

Vulnerability 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.

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.

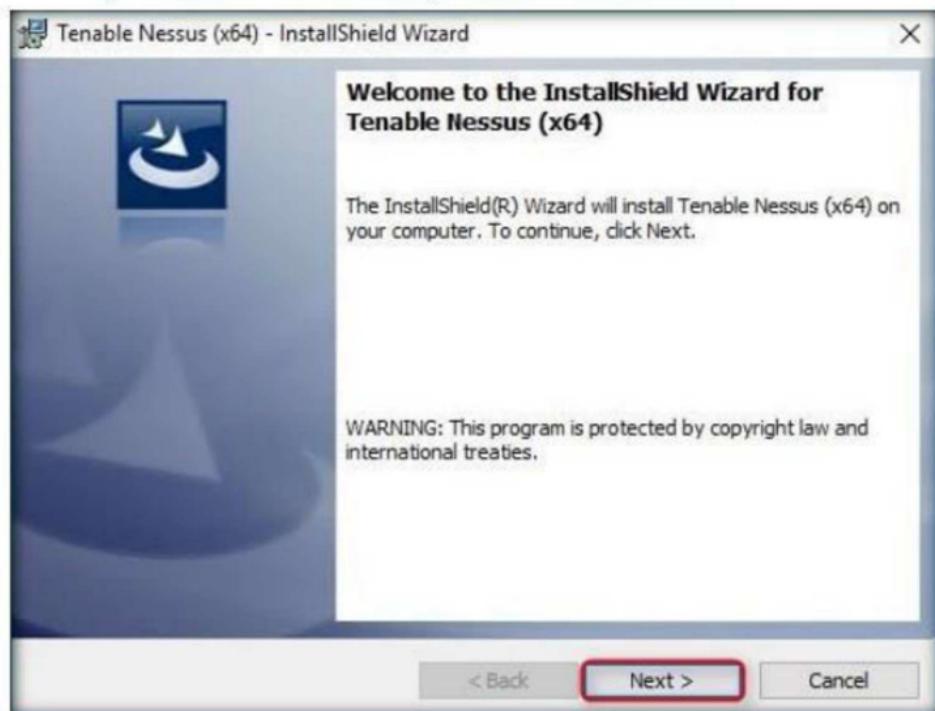


FIGURE 1.1: The Nessus Install Shield Wizard

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.

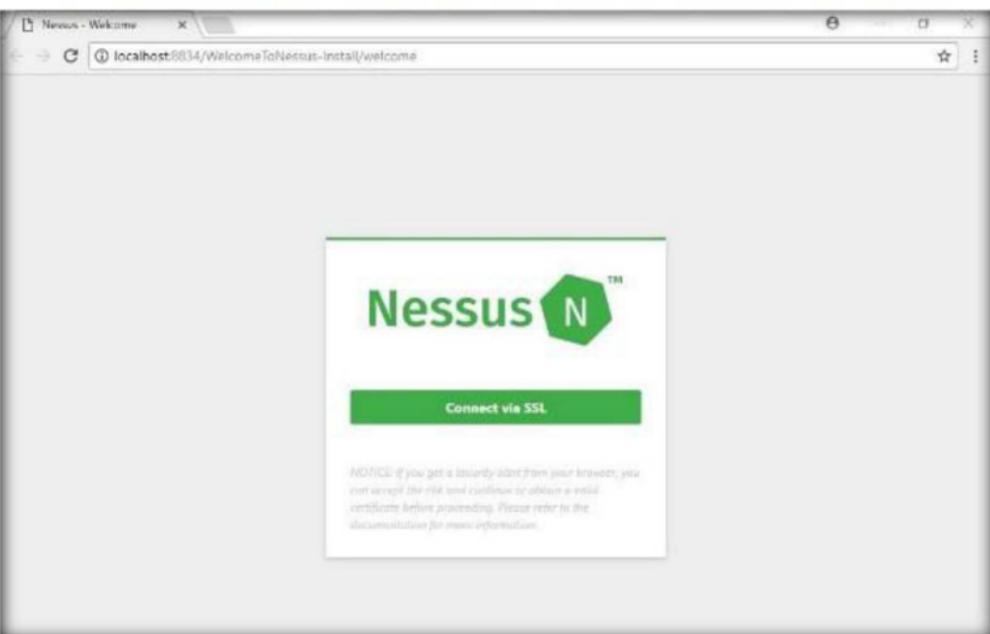


FIGURE 1.2: Nessus window

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**.

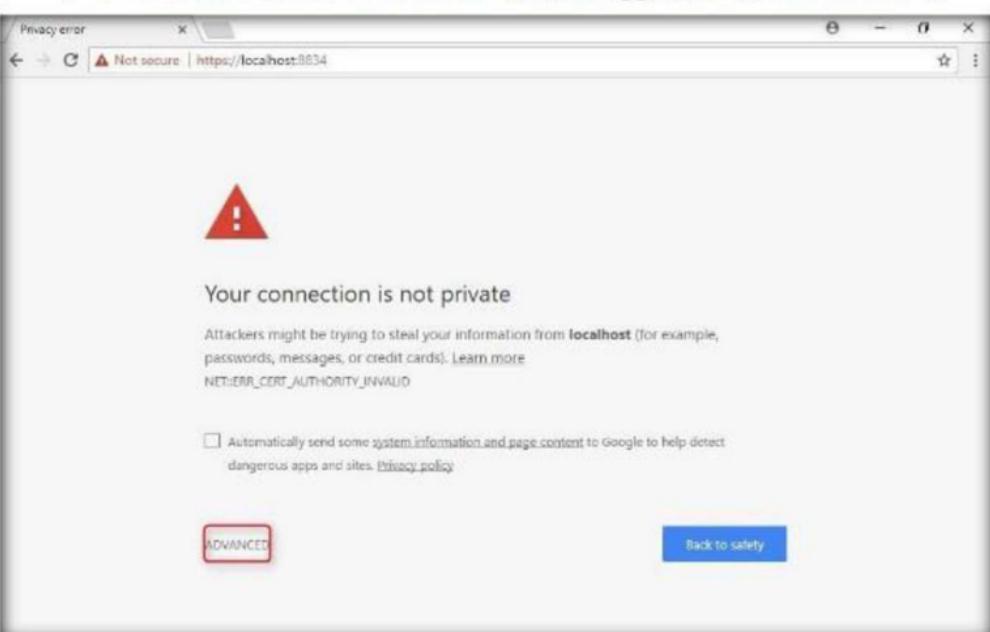


FIGURE 1.3: Browser Security Webpage

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

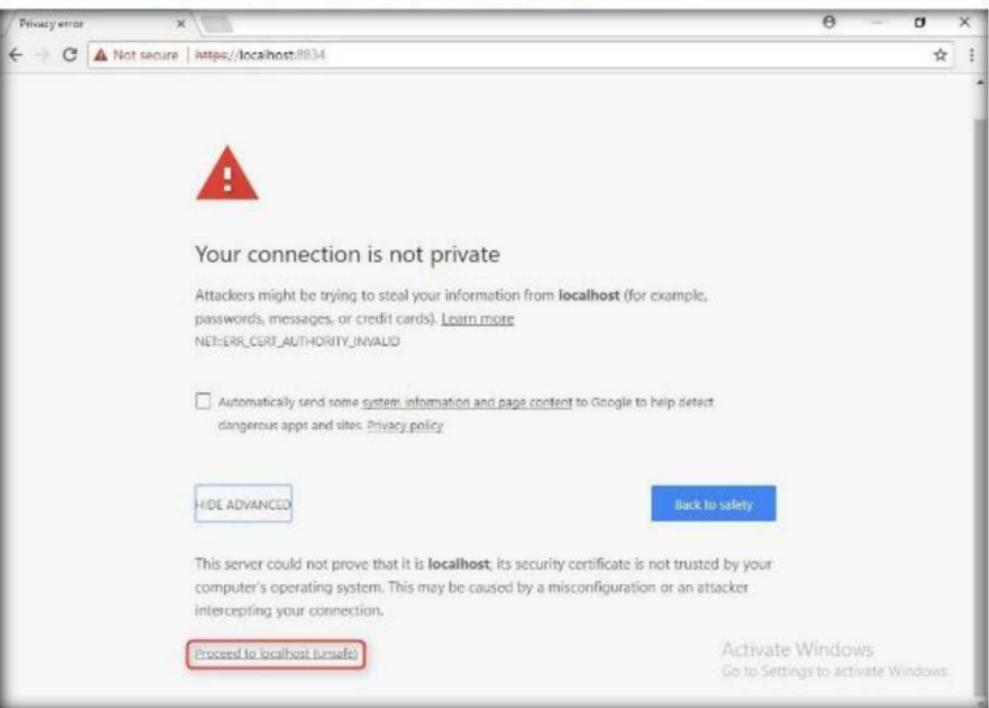


FIGURE 1.4: Browser Security Webpage

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

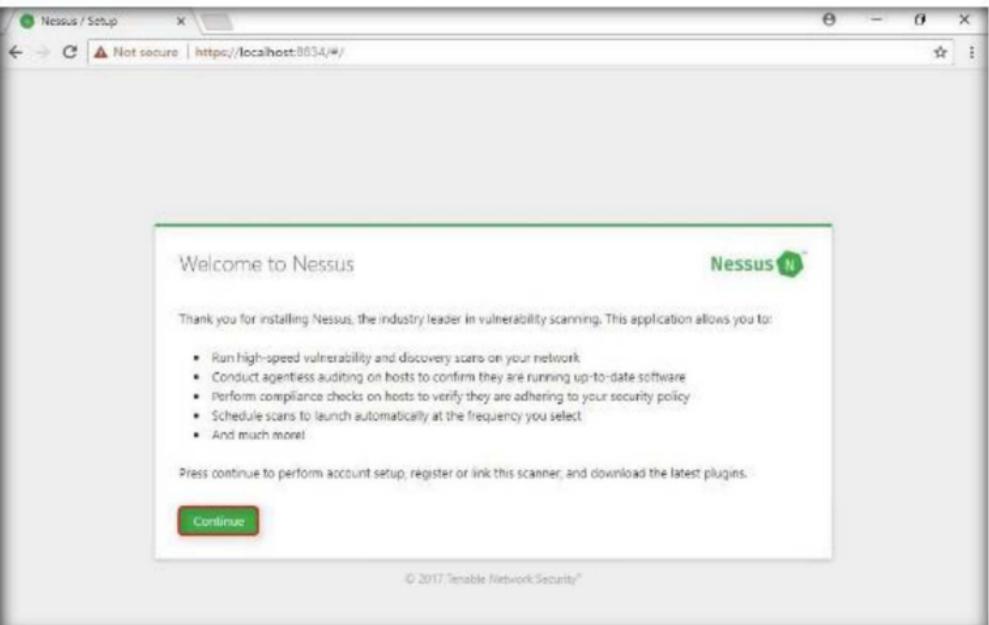


FIGURE 1.5: Welcome to Nessus window

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.

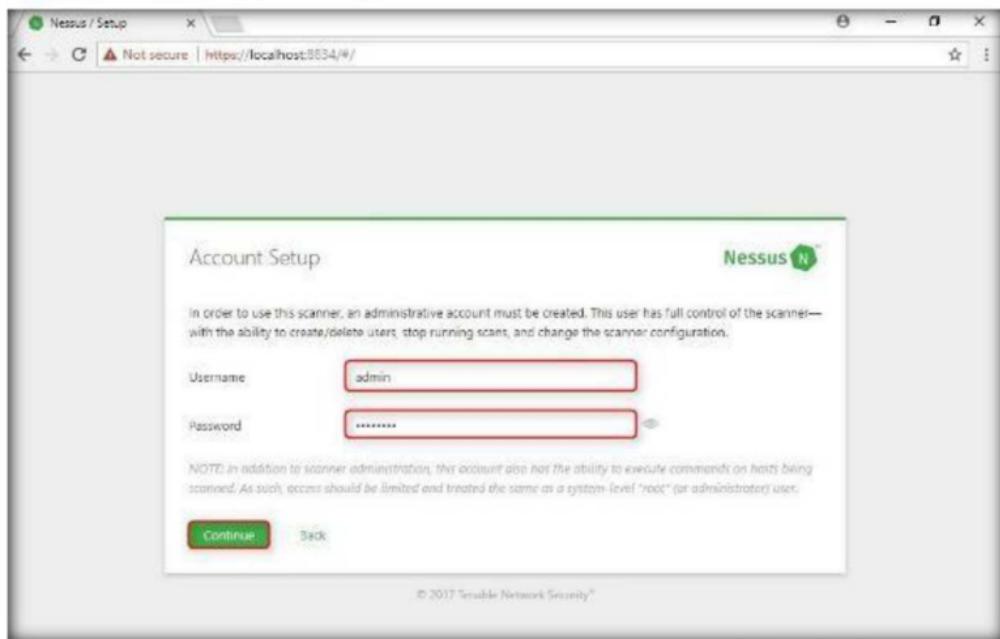


FIGURE 1.6: Account Setup window

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.

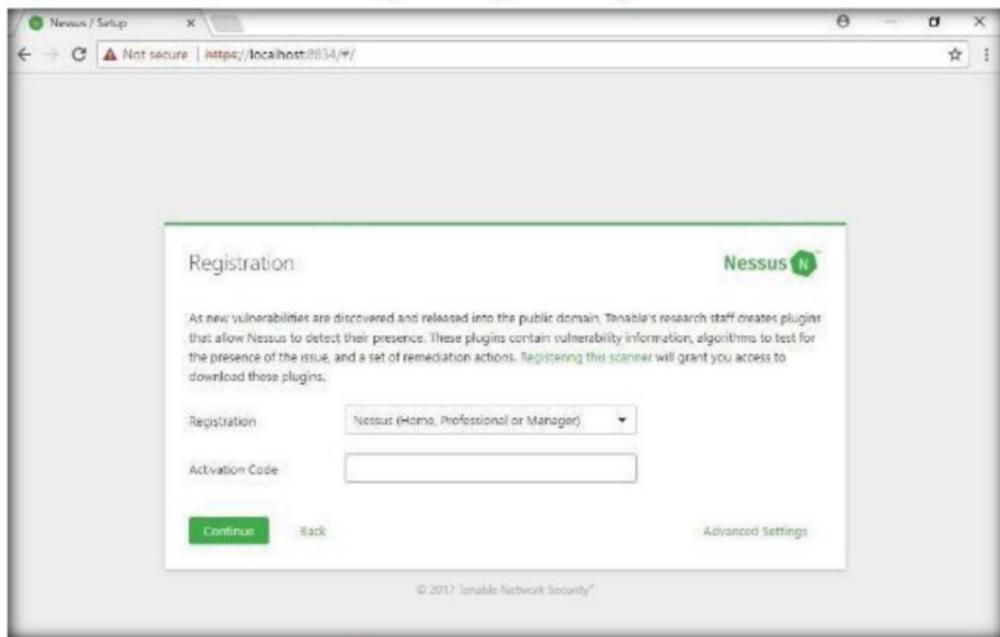


FIGURE 1.7: Plugin Feed Registration window

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.

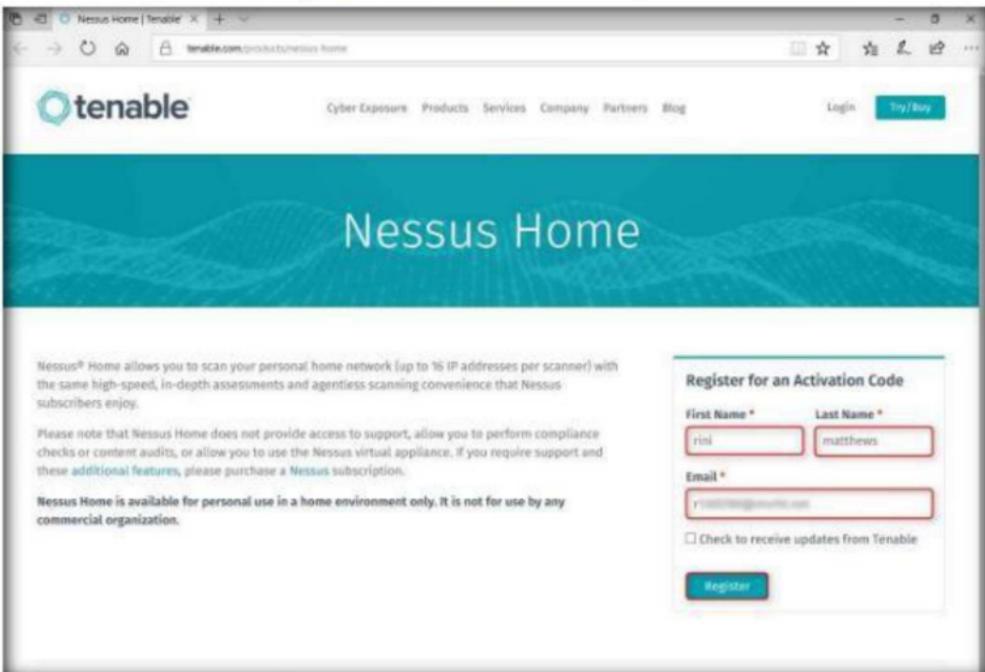


FIGURE 1.8: Registering with Nessus for an activation code

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.

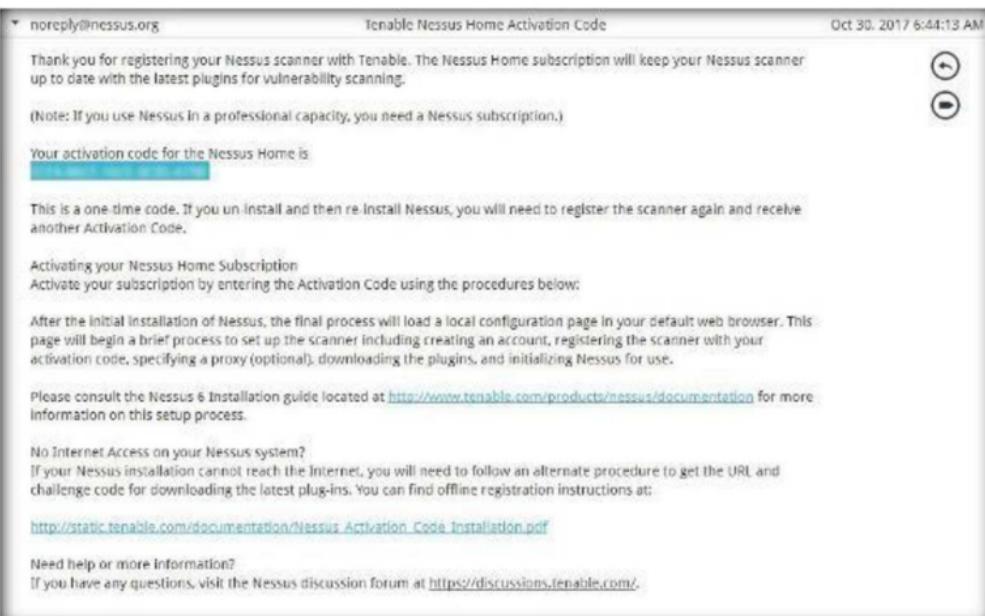


FIGURE 1.9: Activation code sent to your personal mail

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

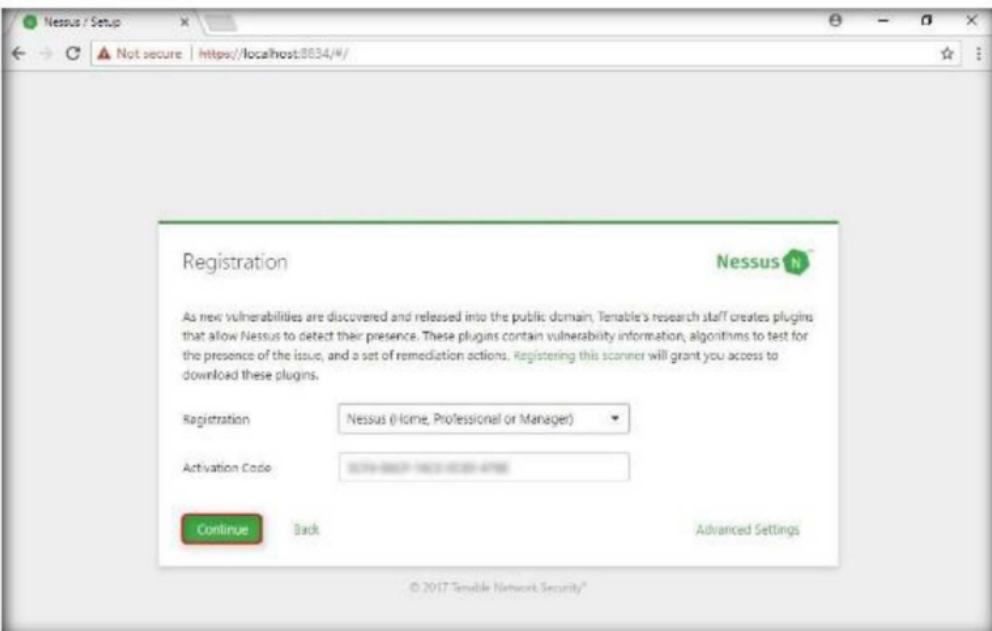


FIGURE 1.10: Registration window

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

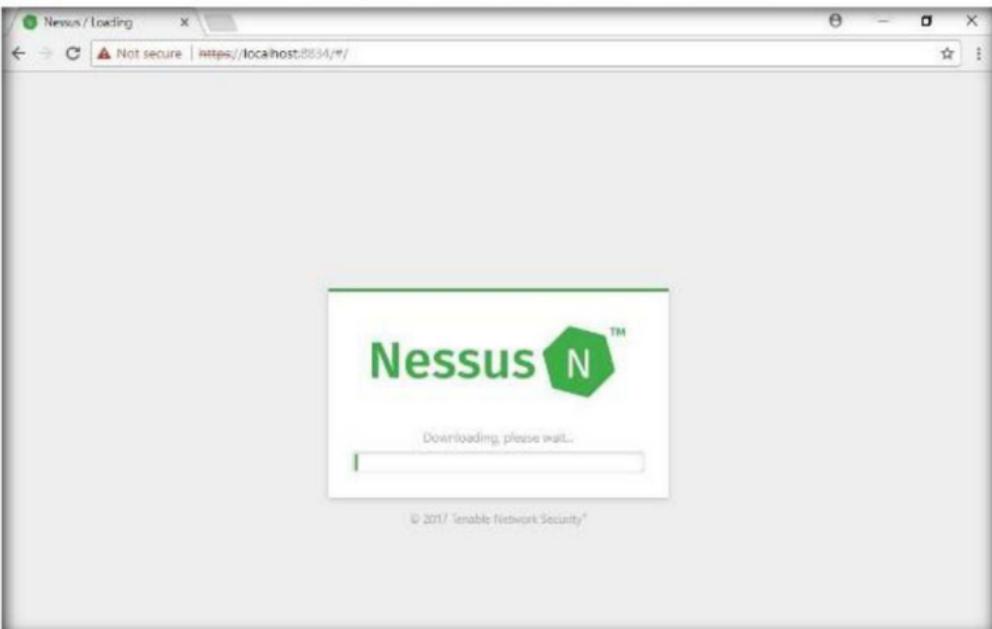


FIGURE 1.11: Nessus fetching the newest plugin set

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

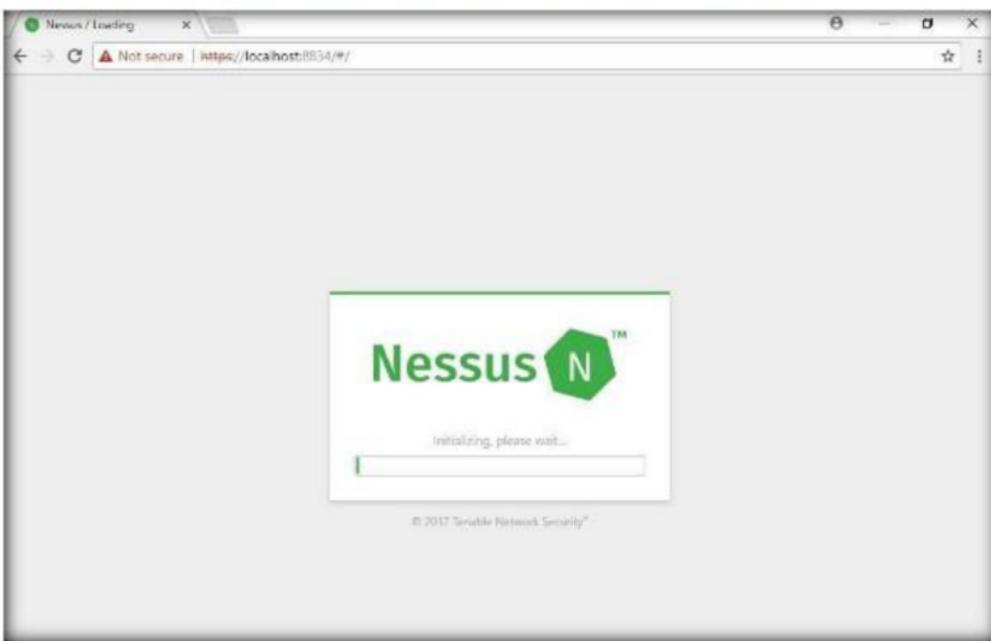


FIGURE 1.12: Nessus being initialized

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

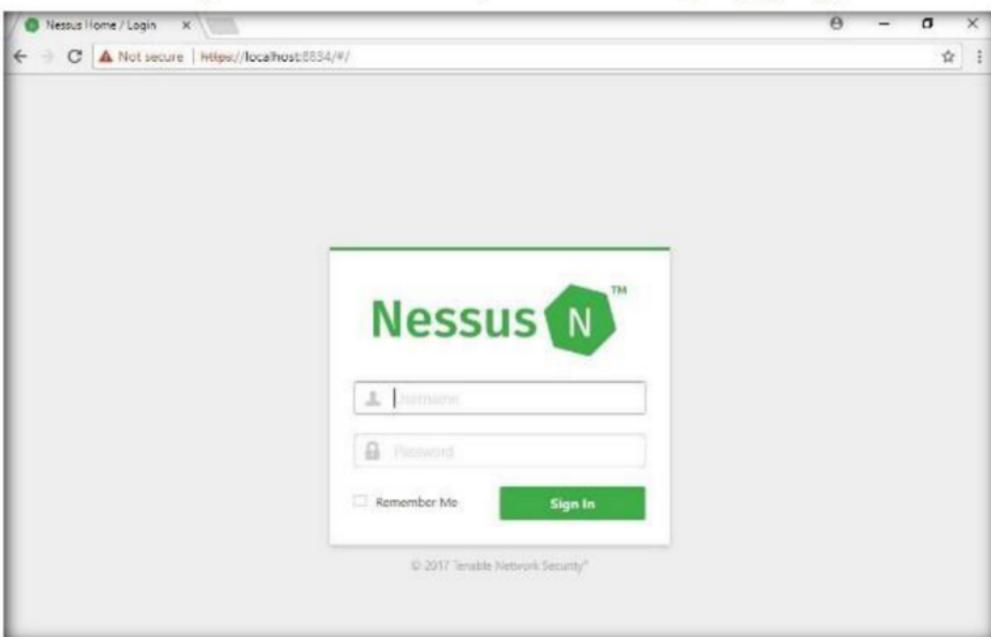


FIGURE 1.13: Nessus Log In screen

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

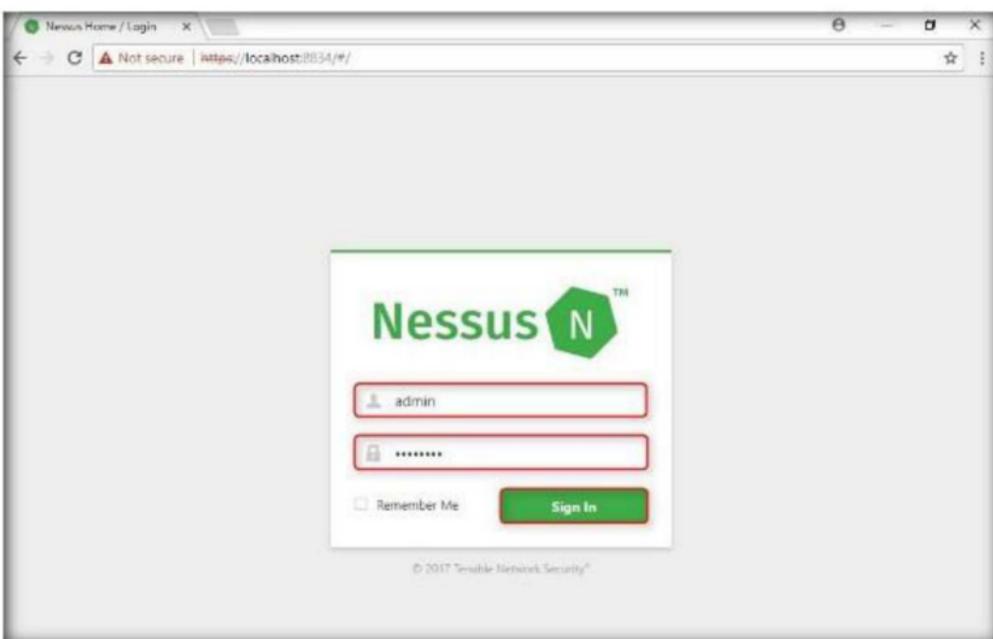


FIGURE 1.14: Signing into Nessus

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

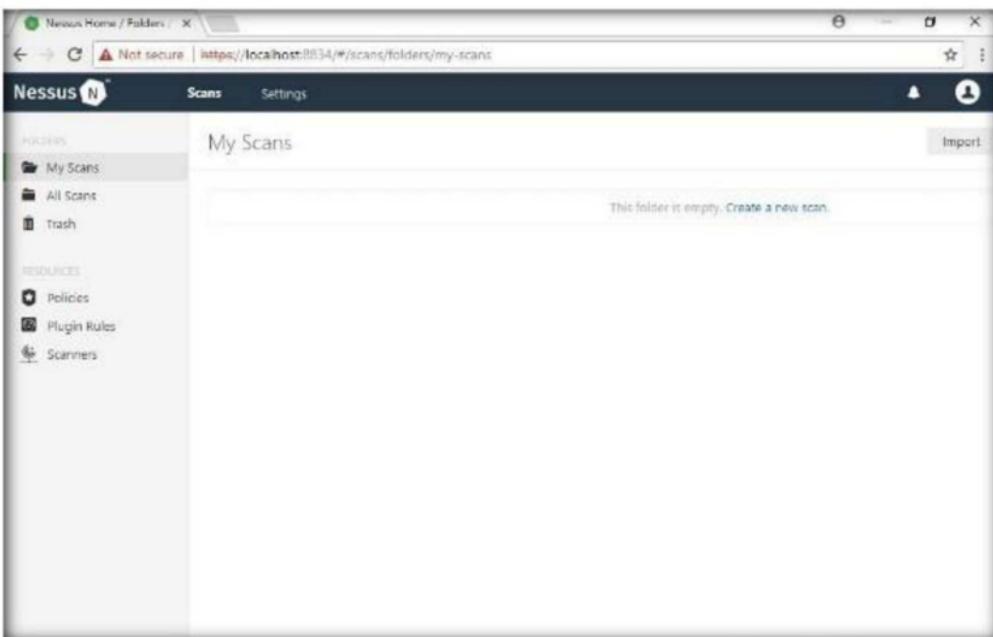


FIGURE 1.15: The Nessus Scans window

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

The screenshot shows the Nessus interface. The top navigation bar includes 'Nessus Home / Folders' and a warning about an 'Not secure' connection. Below the bar, there are tabs for 'Scans' and 'Settings'. On the left, a sidebar under 'FOLDERS' lists 'My Scans', 'All Scans', and 'Trash'. Under 'RESOURCES', the 'Policies' option is highlighted with a red box, while 'Plugin Rules' and 'Scanners' are also listed. The main content area is titled 'My Scans' and displays a message: 'This folder is empty. Create a new scan.' There is an 'Import' button in the top right corner.

FIGURE 1.16: The Nessus Policies window

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

This screenshot shows the 'Policies' page after selecting it from the sidebar. The top navigation bar and sidebar are identical to Figure 1.16. The main content area is titled 'Policies' and contains a circular icon with a gear and a star. A descriptive text block states: 'Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.' Below this, a message says 'No policies have been created.' followed by a red-bordered 'Create a new policy' button.

FIGURE 1.17: Adding a new policy in Nessus

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

This screenshot shows the 'Policy Templates' page. The top navigation bar and sidebar are consistent with previous figures. The main content area is titled 'Policy Templates' and has a 'Back to Policies' link. It features several templates: 'Advanced Scan' (selected and highlighted with a red border), 'Audit Cloud Infrastructure', 'Badlock Detection', 'Basic Network Scan', 'Credentialed Patch Audit', and 'DROWN Detection'. Each template has a small icon and a brief description.

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.

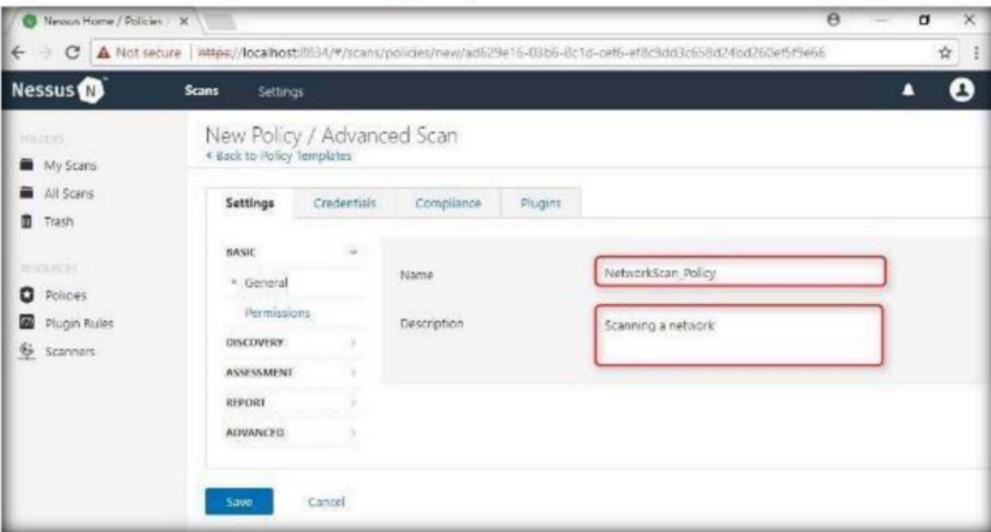


FIGURE 1.19: Customizing the general settings

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

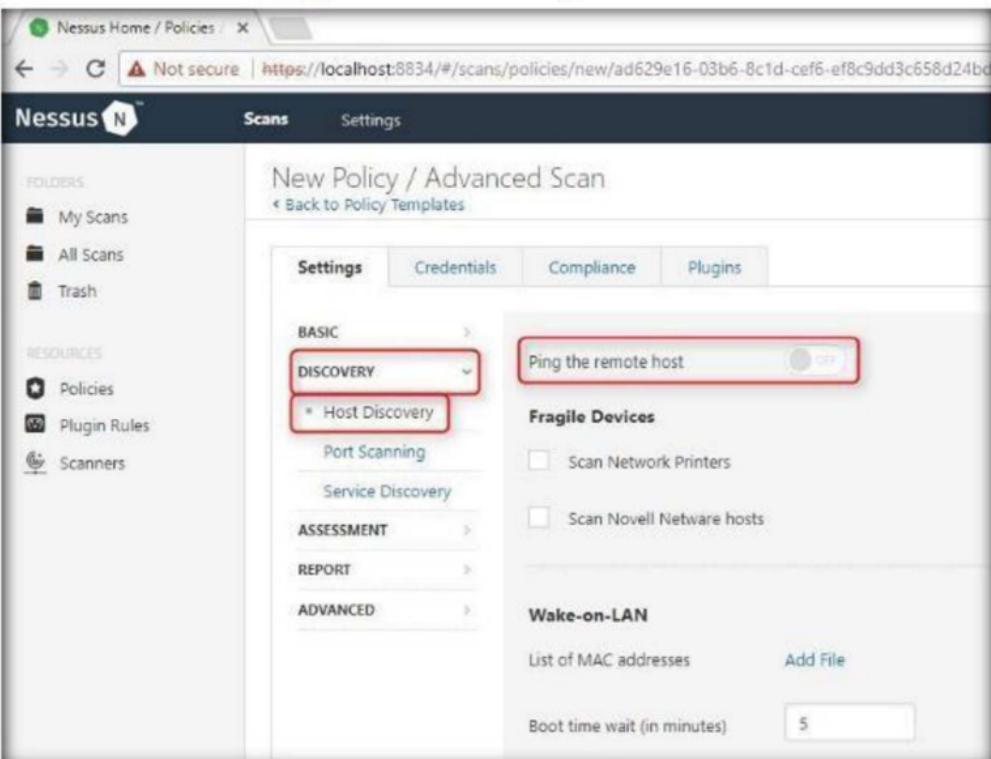


FIGURE 1.20: Policy General Settings window with Port Scanning Setting Type

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.

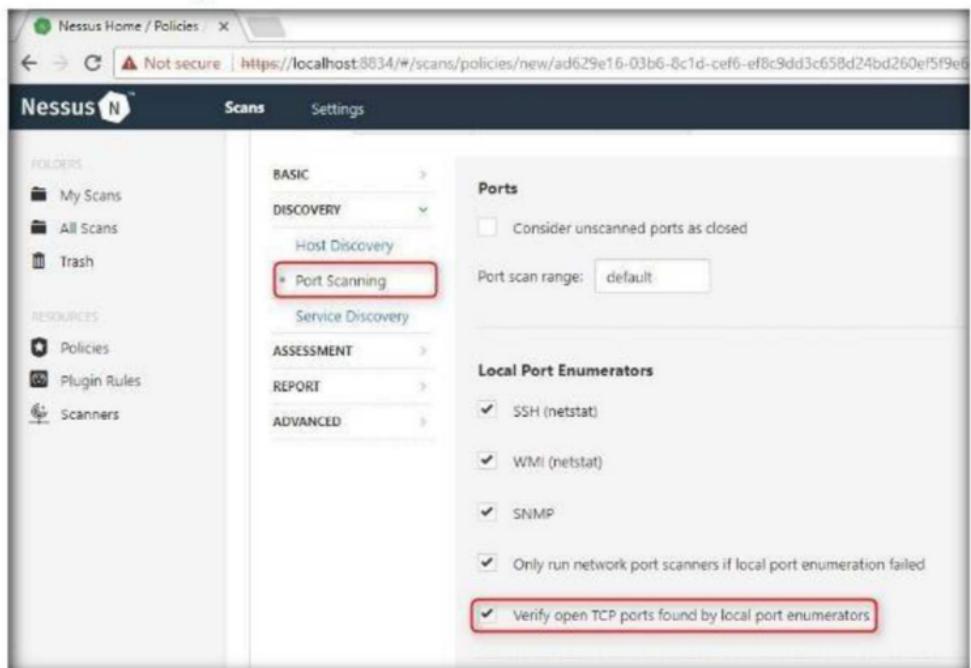


FIGURE 1.21: Customizing the Port Scanning Setting Type

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:

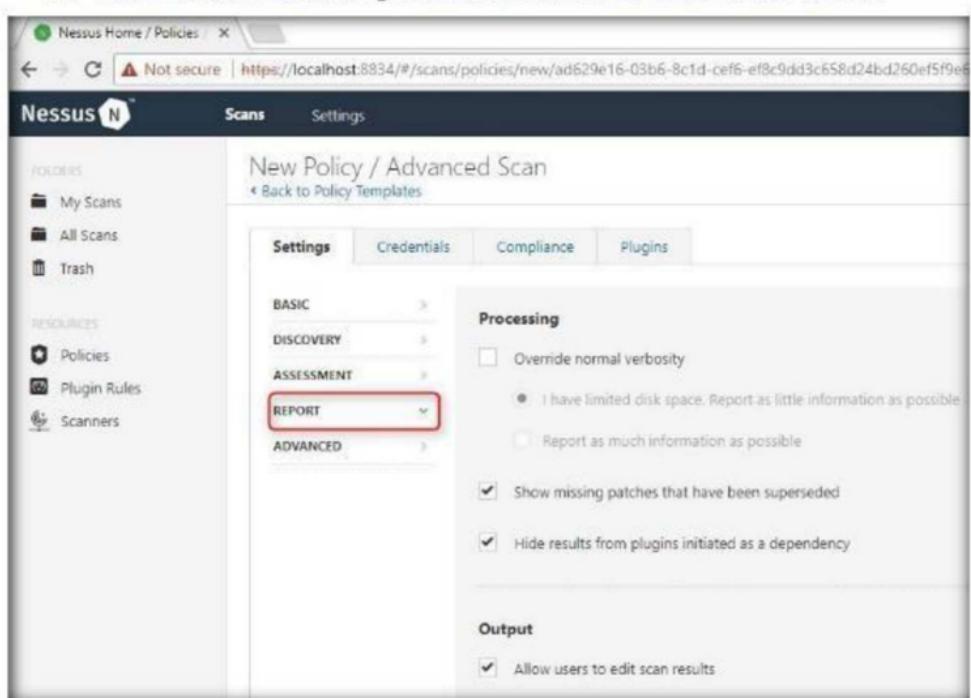


FIGURE 1.22: Policy General Settings window with Performance Setting Type

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

The screenshot shows the Nessus interface for creating a new policy. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Scanners). The main area is titled "New Policy / Advanced Scan" with a "Back to Policy Templates" link. A navigation bar at the top includes "Scans" and "Settings". Below it, tabs for "Settings", "Credentials", "Compliance", and "Plugins" are shown, with "Settings" being active. On the left, a sidebar lists "BASIC", "DISCOVERY", "ASSESSMENT", "REPORT", and "ADVANCED", with "ADVANCED" currently selected and highlighted with a red border. The main content area contains two sections: "General Settings" and "Performance Options". Under "General Settings", there are three checkboxes: "Enable safe checks" (checked), "Stop scanning hosts that become unresponsive during the scan" (unchecked), and "Scan IP addresses in a random order" (unchecked). Under "Performance Options", there are two checkboxes: "Slow down the scan when network congestion is detected" (unchecked) and "Network timeout (in seconds)" with a value of "5". There are also two input fields: "Max simultaneous checks per host" with a value of "5" and "Max simultaneous hosts per scan" with a value of "30".

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**.

This screenshot shows the same Nessus interface as Figure 1.23, but with specific settings changed. The "Max simultaneous checks per host" field now contains "unlimited" and the "Max simultaneous hosts per scan" field also contains "unlimited". The other settings remain the same as in Figure 1.23.

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:

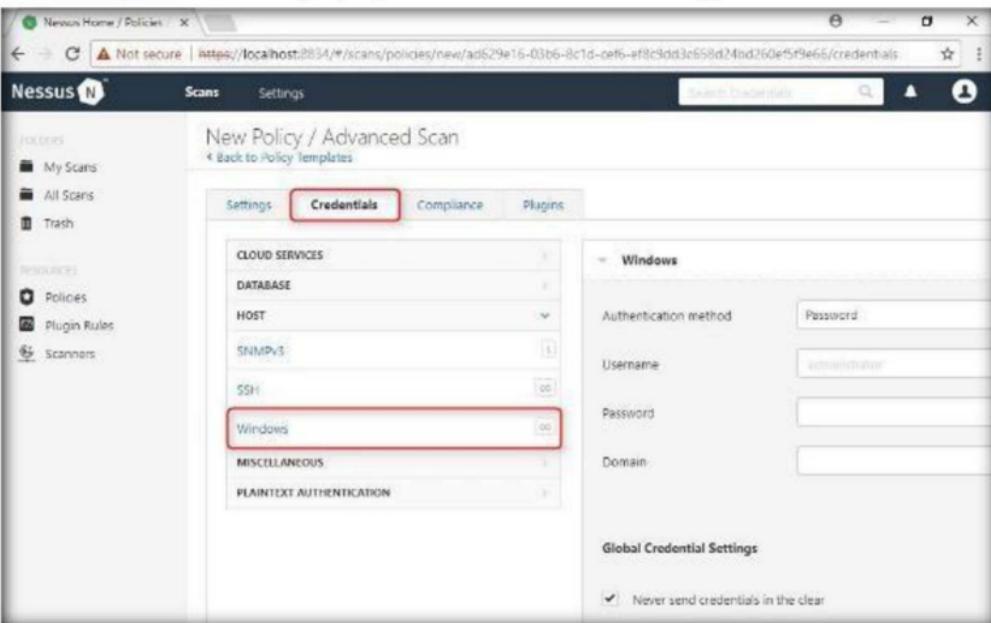


FIGURE 1.25: Adding Policies and setting Credentials

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

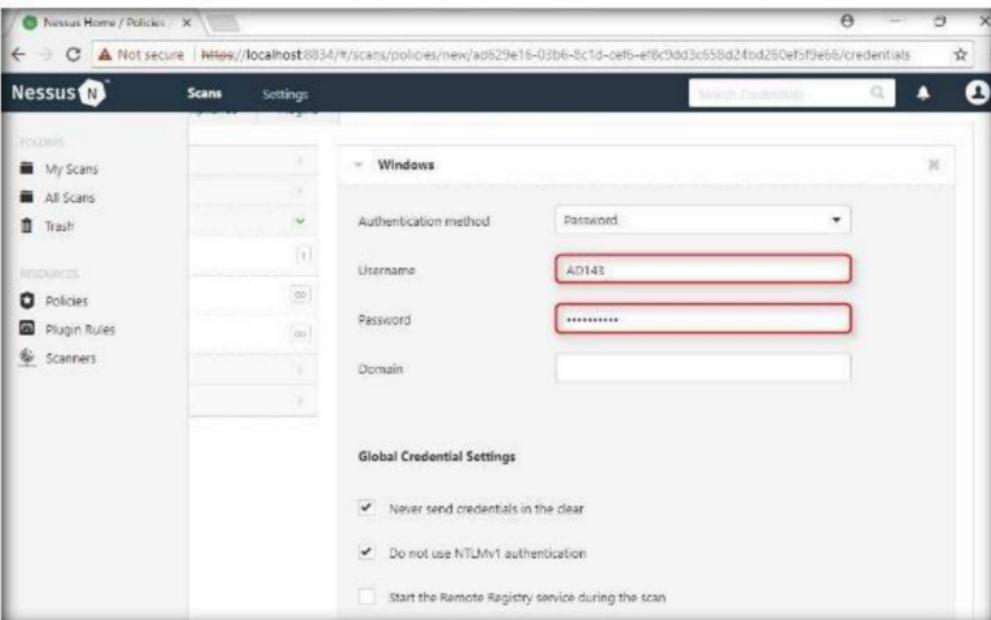


FIGURE 1.26: Customizing the windows credentials

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.**

The screenshot shows the Nessus interface for creating a new policy. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Polices, Plugin Rules, Scanners). The main area has tabs for 'Scans' and 'Settings'. Below that is a 'New Policy / Advanced Scan' section with a 'Back to Policy Templates' link. The 'Plugins' tab is selected, highlighted with a red border. A table lists various plugin families: AIX Local Security Checks (11385), Amazon Linux Local Security Checks (926), Backdoors (111), CentOS Local Security Checks (2489), CGI abuses (3701), CGI abuses : XSS (640), CISCO (875), Databases (549), Debian Local Security Checks (5097), and Default Unix Accounts (153). The status column indicates most are enabled. At the bottom are 'Save' and 'Cancel' buttons, and a Windows activation message: 'Activate Windows Go to Settings to activate Windows.'

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:**

The screenshot shows the Nessus 'Policies' page. The sidebar includes 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Polices, Plugin Rules, Scanners). The main area has a title 'Policies' and a success message 'Policy saved successfully.' in a red box. Below is a description of what policies are: 'Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.' There's a search bar 'Search Policies' and a table showing one policy: 'NetworkScan_Policy' (Template: Advanced Scan, Last Modified: Today at 9:20 PM).

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**.

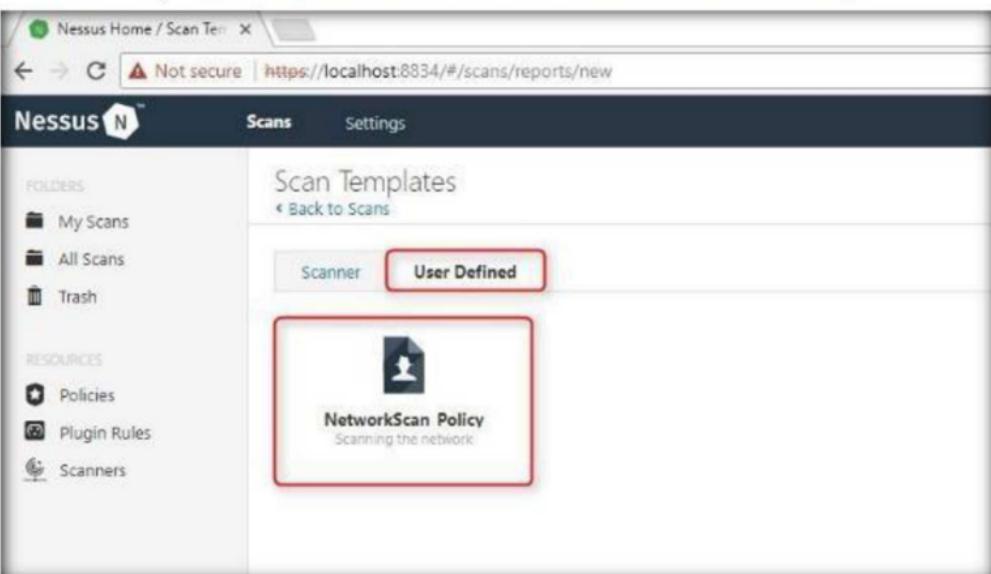


FIGURE 1.30: Setting a new scan in Nessus

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.

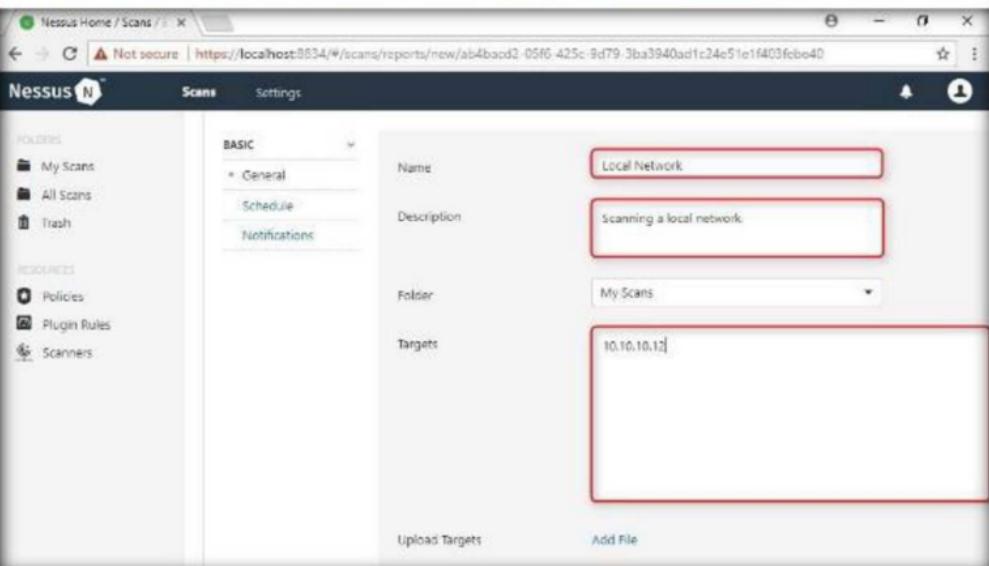


FIGURE 1.31: Configuring the basic settings in the scans window

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

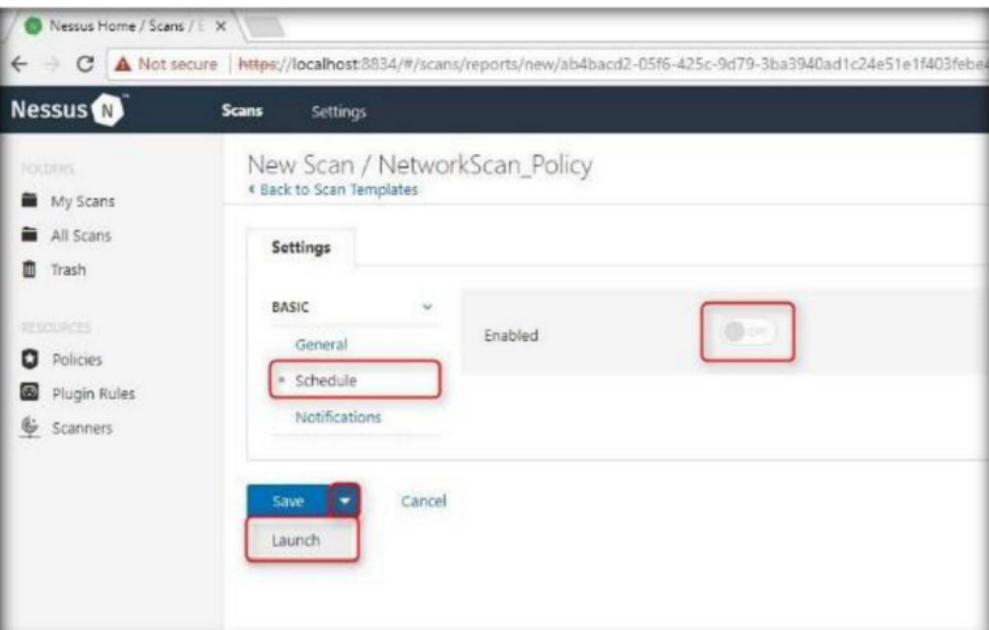


FIGURE 1.32: Setting a scan schedule

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

The screenshot shows the Nessus web interface. In the top left, it says "Nessus Home / Folders". The address bar indicates "Not secure | https://localhost:8544/#/scans/reports/l/history". The main navigation bar has tabs for "Scans" and "Settings". On the left sidebar under "FOLDERS", there are links for "My Scans", "All Scans", and "Trash". Under "RESOURCES", there are links for "Policies", "Plugin Rules", and "Scanners". The central content area is titled "Local Network" with a link to "Back to My Scans". Below this is a search bar with "Search history" and a dropdown for "History". A table shows one entry: "Start Time" (Current, Today at 9:42 ...), "End Time" (N/A), and "Status" (Running). A red box highlights this row. To the right, a panel titled "Scan Details" shows fields for Name (Local Network), Status (Running), Policy (On Demand), Scanner (Nmap), and Start (Today at 9:42). A message box at the top right says "Scan saved successfully."

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.

The screenshot shows the Nessus web interface. The top left says "Nessus Home / Folders". The address bar shows "Not secure | https://localhost:8544/#/scans/folders/my-scans". The main navigation bar has tabs for "Scans" and "Settings". The left sidebar under "FOLDERS" includes "My Scans" (which is highlighted in blue), "All Scans", and "Trash". Under "RESOURCES", there are links for "Policies", "Plugin Rules", and "Scanners". The central content area is titled "My Scans" with a "Import" button. It shows a table with one row: "Name" (Local Network), "Schedule" (On Demand), and "Last Modified" (Today at 9:55). A red box highlights the "Local Network" row.

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:

The screenshot shows the Nessus interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Scanners), and a 'Scans' tab. The main area has a 'History' section with a search bar and a count of '1 Host'. Below it is a 'Vulnerabilities' section with a red-bordered chart showing 66 vulnerabilities across four categories: Critical (red), High (orange), Medium (yellow), and Low (green). To the right is a 'Scan Details' box with the following information:

Name:	Local Network
Status:	Completed
Policy:	NetworkScan_Policy
Scanner:	Local Scanner
Start:	Today at 9:51 PM
End:	Today at 9:55 PM
Elapsed:	4 minutes

Below the details is another 'Vulnerabilities' section with a donut chart and a legend: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

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.

This screenshot shows the 'Vulnerabilities' tab for the 'Local Network / 10.10.10.12' host. The interface includes a 'Configure' button, a 'Filter' dropdown, a search bar, and a count of '53 Vulnerabilities'. A red-bordered table lists the vulnerabilities:

Sev	Name	Family	Count
Critical	Microsoft Windows SMBv1 Multiple Vuln...	Windows	1
Critical	MS14-086: Vulnerability in Schannel Coul...	Windows	1
Critical	MS17-010: Security Update for Microsoft...	Windows	1
Medium	MS16-047: Security Update for SAM and ...	Windows	2
Medium	Microsoft Windows Remote Desktop Pro...	Windows	1
Medium	SSL 64-bit Block Size Cipher Suites Supp...	General	1
Medium	SSL Certificate Cannot Be Trusted	General	1
Medium	SSL Certificate Signed Using Weak Hashi...	General	1
Medium	SSL Certificate with Wrong Hostname	General	1

At the bottom right, there's a message: 'Activate Windows! Go to Settings to activate'.

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.

The screenshot shows the Nessus web interface. On the left, there's a sidebar with 'Scans' (selected), 'Settings', 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Scanners), and 'Local Network / 10.10.10.12' (Configure). The main area is titled 'Vulnerabilities' with 53 results. A search bar and filter options ('Filter', 'Search Vulnerabilities') are at the top. The results table has columns for 'Name', 'Family', 'Count', and edit icons. One row is highlighted with a red border: 'Microsoft Windows SMBv1 Multiple Vuln...' (Windows, Critical, 1). Other rows include 'MS14-066: Vulnerability in Schannel Coul...' (Windows, Critical, 1) and 'MS17-010: Security Update for Microsoft...' (Windows, Critical, 1). A partially visible row at the bottom is 'MS16-047: Security Update for SAM and ...' (Windows, Medium, 2).

FIGURE 1.37: Selecting vulnerability

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

The screenshot shows the detailed report for the selected vulnerability. The title is 'Microsoft Windows SMBv1 Multiple Vulnerabilities'. The report states: 'The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities:'. It lists three types of vulnerabilities: information disclosure (CVE-2017-0287, CVE-2017-0288, CVE-2017-0271, CVE-2017-0274, CVE-2017-0273, CVE-2017-0280), denial of service (CVE-2017-0289, CVE-2017-0273, CVE-2017-0280), and remote code execution (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279). It notes that depending on the host's security policy configuration, the plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (e.g., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version: 100034, 100033, 100037, 100059, 100060, or 100061. The 'Solution' section advises applying the applicable security update for your Windows version. The 'Plugin Details' section includes severity (Critical), ID (100484), version (Revision 1.2.1), type (remote), family (Windows), published date (May 26, 2017), and modified date (August 15, 2017). The 'Risk Information' section shows risk factor (Critical), CVSS Base Score (10.0), CVSS Temporal Score (7.4), CVSS Vector (CVSS:3.0/AV:N/AC:L/PR:N/C:L/I:C/D:L), and CVSS Temporal Vector (CVSS:3.0/EU/R/L/D/C/I/C). The 'Vulnerability Information' section lists CPE (cpe:/o:microsoft:windows), exploit availability (false), known exploits (none), and patch publication date (May 9, 2017).

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.

The screenshot shows the Nessus web interface. On the left, there's a sidebar with sections for 'Discoveries', 'Resources', and 'Scanners'. The main area is titled 'My Scans' and contains a table with one row. The row for 'Local Network' has a red border, indicating it is selected. The table columns are 'Name', 'Schedule', and 'Last Modified'. The 'Local Network' entry shows 'On Demand' under Schedule and 'Today at 9:33 PM' under Last Modified.

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.

This screenshot shows the 'Local Network' scan details page. The left sidebar is identical to Figure 1.39. The main content area displays the 'Scan Details' for the 'Local Network' scan. It includes fields for Name (Local Network), Status (Completed), Policy (NetworkScan_Policy), Scanner (Local Scanner), Start (Today at 9:31 PM), End (Today at 9:35 PM), and Elapsed (4 minutes). Below this, a 'Vulnerabilities' section features a donut chart with segments for Critical, High, Medium, Low, and Info levels. On the right side of the main content area, there's a vertical menu under 'Export' with options: Nessus, PDF, HTML (which is highlighted with a red box), CSV, and Nessus DB.

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.

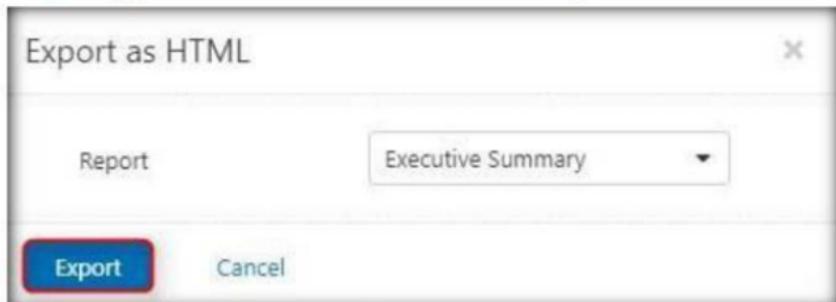


FIGURE 1.41: Export as HTML window appears

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

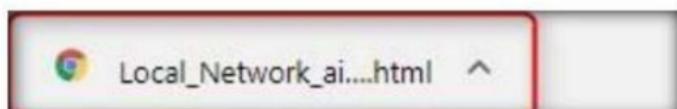


FIGURE 1.42: Chapters Added to Report Content

57. Choose a browser to view the HTML file.

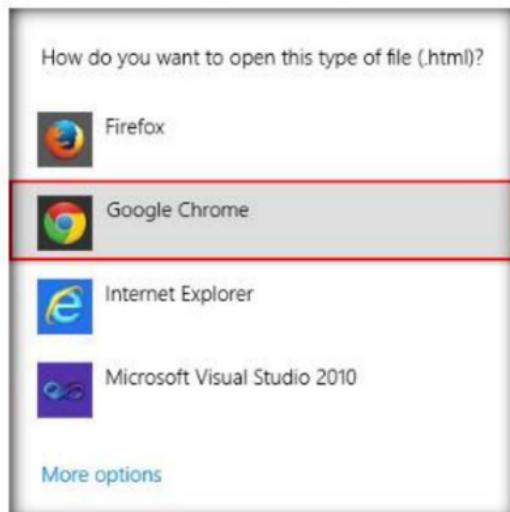


FIGURE 1.43: Choosing a browser to view the HTML.

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

Note: Screenshots might differ in your lab environment.

A screenshot of a web browser window displaying the Nessus Scan Report. The title bar shows 'Nessus Home / Reports' and the address bar shows 'file:///C:/Users/Administrator/Downloads/Local_Network_aigb3.html'. The page header features the Nessus logo and the text 'vulnerability scanner'. Below the header is the 'Nessus Scan Report' section, which includes the date 'Mon, 30 Oct 2017 21:51:22 Pacific Standard Time'. A 'Table Of Contents' section lists 'Hosts Summary (Executive)' and 'Hosts Summary (Executive)'. Under 'Hosts Summary (Executive)', there are buttons for '[+] Collapse All' and '[-] Expand All'. The '192.168.10.12' host summary is expanded, showing a 'Summary' table and a 'Details' table. The 'Summary' table has columns for 'Critical', 'High', 'Medium', 'Low', 'Info', and 'Total'. The 'Details' table lists vulnerabilities with columns for 'Severity', 'Plugin Id.', and 'Name'. Two critical vulnerabilities are listed: one for a SMB exploit and another for ETERNALBLUE.

FIGURE 1.44: Vulnerability Report Displayed in HTML Format

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

The screenshot shows a Nessus Scan Report for host 192.168.1.12. The table lists vulnerabilities categorized by severity: Critical, High, Medium, Low, Info, and Total. A specific vulnerability is selected, highlighted with a red border. The selected row contains the following data:

192.168.1.12					
Summary					
Critical	High	Medium	Low	Info	Total
3	9	10	2	38	53
Details					
Severity	Plugin ID	Name			
Critical (10.0)	29628	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)			
Critical (10.0)	53333	MS17-018: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNTHY) (WannaCry) (EternalRocks) (Felix) (uncredentialed check)			
Critical (10.0)	121454	Microsoft Windows SMBv1 Multiple Vulnerabilities			
Medium (7.0)	30512	MS16-047: Security Update for SAM and LSAD Remote Protocols (3140627) (Badlock) (uncredentialed check)			
Medium (5.0)	51152	SSL Certificate Cannot Be Trusted			
Medium (5.0)	57382	SSL Self-Signed Certificate			
Medium (5.0)	10405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness			
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported			
Medium (5.0)	65411	SSL Certificates with Wrong Hashnames			
Medium (5.0)	84437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)			
Medium (4.0)	52559	Terminal Services Encryption Level Is Medium or Low			
Medium (4.0)	58452	Terminal Services Doesn't Use Network Level Authentication (NLA) Only			
Medium (4.0)	25291	SSL Certificate Signed Using Weak Hashing Algorithm			

FIGURE 1.45: Viewing a Vulnerability in the Report

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

The screenshot shows the details for the selected vulnerability, MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check). The page includes the Tenable logo and navigation links. The main content area displays the synopsis, description, and family information.

Synopsis:
The remote Windows host is affected by a remote code execution vulnerability.

Description:
The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Family: Windows
Nessus Plugin ID: 79638 ()
Bugtraq ID: 70954
CVE ID: CVE-2014-6321

Ready to Amp Up Your Nessus Experience?

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**.

The screenshot shows the Nessus web interface. On the left, there's a sidebar with options like 'My Scans', 'All Scans', 'Trails', 'Policies', 'Plugin Rules', and 'Scanners'. The main content area is titled 'Local Network / Plugin #100464' and shows a 'Vulnerabilities' tab with 53 results. A specific finding is highlighted: 'Microsoft Windows SMBv1 Multiple Vulnerabilities'. The 'Description' section states: 'The remote windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities.' Below this, a note says: '- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. [CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276]'.

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

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**.

The screenshot shows the GFI Software website's registration page. At the top, there are navigation links for LANGUAGE, BLOG, CONTACT US, and BUY NOW. The GFI Software logo is centered above a blue header bar that reads "Confirm your GFI Account trial registration". Below this, a message says "Please enter your details and a password in the fields below to setup your GFI Account.". The page is divided into two main sections: "Contact details" and "Login details". The "Contact details" section contains five input fields: first name ("rini"), last name ("matthews"), company ("XXXXXXXXXX"), address ("XXXXXXXXXX"), and state ("Puerto Rico"). The "Login details" section contains three input fields: email ("rini@xxxxxxxxxx"), password ("XXXXXXXXXX"), and confirm password ("XXXXXXXXXX"). A large green button at the bottom right of the form area is labeled "GET STARTED FOR FREE". At the very bottom of the page, there is a footer with links for Products and Services, Partners, Company, Support, Store, and GFI TechTalk.

FIGURE 2.1: GFI LanGuard Registration page

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

The screenshot shows the GFI Software website with the URL [https://www.gfi.com/languard/Downloads/GFI_LanGuard_Confirmation.aspx](#). The main heading is "Thank you for downloading GFI LanGuard". Below it, there's a note about logging in with a GFI Account and a link to download the evaluation key if it didn't start automatically. It also mentions a 30-day evaluation period via email and links for product documentation and a short video. At the bottom, there's a "Downloads" section showing the file "GFI LanGuard 12.2 (build: 20170912)" with a size of 301,606 KB and a "Download Now" button.

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.

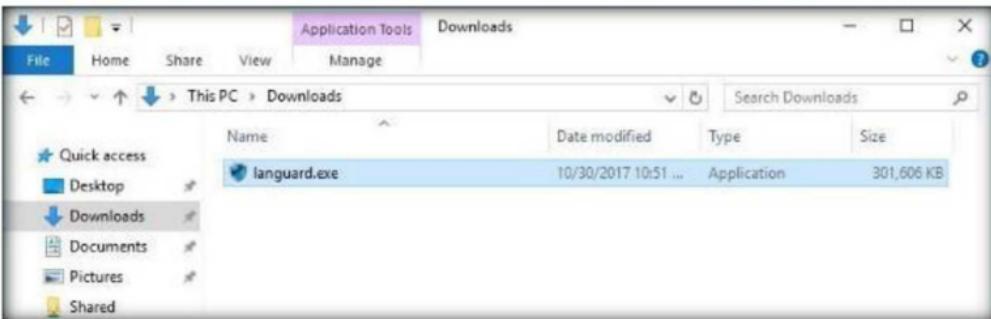


FIGURE 2.3: GFI LanGuard exe file

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

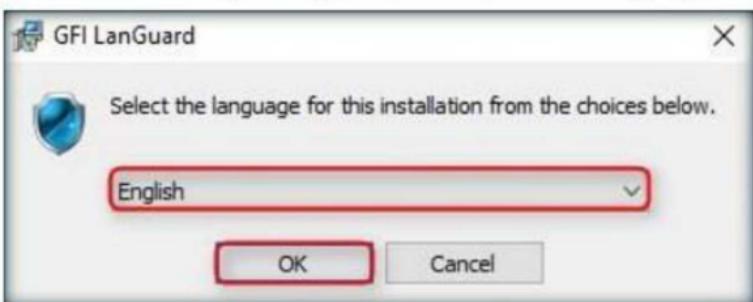


FIGURE 2.4: Selecting a language

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

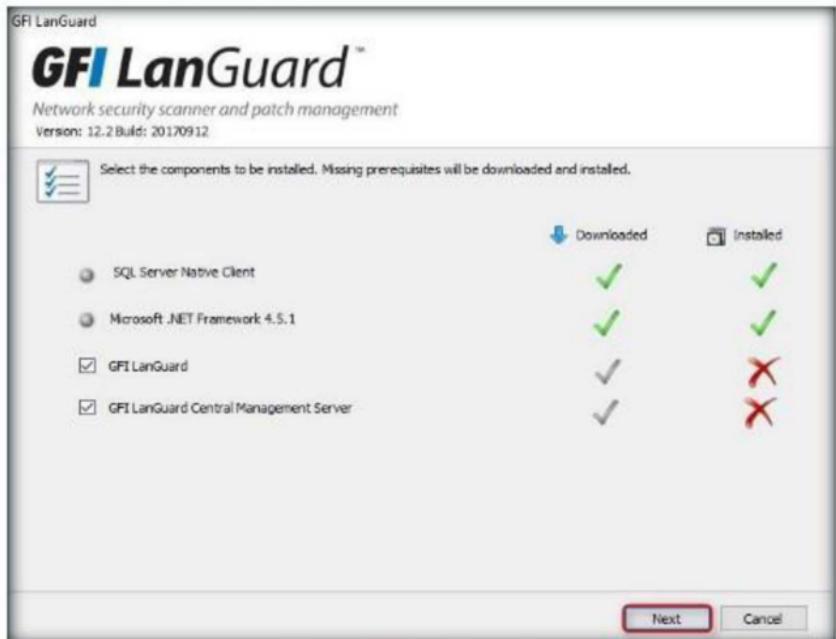


FIGURE 2.5: Installation wizard

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**.

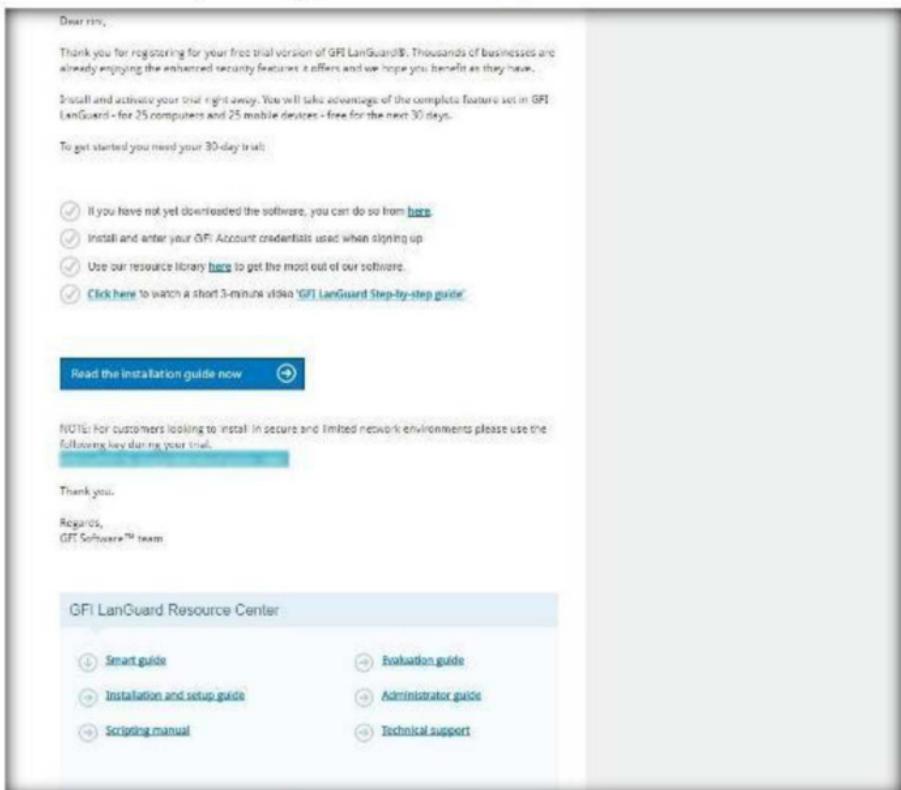


FIGURE 2.7: GFI LanGuard Trial Key

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

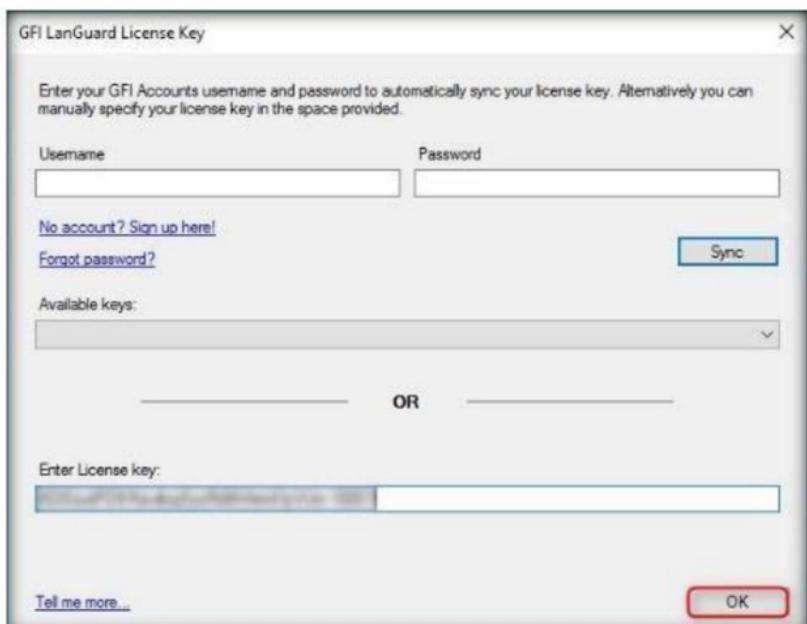


FIGURE 2.8: GFI LanGuard License window

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**.

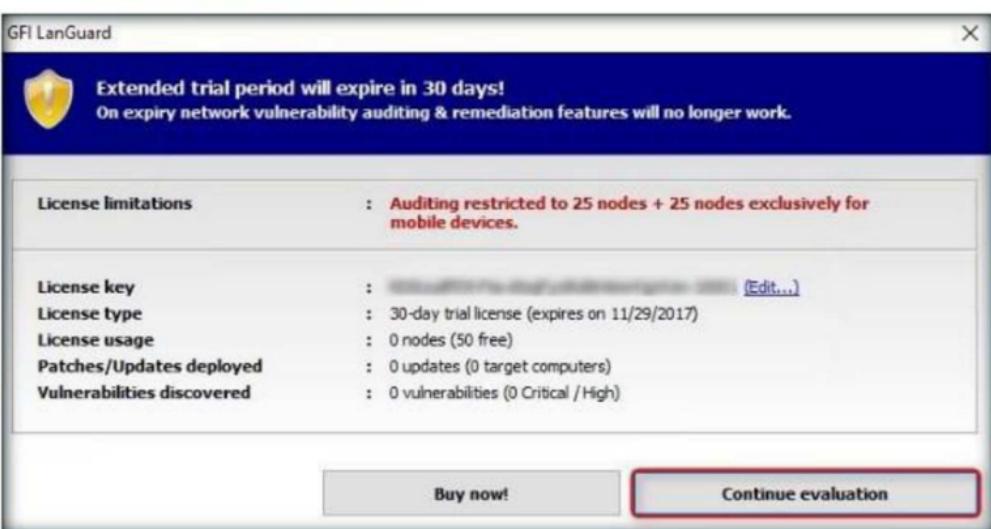


FIGURE 2.18: GFI LanGuard pop-up

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.**

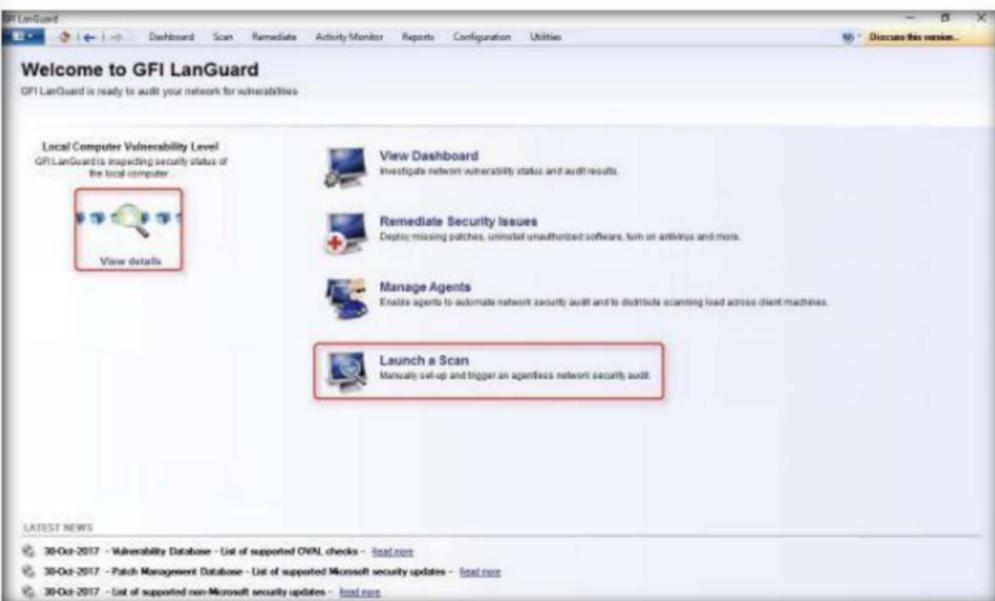


FIGURE 2.19: Launching a scan in GFI LanGuard

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

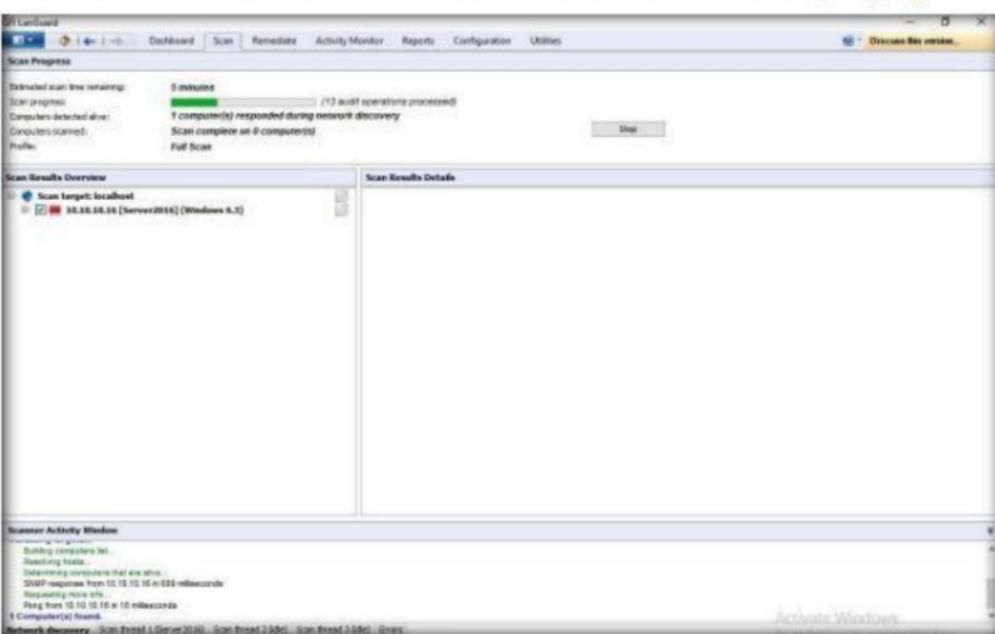


FIGURE 2.20: GFI LanGuard scanning the local machine

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.

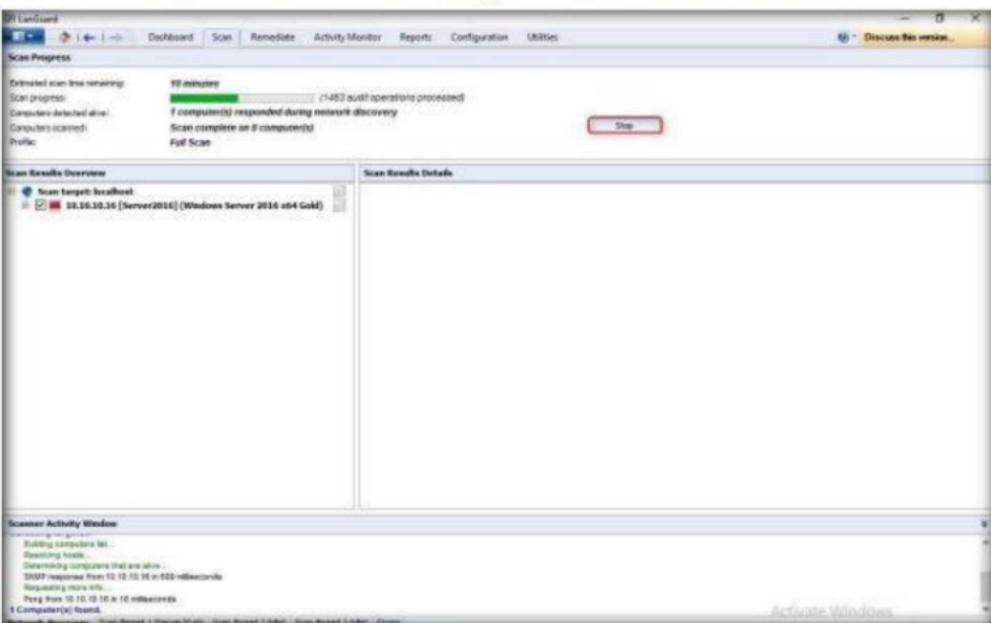


FIGURE 2.21: Stopping the scan

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

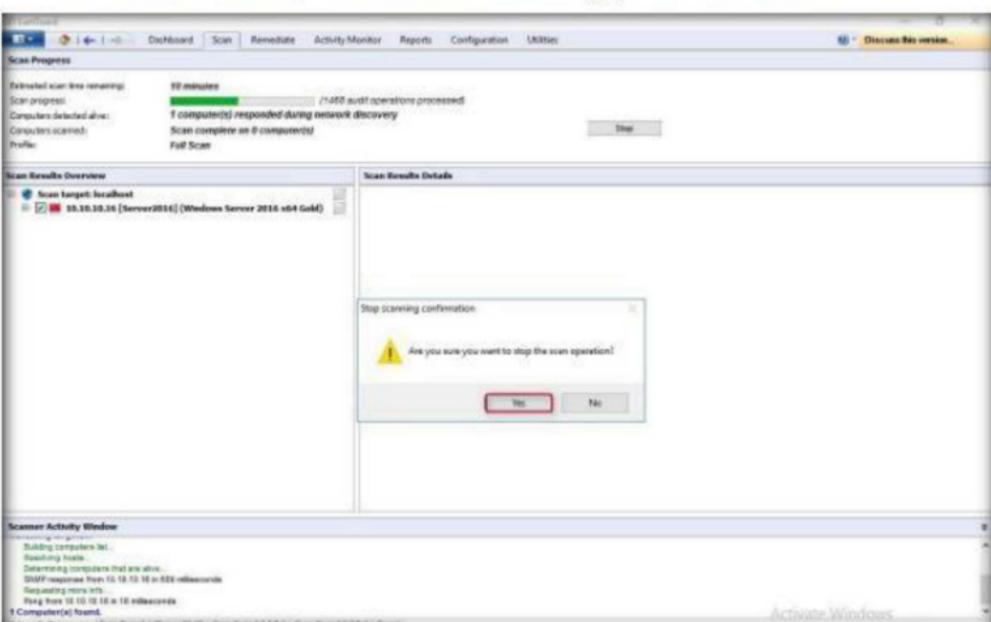


FIGURE 2.22: Stopping the scan

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

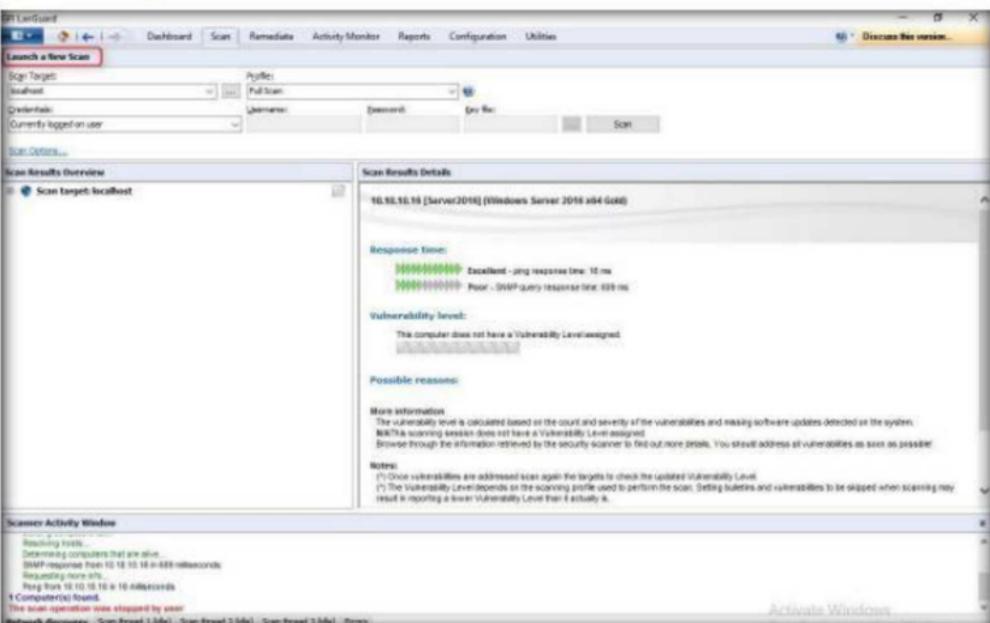


FIGURE 2.23: Launch a New Scan section in GFI LanGuard

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:

- Enter the IP address of the virtual machine in the **Scan Target** field, and select **Full Scan** from the **Profile** drop-down list.
- Select **Alternative credentials** from the **Credentials** drop-down list.

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

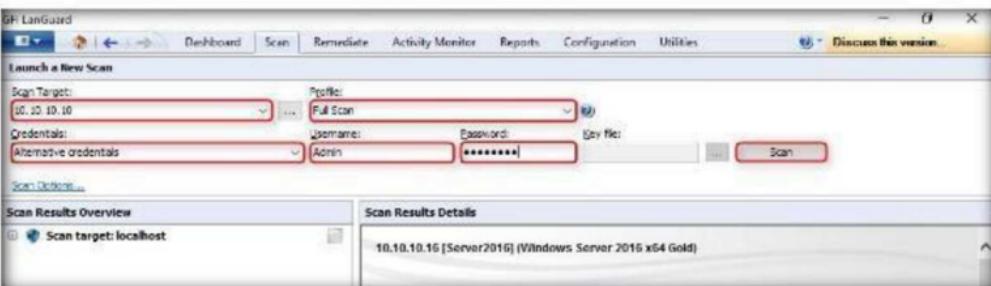


FIGURE 2.25: Customizing the scan settings

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.

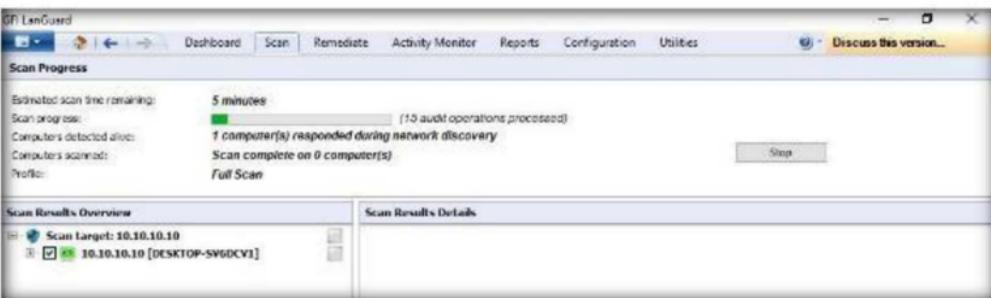


FIGURE 2.26: Vulnerability assessment being performed

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

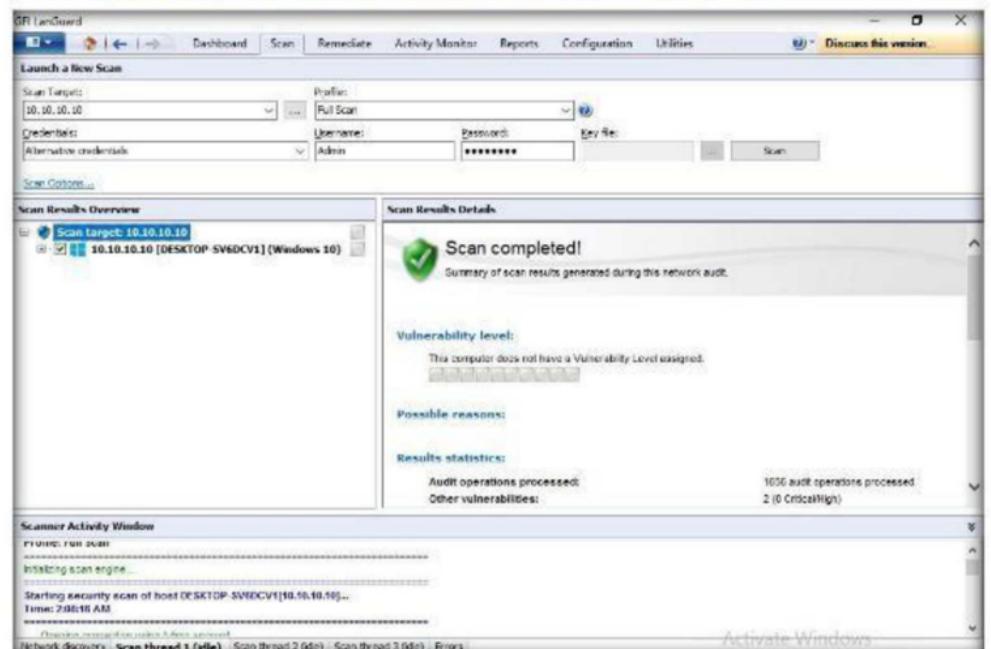


FIGURE 2.27: Scan Results displayed in GFI LanGuard

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

The screenshot shows the GFI LanGuard software interface. At the top, there's a navigation bar with tabs: Dashboard, Scan, Remediate, Activity Monitor, Reports, Configuration, Utilities, and a 'Discuss this version...' button. Below the navigation bar is a 'Launch a New Scan' section with fields for 'Scan Target' (10.10.10.10), 'Profile' (Full Scan), 'Credentials' (Admin), and 'Scan' button. A 'Scan Options...' link is also present. The main area has two panes: 'Scan Results Overview' on the left and 'Scan Results Details' on the right. In the 'Scan Results Overview' pane, under 'Scan target: 10.10.10.10 [DESKTOP-SV6DCV1] (Windows 10)', the 'Vulnerability Assessment' node is selected and highlighted with a red border. The 'Scan Results Details' pane shows a green checkmark icon with the message 'Scan completed!' and a summary: 'Summary of scan results generated during this network audit'. It includes sections for 'Vulnerability level', 'Possible reasons', and 'Results statistics'. The 'Scanner Activity Window' at the bottom lists audit operations processed: 'Audit operations processed: 1658 audit operations processed' and 'Other vulnerabilities: 2 (0 Critical/High)'. A status bar at the bottom shows 'Network discovery - Scan thread 1 (idle) - Scan thread 2 (idle) - Scan thread 3 (idle) - Errors' and an 'Activate Windows' watermark.

FIGURE 2.28: Viewing the scan results

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

This screenshot is identical to Figure 2.28, showing the GFI LanGuard interface. The 'Scan Results Overview' pane shows the 'Vulnerability Assessment' node is selected and highlighted with a red border under 'Scan target: 10.10.10.10 [DESKTOP-SV6DCV1] (Windows 10)'. The 'Scan Results Details' pane displays the same completed scan summary. The 'Scanner Activity Window' at the bottom shows audit operations processed: 'Audit operations processed: 1658 audit operations processed' and 'Other vulnerabilities: 2 (0 Critical/High)'. A status bar at the bottom shows 'Network discovery - Scan thread 1 (idle) - Scan thread 2 (idle) - Scan thread 3 (idle) - Errors' and an 'Activate Windows' watermark.

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.

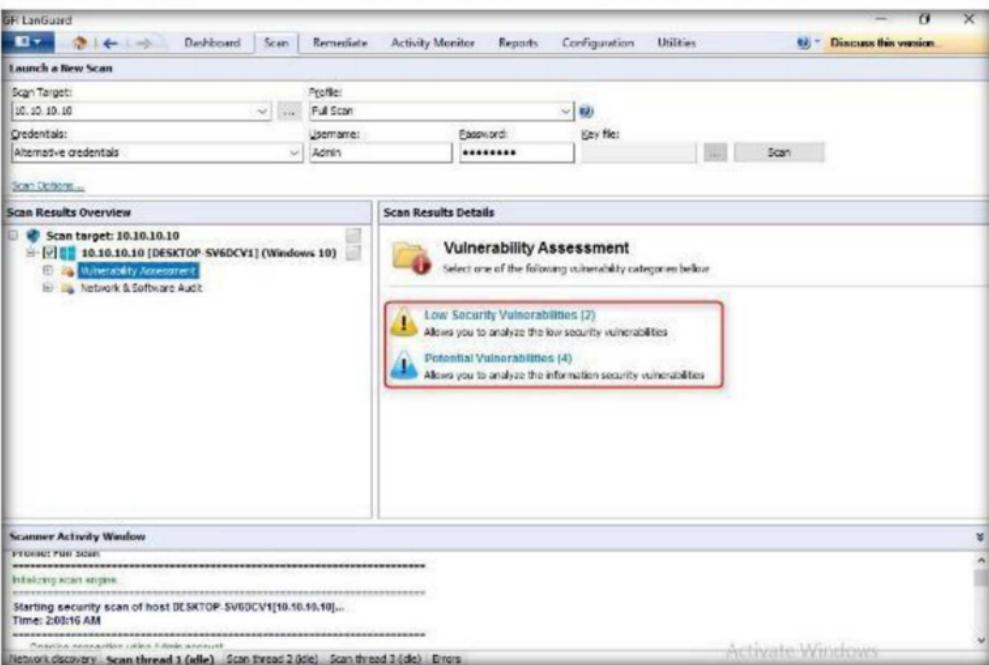


FIGURE 2.30: Vulnerability Assessment categories

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.

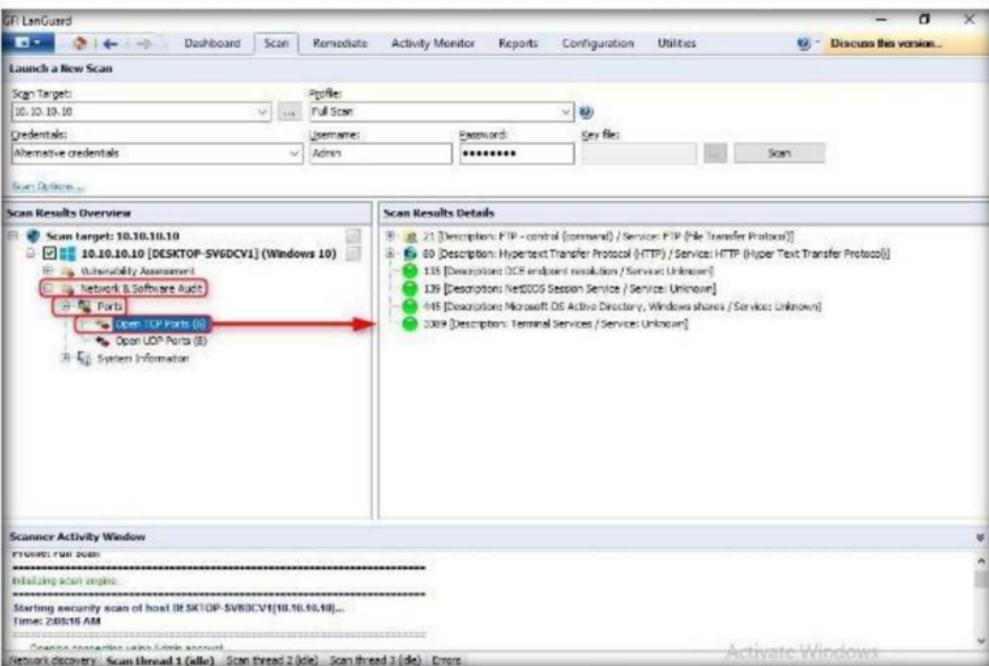


FIGURE 2.31: Scan results for open TCP Ports

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

The screenshot shows the GFI LanGuard interface. The top navigation bar includes 'Dashboard', 'Scan', 'Remediate', 'Activity Monitor', 'Reports', 'Configuration', 'Utilities', and 'Discuss this version...'. Below this is a 'Launch a New Scan' section with fields for 'Scan Target' (10.10.10), 'Profile' (Full Scan), 'Credentials' (Admin), and 'Password' (*****). A 'Scan' button is present. The main area is divided into two panes: 'Scan Results Overview' on the left and 'Scan Results Details' on the right. The 'Scan Results Overview' pane shows a tree structure for the scan target 10.10.10.10, with nodes for Vulnerability Assessment, Network & Software Audit, Ports (selected), and System Information. A red arrow points from the 'Ports' node to the 'Scan Results Details' pane. The 'Scan Results Details' pane lists several UDP services: 137 [NetBIOS Name Service], 138 [NetBIOS Datagram Service], 500 [Internet Security Association and Key Management Protocol (ISAKMP)], 1900 [Microsoft SSDP Online discovery of UPnP devices], 3722 [Web Services Dynamic Discovery (WSD Discovery), used by various components of Windows Vista], 4660 [Proxy NAT Interval (HTTP 3947)], 5323 [Multicast DNS (mDNS)], and 5355 [LMNR - Link-Layer Multicast Name Resolution]. At the bottom of the interface, there is a 'Scanner Activity Window' showing progress and logs, and a status bar with 'Activate Windows'.

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.

This screenshot is identical to Figure 2.32, showing the GFI LanGuard interface with the 'System Information' node selected in the 'Scan Results Overview' pane. A red arrow points from this node to the 'Scan Results Details' pane, which displays the following password policy settings: Minimum password length: 0 chars, Maximum password age: 0 days, Minimum password age: 0 days, Force logoff: never force, and Password history: no history.

FIGURE 2.33: Scan results for Password Policy

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

The screenshot shows the GFI LanGuard interface. In the top navigation bar, the 'Scan' tab is selected. On the left, the 'Scan Targets' dropdown is set to '10.10.10.10'. Below it, the 'Credentials' dropdown is set to 'Administrator' with the password 'Admin'. The 'Scan Options...' button is visible. The main area is titled 'Scan Results Overview' and shows a tree view of the scanned host '10.10.10.10 [DESKTOP-SV6DCV1] (Windows 10)'. Under 'Groups', there are 18 entries listed. A red arrow points from the 'Groups' section to the right panel, which is titled 'Scan Results Details' and lists various local user groups such as Administrators, Backup Operators, and Guests. At the bottom, a progress bar indicates 'INITIATING FULL SCAN' and 'Initializing scan engine...'. The status bar shows 'Starting security scan of host DESKTOP-SV6DCV1[10.10.10.10]... Timer: 200:16 AM'.

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.

The screenshot shows the GFI LanGuard Dashboard. The 'Dashboard' tab is highlighted in red. The left sidebar includes 'Entire Network' (localhost: SERVER2016, Local Domain: WORKGROUP), 'Group', 'Search', and 'Common Tasks' (Manage agents, Add more computers, Scan and refresh information now, Custom scan, Set credentials, Update agents). The main dashboard features several cards: 'Entire Network - 2 computers' (Vulnerability level: Medium, Most Vulnerable Computers: No vulnerable computer), 'Security Sensors' (Software Updates: 0 computers, Firewall Issues: 0 computers, Credentials Setup: 1 computer, Service Packs and Up...: 0 computers, Unauthorized Appli...: 0 computers, Malware Protection Is...: 0 computers, Vulnerabilities: 0 computers, Audit Status: 0 computers, Agent Health Issues: 0 computers), 'Vulnerability Trend Over Time' (No Security Audits performed in the last 30 days), 'Agent Status' (100% status), 'Computer Vulnerability Distribution' (Pie chart: 50% Installed, 50% Not installed), and 'Computers By Operating System' (Pie chart: Windows 10 50%, Windows Server 2016 40%, Linux 10%).

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

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**.

```
File Edit View Search Terminal Help
root@kali:~# nikto -H
```

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.

```
File Edit View Search Terminal Help
o-name)
    -ssl          Force ssl mode on port
    -Tuning+      Scan tuning:
                  1 Interesting File / Seen in logs
                  2 Misconfiguration / Default File
                  3 Information Disclosure
                  4 Injection (XSS/Script/HTML)
                  5 Remote File Retrieval - Inside Web Root
                  6 Denial of Service
                  7 Remote File Retrieval - Server Wide
                  8 Command Execution / Remote Shell
                  9 SQL Injection
                 0 File Upload
                 a Authentication Bypass
                 b Software Identification
                 c Remote Source Inclusion
                 d WebService
                 e Administrative Console
                 x Reverse Tuning Options (i.e., include all e
xcept specified)
    -timeout+     Timeout for requests (default 10 seconds)
    -Userdbs      Load only user databases, not the standard databases
                  all Disable standard dbs and load only user dbs
                  tests Disable only db tests and load udb tests
```

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.

```
File Edit View Search Terminal Help
root@kali:~# nikto -h http://www.certifiedhacker.com -Tuning x
```

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.

```
root@kali:~# nikto -h http://www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:        2017-12-28 07:53:16 (GMT-5)

+ Server: nginx/1.12.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-3092: /cgi-sys/: This might be interesting... possibly a system shell found.
+ OSVDB-3092: /img-sys/: Default image directory should not allow directory listing.
+ OSVDB-3092: /java-sys/: Default Java directory should not allow directory listing.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ 9953 requests: 1 error(s) and 10 item(s) reported on remote host
+ End Time:          2017-12-28 08:39:51 (GMT-5) (2795 seconds)

+ 1 host(s) tested
root@kali:~#
```

FIGURE 3.4: Nikto scan output

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

```
root@kali:~# nikto -h http://www.certifiedhacker.com -Cgidirs all
```

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.

The terminal window shows the command "nikto -h http://www.certifiedhacker.com -Cgidirs all" being run by a user with root privileges. The output of the scan is displayed, detailing various security findings across different ports and paths on the target server.

```
root@kali:~# nikto -h http://www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:        2017-12-28 07:33:33 (GMT-5)

+ Server: nginx/1.12.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3233: /mailman/listinfo/: Mailman was found on the server.
+ OSVDB-3092: /cgi-sys/: This might be interesting... possibly a system shell found.
+ OSVDB-3092: /img-sys/: Default image directory should not allow directory listing.
+ OSVDB-3092: /java-sys/: Default Java directory should not allow directory listing.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ 26150 requests: 1 error(s) and 10 item(s) reported on remote host
+ End Time:          2017-12-29 00:20:42 (GMT-5) (60429 seconds)

+ 1 host(s) tested
root@kali:~#
```

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