

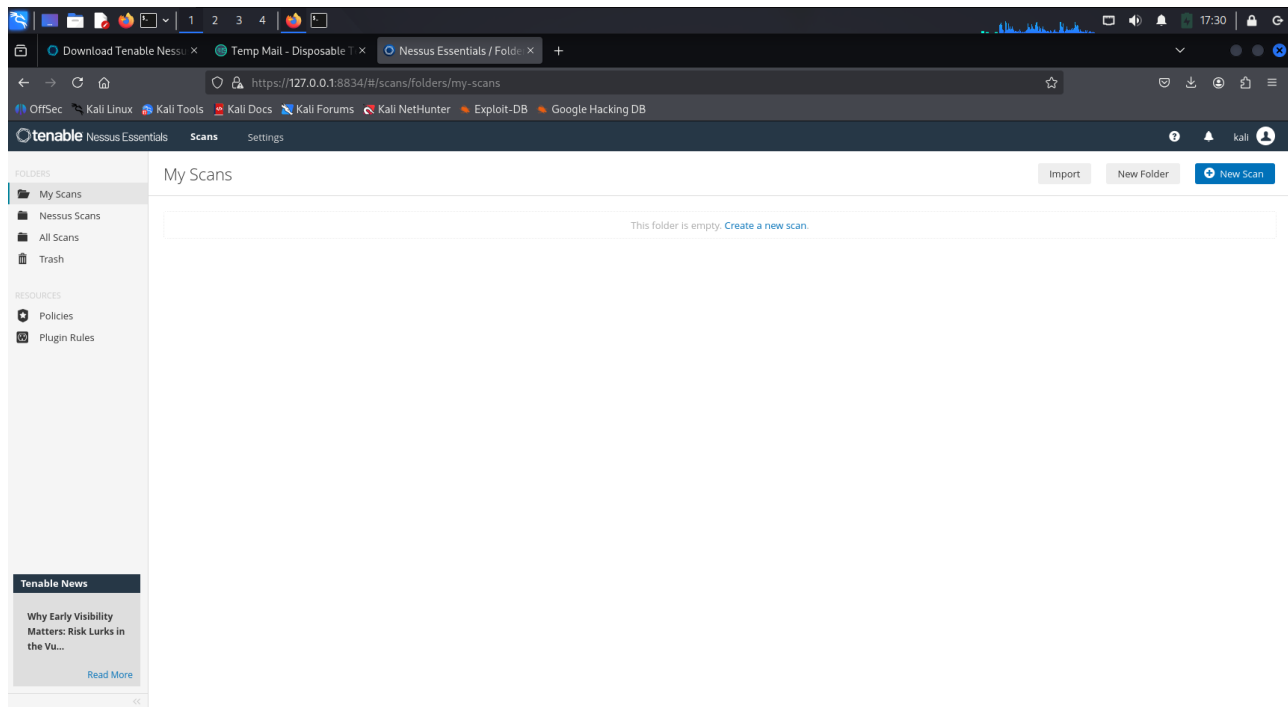
Task 3 : Perform a Basic Vulnerability Scan on Your PC.

Using Nessus for vulnerability scanning :-

The Vulnerable Metasploit machine I active and scanning it to get the whole vulnerabilities scans.

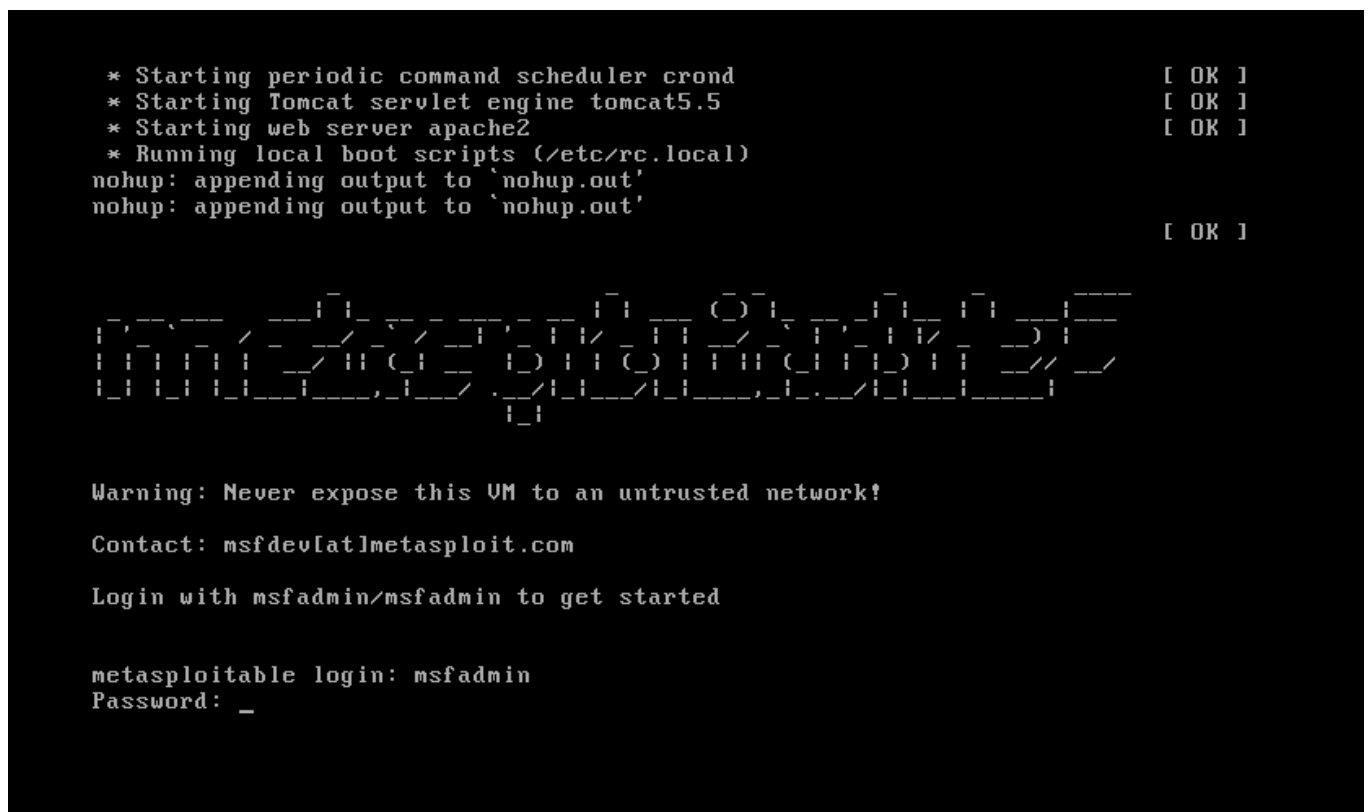
Step 1:-

Open the Nessus.



Step 2 :-

Starting the vulnerable lab and get the Ip address to scan it.



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:14:64:ae
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c29:1464:ae00:0000 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4588 (4.4 KB)  TX bytes:6826 (6.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

Step 3 :-

Now, scan the Ip address using Nessus tool.


Scan Templates


[Back to Scans](#)

Scanner


Search Library


DISCOVERY


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


**Ping-Only Discovery**
A simple scan to discover live hosts with minimal network traffic.


VULNERABILITIES


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


**Credential Validation**
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.


**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.


**Nessus 10.8.0 / 10.8.1 Agent Reset**
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.

**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


COMPLIANCE


**Compliance icon 1**

**Compliance icon 2**

**Compliance icon 3**

**Compliance icon 4**

**Compliance icon 5**

**Compliance icon 6**

Step 4 :-

We will use Basic Scan to find vulnerabilities.

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings | **Credentials** | **Plugins**

BASIC

- General
- Schedule
- Notifications

DISCOVERY**ASSESSMENT****REPORT****ADVANCED**

NameTask_3

DescriptionScanning on vulnerable machine

FolderMy Scans

Targets192.168.117.130

Upload TargetsAdd File


Save Cancel

My Scans

Import New Folder New Scan

Search Scans

1 Scan

<input type="checkbox"/>	Name	Scan Type	Schedule	Last Scanned ▾		
<input type="checkbox"/>	Task_3	Vulnerability	On Demand	 Today at 5:48 PM		≡

Now, its time to check the result

My Scans

Import New Folder New Scan

Search Scans

1 Scan

<input type="checkbox"/>	Name	Scan Type	Schedule	Last Scanned ▾
<input type="checkbox"/>	Task_3	Vulnerability	On Demand	✔ Today at 6:05 PM

Task_3

[Back to All Scans](#)

Configure Audit Trail Launch Report Export

Hosts1Vulnerabilities70Remediations2History1

Filter Search Hosts1 Host

Host	Auth	Vulnerabilities
192.168.117.130	Fail	<div><div>10</div><div>7</div><div>26</div><div>9</div><div>142</div></div>

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:45 PM
End: Today at 6:05 PM
Elapsed: 19 minutes

Vulnerabilities

Critical

High

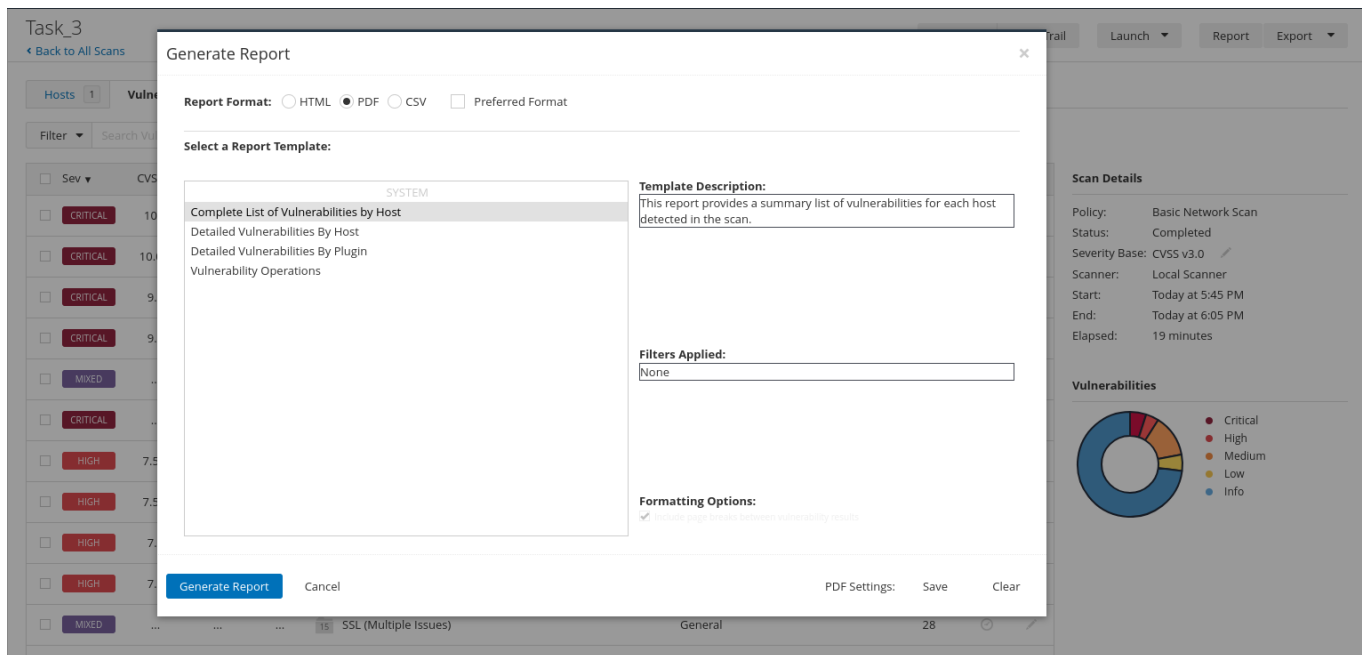
Medium

Low

Info

Step 5 :-

Let's generate the Report



Step 6 :-

Analyse the report and find the critical vulnerabilities.

CRITICAL	9.8	8.9	0.9447	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password

Step 7 :-

Give some solutions to these critical vulnerabilities that are found.

1. 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat) :-

Solution :- Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

2. 171340 - Apache Tomcat SEoL (<= 5.5.x) :-

Solution :- Upgrade to a version of Apache Tomcat that is currently supported.

3. 51988 - Bind Shell Backdoor Detection :-

Solution :- Verify if the remote host has been compromised, and reinstall the system if necessary.

4. 201352 - Canonical Ubuntu Linux SEoL (8.04.x) :-

Solution :- Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

5. 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness :-

Solution :- Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

6. 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) :-

Solution :- Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

7. 20007 - SSL Version 2 and 3 Protocol Detection :-

Solution :- Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

8. 61708 - VNC Server 'password' Password :-

Solution :- Secure the VNC service with a strong password.