



Penetration Testing using Nessus Tool

Aseel Abujaber

Feb,10-2025

Contents

1. Introduction to Nessus Tool.....	3
2. Environment Setup:	3
3. Connectivity and Ping Test:	4
4. Firewall Check on Windows 7	4
5. Nessus Installation and Service Activation	5
6. Nessus Setup Process:.....	7
7. Creating a New Scan in Nessus	9
8. Security Assessment Report.....	12
9. Vulnerability Scan:	14
10. Summary of Critical Vulnerabilities.....	15
11. Summary of High Vulnerabilities	16
12. Summary of Medium Vulnerabilities.....	16
13. Conclusion.....	17
14. Actionable Recommendations	18

1. Introduction to Nessus Tool

Nessus is a powerful vulnerability scanner widely used in cybersecurity for detecting and assessing vulnerabilities across various systems. It provides both a Graphical User Interface (GUI) and a command-line interface.

The GUI allows users to easily configure scans, view scan results, and navigate through vulnerabilities in a more user-friendly manner. With the GUI, users can run scans with just a few clicks, filter results, and generate comprehensive reports, making the tool accessible to both beginner and advanced users.

However, it's important to note that Nessus can be resource-intensive, especially during deep scans. It can consume a significant portion of both the processor (CPU) and memory (RAM), potentially leading to system performance issues.

Resource Management:

To alleviate stress on system resources, an external hard disk is used to store and scan large files. This helped reduce the load on the internal storage and improved disk performance, allowing for smoother scanning. However, CPU and memory usage remained dependent on the scanning process itself

2. Environment Setup:

“ The follow machines were configured on the same simulated network to ensure they could communicate with each other and access the internet for updates and scans”

This exersie was done on the following lap setup:

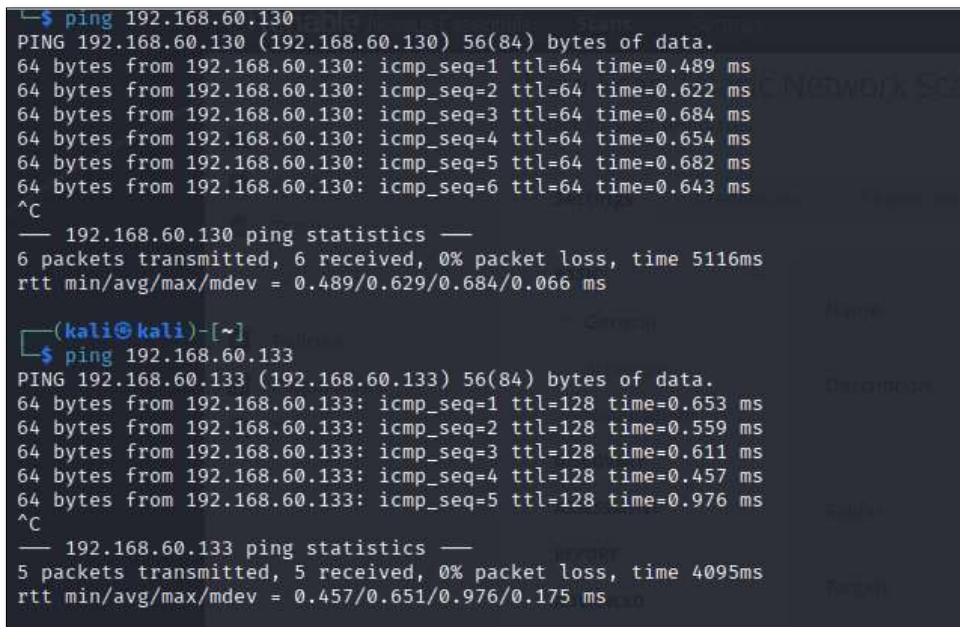
Device	IP Address	Operating System
Kali Linux	192.168.60.132	Kali Linux 2023
Windows 7	192.168.60.133	Windows 7
Metasploitable	192.168.60.130	Metasploitable

3. Connectivity and Ping Test:

As a first step after setting up the lab and to ensure all devices were properly connected within the same network, a ping test was applied between the systems. This step is crucial for verifying network connectivity and ensuring that the Nessus scanner can successfully detect and analyse the systems.

- **Ping Test Results:**

A successful ping test indicates that all machines can communicate with each other, which is essential for conducting network scans and security assessments.



```
$ ping 192.168.60.130
PING 192.168.60.130 (192.168.60.130) 56(84) bytes of data.
64 bytes from 192.168.60.130: icmp_seq=1 ttl=64 time=0.489 ms
64 bytes from 192.168.60.130: icmp_seq=2 ttl=64 time=0.622 ms
64 bytes from 192.168.60.130: icmp_seq=3 ttl=64 time=0.684 ms
64 bytes from 192.168.60.130: icmp_seq=4 ttl=64 time=0.654 ms
64 bytes from 192.168.60.130: icmp_seq=5 ttl=64 time=0.682 ms
64 bytes from 192.168.60.130: icmp_seq=6 ttl=64 time=0.643 ms
^C
--- 192.168.60.130 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5116ms
rtt min/avg/max/mdev = 0.489/0.629/0.684/0.066 ms

(kali@kali)-[~]
$ ping 192.168.60.133
PING 192.168.60.133 (192.168.60.133) 56(84) bytes of data.
64 bytes from 192.168.60.133: icmp_seq=1 ttl=128 time=0.653 ms
64 bytes from 192.168.60.133: icmp_seq=2 ttl=128 time=0.559 ms
64 bytes from 192.168.60.133: icmp_seq=3 ttl=128 time=0.611 ms
64 bytes from 192.168.60.133: icmp_seq=4 ttl=128 time=0.457 ms
64 bytes from 192.168.60.133: icmp_seq=5 ttl=128 time=0.976 ms
^C
--- 192.168.60.133 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4095ms
rtt min/avg/max/mdev = 0.457/0.651/0.976/0.175 ms
```

4. Firewall Check on Windows 7

Before initiating the scan need to check the firewall on **Windows 7** and make sure its disabled. Firewalls can block or restrict the communication necessary for the scanner to perform its tasks, and disabling it ensures that Nessus can freely assess the machine's vulnerabilities.

- **Firewall Status:**

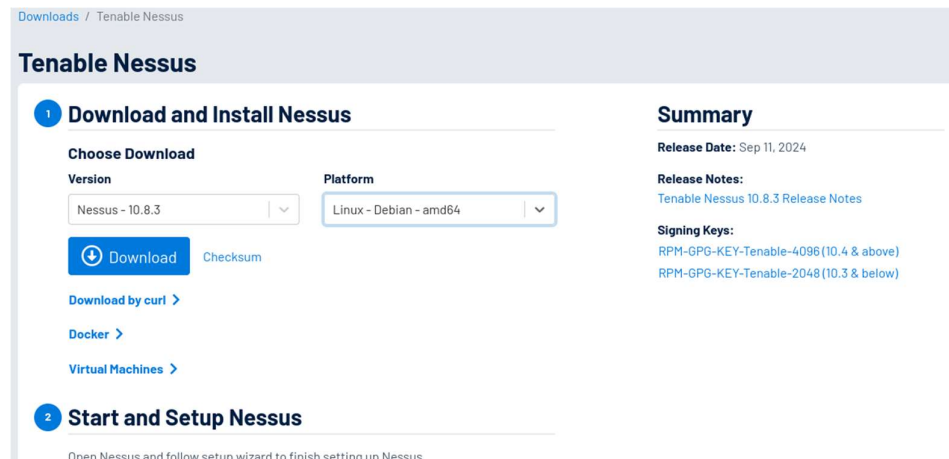
To confirm the firewall was disabled on Windows 7, the settings was checked and ensured there were no restrictions that would hinder the scanning process.

This setup, with all systems on the same NAT network and proper configurations in place, provided a stable environment for conducting thorough vulnerability assessments. By using **Nessus** efficiently and managing system resources wisely this made it able to run the scans smoothly and obtain valuable results for the security evaluation of each system.

5. Nessus Installation and Service Activation

To begin, the **Nessus** package was downloaded for **Debian 10 (AMD 64)** from the official Tenable website. You can find the download link here:

[Nessus Download](#).



Downloads / Tenable Nessus

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version:

Platform:

[Download](#) [Checksum](#)

[Download by curl](#)

[Docker](#)

[Virtual Machines](#)

Summary

Release Date: Sep 11, 2024

Release Notes:
[Tenable Nessus 10.8.3 Release Notes](#)

Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

The package downloaded is called **NESSUS-10.8.3-DEBIAN10_AMD64.DEB**. After downloading, the following command was used to install the Nessus package:

```
(kali@kali)-[~/Desktop]
$ sudo dpkg -i Nessus-10.8.3-debian10_amd64.deb

Selecting previously unselected package nessus.
(Reading database ... 392692 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-debian10_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

Once the installation was complete, a URL appeared in the terminal. This URL can be clicked to open the Nessus web interface, where you can manage scans and settings. However, before accessing it, it's crucial to verify that the Nessus service is running. To do this, the following command was used to start the service. Next, the status of the Nessus service was checked to ensure it was running properly:

```
(kali@kali)-[~/Desktop]
$ sudo systemctl start nessusd

(kali@kali)-[~/Desktop]
$ sudo systemctl status nessusd.service

● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-02-08 16:13:02 EST; 1min 11s ago
     Main PID: 9763 (nessus-service)
        Tasks: 17 (limit: 21939)
      Memory: 197.2M
         CPU: 41.186s
       CGroup: /system.slice/nessusd.service
              └─9763 /opt/nessus/sbin/nessus-service -q
                └─9764 nessusd -q

Feb 08 16:13:02 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Feb 08 16:13:03 kali nessus-service[9764]: Cached 0 plugin libs in 0msec
Feb 08 16:13:03 kali nessus-service[9764]: Cached 0 plugin libs in 0msec

(kali@kali)-[~/Desktop]
$
```

At this point, an increase in memory usage was noticed after checking the status twice. This increase in resource consumption is expected since Nessus is a resource-intensive tool, especially when it's running. This increased load can be observed when monitoring the system's memory usage during the process.

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo systemctl status nessusd.service

● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-02-08 17:40:05 EST; 22h ago
     Main PID: 5270 (nessus-service)
        Tasks: 17 (limit: 7616)
      Memory: 3.5G
         CPU: 3h 22min 52.278s
       CGroup: /system.slice/nessusd.service
              └─5270 /opt/nessus/sbin/nessus-service -q
                └─5272 nessusd -q

Feb 08 17:40:05 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Feb 08 18:06:26 kali nessus-service[5272]: Cached 0 plugin libs in 0msec
Feb 08 18:06:26 kali nessus-service[5272]: Cached 304 plugin libs in 60msec
Feb 08 18:06:26 kali nessus-service[5272]: Cached 304 plugin libs in 58msec
lines 1-15/15 (END) ... skipping ...

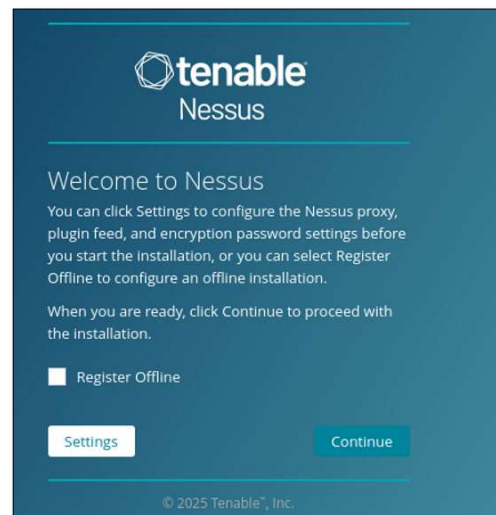
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-02-08 17:40:05 EST; 22h ago
     Main PID: 5270 (nessus-service)
        Tasks: 17 (limit: 7616)
      Memory: 3.5G
         CPU: 3h 22min 52.278s
       CGroup: /system.slice/nessusd.service
              └─5270 /opt/nessus/sbin/nessus-service -q
                └─5272 nessusd -q
```


Once the service was active and running, the page containing the URL from the terminal needed to be refreshed. When accessing the Nessus web interface for the first time, a warning appeared in the browser: "Potential Security Risk Ahead." This warning is expected since the Nessus interface is typically accessed via HTTPS, but a self-signed certificate is used.

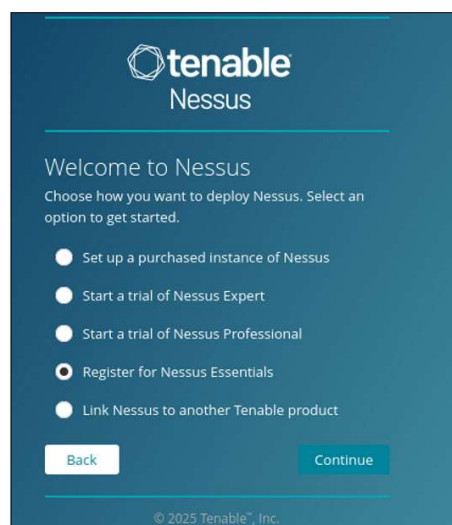
- **Action:** "Advanced", was selected then clicked "Accept the Risk and Continue" to proceed to the Nessus login page.

6. Nessus Setup Process:

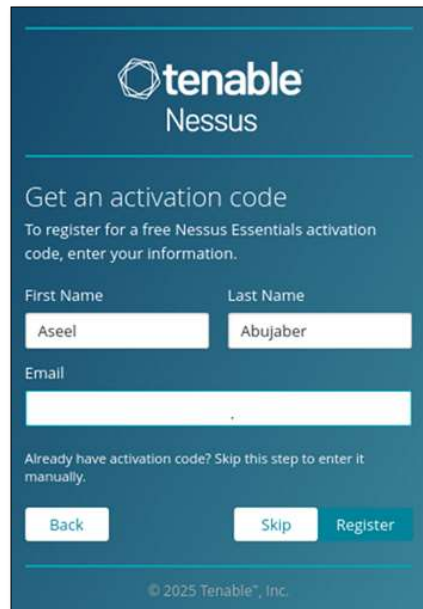
After completing the installation and refreshing the page, you will be directed to the Welcome Screen of Nessus. On this screen, click "Continue" to proceed.



Next, you will be prompted to select the Nessus Essentials option, which is the free version of Nessus. This is a great choice for those who are testing Nessus in a non-commercial environment, as it provides a limited number of scans but is still highly effective for learning and vulnerability assessments.

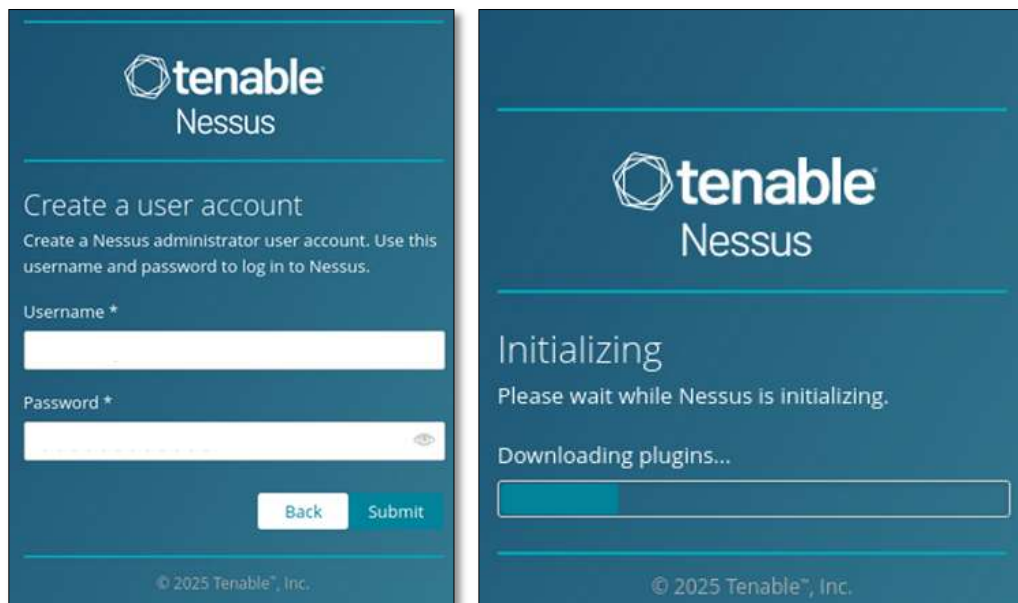


Once you select Nessus Essentials, click **Continue**. You will then be asked to provide your name and email address to receive the activation code. After entering your details, click Continue. The activation code will be sent to your email, and you can enter it to proceed.



The screenshot shows the Nessus registration page. At the top is the Tenable Nessus logo. Below it, the heading "Get an activation code" is followed by the instruction: "To register for a free Nessus Essentials activation code, enter your information." There are two input fields for "First Name" (containing "Aseel") and "Last Name" (containing "Abujaber"). Below these is an "Email" input field. A link "Already have activation code? Skip this step to enter it manually." is present. At the bottom are three buttons: "Back", "Skip", and "Register". The footer shows "© 2025 Tenable®, Inc."

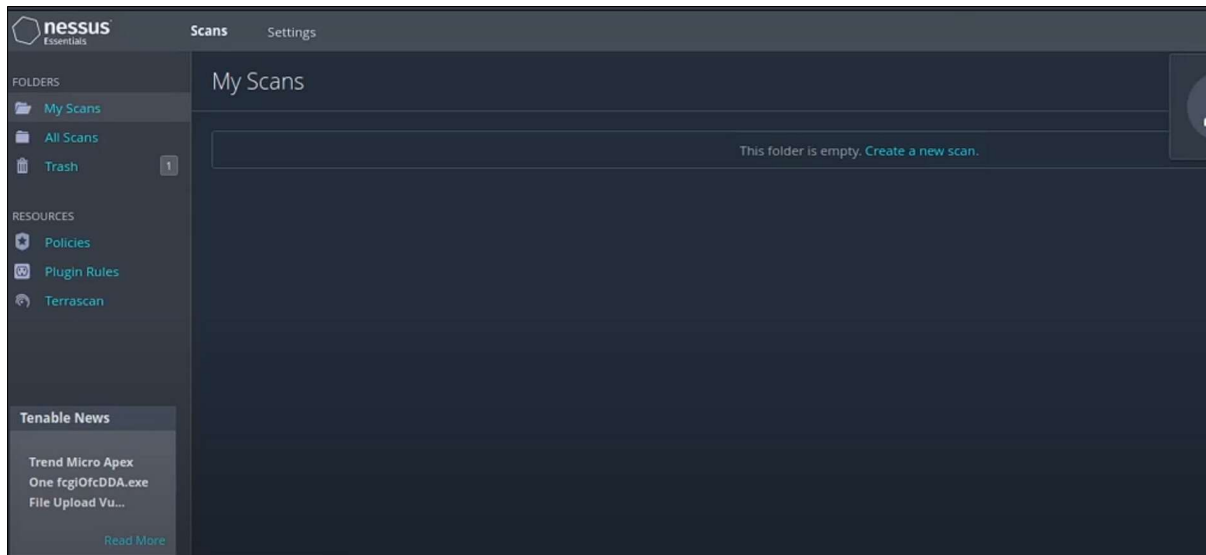
Once you've entered the activation code, Nessus will begin to load, and you'll be prompted to create your account. Set a username and password for your account to secure access to the Nessus interface.



The left screenshot shows the "Create a user account" page. It has the Tenable Nessus logo and the heading "Create a user account". Below it, the instruction says: "Create a Nessus administrator user account. Use this username and password to log in to Nessus." There are two input fields: "Username *" and "Password *". The password field has a toggle icon. At the bottom are "Back" and "Submit" buttons. The footer shows "© 2025 Tenable®, Inc.".

The right screenshot shows the "Initializing" page. It has the Tenable Nessus logo and the heading "Initializing". Below it, the text says: "Please wait while Nessus is initializing." and "Downloading plugins...". There is a progress bar. The footer shows "© 2025 Tenable®, Inc."

After completing the registration and account setup, the Nessus GUI (Graphical User Interface) will appear. From here, you can start configuring and running vulnerability scans.



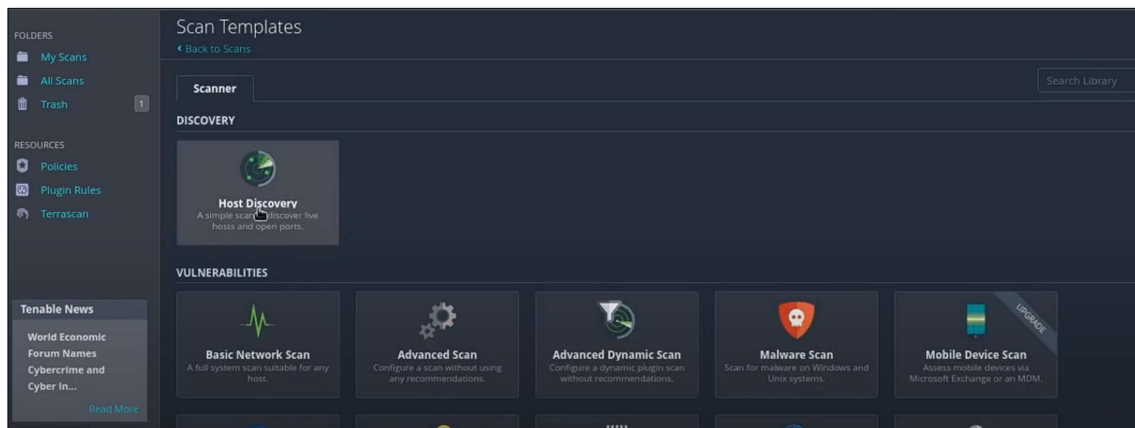
7. Creating a New Scan in Nessus

After successfully setting up Nessus and logging into the web interface, you will be directed to the **Nessus Dashboard**. To begin a new scan, click on the **"Create a New Scan"** button. You will then be taken to the scan creation page where you can configure the scan settings.

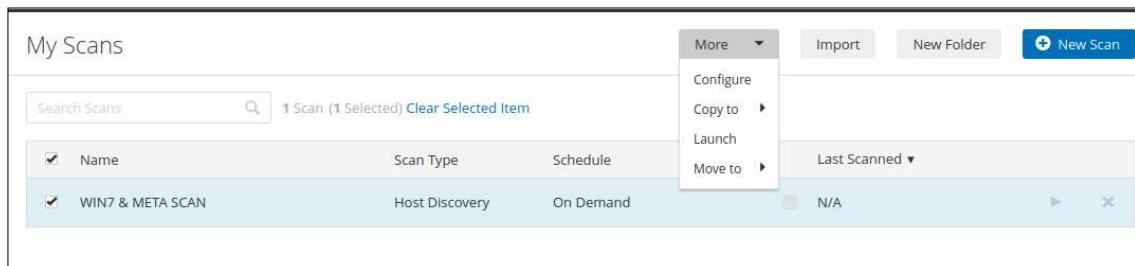
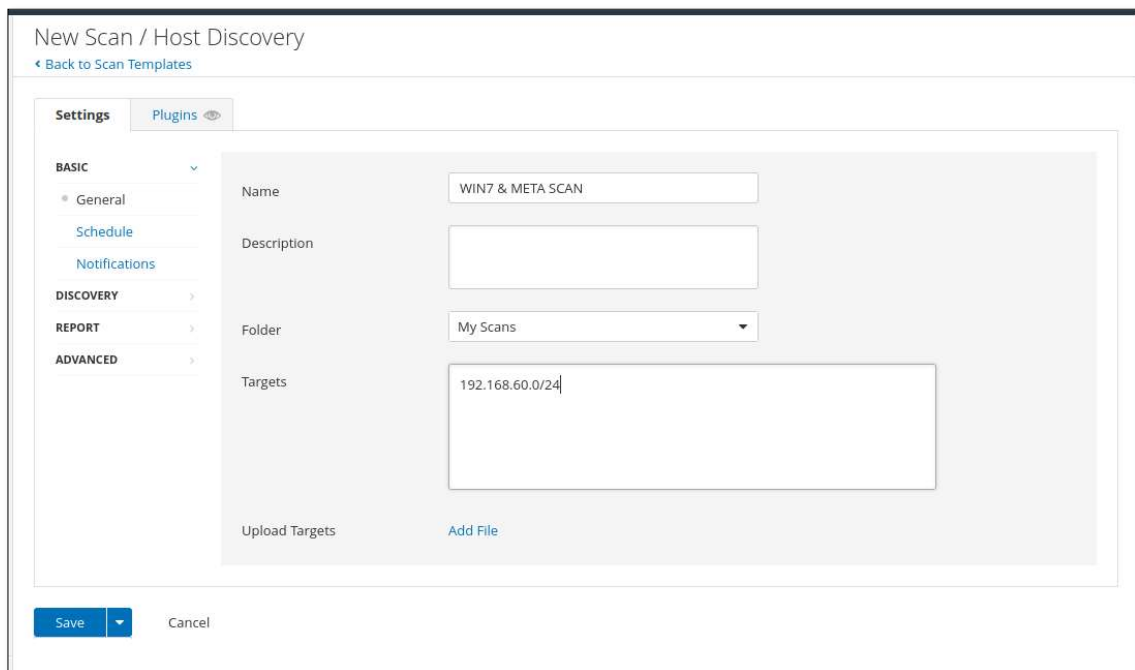
On this page, you will see several predefined scan templates. Nessus offers various templates, each designed for specific use cases. For example, there are templates like **Basic Network Scan**, **Advanced Scan**, and **Web Application Tests**. You can also use **pre-made scan files** that are available, or you can import **your own custom scan file** with specific settings.

"Paid Features: Nessus provides additional premium features that go beyond the basic scanning capabilities offered in the free version. These features include advanced scanning options, such as credentialed scans, more comprehensive vulnerability assessments, and access to a broader range of plugins. To explore these advanced options, you can follow the link provided in the interface to learn more about the premium services and how to upgrade to Nessus Professional."

Penetration Testing using Nessus Tool



Performing a **Host Discovery** scan in Nessus by selecting the scan type, naming it, configuring the IP range (192.168.60.0/24), filling in the necessary details, saving the configuration to initiate the scan, and reviewing the results to identify active hosts within the specified range. After that, click **More** and select **Launch** to start the scan.



After the scan was completed, the date and time of the test were displayed. To view the results, click On Demand to see the detailed outcome of the scan.

My Scans

ImportNew FolderNew Scan

Search Scans1 Scan

<input type="checkbox"/>	Name	Scan Type	Schedule	Last Scanned
<input type="checkbox"/>	WIN7 & META SCAN	Host Discovery	On Demand	✓ Today at 6:26 PM

WIN7 & META SCAN

ConfigureAudit TrailLaunchReportExport

Hosts6Vulnerabilities2History1

FilterSearch Hosts6 Hosts

<input type="checkbox"/>	Host	Ports
<input type="checkbox"/>	192.168.60.254	
<input type="checkbox"/>	192.168.60.133	135, 139, 445, 49152, 49153, 49154, 49155, 49156, 49159
<input type="checkbox"/>	192.168.60.132	
<input type="checkbox"/>	192.168.60.130	111, 139, 445, 2049, 36960, 44803, 47042, 47926, 52643, 55912
<input type="checkbox"/>	192.168.60.2	
<input type="checkbox"/>	192.168.60.1	

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:24 PM
End: Today at 6:26 PM
Elapsed: 2 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

8. Security Assessment Report

Objective:

This report highlights the open ports discovered on systems with IP addresses **192.168.6.133** (Windows 7) and **192.168.60.130** (Metasploitable) during a Nessus Essentials scan, along with associated vulnerabilities and recommendations for mitigating risks.

System Details:

Windows 7 (IP: 192.168.6.133)

- **Operating System:** Windows 7
- **Open Ports:** 135, 139, 445, 49152-49159

Metasploitable (IP: 192.168.60.130)

- **Operating System:** Metasploitable
- **Open Ports:** 111, 139, 445, 2049, 36960, 44803, 47926, 52643, 55912

Open Ports and Associated CVEs:

1. Windows 7 (IP: 192.168.6.133)

Port	Service	CVE
135	Microsoft RPC	CVE-2008-4250, CVE-2017-0213
139	NetBIOS Session	CVE-2019-0708 (BlueKeep), CVE-2015-0004
445	Microsoft SMB	CVE-2017-0144 (EternalBlue), CVE-2017-0145, CVE-2020-0796
49152-49159	Dynamic Ports	CVE-2019-0708 (BlueKeep)

2. Metasploitable (IP: 192.168.60.130)

Port	Service	CVE
111	RPCbind	CVE-2014-9176
139	NetBIOS Session	CVE-2019-0708 (BlueKeep)
445	Microsoft SMB	CVE-2017-0144 (EternalBlue), CVE-2017-0145
2049	NFS	CVE-2018-5741
36960, 44803, 47926, 52643, 55912	Ephemeral Ports	CVE-2018-15665

Risk Analysis:

Windows 7 (IP: 192.168.6.133):

The scan revealed critical vulnerabilities on **ports 135, 139, 445**, including **EternalBlue** and **BlueKeep**, which can lead to remote code execution and unauthorized access. **Dynamic Ports (49152-49159)** also present a potential risk if unpatched services are active.

Metasploitable (IP: 192.168.60.130):

Several vulnerable services were found, including **RPCbind** (port 111), **NetBIOS** (port 139), and **SMB** (port 445). These ports are commonly exploited for remote code execution.

Recommendations:

For Windows 7 (IP: 192.168.6.133):

- Disable **SMBv1** and use **SMBv2** or **SMBv3**.
- Regularly apply **Windows security updates**.
- Restrict access to **dynamic ports** (49152-49159).

For Metasploitable (IP: 192.168.60.130):

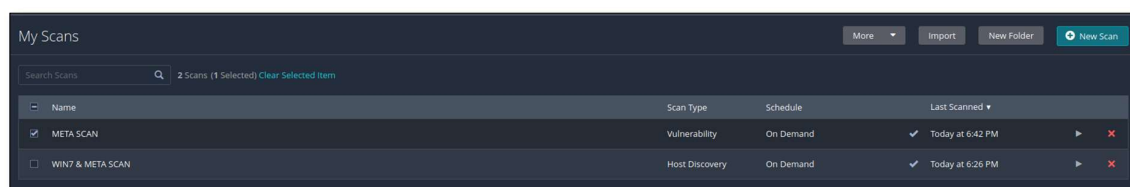
- Disable unnecessary services like **NFS**, **RPC**, and **SMB**.
- Apply patches for **CVE-2014-9176** (RPCbind) and **CVE-2018-5741** (NFS).
- Use **firewalls** to block high-risk ports, particularly **445** and **111**.

Conclusion:

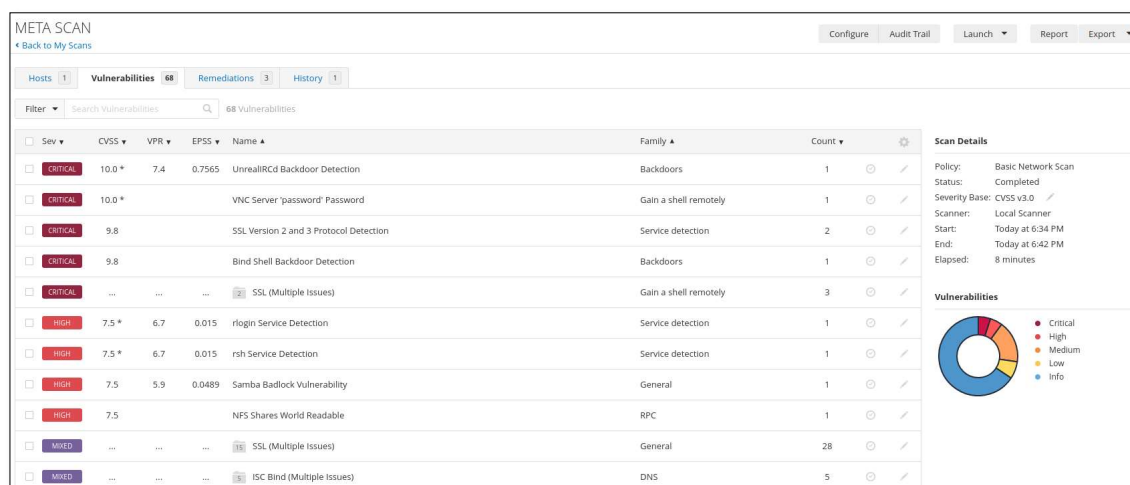
The open ports on both **Windows 7** and **Metasploitable** expose systems to significant security risks. Immediate action is needed to patch vulnerabilities, disable unneeded services, and implement security controls to reduce the attack surface and enhance security.

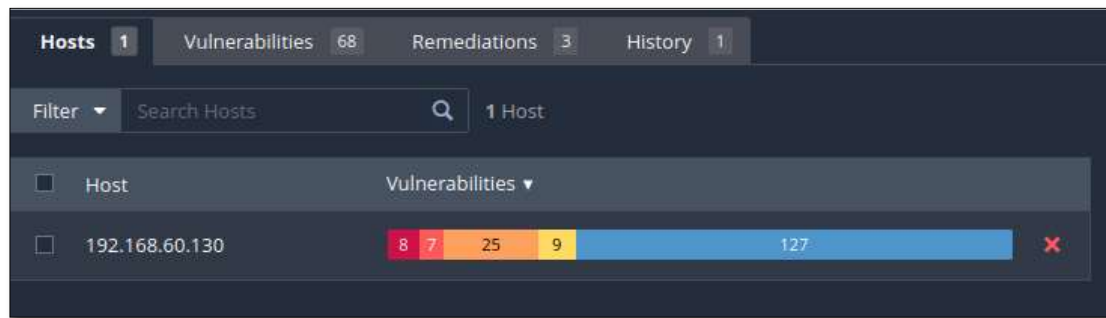
9. Vulnerability Scan:

Using the free **Vulnerability Scan** tool for scanning the **Metasploitable** system through the **Basic Network Scan**, following the same steps explained earlier in the previous pages. This process involved selecting the appropriate scan type, configuring the scan settings, inputting the target IP address for **Metasploitable**, and launching the scan to identify open ports, services, and potential vulnerabilities. The results of the scan were then reviewed to assess the system's security posture and identify any necessary mitigation actions.



After the **Vulnerability Scan** finishes, CLICK ON DEMAND you will see a circle representing the risk levels of the detected vulnerabilities. The circle includes categories such as **Critical**, **High**, **Medium**, **Low**, **Info**, and **Mixed**. The **Mixed** category shows a combination of **Low**, **High**, and **Medium** risk vulnerabilities, indicating that different types of issues have been identified. The **Critical** and **High** risks require immediate attention, as they represent the most severe vulnerabilities that could lead to exploitation. **Medium** and **Low** risks should also be considered, as they can contribute to the overall security exposure if left unaddressed.





The following sections summarize the identified vulnerabilities, their descriptions, CVE identifiers, risk levels, and recommended actions for mitigation.

10. Summary of Critical Vulnerabilities

Vulnerability	Description	CVE	Risk Level	Recommendation
UnrealIRCd Backdoor	A backdoor in UnrealIRCd allows remote code execution.	CVE-2010-2075	Critical	Disable or update to a patched version.
VNC Server Password	VNC server has weak/no password protection.	CVE-2005-0143	Critical	Set strong passwords or use alternatives like SSH.
SSL Version 2 and 3 Protocols	Weak SSL protocols vulnerable to attacks (POODLE, BEAST).	CVE-2014-3566 (POODLE), CVE-2011-3389 (BEAST)	Critical	Disable SSLv2/SSLv3, enforce TLS 1.2+ .
Bind Shell Backdoor	A bind shell backdoor allows remote control of the system.	CVE-2009-3547	Critical	Remove or disable backdoors immediately.
SSL (Multiple Issues)	Weak ciphers and outdated SSL configurations.	Multiple CVEs	Critical	Review and update SSL configurations.

11. Summary of High Vulnerabilities

Vulnerability	Description	CVE	Risk Level	Recommendation
RLogin Service	The RLogin service is exposed and insecure.	CVE-2016-0782	High	Disable RLogin , use SSH instead.
RSH Service	The RSH service transmits data unencrypted.	CVE-2000-0527	High	Disable RSH , use SSH instead.
Samba Badlock Vulnerability	Vulnerability in Samba allows remote code execution.	CVE-2016-2118	High	Patch Samba and disable SMBv1 .
NFS Shares World Readable	NFS shares are world-readable, exposing sensitive data.	CVE-2014-9176	High	Restrict NFS shares to trusted clients.

12. Summary of Medium Vulnerabilities

Vulnerability	Description	CVE	Risk Level	Recommendation
Mixed SSL (Multiple Issues)	Weak SSL/TLS configurations with insecure ciphers.	Multiple CVEs	Medium	Update SSL/TLS configurations, disable weak ciphers.
ISC BIND (Multiple Issues)	Vulnerabilities in BIND DNS server could allow code execution or denial of service.	CVE-2017-3144 , CVE-2016-1276	Medium	Update BIND to the latest version.

13. Conclusion

The system exhibits vulnerabilities with varying levels of severity:

1. Critical Vulnerabilities:

- Vulnerabilities such as the UnrealIRCd backdoor and SSL issues expose the system to severe risks, including the potential for remote code execution and unauthorized access. These must be addressed immediately to prevent exploitation.

2. High Vulnerabilities:

- Services like RLogin and RSH are vulnerable due to the lack of encryption and reliance on weak authentication mechanisms. These pose significant risks and should be mitigated to safeguard the system from unauthorized access.

3. Medium Vulnerabilities:

- Issues in SSL and BIND should still be addressed, as they have the potential to cause service disruptions or security breaches, though their immediate risk is lower compared to critical and high vulnerabilities.

14. Actionable Recommendations

1. Immediate Actions:

- Patch or disable unnecessary services such as RLogin, RSH, and VNC to minimize the attack surface and prevent unauthorized access.

2. Enhance SSL/TLS Security:

- Disable outdated protocols such as SSLv2 and SSLv3, and update cipher suites to use more secure alternatives. Ensure TLS 1.2 or higher is enforced for all encrypted communications.

3. Regular Audits and Updates:

- Perform regular audits and updates on critical services like NFS, Samba, and BIND to ensure they are securely configured and up to date, reducing the risk of vulnerabilities being exploited.

Note: “A detailed report, including the proposed solutions and the severity levels, can be obtained by clicking on REPORT, then selecting the FORMAT and report type. Afterward, click GENERATE REPORT. In this exercise the PDF format was selected with the VULNERABILITIES BY PLUGIN option”

