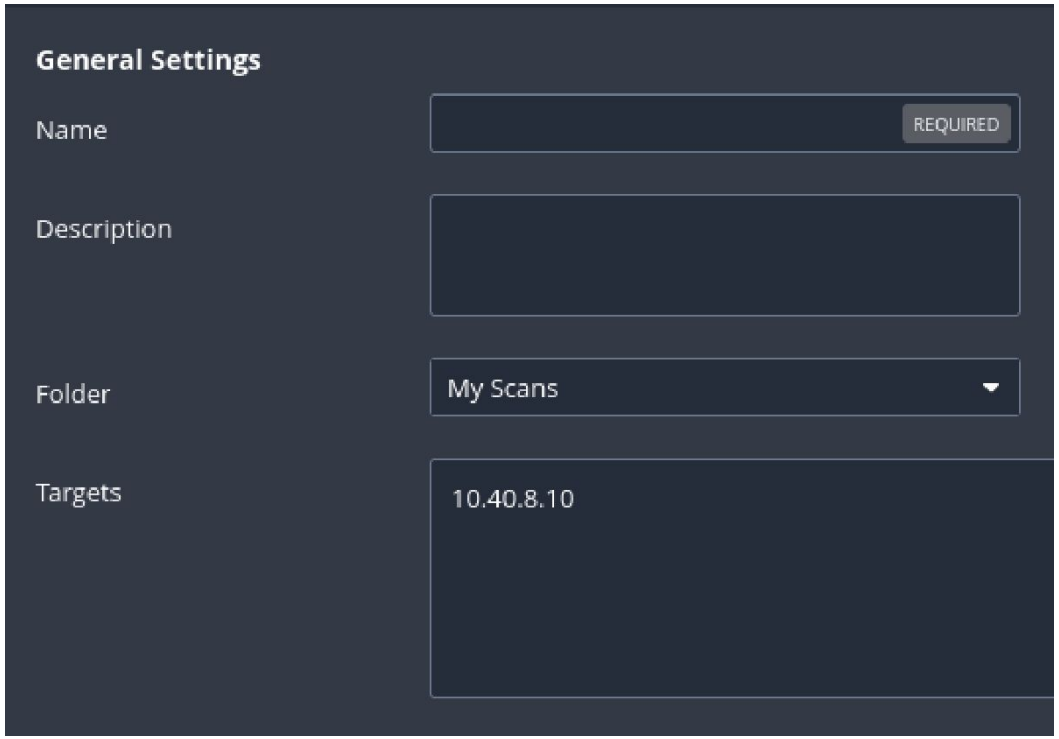
Start Scanning

Step 1: go to 'New Scan'.

Step 2: Select 'Basic Network Scan'.

Step 3: Enter Name Description

Step 4: Enter Target IP.



Analyzing report on target IP

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	13	14	2	34

Vulnerabilities Total: 65

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.9743	133845	Apache Tomcat 9.0.0.M1 < 9.0.31 multiple vulnerabilities
CRITICAL	9.8	9.4	0.0004	213078	Apache Tomcat 9.0.0.M1 < 9.0.98 multiple vulnerabilities
HIGH	7.5	6.7	0.0049	132419	Apache Tomcat 9.0.0.M1 < 9.0.30
HIGH	7.5	4.4	0.0096	138098	Apache Tomcat 9.0.0.M1 < 9.0.36
HIGH	7.5	3.6	0.9123	138591	Apache Tomcat 9.0.0.M1 < 9.0.37 multiple vulnerabilities
HIGH	7.5	4.4	0.0029	144050	Apache Tomcat 9.0.0.M1 < 9.0.40 multiple vulnerabilities
HIGH	7.5	5.9	0.002	147164	Apache Tomcat 9.0.0.M1 < 9.0.43 multiple vulnerabilities

Analyzing report on target IP

Based on 3 parameters severity of vulnerabilities can be understood:

1. **CVSSv3 (Common Vulnerability Scoring System v3).**
2. **VPR (Vulnerability Priority Rating).**
3. **EPSS (Exploit Prediction Scoring System)**

Analyzing report on target IP

CVSSv3 (Common Vulnerability Scoring System v3)

- **Purpose:** Measures the **severity** of a vulnerability.
- **Score Range: 0.0 – 10.0** (Higher score = Higher severity).
- **Components:**
  - **Base Score:** Represents the intrinsic qualities of a vulnerability (e.g., attack vector, complexity, etc.).
  - **Temporal Score:** Reflects factors like exploit code availability or remediation efforts.
  - **Environmental Score:** Considers specific security controls or impacts in your environment.

Example CVSSv3 Score Breakdown:

- **Low:** 0.1 – 3.9
- **Medium:** 4.0 – 6.9
- **High:** 7.0 – 8.9
- **Critical:** 9.0 – 10.0

Best for understanding the technical impact and exploitability of a vulnerability.

Analyzing report on target IP

2. VPR (Vulnerability Priority Rating)

- **Purpose:** Provides a **dynamic risk score** based on real-world threat intelligence.
- **Score Range: 0.0 – 10.0** (Higher score = Higher risk).
- **Factors Considered:**
  - Age of the vulnerability.
  - Exploit code availability and complexity.
  - Active exploitation in the wild.
  - Popularity among threat actors.

Key Benefit: VPR adjusts over time as new threat intelligence emerges, making it ideal for prioritizing threats that pose immediate risks.

Analyzing report on target IP

3. EPSS (Exploit Prediction Scoring System)

- **Purpose:** Predicts the **likelihood** that a vulnerability will be exploited in the next 30 days.
- **Score Range: 0.0 – 1.0** (Closer to 1 = Higher chance of exploitation).
- **Driven by Data:** Uses machine learning models analyzing data from real-world exploits, threat intelligence feeds, and CVE metadata.

Key Benefit: EPSS is highly effective for understanding the **probability of exploitation**, even for low-severity vulnerabilities.

When to Use Each Score

- **CVSSv3:** For understanding technical severity and potential impact.
- **VPR:** For prioritizing urgent threats that require immediate action.
- **EPSS:** For identifying vulnerabilities that are likely to be exploited soon, regardless of their CVSS score.

Analyzing report on target IP

Vulnerabilities 1 : Apache Tomcat Version 9.0.0.M1 < 9.0.31

(risk level : **Critical**)

Vulnerabilities 2 : SMB Signing (risk level : **Medium**)

Vulnerabilities in apache Tomcat 9.0.0.M1 < 9.0.31

1. CVE-2020-1938 (Ghostcat)

- **Type:** File Inclusion / Directory Traversal
- **CVSSv3 Score: 9.8 (Critical)**
- **Impact:** Allows remote attackers to read or include files on the server by exploiting the **AJP (Apache JServ Protocol)** connector.
- **Affected Component:** AJP Connector enabled by default on port **8009**.

2. CVE-2020-9484

- **Type:** Deserialization of Untrusted Data
- **CVSSv3 Score: 8.1 (High)**
- **Impact:** Allows attackers to execute arbitrary code via crafted data in Apache Tomcat's **PersistentManager** when using **FileStore.**

3. CVE-2019-17563

- **Type:** Improper Handling of Malformed Headers
- **CVSSv3 Score: 7.0 (High)**
- **Impact:** May allow attackers to bypass security filters or access restricted resources.

metasploit script on Tomcat 9.0.0.M1 < 9.0.31

- This information is for **educational** and **authorized penetration testing** only.
- Exploiting systems without permission is **illegal**

use exploit/multi/http/tomcat_ghostcat

SMB Signing not required

When SMB signing is disabled:

- **Man-in-the-Middle (MitM) Attacks:** An attacker can intercept and manipulate SMB traffic without being detected.
- **Session Hijacking:** Attackers can inject malicious payloads or impersonate legitimate users.
- **Data Integrity Risks:** Without SMB signing, data may be modified in transit without the client or server detecting the tampering.

MEDIUM	5.3	1.4	0.1554	152182	Apache Tomcat 9.0.0.M1 < 9.0.48
MEDIUM	5.3	6.7	0.8556	182809	Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.3	1.4	0.0012	141446	Apache Tomcat 9.0.0.M1 < 9.0.38
MEDIUM	4.3	2.2	0.0013	173251	Apache Tomcat 9.0.0.M1 < 9.0.72
LOW	3.7	1.4	0.0015	159464	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell CVE-2021-439

Thank You