U.S. DEPARTMENT OF ENERGY'S CYBERFORCE® PROGRAM

CyberForce® 101

Nessus

October 2023

cyberforcecompetition@anl.gov

Nessus 101

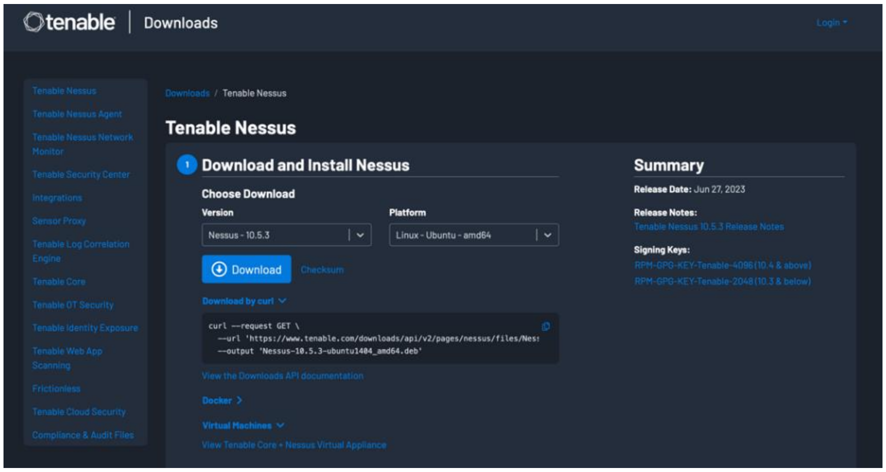
Introduction

Nessus is an open-source network vulnerability scanner developed by Tenable, Inc. It identifies and assesses security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. With its extensive database of known vulnerabilities and regular updates, Nessus enables users to proactively identify and mitigate potential risks before malicious actors can exploit them. Scanning for vulnerabilities is vital to network security for organizations that want to protect their data and assets.

Installation

This guide will demonstrate how to start with Nessus on a Linux machine. Please note that some steps may vary depending on your operating system. Before you begin, you'll need an activation code, which you can get by visiting Tenable.com and registering for free. Once you get an activation code, you can move on to the next step.

First, download the Nessus package file from the Tenable download page, shown in Figure 1 below. Make sure to select the correct package for your OS.



Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.5.3

Platform: Linux - Ubuntu - amd64

```
curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nes:
  --output 'Nessus-10.5.3-ubuntu1404_amd64.deb'
```

Summary

Release Date: Jun 27, 2023

Release Notes: Tenable Nessus 10.5.3 Release Notes

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

Figure 1. *Tenable Nessus download page*

Alternatively, you can run the following command to download the package for users following along on Ubuntu.

```
curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.5.3-ubuntu1404_amd64.deb' \
  --output 'Nessus-10.5.3-ubuntu1404_amd64.deb'
```

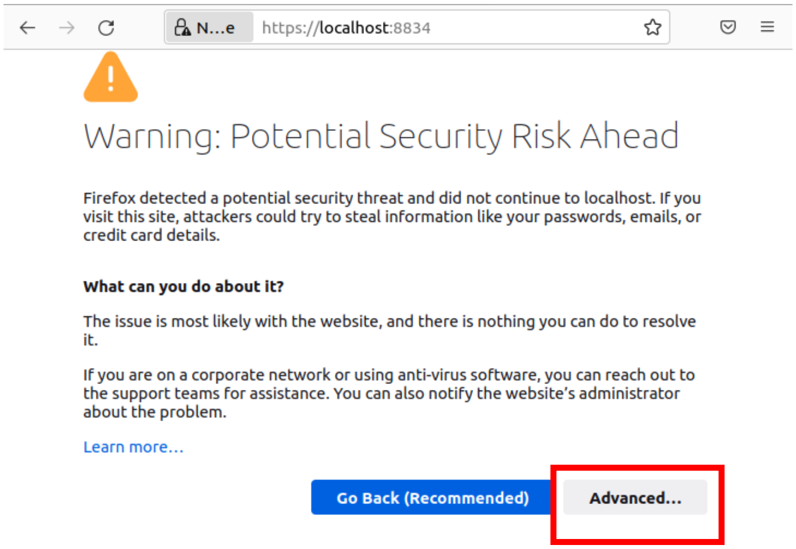
Once the package is downloaded from the command line, navigate to where the package is saved and run the command below. This command will install the program on your machine.

```
# dpkg -i Nessus*.deb
```

When the installation completes, you can start Nessus with the following command:

```
# systemctl start nessusd
```

Next, open any browser and go to https://localhost:8834. This will allow you to access Nessus through the browser. When you first visit this page, you will encounter a security warning, shown in Figure 2. This is normal, and you can proceed by clicking through the warning sign. You will be greeted with a welcome screen like the one in. Click "Next" to continue.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to localhost. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

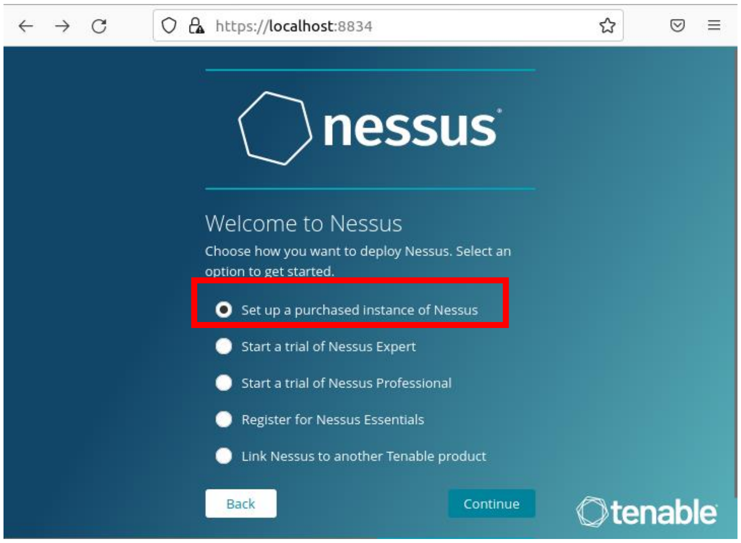
The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Figure 2. Nessus Security Risk Warning.

On the next page, shown in Figure 3, select the 'Set up a purchased instance of Nessus' option and click Continue. You will be asked to register, but you can skip this step. On the next page, enter the activation code you received when you registered. Upon entering your code, you must create an admin account; ensure you save these credentials safely.

You are now finished installing Nessus and can start performing scans.



Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

● Set up a purchased instance of Nessus
○ Start a trial of Nessus Expert
○ Start a trial of Nessus Professional
○ Register for Nessus Essentials
○ Link Nessus to another Tenable product

Figure 3. Nessus Welcome Page.

Your First Scan

To create your first scan, click' Scans' on the navigation bar, then click the blue 'New Scan' button in the upper right corner. This page will show you a list of different scan templates you can choose from, See Figure 4. These templates make scanning much faster and easier by already having pre-configured settings. You can also create your own templates or modify the existing ones to suit your needs.

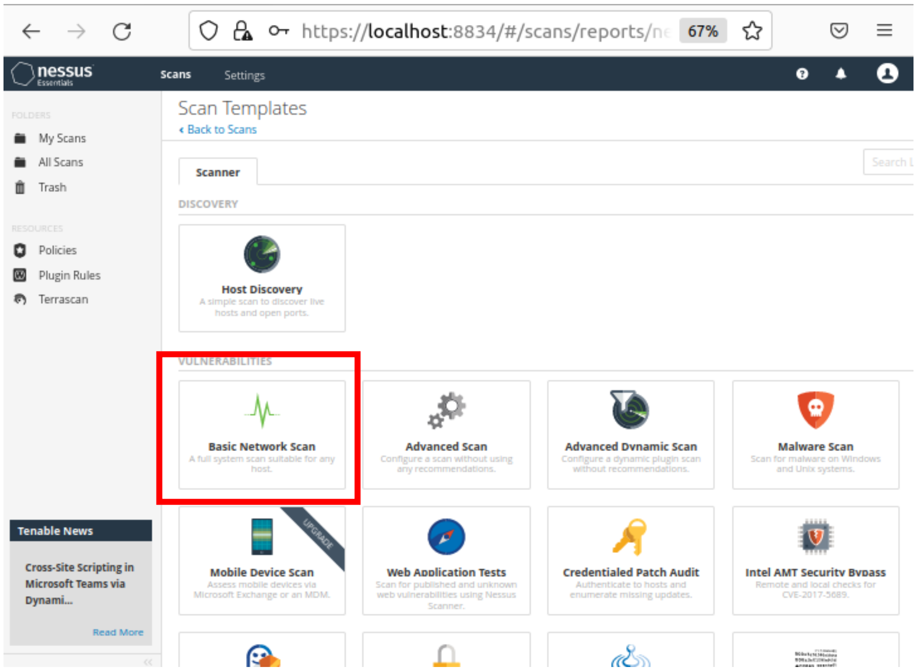
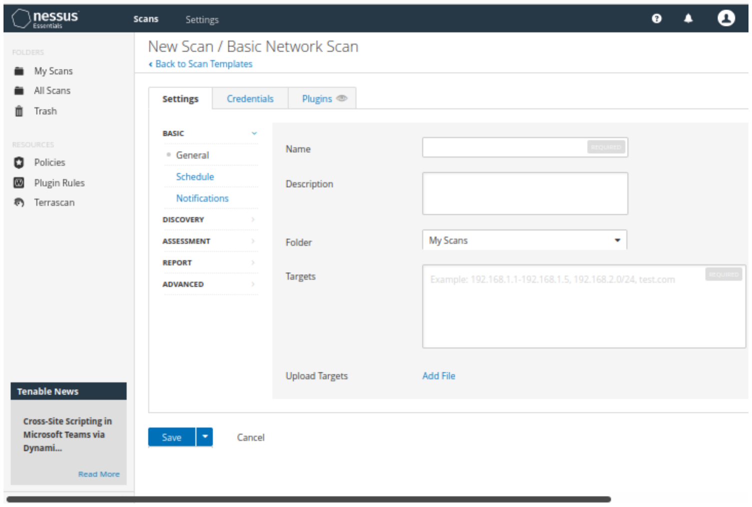

https://localhost:8834/#/scans/reports/ne
67%
nessus Essentials
Scans
Settings
Scan Templates
‹ Back to Scans
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Scanner
Search L
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
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.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Tenable News
Cross-Site Scripting in Microsoft Teams via Dynami...
Read More

Figure 4. Nessus Console Home Page

Now, click on the ‘Basic Network Scan’ template and configure the basic setting. You should be on the page shown in Figure 5. For 'Targets,' enter the network CIDR range you wish to scan. You can leave the rest of the settings as default. However, reviewing the settings in the Discovery, Assessment, Report, and Advanced tabs is recommended to ensure they are appropriate for your environment.



Name

Description

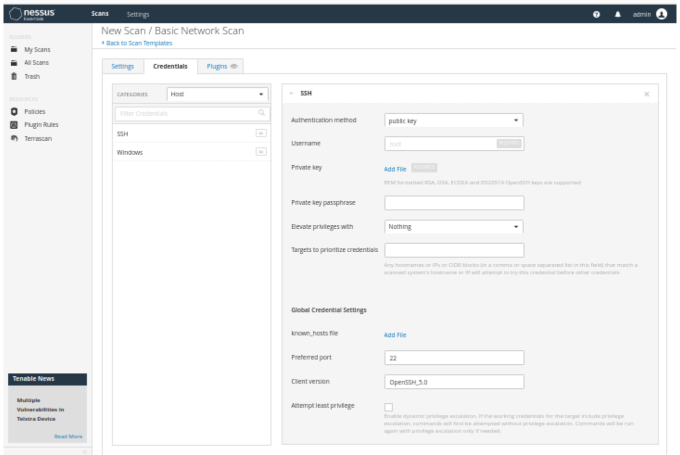
Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Upload Targets: Add File

Figure 5. Nessus New Scan Page.

Next, you have the option to set up Credentials for a scan, see Figure 6. This will allow Nessus to run credentialed scans, which can significantly help in identifying more security flaws in your environment.



Authentication method: public key

Username: root

Private key: Add File

PEM formatted RSA, DSA, ECDSA and ED25519 OpenSSH keys are supported

Private key passphrase

Elevate privileges with: Nothing

Targets to prioritize credentials

Any hostnames or IPs or CIDR blocks (in a comma or space separated list in this field) that match a scanned system's hostname or IP will attempt to try this credential before other credentials

Global Credential Settings

known_hosts file: Add File

Preferred port: 22

Client version: OpenSSH_5.0

Attempt least privilege: □

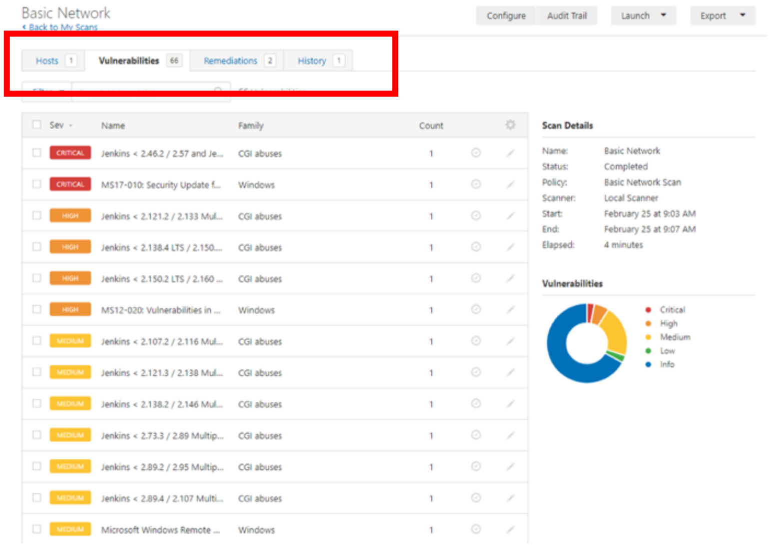
Enable dynamic privilege escalation. If the working credentials for the target include privilege escalation, commands will first be attempted without privilege escalation. Commands will be run again with privilege escalation only if needed.

Figure 6. New Scan Credentials Settings.

Once you finish configuring your settings, you can save your scan and run it later or click on the ▾ button and click 'Launch' to start the scan.

Results

To view the results of your scan, navigate back to the scans page. Here you will see the scan that you just performed. Click on the name of your scan to view the results. Your page should now look like Figure 7.



Sev	Name	Family	Count
CRITICAL	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1
CRITICAL	MS17-010: Security Update f...	Windows	1
HIGH	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1
HIGH	Jenkins < 2.138.4 LTS / 2.150....	CGI abuses	1
HIGH	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1
HIGH	MS12-020: Vulnerabilities in ...	Windows	1
MEDIUM	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1
MEDIUM	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1
MEDIUM	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1
MEDIUM	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1
MEDIUM	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1
MEDIUM	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1
MEDIUM	Microsoft Windows Remote ...	Windows	1

Scan Details

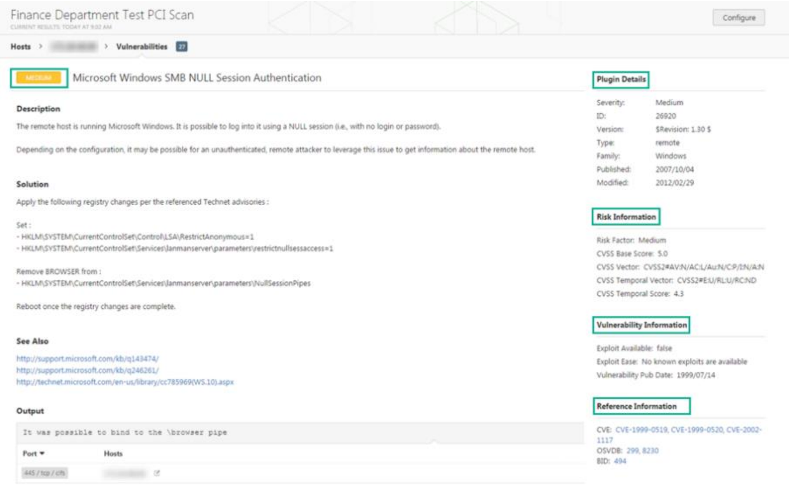
Name:	Basic Network
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Start:	February 25 at 9:03 AM
End:	February 25 at 9:07 AM
Elapsed:	4 minutes

Vulnerabilities

Figure 7. Nessus Scan Results.

The results page will display four different tabs at the top. The 'Hosts' tab shows all the targets identified and scanned, along with information about the vulnerabilities on each host.

The Vulnerabilities tab will show you all the vulnerabilities that the scan identified. These will be organized and sorted by its severity. Clicking into a specific vulnerability will give you more detailed information including what host has this flaw. See Figure 8 for an example.



Finance Department Test PCI Scan

CURRENT RESULTS: TODAY AT 9:02 AM

Hosts > [redacted] > Vulnerabilities 27

MEDIUM Microsoft Windows SMB NULL Session Authentication

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution

Apply the following registry changes per the referenced Technet advisories :

Set :
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

See Also

http://support.microsoft.com/kb/q143474/
http://support.microsoft.com/kb/q246261/
http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx

Output

```
It was possible to bind to the \browser pipe
```

Port ▾	Hosts
445 / tcp / cifs	[redacted]

Plugin Details

Severity:	Medium
ID:	26920
Version:	$Revision: 1.30 $
Type:	remote
Family:	Windows
Published:	2007/10/04
Modified:	2012/02/29

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:ND
CVSS Temporal Score: 4.3

Vulnerability Information

Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 1999/07/14

Reference Information

CVE: CVE-1999-0519, CVE-1999-0520, CVE-2002-1117
OSVDB: 299, 8230
BID: 494

Figure 8. *Nessus Scan Details.*

The next tab is for Remediations. If the scan produces remediations, they will be listed here. This list shows suggested remediations that address the highest number of vulnerabilities.

Lastly, the History tab will show you a list of scans with the start/stop time and the scan statuses.

Sources

- https://docs.tenable.com/nessus/Content/GetStarted.htm
- https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus
- https://www.hackingarticles.in/beginners-guide-to-nessus/
- https://www.youtube.com/watch?v=lT6Px9zJM3s&t=170s
- https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scaning-security-data-windows-unix-linux/
- https://www.techtarget.com/searchnetworking/definition/Nessus