Experiment 14

Aim: Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities

Roll No.	37
Name	Mikil Lalwani
Class	D15-B
Subject	Security Lab
LO Mapped	LO4: Use tools like sniffers, port scanners, and other related tools for analyzing packets in a network.

Aim:

Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities

Theory:

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Suppose you are an administrator in charge of any computer (or group of computers) connected to the internet. In that case, Nessus is a great tool to help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

Features of Nessus:

1. Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.

2. Nessus is very extensible, providing a scripting language to write tests specific to your system once you become more familiar with the tool. It also provides a plug-in interface; many free plugins are available from the Nessus plug-in site. These plugs are often specific to detecting a common virus or vulnerability.

3. Up-to-date information about new vulnerabilities and attacks. The Nessus team updates the list of what vulnerabilities to check for on a daily basis in order to minimize the window between an exploit appearing in the wild, and you being able to detect it with Nessus.

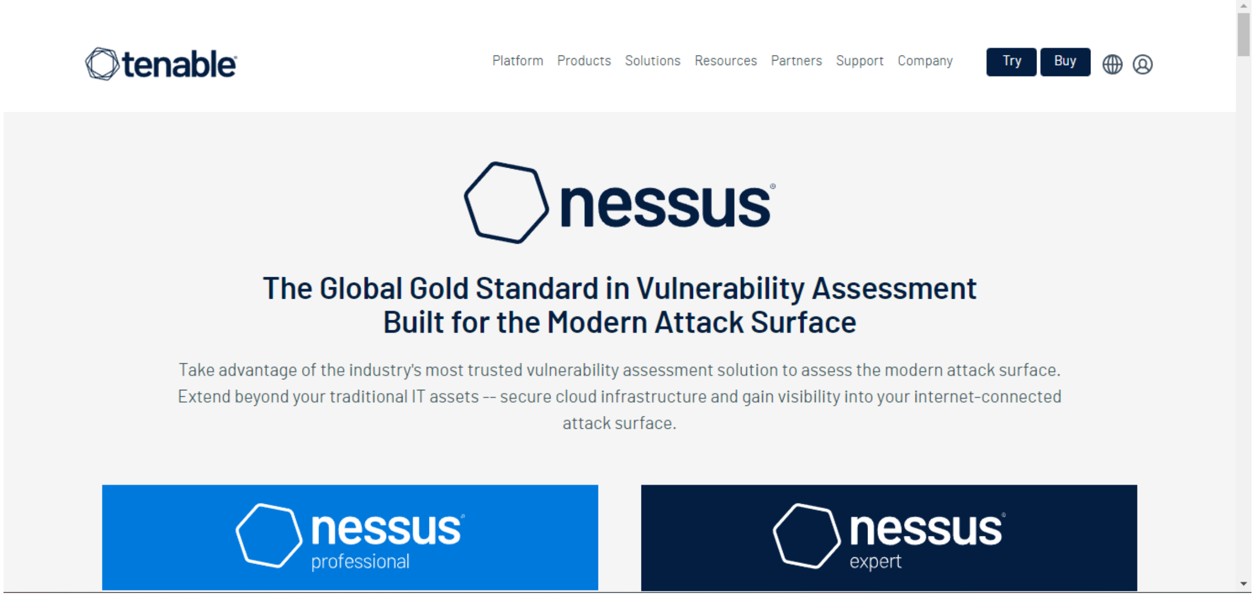
4. Open-source. Nessus is open source, meaning it costs nothing, and you are free to see and modify the source as you wish.

5. Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way you can mitigate the vulnerability.

Output:

STEP 1:

Download and Install Nessus In order to download Nessus, you’ll first need to sign up for an online account so you can download the software and get an activation code.

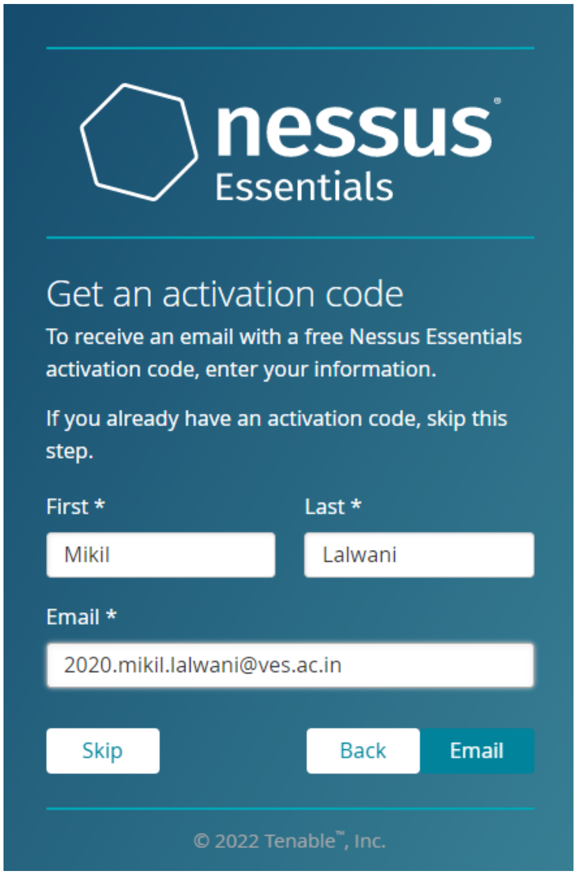


The Global Gold Standard in Vulnerability Assessment Built for the Modern Attack Surface

Take advantage of the industry's most trusted vulnerability assessment solution to assess the modern attack surface. Extend beyond your traditional IT assets -- secure cloud infrastructure and gain visibility into your internet-connected attack surface.

STEP 2:

Set Up Your Nessus Account and Activation Code Once Nessus is installed, point your web browser to https://localhost:8834/. This is where we'll complete the signup process and activate your copy of Nessus.



Get an activation code

To receive an email with a free Nessus Essentials activation code, enter your information.

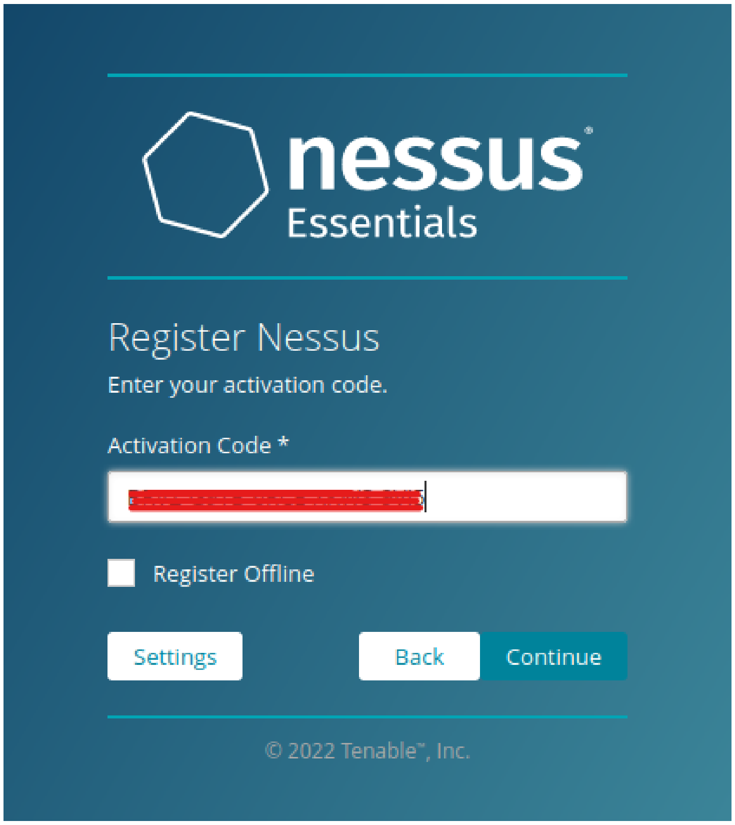
If you already have an activation code, skip this step.

First * Mikil

Last * Lalwani

Email * 2020.mikil.lalwani@ves.ac.in

© 2022 Tenable™, Inc.



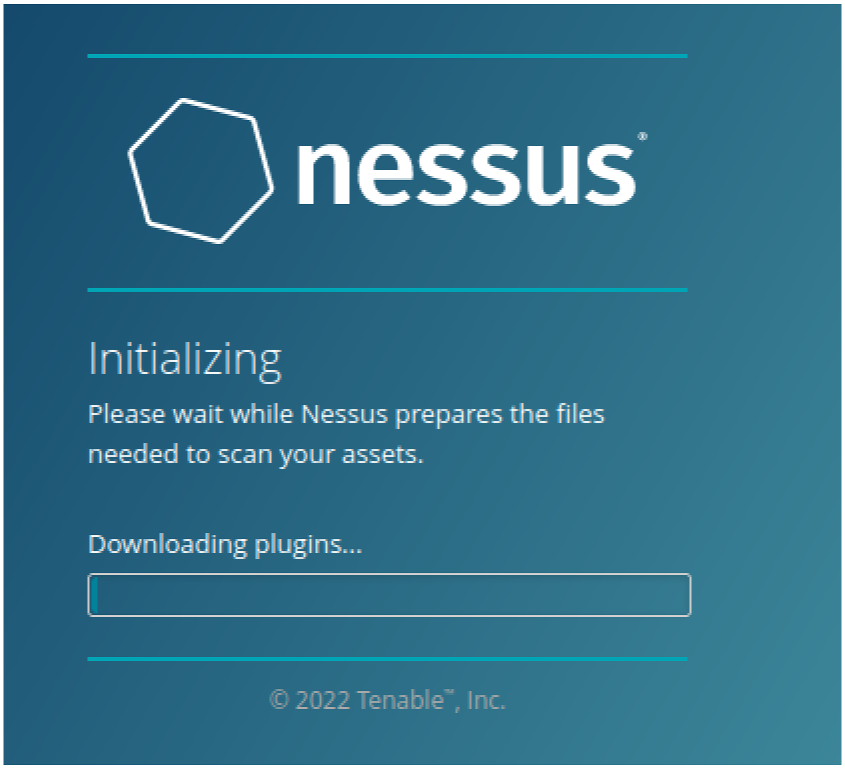
Register Nessus

Enter your activation code.

Activation Code * [redacted]

□ Register Offline

© 2022 Tenable™, Inc.



Initializing

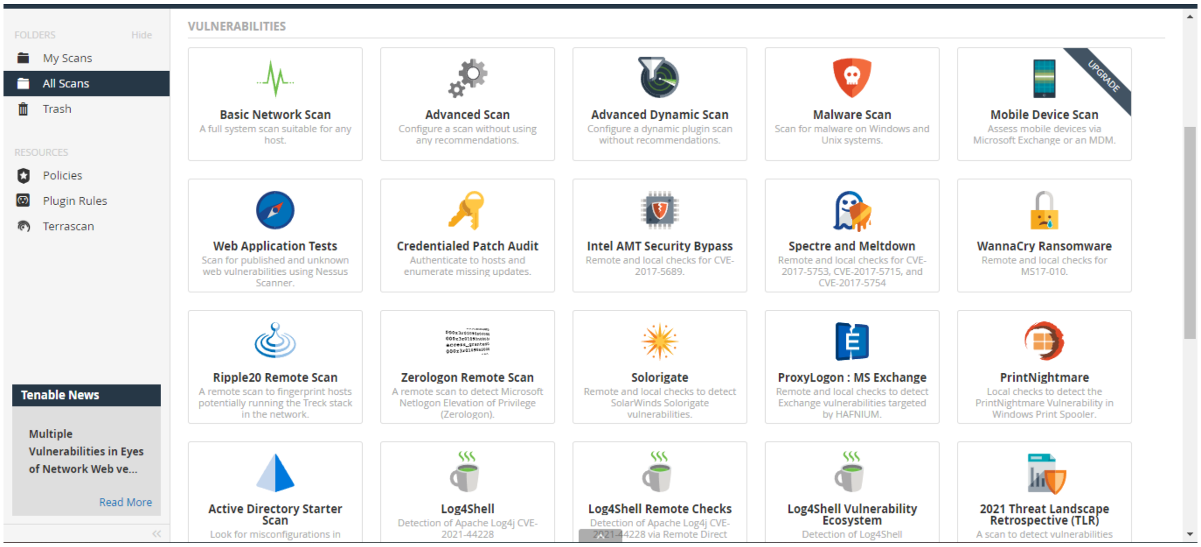
Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

© 2022 Tenable™, Inc.

STEP 3:

Start a Vulnerability Scan It’s time to actually test your network. Nessus can actually scan for quite a few different problems, but most of us will be content using the Basic Network Scan because it offers a good overview.



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.

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.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware Remote and local checks for MS17-010.

Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan Look for misconfigurations in

Log4Shell Detection of Apache Log4j CVE-2021-44228

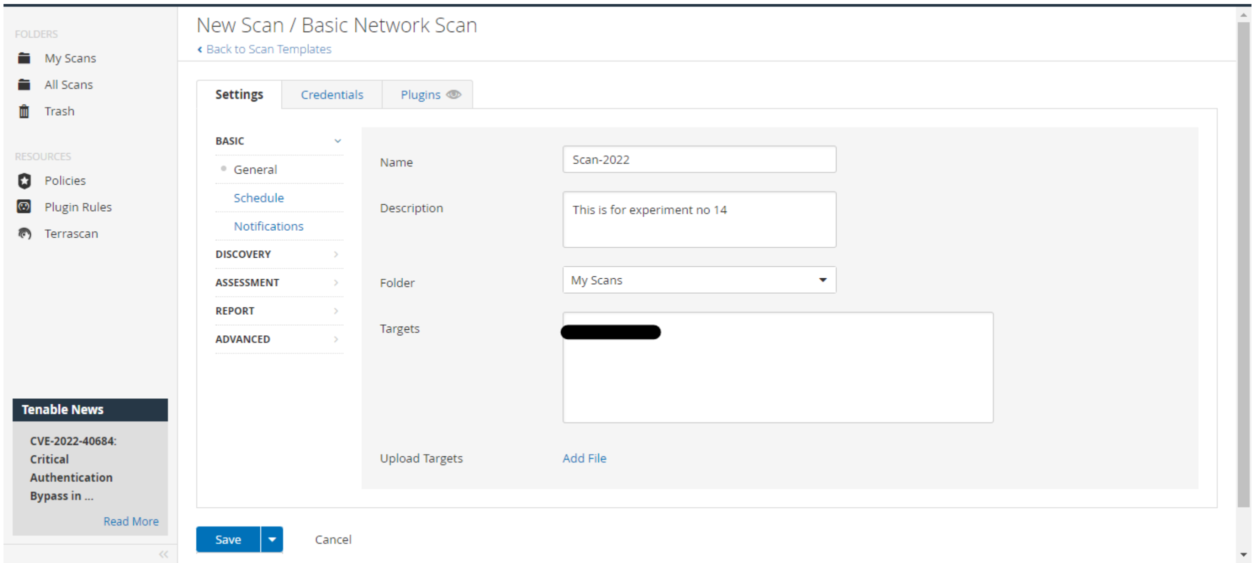
Log4Shell Remote Checks Detection of Apache Log4j CVE-2021-44228 via Remote Direct

Log4Shell Vulnerability Ecosystem Detection of Log4Shell

2021 Threat Landscape Retrospective (TLR) A scan to detect vulnerabilities

Multiple Vulnerabilities in Eyes of Network Web ve...

a. Click the “New Scan.”
b. Click “Basic Network Scan.”
c. Name your scan and add a description.
d. In the “Targets” field, you’ll want to enter IP scanning details about your home network. For example, if your router is at 192.168.0.1, you’d want to enter 192.168.0.1/24. This will make it so Nessus scans all the devices on your network (unless you have a ton of devices this is probably as high as you’d need to go).



New Scan / Basic Network Scan

Name: Scan-2022

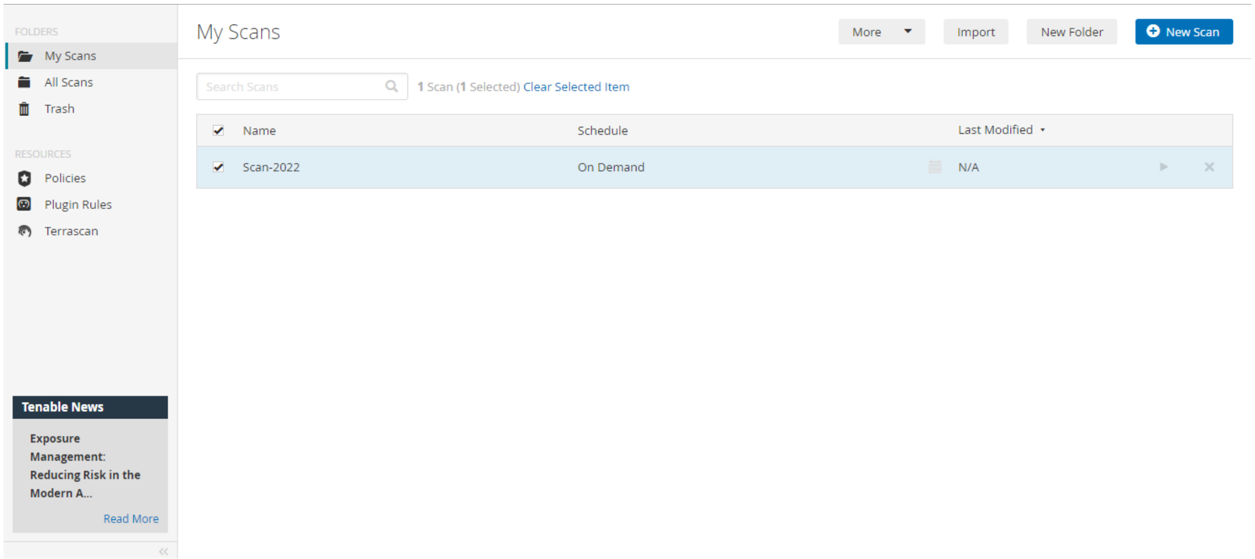
Description: This is for experiment no 14

Folder: My Scans

Targets: [redacted]

Upload Targets: Add File

5. Click “Save.”
6. On the next screen, click the Play icon to launch the scan.



My Scans

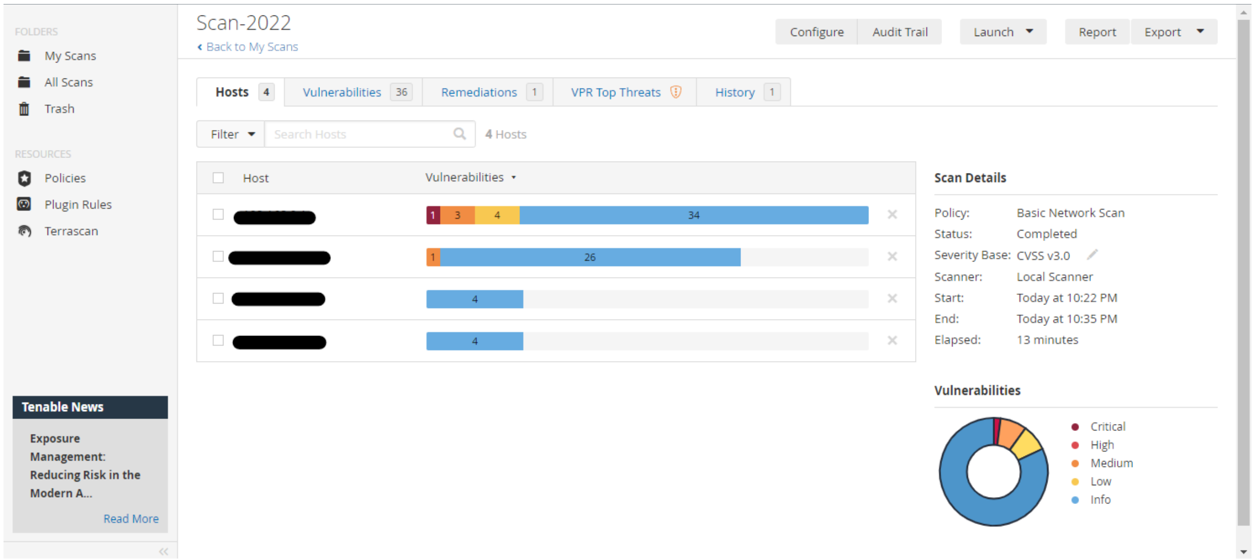
1 Scan (1 Selected) Clear Selected Item

☑	Name	Schedule	Last Modified
☑	Scan-2022	On Demand	N/A

Depending on what and how many devices you have on your network, the scan takes a while.

STEP 4:

Viewing Your Results Once Nessus finishes, you'll see a bunch of color-coded graphs for each device (referred to as hosts) on your network. Each color of the graph signifies the danger of a vulnerability, from low to critical.



Scan-2022

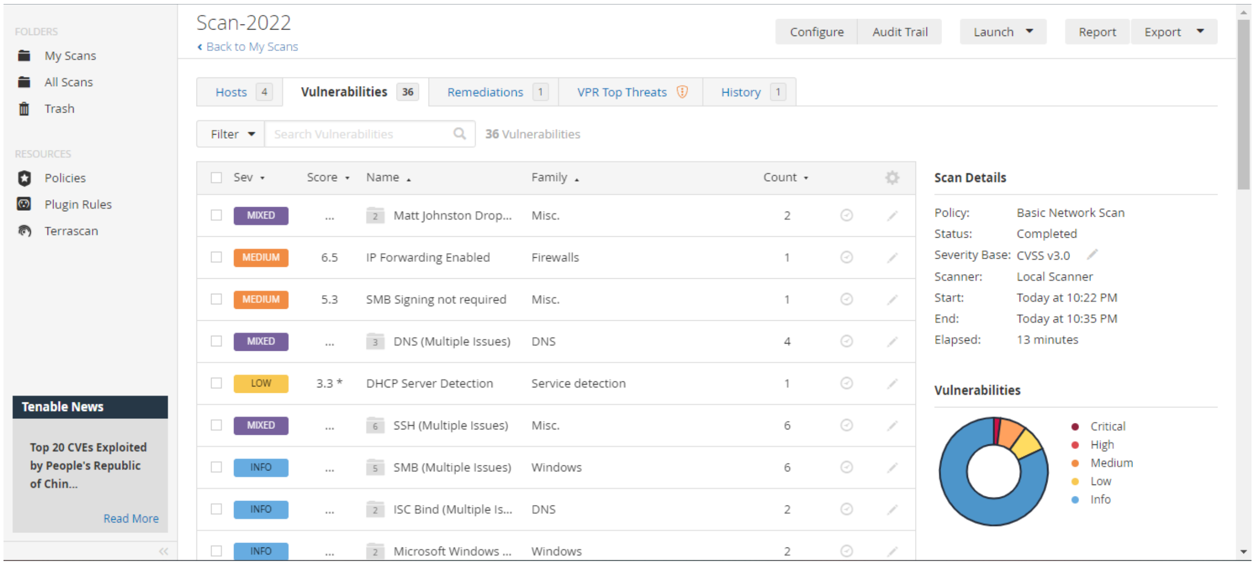
Host	Vulnerabilities
[redacted]	1 3 4 34
[redacted]	1 26
[redacted]	4
[redacted]	4

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:22 PM
End: Today at 10:35 PM
Elapsed: 13 minutes

Vulnerabilities

(My IP address has been blacked out)



Scan-2022

Sev	Score	Name	Family	Count
MIXED	...	2 Matt Johnston Drop...	Misc.	2
MEDIUM	6.5	IP Forwarding Enabled	Firewalls	1
MEDIUM	5.3	SMB Signing not required	Misc.	1
MIXED	...	3 DNS (Multiple Issues)	DNS	4
LOW	3.3 *	DHCP Server Detection	Service detection	1
MIXED	...	6 SSH (Multiple Issues)	Misc.	6
INFO	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	2 ISC Bind (Multiple Is...	DNS	2
INFO	...	2 Microsoft Windows ...	Windows	2

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:22 PM
End: Today at 10:35 PM
Elapsed: 13 minutes

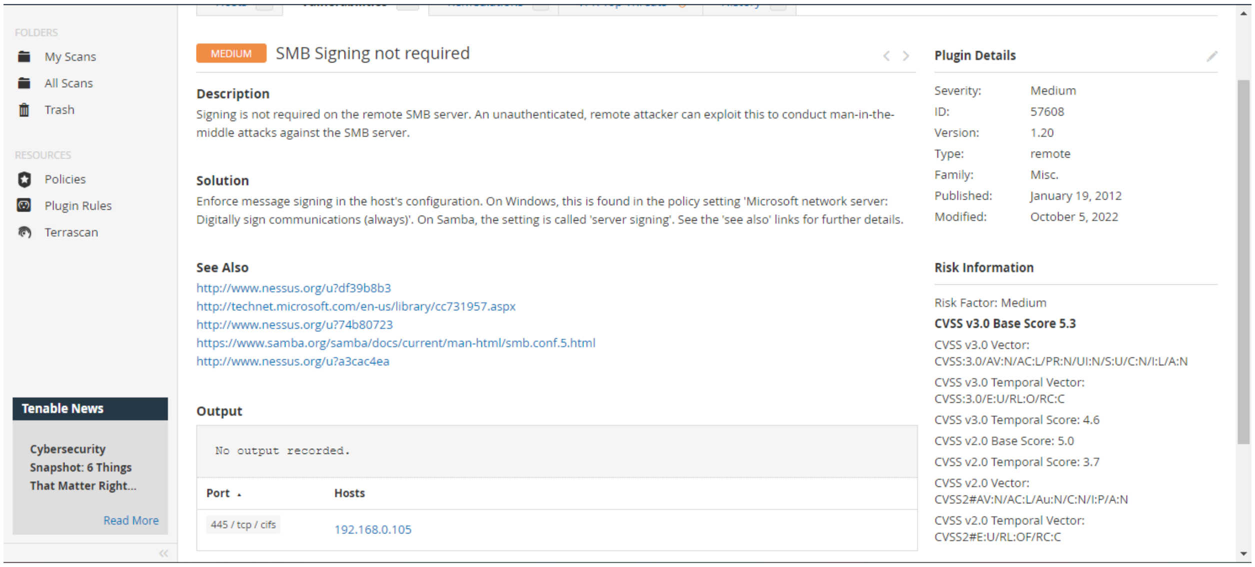
Vulnerabilities

Your results should include all the devices on your local network, from your router to your

Wi-Fi-enabled printer. Click the graph to reveal more information about the vulnerabilities on each device. Vulnerabilities are listed as "plugins," which is just Nessus' way of discovering vulnerabilities. Click on any plugin to get more information about the vulnerability, including white papers, press releases, or patch notes for potential fixes. You can also click the Vulnerabilities tab to see an overview of all the potential vulnerabilities on the network as a whole.

STEP 5:

Reporting Your Results Nessus gives you all this data, but what exactly are you supposed to do with it? That depends on which vulnerabilities Nessus finds. After your scan is complete, you'll find the biggest potential security holes in your network. All of these issues are easily remedied by either updating or deleting old software. While all this might sound a little scary, it's worth noting that while Nessus gives you a lot of the potential ways into a network, it's not a foolproof guide. On top of needing to be in your network in the first place (which of course, isn't terribly complicated), they'd also need to know how to actually use the variety of exploitation tools Nessus suggests.



SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

```
No output recorded.
```

Port	Hosts
445 / tcp / cifs	192.168.0.105

Plugin Details

Severity: Medium
ID: 57608
Version: 1.20
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: October 5, 2022

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Conclusion:

Hence, we understood how to use the NESSUS to scan the network for vulnerabilities.