lnerability Analysis

Module 05

Vulnerability Scanning

Vulnerability Scanning refers to auditing hosts, ports, and services running in a network to assess the security posture and search for security loopholes.

Lab Scenario

Earlier, all possible information about the target, such as IP address range and network topology were gathered.

Now, as an ethical hacker, or pen-tester, your next step will be to perform port scanning, network scanning, and vulnerability scanning on the IP addresses obtained in the information gathering phase. This will help in identifying IP/host name, ports, services, live hosts, vulnerabilities, and services running on the target network.

Port scanning will help in identifying the open ports and the services running on specific ports, which involves connecting to TCP and UDP system ports. Port scanning is used to find out the vulnerabilities in the services running on a port.

Vulnerability scanning determines the possibility of network security attacks. It evaluates the organization's systems and network for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Vulnerability scanning is a critical component of any penetration testing assignment.

The labs in this module will provide you with real-time experience in network scanning and vulnerability scanning.

Lab Objectives

The objective of this lab is to help students in conducting vulnerability scanning, analyzing the network vulnerabilities, and so on.

You need to perform a network scan to:

- Check live systems and open ports
- Perform banner grabbing and OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts

Lab Environment

In this lab, you need:

- Windows Server 2016 system
- Windows Server 2012 system
- Windows 10 system
- Windows 8 system
- Kali Linux system

- A Web browser with Internet access
- Administrative privileges to run tools and perform scans

Lab Duration

Time: 40 Minutes

Overview of Vulnerability Scanning

Vulnerability scanning is a process of identifying security vulnerabilities of systems in a network to determine if and where a system can be exploited. Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures such as ping sweeps and port scans gather information about which IP addresses map to live hosts that are active on the network, and services running on it.

Lab Tasks

Recommended labs to assist in scanning networks:

- Vulnerability Analysis using **Nessus**
- Scanning for Network Vulnerabilities using the **GFI LanGuard**
- CGI Scanning with **Nikto**

Lab Analysis

Analyze and document the results related to the lab exercise. Give opinion on your target's security posture and exposure using information collected through scanning.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Vulnerability Analysis using Nessus

Nessus allows to remotely audit a network and determine if it has been broken into or misused in some way. It also provides the ability to locally audit a specific machine for vulnerabilities.

Lab Scenario

Different types of scanning on target network reveals open ports and services running on the target network system. Next step should be vulnerability scanning to detect possible vulnerabilities of the system in the target network. So, as a professional ethical hacker or penetration tester, you should be able to perform vulnerability scanning on the target network. This lab will demonstrate how to perform vulnerability scanning on the target network.

Lab Objectives

This lab will give real-time experience while using the Nessus tool to scan for network vulnerabilities.

Lab Environment

To carry out this lab, you need:

- Nessus, located at **Z:\CEH-Tools\CEHv10 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus**. You can also download the latest version of Nessus from the link **http://www.tenable.com/products/nessus/select-your-operating-system**. If you decide to download the latest version, then screenshots shown in the lab might differ
- Windows Server 2016 system
- Windows Server 2012 system
- A web browser with Internet access
- Administrative privileges to run the Nessus tool

Lab Duration

Time: 20 Minutes

Overview of Vulnerability Scanning

Vulnerability scanning is a type of security assessment activity performed by security professionals on their home network. It helps in finding possible network vulnerabilities.

Lab Tasks

1. Launch **Windows Server 2012** virtual machine before beginning this lab.
2. Switch to Windows Server 2016, navigate to **Z:\CEH-Tools\CEHv10 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus**, and double-click **Nessus-7.0.2-x64.msi**.
3. If the **Open File - Security Warning** pop-up appears, click **Run**.
4. **Tenable Nessus Installation Wizard** appears. Follow the installation steps to install Nessus. Accept all installation defaults.

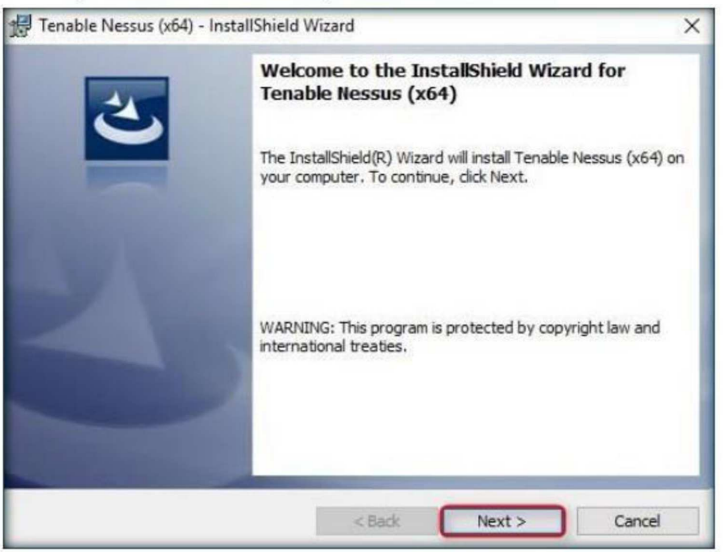

FIGURE 1.1: The Nessus Install Shield Wizard

5. During installation, if a **Windows Security** pop-up appears, click **Install** or skip to the next step.
6. During installation, if a **winPcap** pop-up appears, cancel the installation and skip to the next step.
7. After installation, Nessus opens in the default browser.

8. The **Nessus** window appears. Click **Connect via SSL** button to proceed.

FIGURE 1.2: Nessus window

Note: Throughout the lab, the logo of Nessus and the page background may differ in your lab environment.

9. **Your connection is not private** window appears. Click **ADVANCED**.

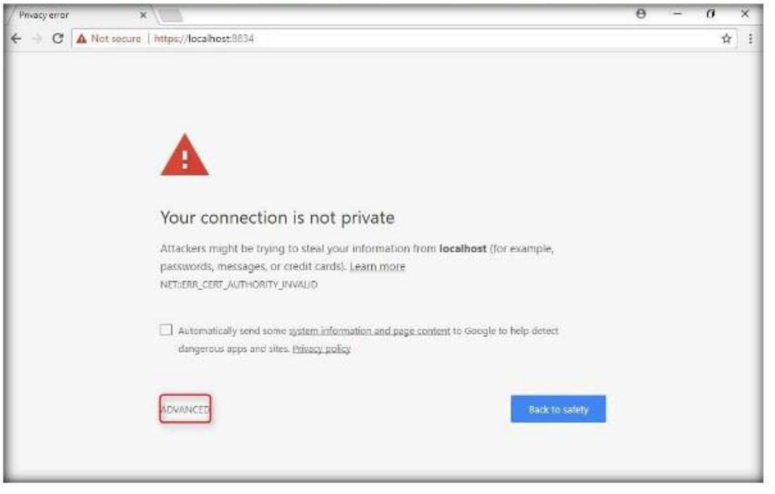

FIGURE 1.3: Browser Security Webpage

10. Now, click **Proceed to localhost (unsafe)** link.

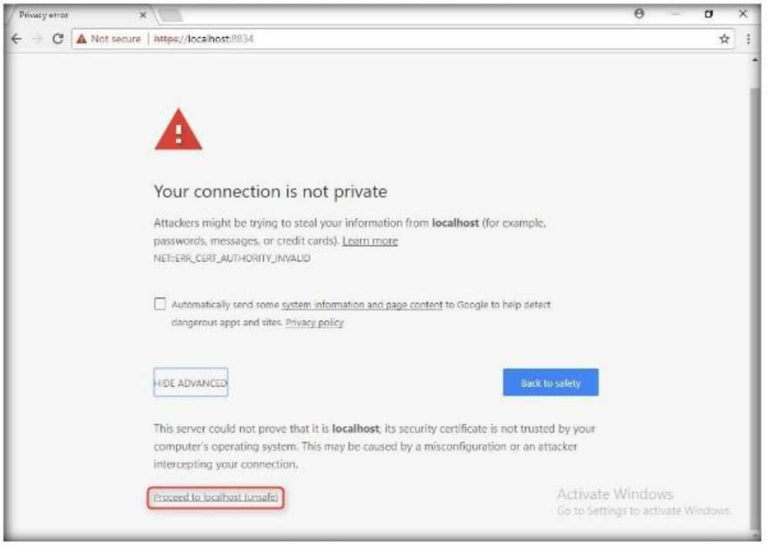

FIGURE 1.4: Browser Security Webpage

11. The **Welcome to Nessus** window appears. Click the **Continue** button.

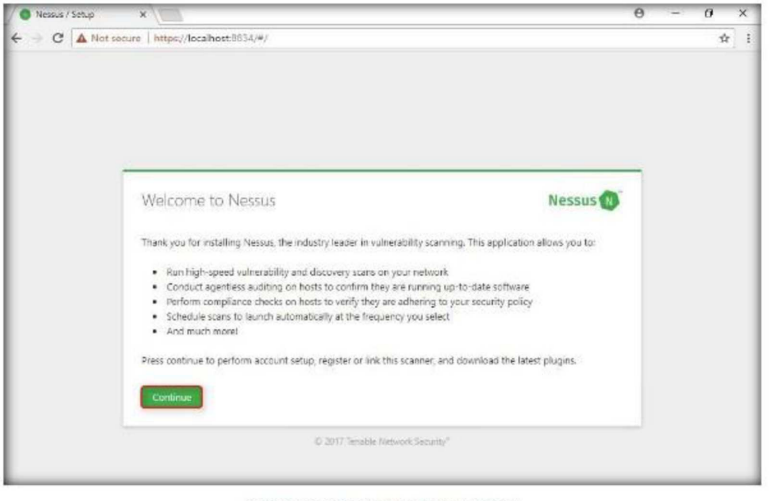

FIGURE 1.5: Welcome to Nessus window

12. **Account Setup** window appears.

13. Create credentials for administrative control of the scanner. You can use **"admin"** and **"password"** here, then click **Continue**.

14. These credentials will be used to log in to Nessus at the time of vulnerability scanning.

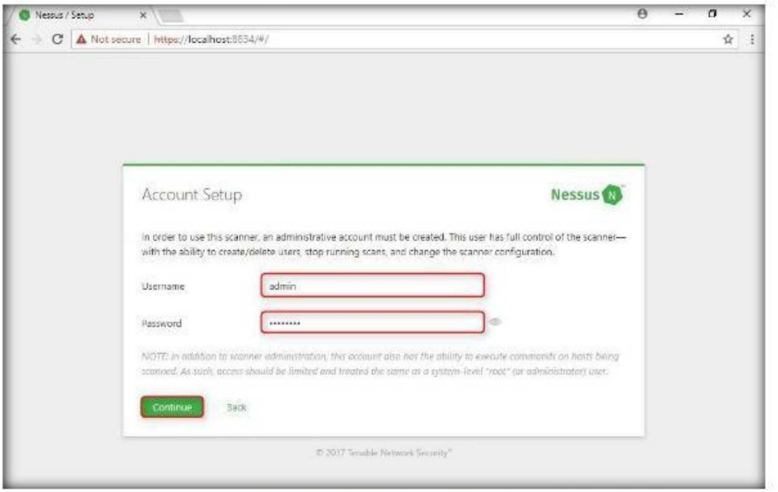

FIGURE 1.6: Account Setup window

15. The **Registration** window appears, enter an activation code in that. Navigate to the Tenable web page and register for an activation code. Proceed to the next step to complete the process.

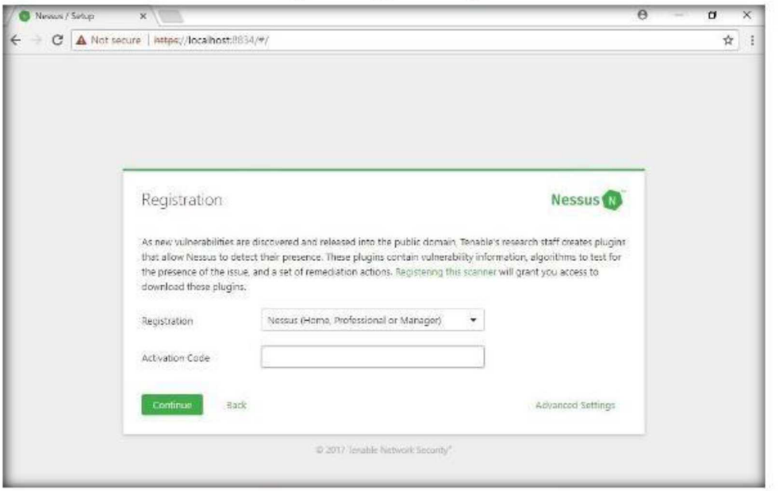

FIGURE 1.7: Plugin Feed Registration window

16. Open a new tab in the browser and type the link **http://www.tenable.com/products/nessus-home** in the address bar. Press **Enter**.

17. The Nessus home page appears. Enter the details under **Register for an Activation Code**, fill in the required details and click **Register**. You can use an alias, but you will need a valid e-mail to retrieve the activation code. Consider creating an alias e-mail account if you do not have one.

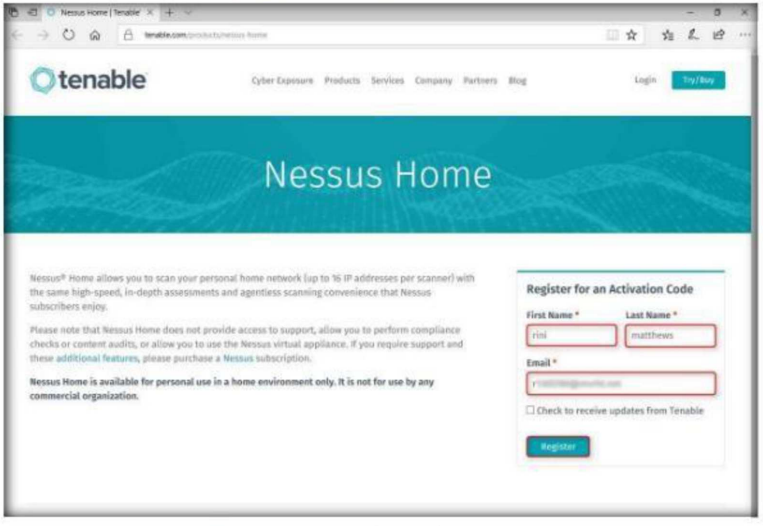

FIGURE 1.8: Registering with Nessus for an activation code

18. Once it's done, close the window.

19. Log in to your email account, open the mail from Tenable Nessus, and copy the activation code.

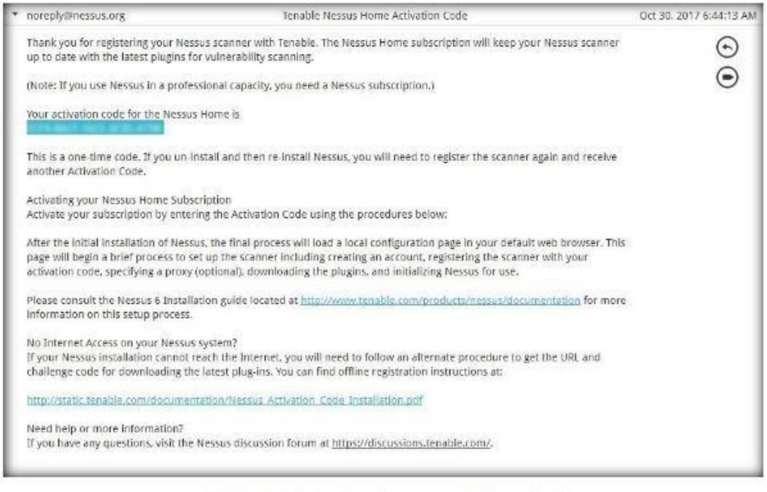

FIGURE 1.9: Activation code sent to your personal mail

20. Switch to the **Registration** window, and paste the activation code in the **Activation Code** text field. Click **Continue**.

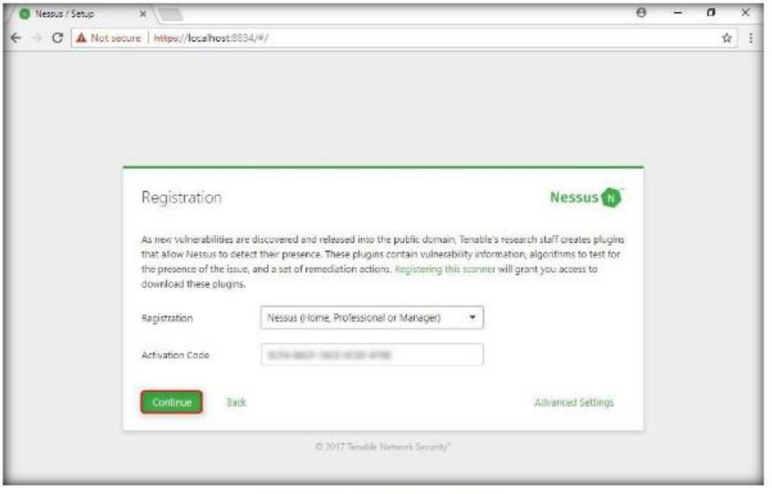

FIGURE 1.10: Registration window

21. Nessus will start fetching the plugins and will install them. It will take time to download plugins and perform the initialization.

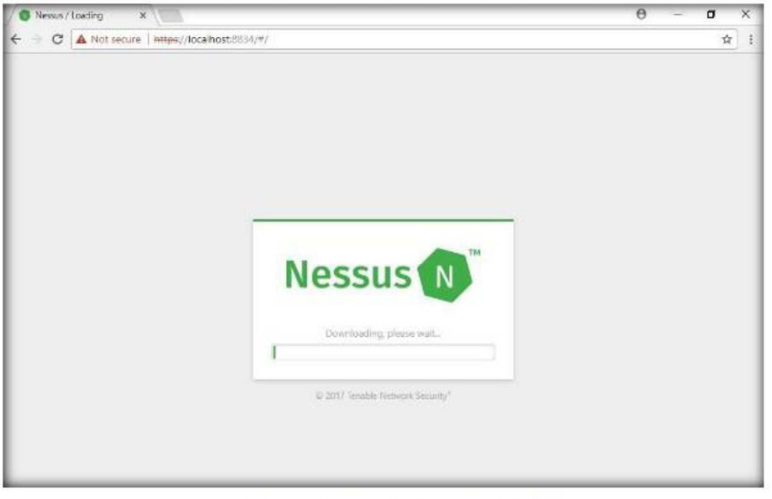

FIGURE 1.11: Nessus fetching the newest plugin set

22. Nessus begins to initialize, it takes some time to initialize.

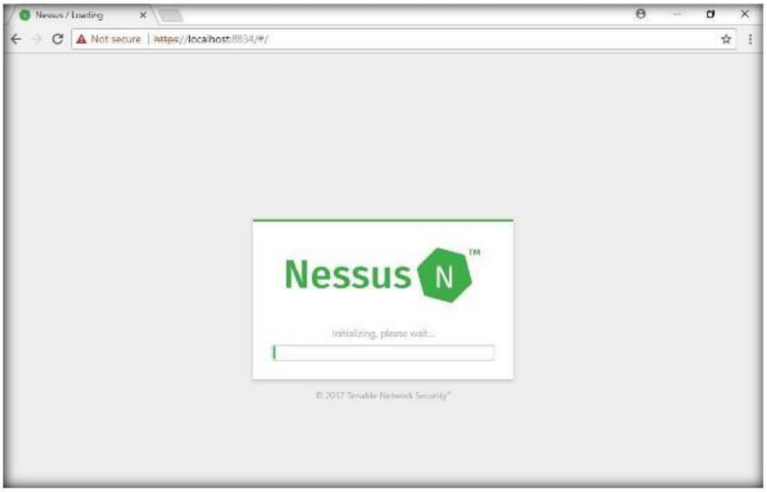

FIGURE 1.12: Nessus being initialized

23. On completion of initialization, the **Nessus Log In** page appears.

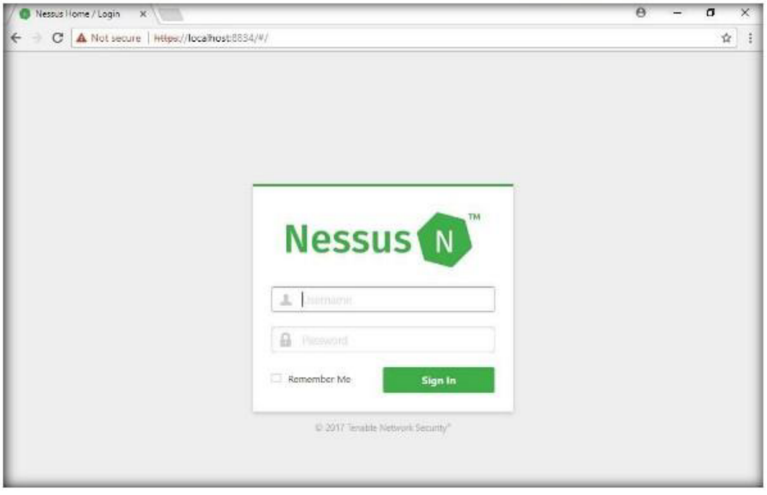

FIGURE 1.13: Nessus Log In screen

24. Enter the **Username** and **Password** from the prior Initial Account Setup step (Recommended User: **admin**; Password: **password**), and click **Sign In**.

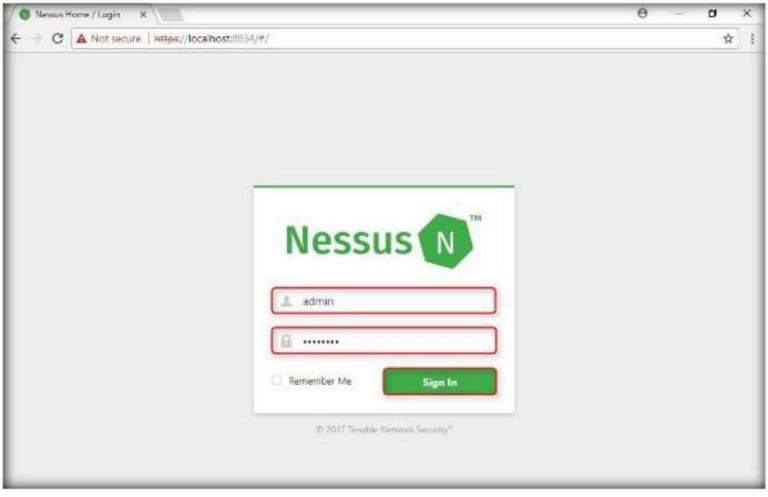

FIGURE 1.14: Signing into Nessus

25. After successful login, the **Nessus/ Scans** window opens, as shown in the screenshot below:

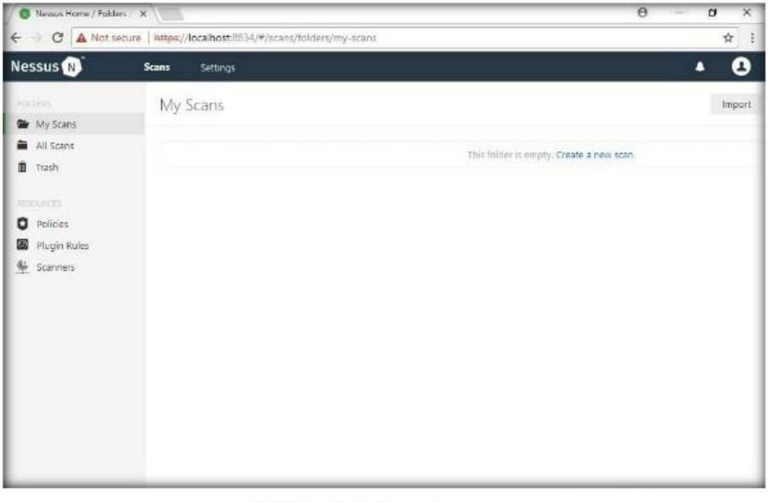

FIGURE 1.15: The Nessus Scans window

26. To add a new policy, click **Policies** button in the **RESOURCES** menu on the left pane.

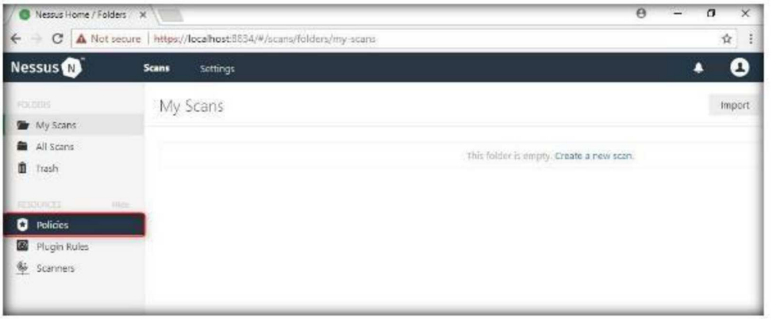

FIGURE 1.16: The Nessus Policies window

27. The **Nessus/ Policies** window opens; click **Create a new policy**.

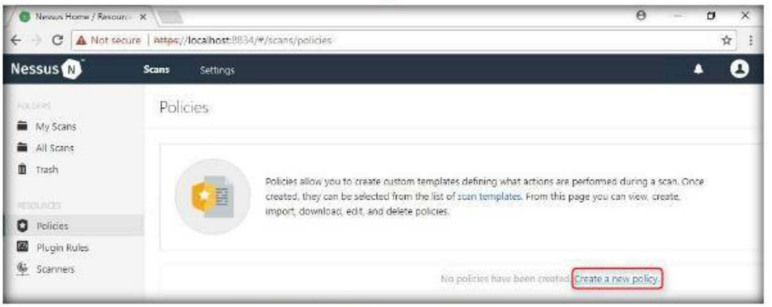

FIGURE 1.17: Adding a new policy in Nessus

28. **Policy Templates** window appears, click **Advanced Scan**.

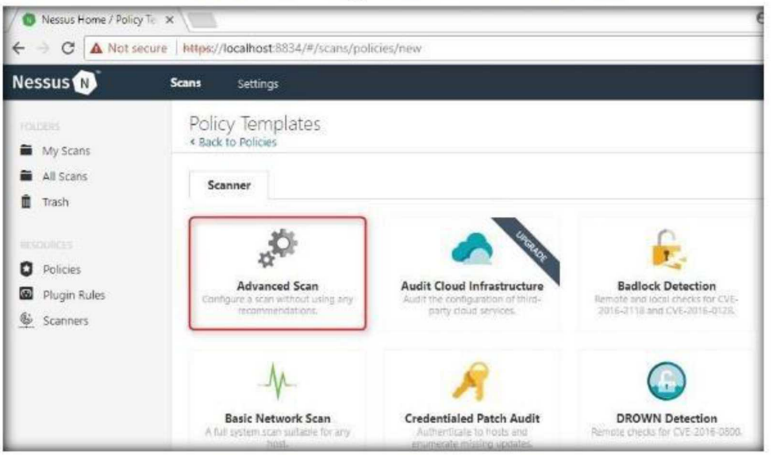

FIGURE 1.18: Choosing Advance Policy from the policy templates

29. The **Policy General Settings** section with **BASIC** setting type appears, specify a policy name in the **Name** field (**NetworkScan_Policy**), and give a **Description** about the policy.

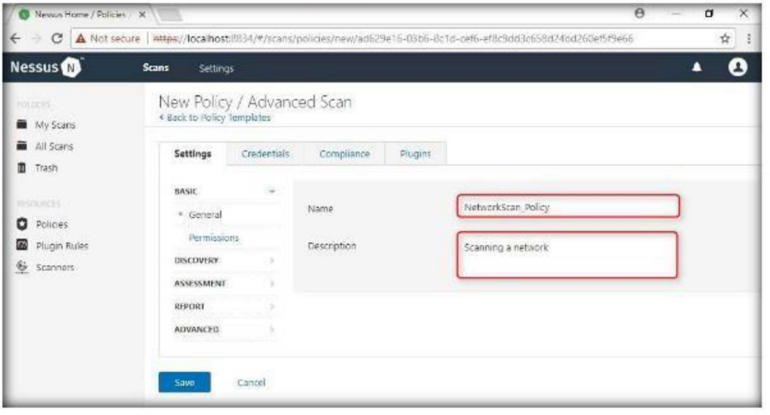

FIGURE 1.19: Customizing the general settings

30. In Setting field, select **Host Discovery** from the **DISCOVERY** drop-down list. Turn off **Ping the remote host** option.

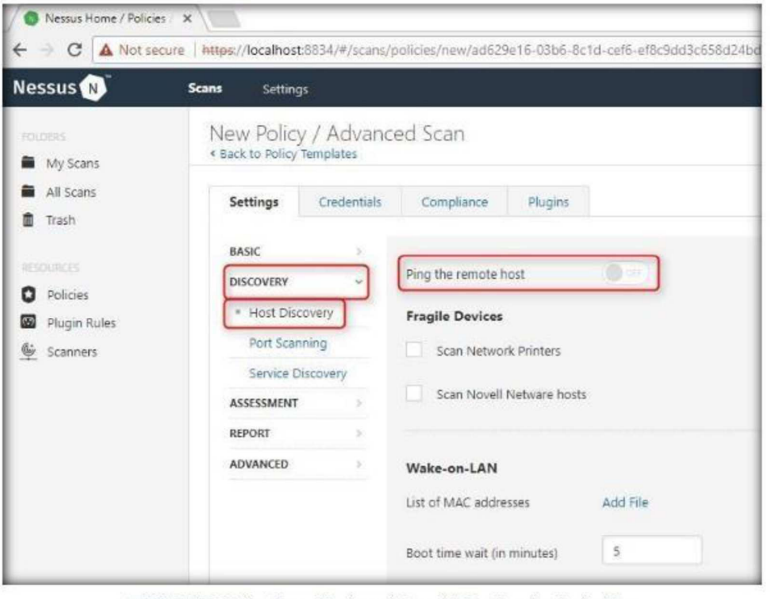

FIGURE 1.20: Policy General Settings window with Port Scanning Setting Type

31. Select **Port Scanning** setting type and check the **Verify open TCP ports found by local port enumerators** option. Leave the other fields with default options, as shown in the screenshot.

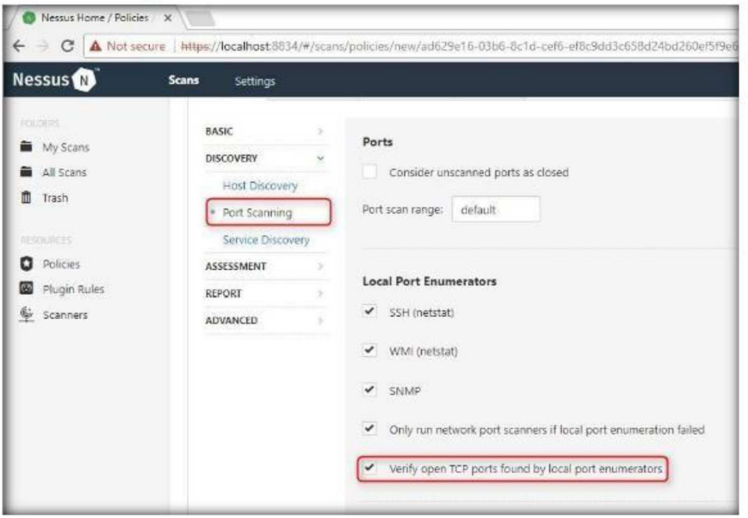

FIGURE 1.21: Customizing the Port Scanning Setting Type

32. In the **Setting** field, select **REPORT** and do not alter any options in this Setting type.

33. Proceed with default options as shown in the screenshot below:

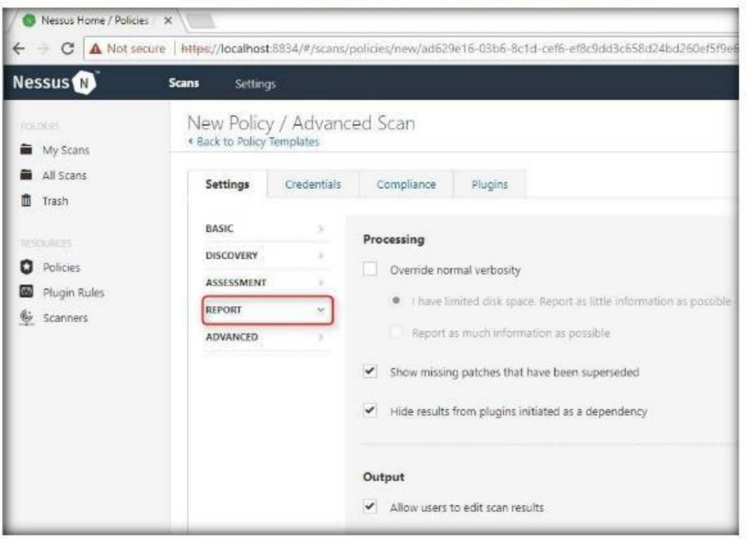

FIGURE 1.22: Policy General Settings window with Performance Setting Type

34. In the **Setting** field, select **ADVANCED**. The Policy General Settings window with **Advanced** Setting type appears.

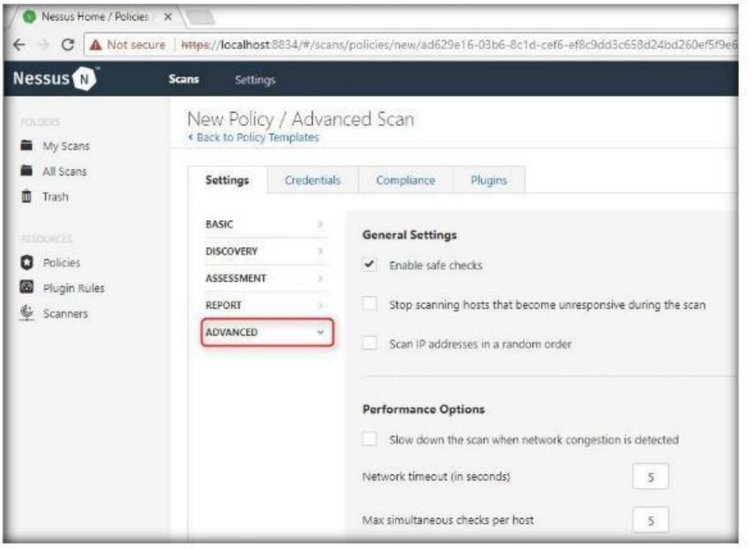

FIGURE 1.23: Customizing the Performance Setting Type

35. Set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **unlimited**.

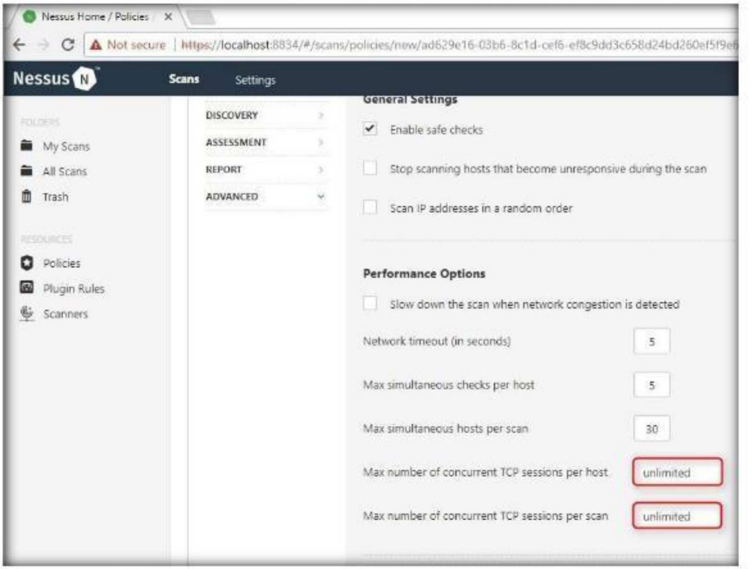

FIGURE 1.24: Policy General Settings window with Advanced Setting Type

36. To configure the credentials of new policy, click the **Credentials** tab. The Policy Credentials window, with the **Windows Credentials** Credential Type field, is displayed, as shown in the following screenshot:

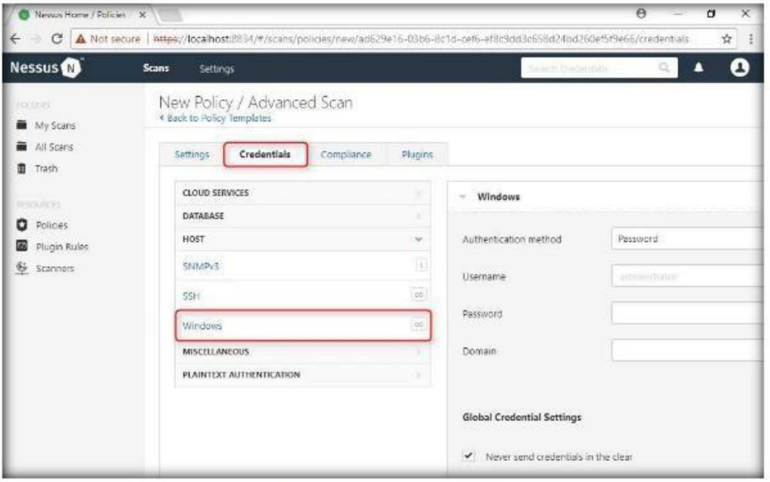

FIGURE 1.25: Adding Policies and setting Credentials

37. Specify the **Username** (same as shown in the screenshot) and **Password** in the window. Here, specify the credentials as **AD143/qwerty@123**.

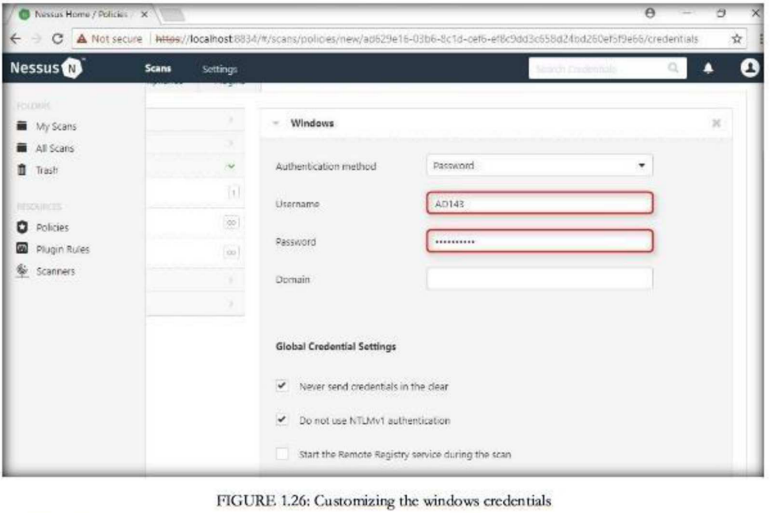

FIGURE 1.26: Customizing the windows credentials

38. To select the required plugins, click the **Plugins** tab.

39. Do not alter any of the options in this window and click **Save** button.

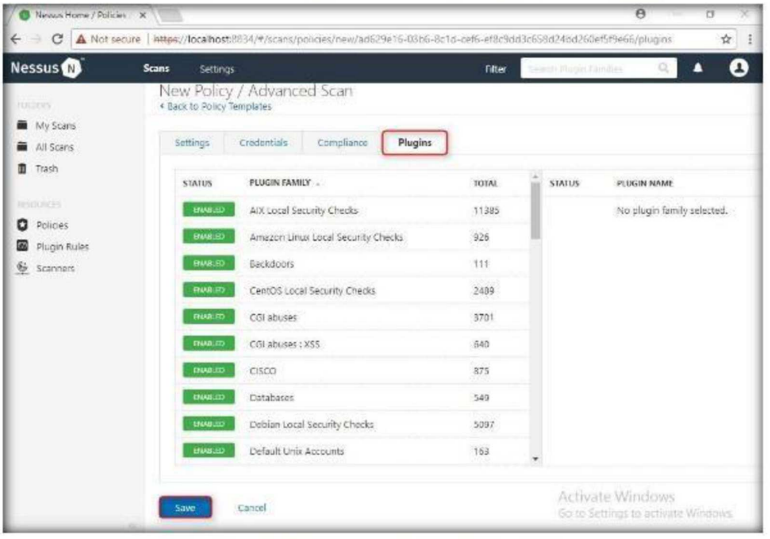

FIGURE 1.27: The Nessus - Policy Plugin Configurations window

40. A **Policy saved successfully** notification pop-up appears, and the policy is added in the Policies window as shown in the following screenshot:

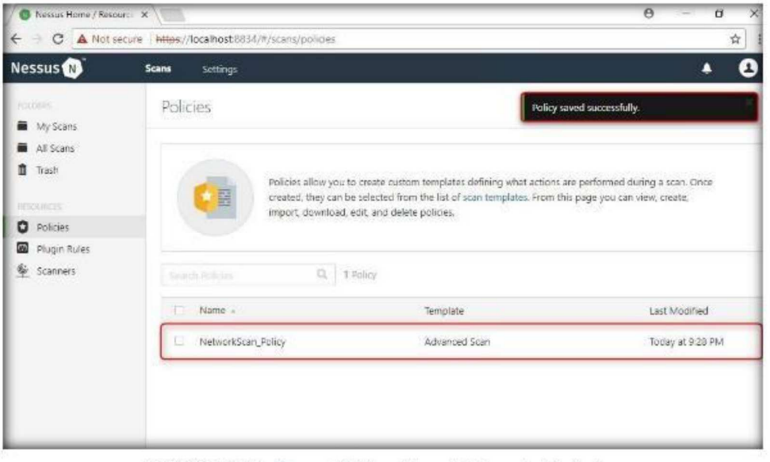

FIGURE 1.28: The Nessus - Policies window with the newly added policy

41. Now, click **Scans** to open the **My Scans** window. Click **Create a new scan** option to view the Scan Templates window as shown in the screenshot.

FIGURE 1.29: Setting a new scan in Nessus

42. Now, click **User Defined** tab and select **NetworkScan Policy**.

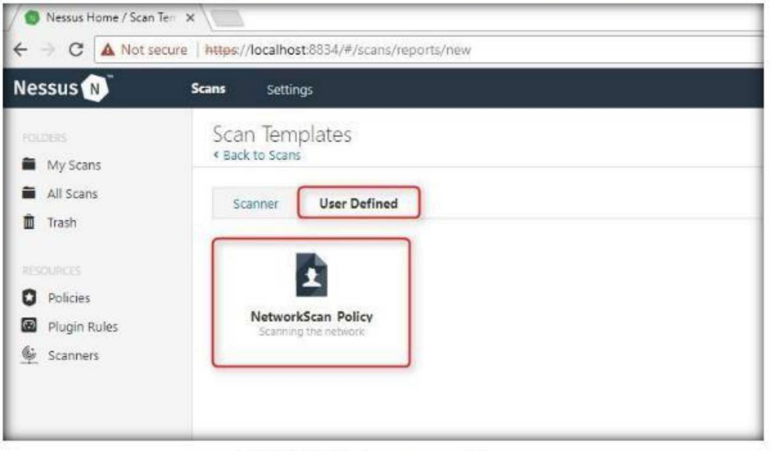

FIGURE 1.30: Setting a new scan in Nessus

43. Input the **Name** of the scan (here, **Local Network**), enter the **Description** for the scan, in **Targets** field, enter the IP address of the target on which you want to perform the vulnerability assessment. In this lab, it is **Windows Server 2012** virtual machine whose IP address is **10.10.10.12**.

Note: The IP addresses may vary in your lab environment.

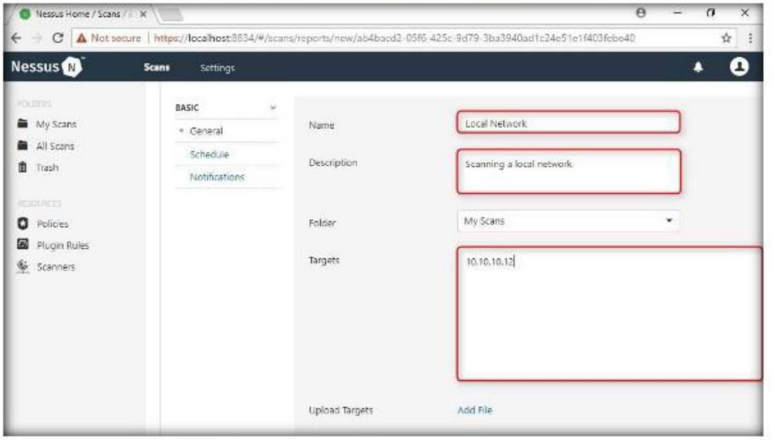

FIGURE 1.31: Configuring the basic settings in the scans window

44. Click **Schedule** settings and turn off the **Enabled** switch, select **Launch** from the drop-down list to start the scan.

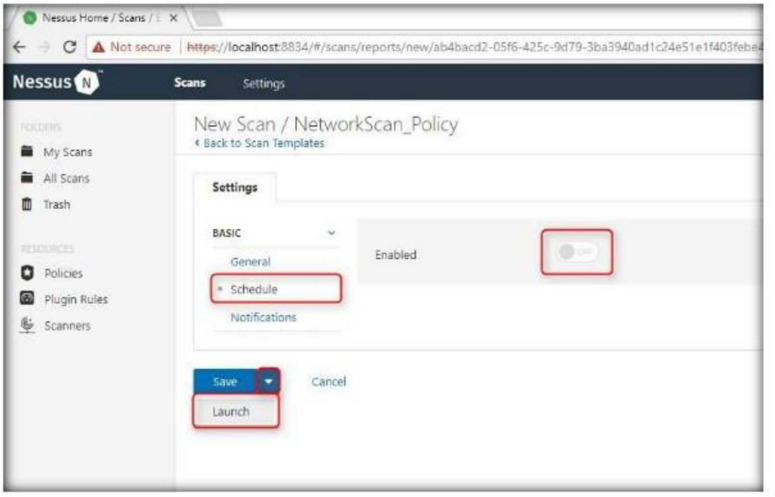

FIGURE 1.32: Setting a scan schedule

45. The scan is launched, and Nessus begins to scan the target.

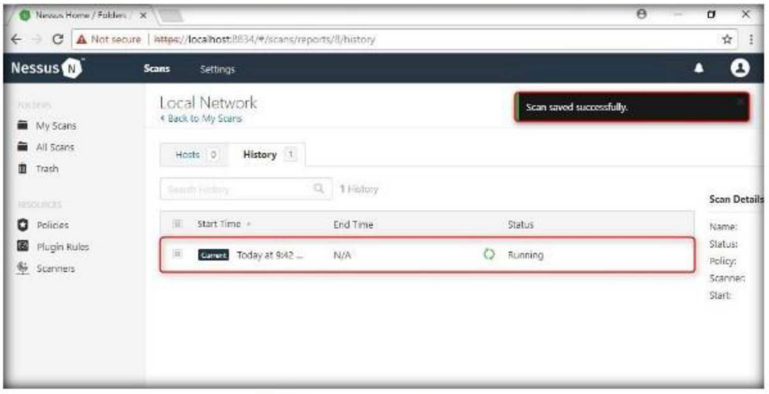

FIGURE 1.33: Local Network scanning

46. After the scan is complete, the status of the scan changes to **Completed**.

47. Click the tab to view the detailed results.

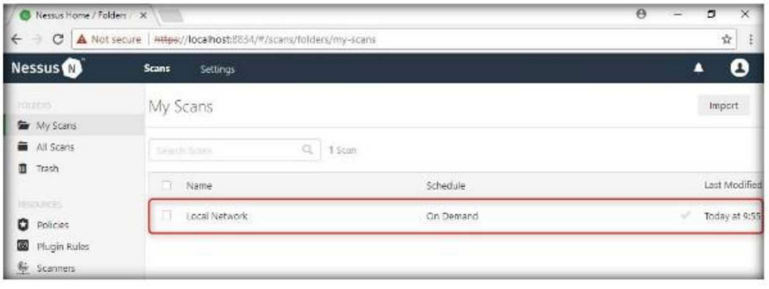

FIGURE 1.34: Selecting local network scan

48. The Local Network window opens, displaying the summary of hosts as well as **Scan Details**, as shown in the following screenshot:

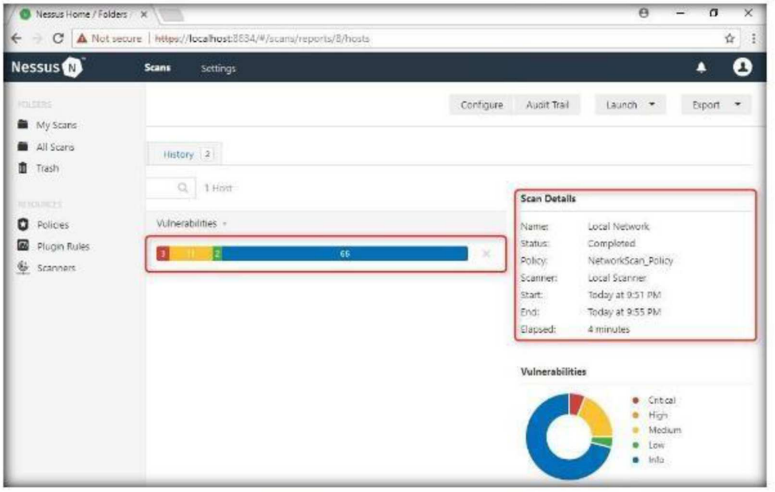

FIGURE 1.35: Hosts Summary window

49. Click the **Vulnerabilities** tab, and scroll down the window to view all the vulnerabilities associated with the target machine.

Note: The list of vulnerabilities may differ in your lab environment.

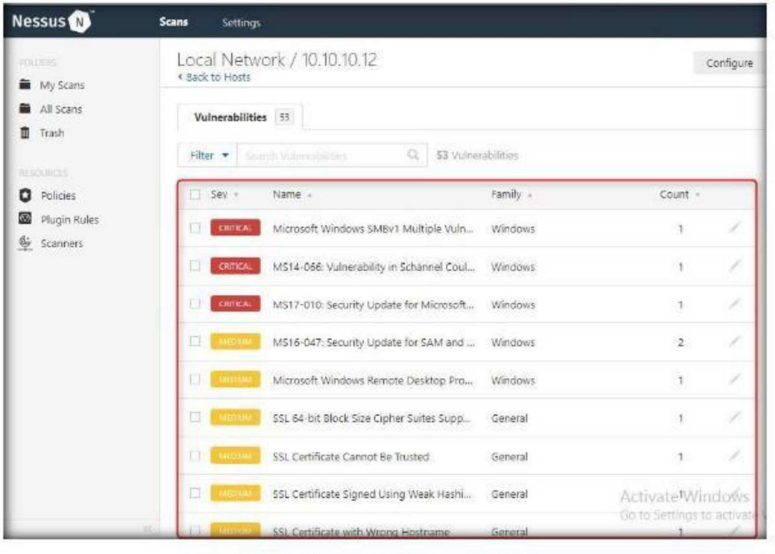

FIGURE 1.36: Vulnerability Summary window

50. Click these vulnerabilities to view detailed report about each of them. For instance, in this lab, **Microsoft Windows SMBv1 Multiple Vulnerabilities** is selected.

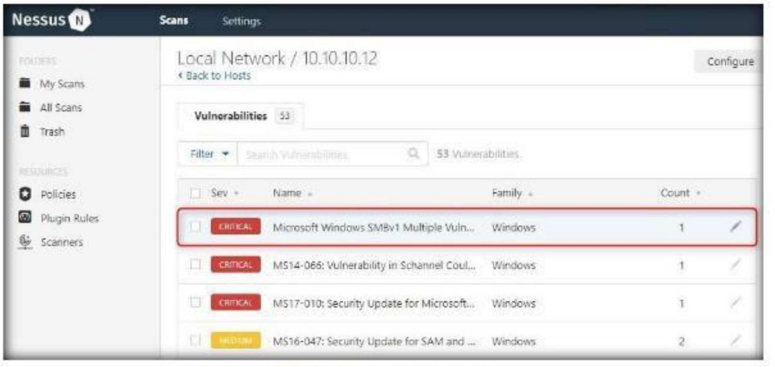

FIGURE 1.37: Selecting vulnerability

51. The report appears as shown in the following screenshot:

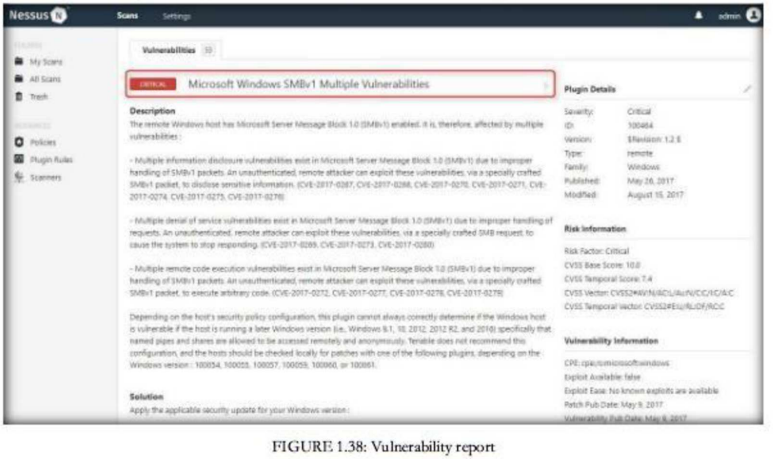

FIGURE 1.38: Vulnerability report

52. On completing the vulnerability analysis, first click **Scans** and then click the recently performed scan (here named as **Local Network**).

53. You may download the report for future reference. To download a report, login to Nessus, open the **Scans** section, and select the **Local Network** scan.

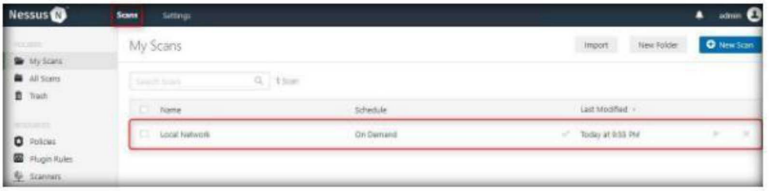

FIGURE 1.39: Selecting Local Network Scan

54. Click the **Export** tab, and choose a file format (here, **HTML**) from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.

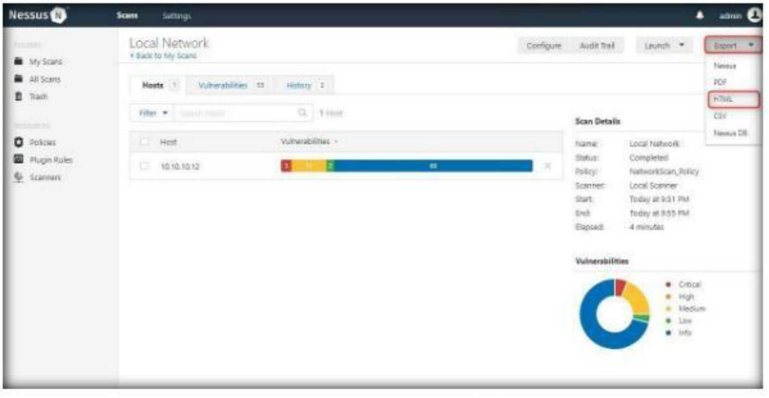

FIGURE 1.40: Exporting Report to HTML Format

55. The **Export as HTML** window opens with **Executive Summary** as default report type, click **Export** to download the report.

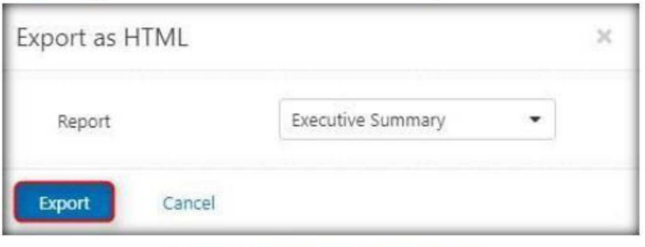

FIGURE 1.41: Export as HTML window appears

56. When the Report download completes, click the downloaded content to open it.

FIGURE 1.42: Chapters Added to Report Content

57. Choose a browser to view the HTML file.

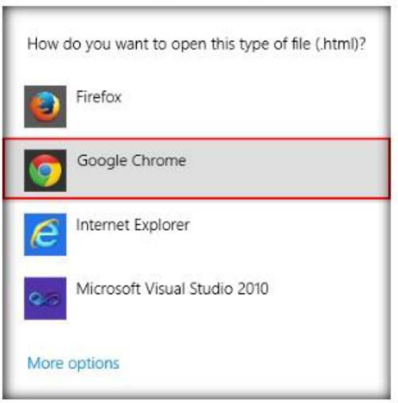

FIGURE 1.43: Choosing a browser to view the HTML

58. The Nessus Scan Report appears in the web browser as shown in the following screenshot:

Note: Screenshots might differ in your lab environment.

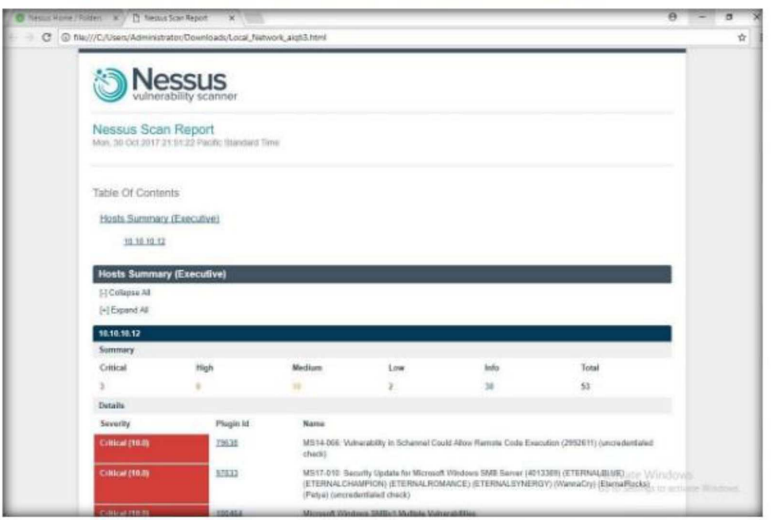

FIGURE 1.44: Vulnerability Report Displayed in HTML Format

59. You can choose a chapter from the **Table Of Contents** by clicking on it.

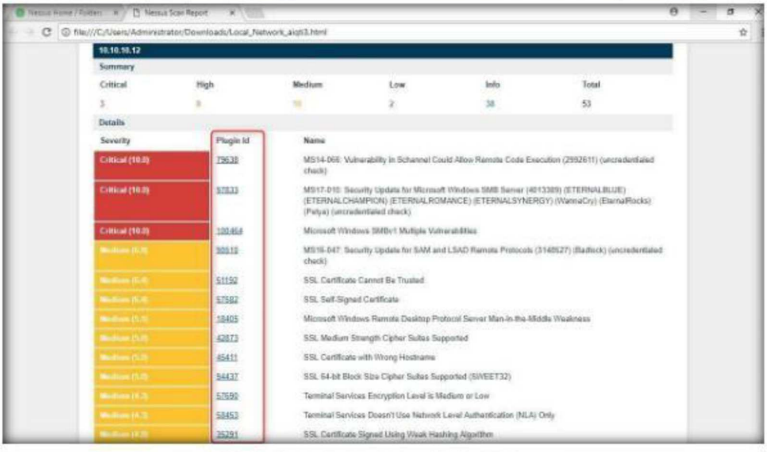

FIGURE 1.45: Viewing a Vulnerability in the Report

60. The selected vulnerability details are listed, as shown in the following screenshot:

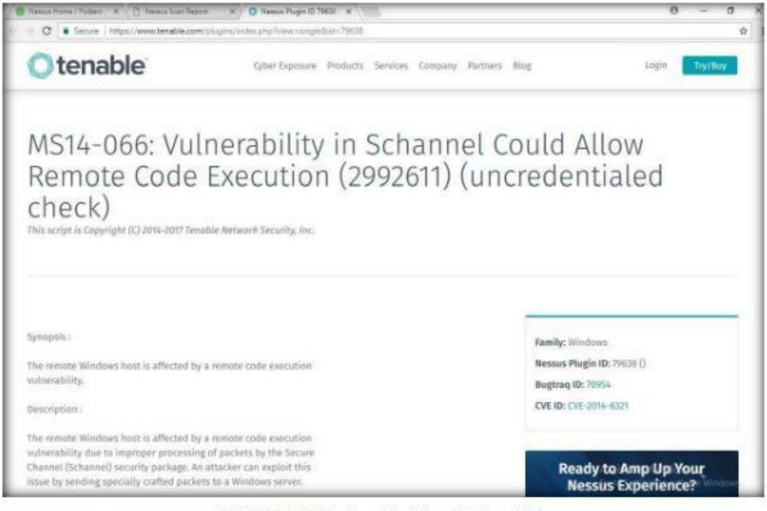

FIGURE 1.46: Details of the Selected Vulnerability

61. In this way, you can select a vulnerability of your choice to view the complete details.

62. Once the vulnerability analysis is done, click **admin → Sign Out**.

FIGURE 1.47: Signing out of Nessus

63. Once the session is successfully logged out, the following window appears stating: **Signed out successfully. Goodbye, admin**. Close the browser.

FIGURE 1.48: Signed out successfully

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

2

Scanning for Network Vulnerabilities using the GFI LanGuard

GFI LanGuard scans networks and ports to detect, assess, and correct any security vulnerabilities found.

Lab Scenario

Scanning vulnerabilities using only one vulnerability-scanning tool might not be sufficient. As a professional ethical hacker or pen-tester, you should always try to perform vulnerability scanning with different kinds of vulnerability scanning tools. It is important to become proficient in using different kinds of vulnerability scanning tools and techniques. This lab demonstrates the vulnerability scanning with another vulnerability-scanning tool.

Lab Objectives

The objective of this lab is to help students conduct vulnerability scanning using GFI LanGuard network vulnerability scanner.

Lab Environment

The following are required to perform this lab:

- Register on the GFI website **http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download** to obtain a license key
- For subscription and activation code, you will receive an email with an activation code
- If the latest version is downloaded, then screenshots shown in the lab might differ
- Windows Server 2016 system required
- Windows 10 in a virtual machine

- Administrator privileges to run the GFI LanGuard Network Security Scanner

Lab Duration

Time: 15 Minutes

Overview of GFI LanGuard

GFI LanGuard can help in discovering and listing vulnerabilities of the operating system on remote computers (missing security patches), as well as vulnerabilities of installed software, system configuration, and so on.

Lab Tasks

1. Launch a web browser, type the URL **http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download** in the address bar, and press **Enter**.
2. The GFI LanGuard registration page appears. Enter details, and click **GET STARTED FOR FREE**.

FIGURE 2.1: GFI LanGuard Registration page

3. You will be redirected to the download page, click **Download Now**.

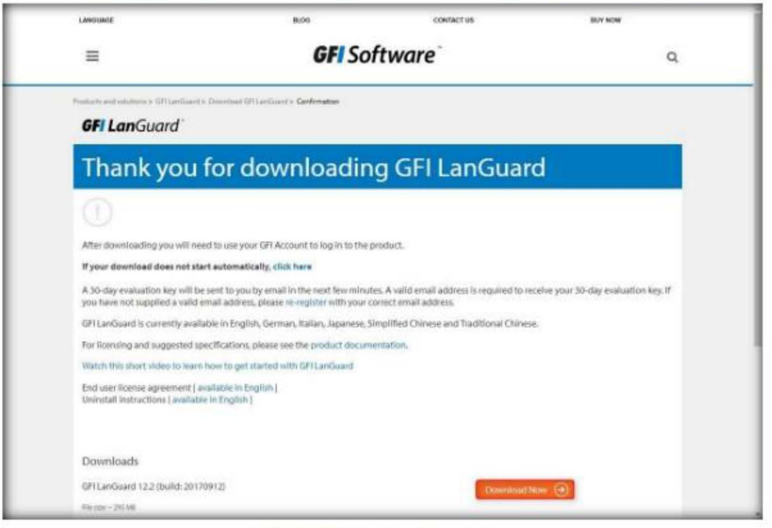

FIGURE 2.2: GFI LanGuard Download page

4. The application is downloaded on the local drive. Navigate to the download location and double-click **languard.exe** to install.

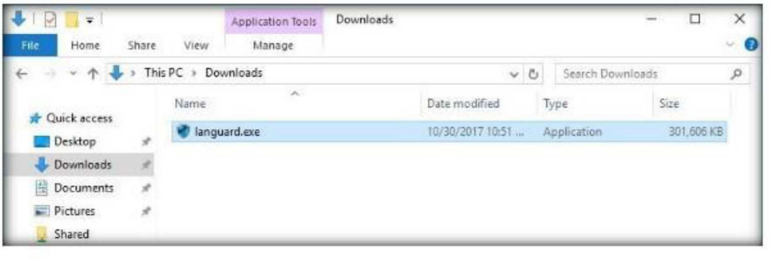

FIGURE 2.3: GFI LanGuard exe file

5. If the **Open File - Security Warning** pop-up appears, click **Run**.
6. **GFI LanGuard** dialog box appears, select preferred language and click **OK**.

FIGURE 2.4: Selecting a language

7. **GFI LanGuard** wizard appears with selected components for installation, click **Next** to proceed.

FIGURE 2.5: Installation wizard

8. **Database Configuration** window opens, key in the SQL server name (here, .\SQLEXPRESS). Click **OK**.

Note: The SQL server name might differ in your lab environment.

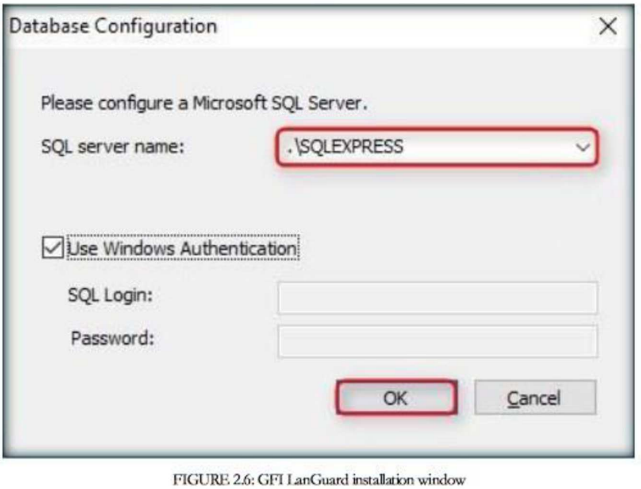

FIGURE 2.6: GFI LanGuard installation window

9. Wait until the necessary files are downloaded. Log in to the mail account created at the time of registration, open the received mail sent from **GFI Downloads**, and copy the **license key**.

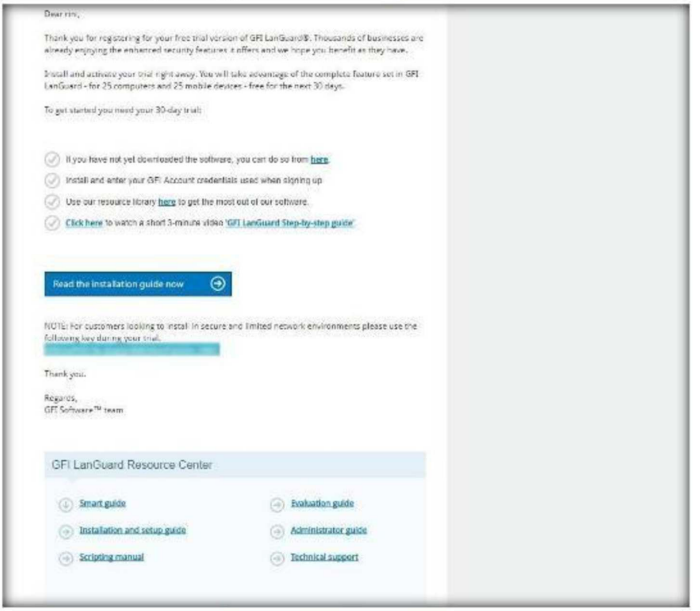

FIGURE 2.7: GFI LanGuard Trial Key

10. Now, maximize the **GFI LanGuard Liscense Key** window. Specify the **License Key** received. Click **OK**.

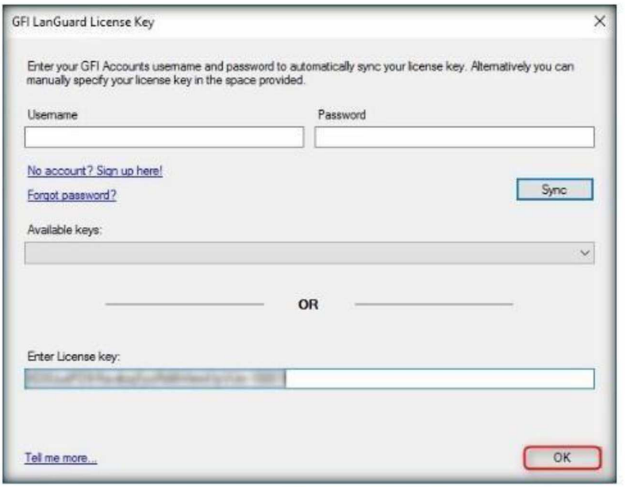

FIGURE 2.8: GFI LanGuard License window

11. The **GFI LanGuard Setup** window opens; click **Next**.

FIGURE 2.9: GFI LanGuard Setup window

12. **End-User License Agreement** window appears, accept the terms and click **Next**.

FIGURE 2.10: GFI LanGuard License agreement

13. In the **Attendant service credentials** section, leave the **Name** field (Administrator user account) set to its default, and enter the **Password** of the admin account; and click **Next >**.

Note: The Name field might differ in your lab environment.

FIGURE 2.11: GFI LanGuard Attendant service credentials section

14. In the **Choose Destination Location** section, select the location where you want to install the application, and click **Install**.

FIGURE 2.12: Choosing a folder location

15. The **GFI LanGuard Central Management Server Setup** window opens; click **Next**.

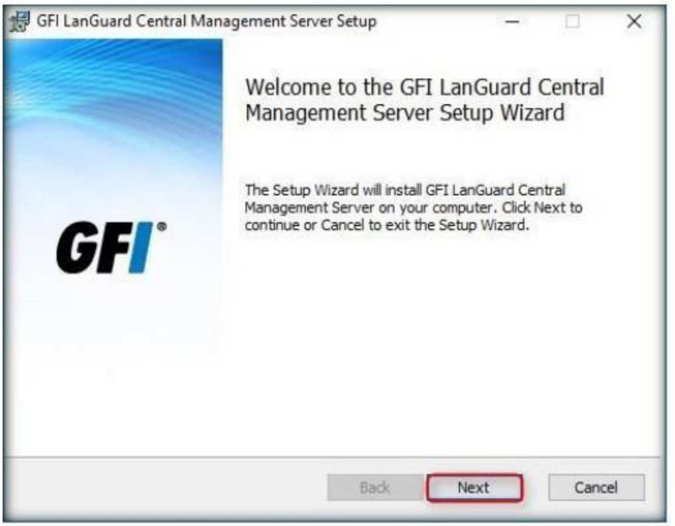

FIGURE 2.13: GFI LanGuard Central Management Server Setup window

16. In the **Service logon information** section, leave the **User Name** field (Administrator user account) set to its default, and enter the **Password** of the admin account, and click **Next**.

Note: The Name field might differ in your lab environment.

FIGURE 2.14: GFI LanGuard Service logon information section

17. **HTTPS Settings** section appears, leave the name to default and click **Next**.

Note: The Name field might differ in your lab environment.

FIGURE 2.15: GFI LanGuard HTTPS Settings section

18. In the **Destination Folder** section, choose the location where you want to install the application, and click **Next**.

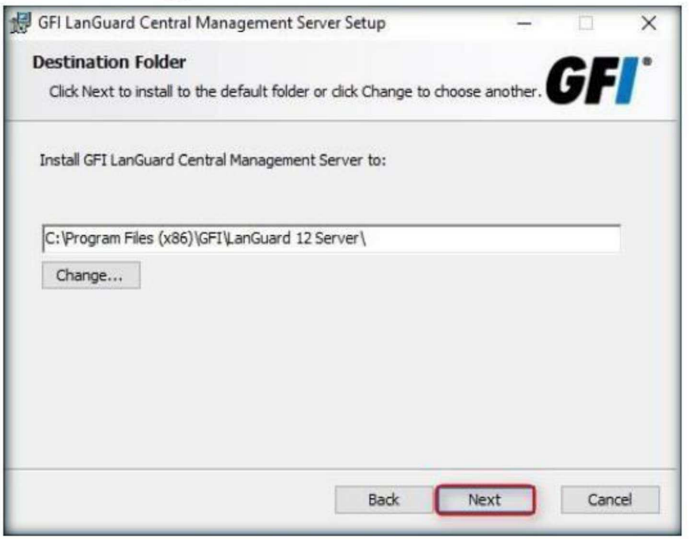

FIGURE 2.16: Choosing a folder destination

19. The **Ready to install** section appears, click **Install** to proceed.

FIGURE 2.17: GFI LanGuard Central Management Server Setup window

20. Once the installation is complete, it takes some time for the application to load.

21. A **GFI LanGuard** pop-up appears on the main window of the application. Click **Continue evaluation**.

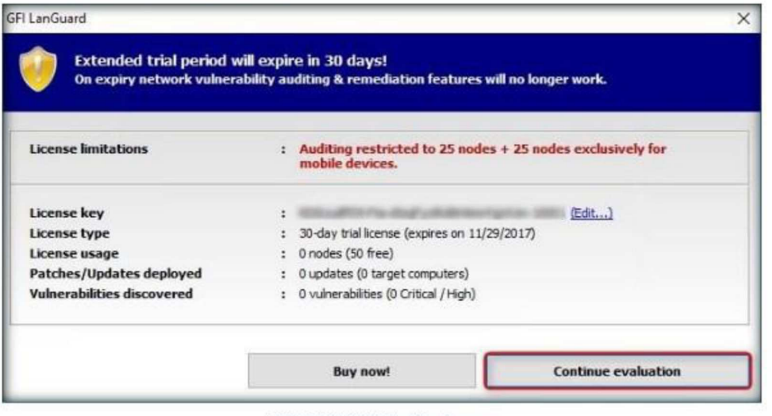

FIGURE 2.18: GFI LanGuard pop-up

22. The **GFI LanGuard** main window opens, and it begins to inspect the security status of the local computer.

23. Click **Launch a Scan** or **View details**.

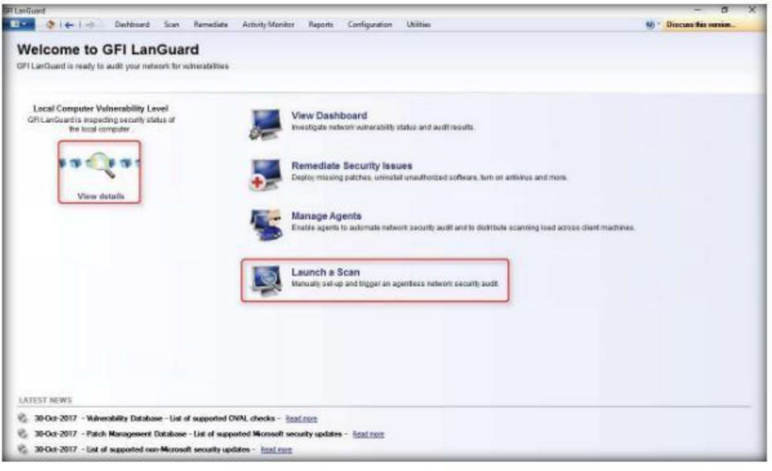

FIGURE 2.19: Launching a scan in GFI LanGuard

24. A window indicates that a scan on the local machine is already in progress.

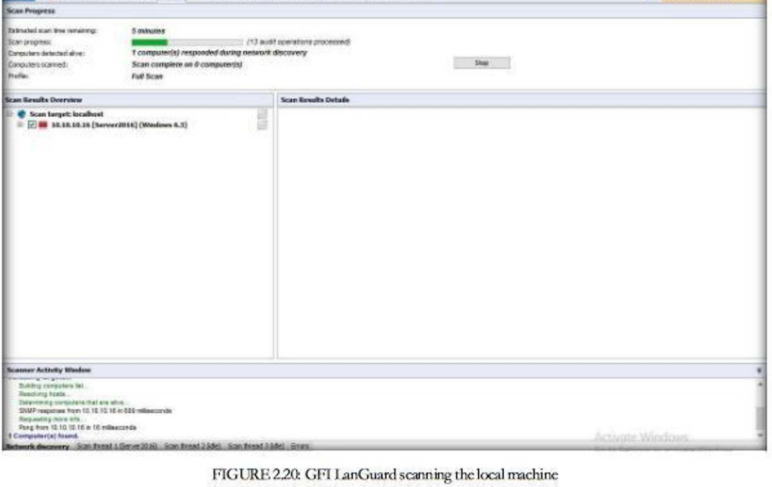

FIGURE 2.20: GFI LanGuard scanning the local machine

Note: You may allow the scan to finish analyzing vulnerabilities in the host machine.

25. Click **Stop** to halt the vulnerability scan on the host machine.

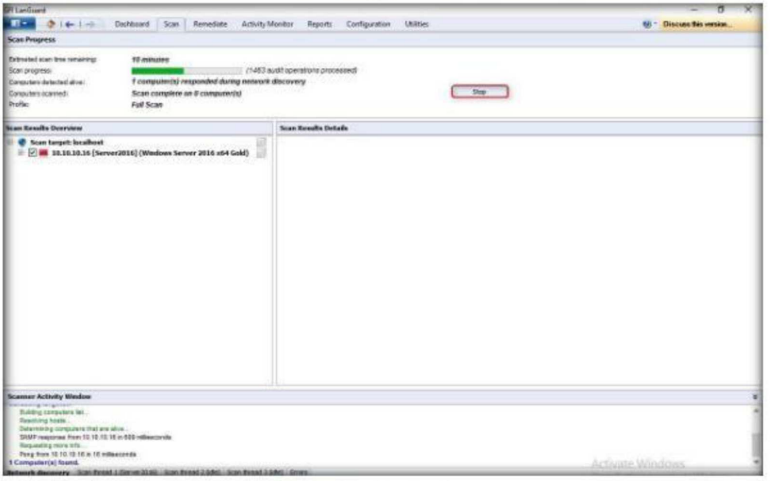

FIGURE 2.21: Stopping the scan

26. A **Stop scanning confirmation** window appears. Click **Yes**.

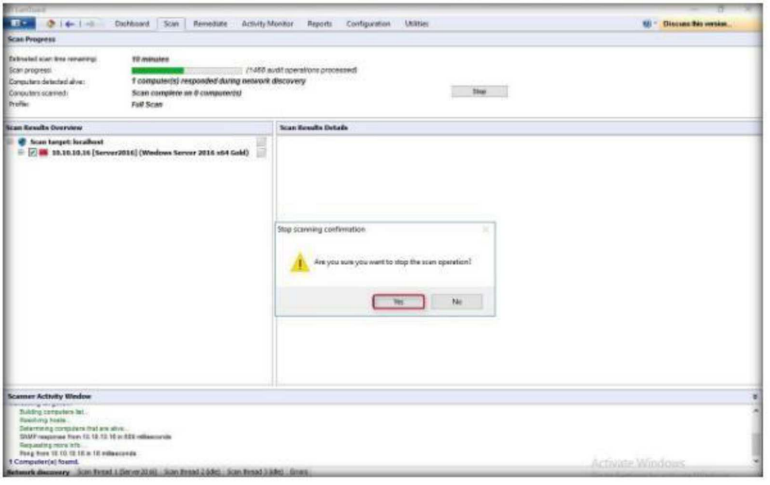

FIGURE 2.22: Stopping the scan

27. The **Launch a New Scan** section appears, specify the details required to scan a target/virtual machine.

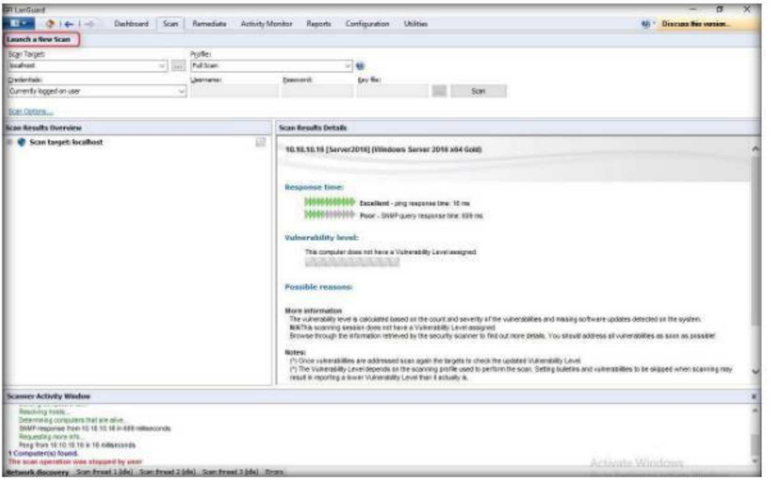

FIGURE 2.23: Launch a New Scan section in GFI LanGuard

28. Log on to a virtual machine, here **Windows 10**.

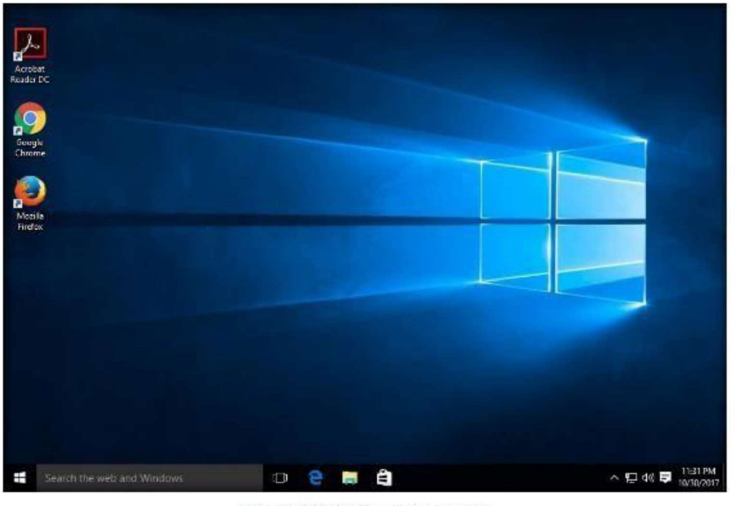

FIGURE 2.24: Windows 10 Desktop view

29. Switch to the host machine, and in GFI LanGuard window:
    a. Enter the IP address of the virtual machine in the **Scan Target** field, and select **Full Scan** from the **Profile** drop-down list.
    b. Select **Alternative credentials** from the **Credentials** drop-down list.

c. Enter the credentials of the Windows 10 machine: **Username**: **Admin**; and **Password**: **Pa$$w0rd**. Then click **Scan**.

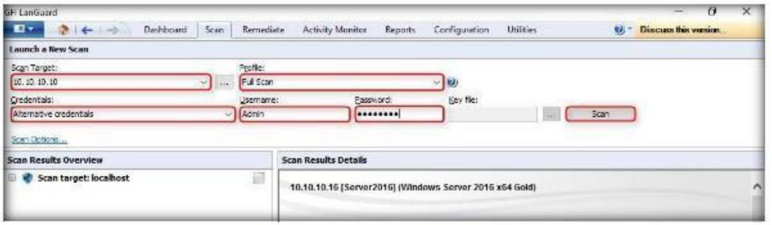

FIGURE 2.25: Customizing the scan settings

Note: The **Windows 10** IP address is **10.10.10.10**. This may vary in your lab environment.

30. GFI LanGuard takes some time to perform the vulnerability assessment on the intended virtual machine.

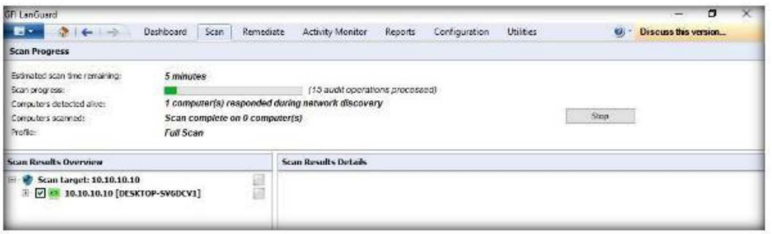

FIGURE 2.26: Vulnerability assessment being performed

31. Once the scanning is complete, **Scan Results Overview** and **Scan Results Details** are displayed, as shown in the following screenshot:

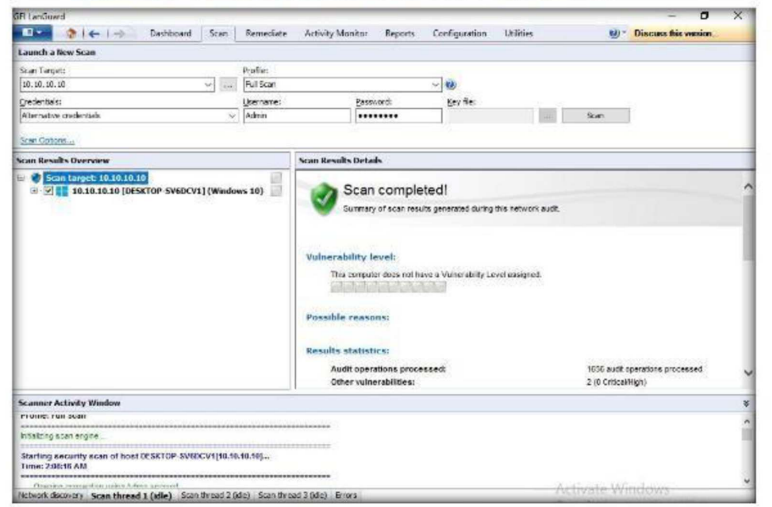

FIGURE 2.27: Scan Results displayed in GFI LanGuard

32. To check the Scan Result Overview, click the **IP address** node.

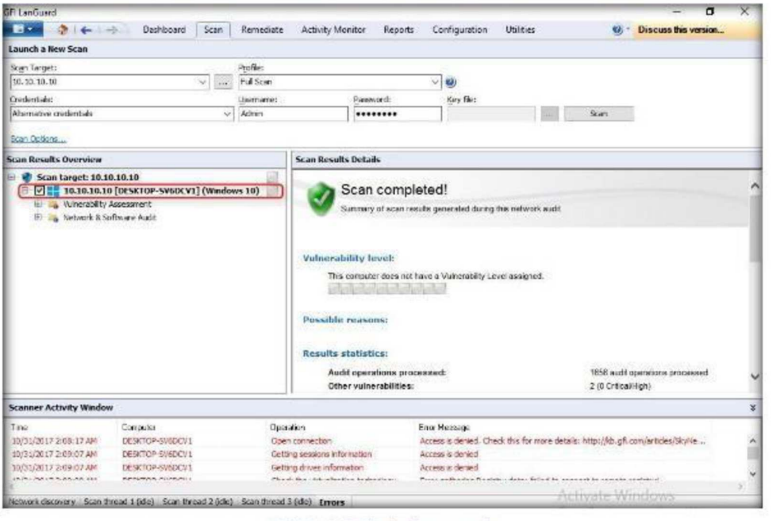

FIGURE 2.28: Viewing the scan results

33. It displays **Vulnerability Assessment** and **Network & Software Audit** nodes. Click **Vulnerability Assessment**.

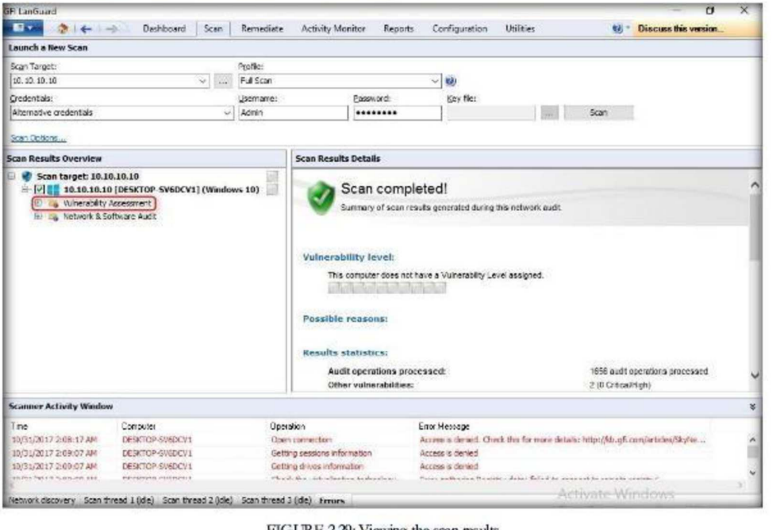

FIGURE 2.29: Viewing the scan results

34. It shows category-wise details of **Vulnerability Assessment**. Click each category to view the vulnerabilities in the virtual machine.

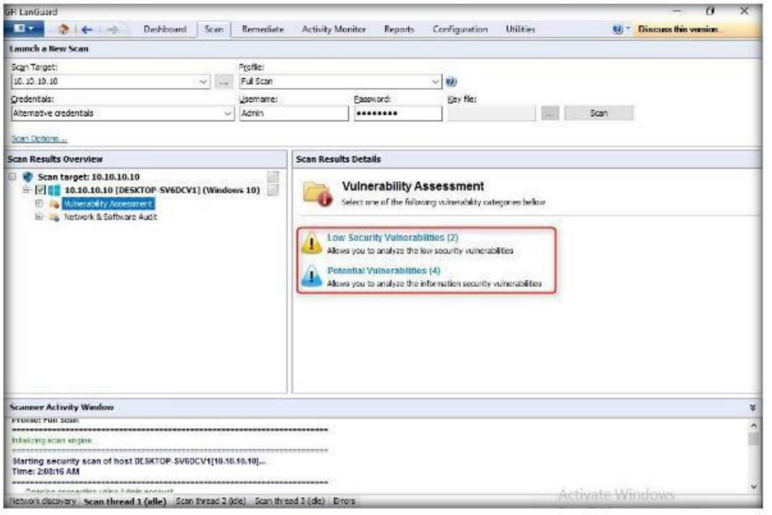

FIGURE 2.30: Vulnerability Assessment categories

35. Expand the **Network & Software Audit** node in the left pane, expand **Ports**, and click **Open TCP Ports** to view all the open TCP Ports.

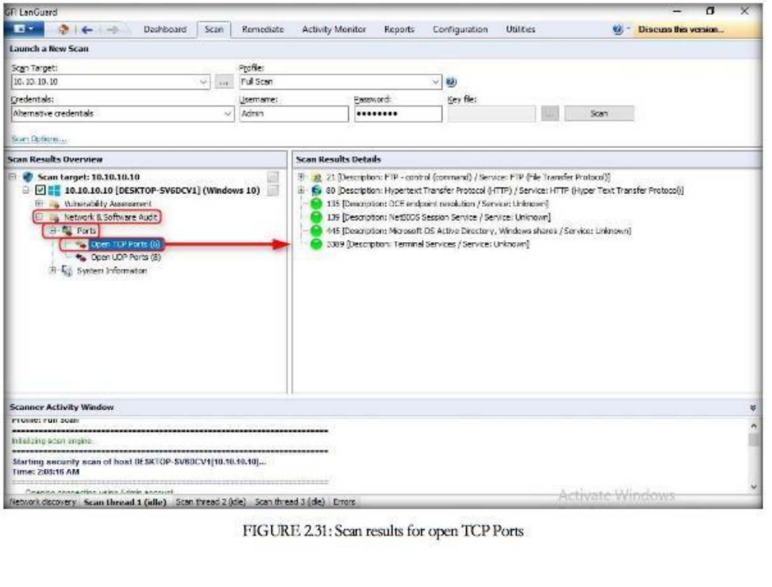

FIGURE 2.31: Scan results for open TCP Ports

36. In the same way, click **Open UDP Ports** to view all the open UDP Ports.

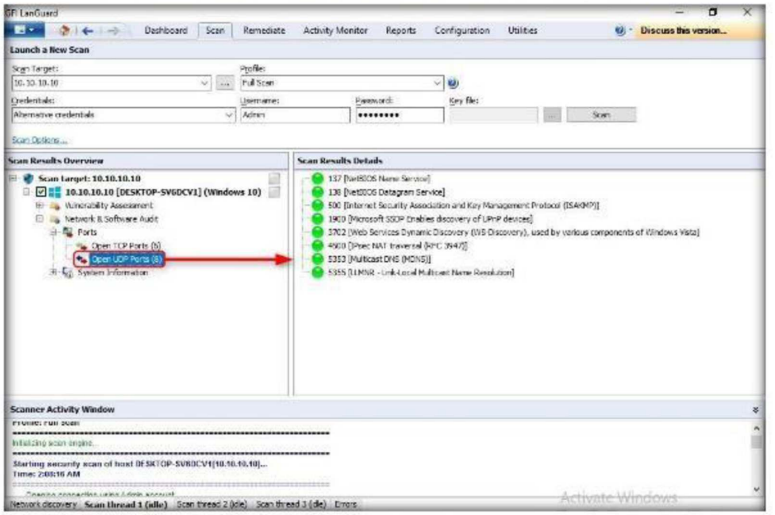

FIGURE 2.32: Scan results for open UDP Ports

37. Click **System Information** in the left pane to display details of the system.

38. Click **Password policy** to view the password details set in the virtual machine.

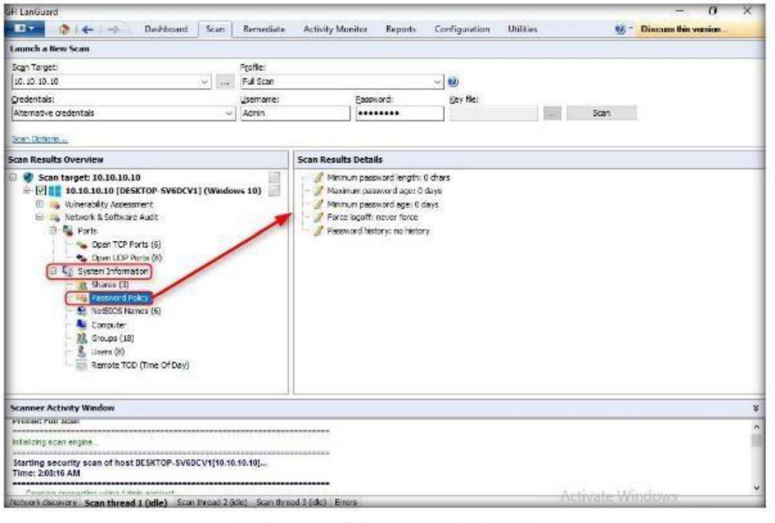

FIGURE 2.33: Scan results for Password Policy

39. Click **Groups** to display all the groups presently available in the system.

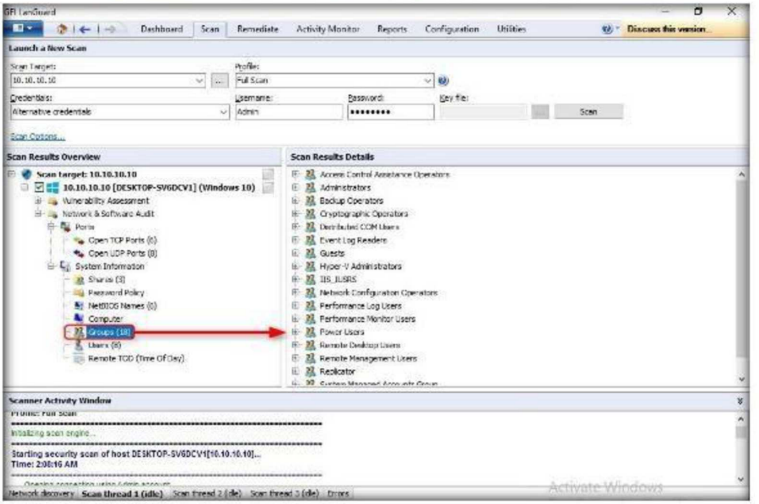

FIGURE 2.34: Information about the Groups

40. Click the **Dashboard** tab to display all the scanned network information. In real time, an attacker collects the vulnerability information about the target and develops exploits suitable to break into a network or single target.

FIGURE 2.35: Overview of the Scan in Dashboard

Lab Analysis

Document all the results, threats, and vulnerabilities discovered during the scanning and auditing process.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab

3

CGI Scanning with Nikto

Nikto Web Scanner is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems.

Lab Scenario

As an expert ethical hacker or penetration tester, you should have sound knowledge of different techniques used to scan a webserver and protect any websites/web applications before they are attacked. In this lab, you will learn to scan a web server for vulnerabilities.

Lab Objectives

This lab will help in understanding how to use nikto for web server scanning.

Lab Environment

To carry out this lab, following is required:

- Windows Server 2016 system
- Kali Linux virtual machine

Lab Duration

Time: 5 Minutes

Overview of Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers. It also scans server configuration items such as the presence of multiple index files, HTTP server options, and attempts to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated. Nikto is not a stealthy tool, it scans a webserver in the shortest time but gets logged in an IDS/IPS.

Lab Tasks

1. Log into the **Kali Linux** machine and open a **Terminal** window, and type **nikto -H** and press **Enter**.

FIGURE 3.1: Nikto help command

2. Here **-H** is the switch to find the available help commands within the Nikto. We will use the Tuning option to do a more deep and comprehensive scan of the target webserver.

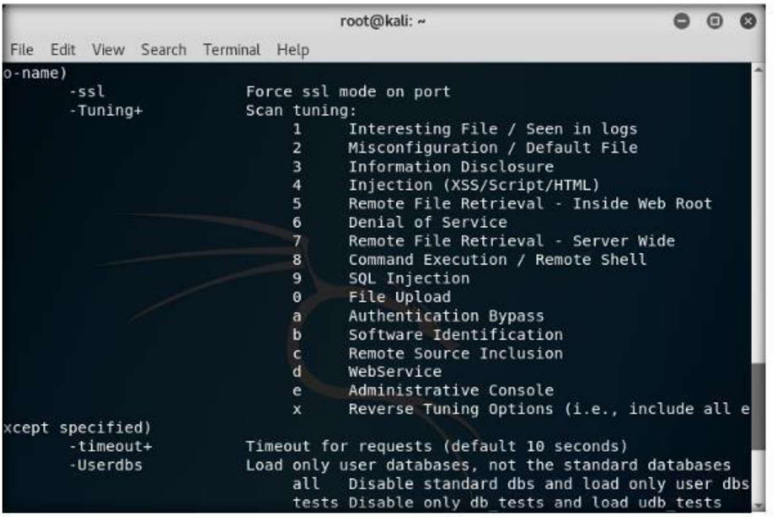

FIGURE 3.2: Nikto tuning options

3. In the terminal window, type **nikto -h http://www.certifiedhacker.com -Tuning x** and press **Enter**. Nikto starts the webserver scanning with all the tuning options enabled.

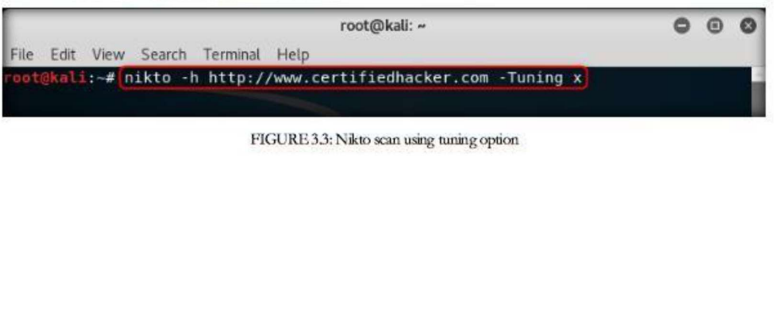

FIGURE 3.3: Nikto scan using tuning option

4. Here we find a cgi directory with OSVDB 3092 vulnerability. So, we will check for more cgi directories with the **-Cgidirs** option. In this option, search for specific directories or use the **all** option to search for all the available directories.

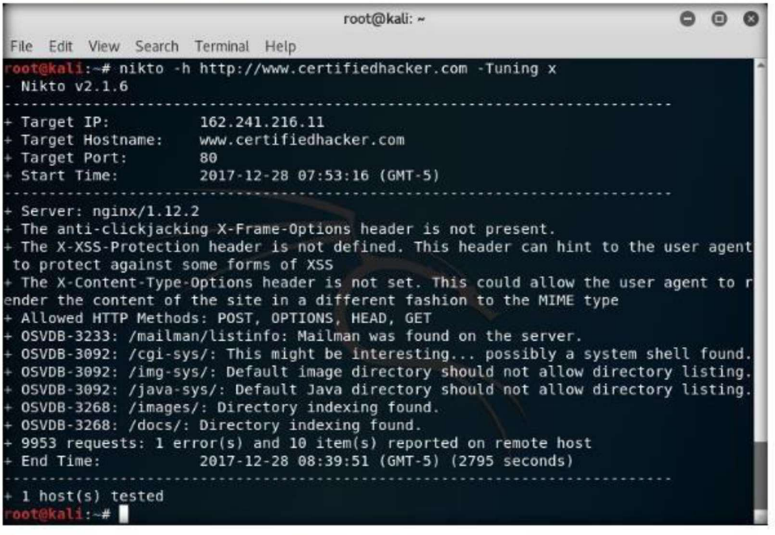

FIGURE 3.4: Nikto scan output

5. In the terminal window, type **nikto -h http://www.certifiedhacker.com -Cgidirs all** and hit **Enter**.

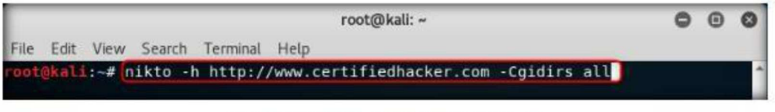

FIGURE 3.5: Nikto option to scan CGI directories

6. Nikto takes a little longer to scan the web server as it looks for vulnerable CGI directories. It scans the web server and lists out the directories as shown in the screenshot. Use the vulnerability ID to scan the vulnerability in detail.

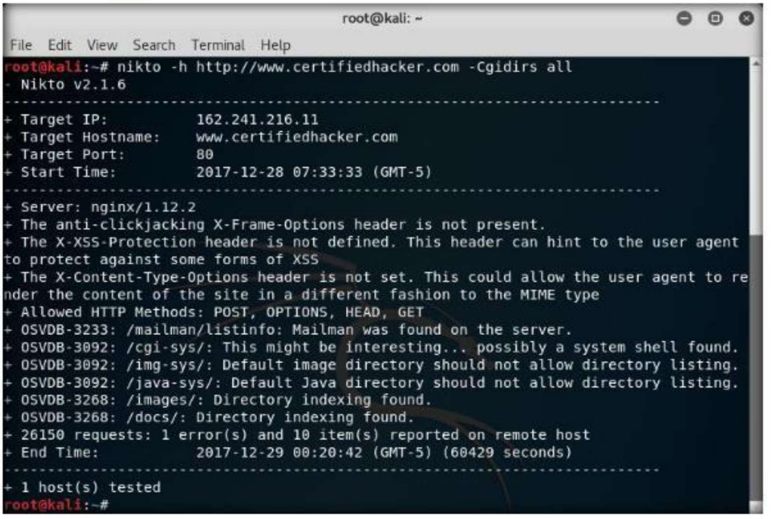

FIGURE 3.6: Nikto scan results

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs