

Security Lab

Lab Assignment No. 11

Aim: Use the NESSUS to scan the network for vulnerabilities.

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.

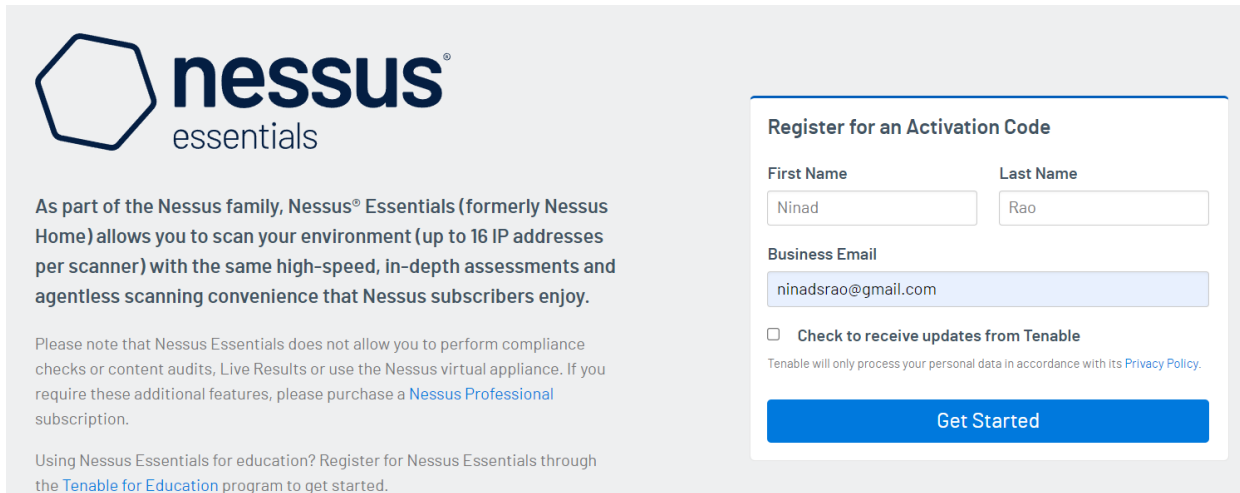
If you are an administrator in charge of any computer (or group of computers) connected to the internet, Nessus is a great tool to help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

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 for you to write tests specific to your system once you become more familiar with the tool. It also provides a plug-in interface, and many free plug-ins 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.

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.



nessus
essentials

As part of the Nessus family, Nessus® Essentials (formerly Nessus Home) allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a [Nessus Professional](#) subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the [Tenable for Education](#) program to get started.

Register for an Activation Code

First Name: Last Name:

Business Email:

☐ Check to receive updates from Tenable

Tenable will only process your personal data in accordance with its [Privacy Policy](#).

Get Started

1. Head to the [Nessus Home](#) landing page, enter a name and email address, and then click the Register button. You'll want to use a real email address here because Nessus sends you an activation code that you'll need in a step later.
2. Click the Download button, then download Nessus for your operating system. It's available for Windows, Mac, and Linux.
3. Once the download is complete, run the installer package and follow the on-screen instructions to finish installation.

Nessus creates a local server on your computer and runs from there, so don't be surprised that the installation process is a little different than you're used to.

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.


















1. When you launch Nessus for the first time, you get a *"Your connection is not secure"* warning from your browser. Click *"Advanced"* and then *"Proceed to localhost"* to bypass this warning.
2. Create an account on the Account Setup screen, leave the Registration as *"Home, Professional, or Manager,"* and then enter the Activation Code from your email. Click *"Continue."*

Next, Nessus will download a number of tools and plugins so it can properly scan your network with updated utilities.

STEP 3: Start a Vulnerability Scan

It's time to actually test your network. This is the fun part. 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.	 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.	 ZeroLoqon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (ZeroLoqon).	 Solorigate Remote and local checks to detect SolarWinds Solorigate vulnerabilities.	 2020 Threat Landscape Retrospective (TLR) A scan to detect vulnerabilities featured in our End of Year report.	 ProxyLoqon : 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 Active Directory.			

1. Click the “New Scan.”
2. Click “Basic Network Scan.”
3. Name your scan and add a description.
4. 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

[← Back to Scan Templates](#)

Settings | [Credentials](#) | [Plugins](#)

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

MyScan

Description

My very first vulnerability scan

Folder

My Scans

Targets

Upload Targets

[Add File](#)

Save

Cancel

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

My Scans

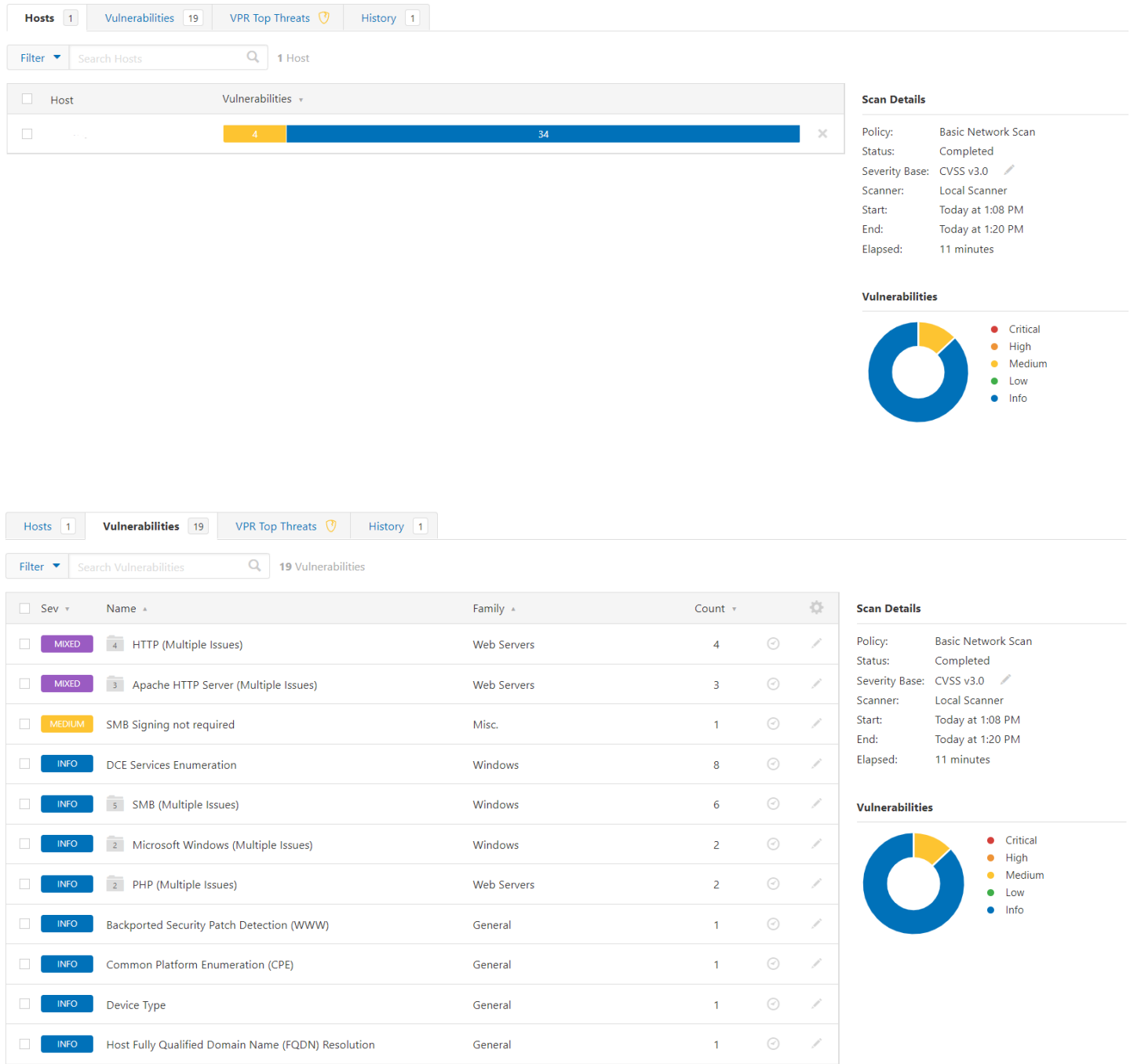
[More](#) | [Import](#) | [New Folder](#) | [New Scan](#) Search Scans 2 Scans (1 Selected) [Clear Selected Item](#)

	Name	Schedule	Last Modified
	MyScan	On Demand	N/A

Depending on what and how many devices you have on your network, the scan takes a while, so sit back and relax while Nessus does its work.

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.



Vulnerabilities 19

MEDIUM 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	

Plugin Details

Severity: Medium
ID: 57608
Version: 1.19
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: March 15, 2021

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:O/RC:C

There's a chance some of these vulnerabilities will be a bit obvious. For example, Nessus picks up on any device still using a default password or points out when a computer or device is running an outdated firmware. Most of the time though, you probably won't understand what the heck you're looking at with these results.

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 the exploitation tools Nessus suggests.

Vulnerabilities 19

MEDIUM Apache mod_info /server-info Information Disclosure

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

See Also


https://www.owasp.org/index.php/SCG_WS_Apache

Output

```
Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://LAPTOP-VFQ11P8O/server-info

Attached is a copy of the response
```

Port	Hosts
80 / tcp	

Plugin Details

Severity: Medium
ID: 10678
Version: 1.29
Type: remote
Family: Web Servers
Published: May 28, 2001
Modified: August 9, 2018

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:L/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

CPE: cpe:/a:apache:http_server
Vulnerability Pub Date: January 1, 1999

Nessus is a great starting point for finding the most obvious vulnerabilities that could make you an easy target, or to just explore your home network. With very limited searching on Google, Nessus will lead you to tons of different hacking tools and a wide variety of software, so dig in and learn as much as you can.

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