Network Risk and Vulnerability Management

Module 12

Lab 1

Vulnerability Analysis Using the Nessus

Nessus allows you 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.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a network administrator, you are require to perform vulnerability scanning on you network as a part of network operation. This enables you to find various vulnerabilities that may exist in your network. These vulnerabilities, if not mitigated in time, can create huge risk to the network. Attackers may take advantage of these vulnerabilities to compromise your network. As a network administrator, you should be able to perform a detailed vulnerability scan on your network. This lab will demonstrate how to perform vulnerability scanning on the target network.

Lab Objectives

This lab will teach you how to use the Nessus tool to perform a vulnerability scan on the target network.

Lab Environment

To carry out this lab, you need:

- Nessus, located at **Z:\CND-Tools\CND Module 12 Network Risk and Vulnerability Management\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, the screenshots shown in the lab might differ
- A virtual machine running Windows Server 2012
- A virtual machine running Windows 10

- A virtual machine running Windows Server 2008
- A web browser with Internet access
- Administrative privileges to run the Nessus tool

Lab Duration

Time: 35 Minutes

Overview of Vulnerability Scanning

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

Lab Tasks

TASK 1

Install and Configure Nessus

Note: Before starting this Lab Exercise turn off Windows Update in the Windows Server 2008 machine. To turn Windows update off launch Control Panel → Windows Update → Change settings and select the Never check for updates (not recommended) radio button and click **OK** then close all the windows.

1. Launch the Windows Server 2012 virtual machine before beginning this lab.
2. Navigate to **Z:\CND-Tools\CND Module 12 Network Risk and Vulnerability Management\Vulnerability Assessment Tools\Nessus,** and double-click **Nessus-6.6.2-x64.msi**
3. If the **Open File - Security Warning** pop-up appears, click **Run**.
4. The **Tenable Nessus Installation Wizard** appears. Follow the installation steps to install Nessus. You should accept all of the installation defaults.

Nessus is designed to automate the testing and discovery of known security problems.

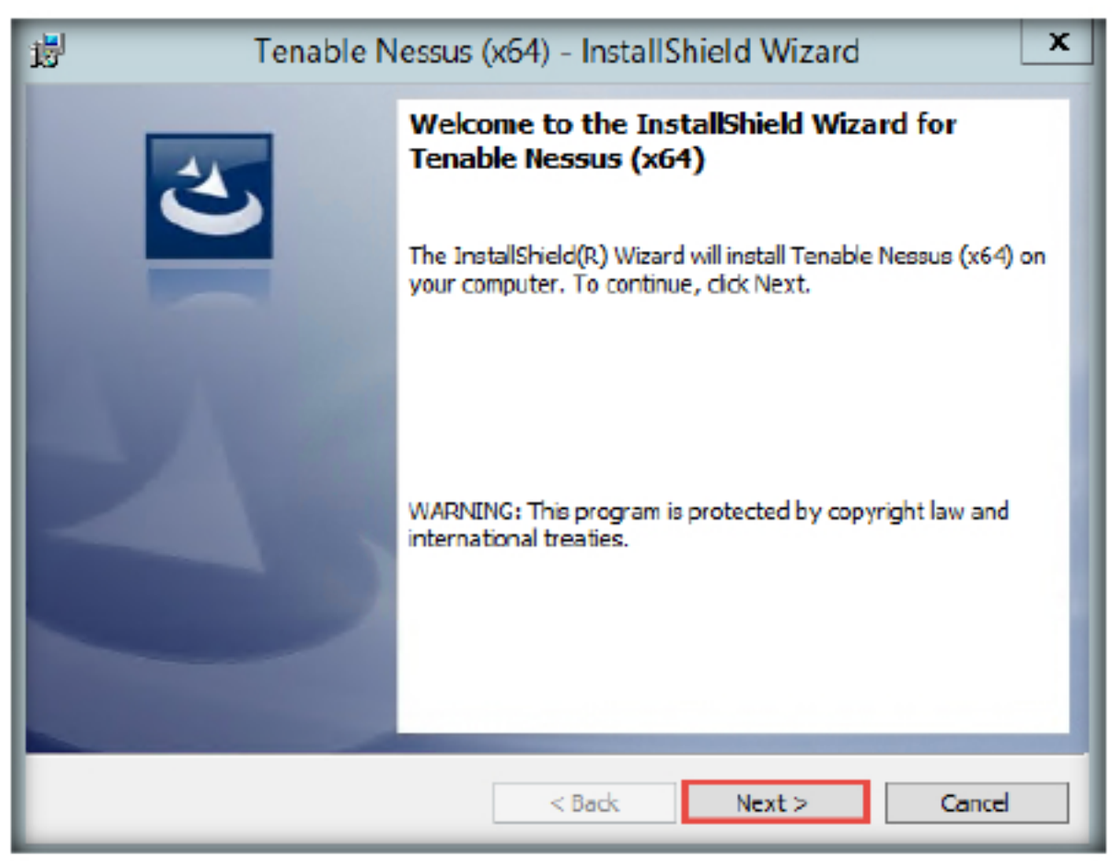


FIGURE 1.1: The Nessus Install Shield Wizard

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

Note: In this lab demonstration the default browser is Chrome, if you are using different browser the screenshots may vary in your lab environment.

Nessus security scanner includes NASL (Nessus Attack Scripting Language).

7. The **Welcome to Nessus** window appears. Click the **clicking here** link to connect via **SSL.**

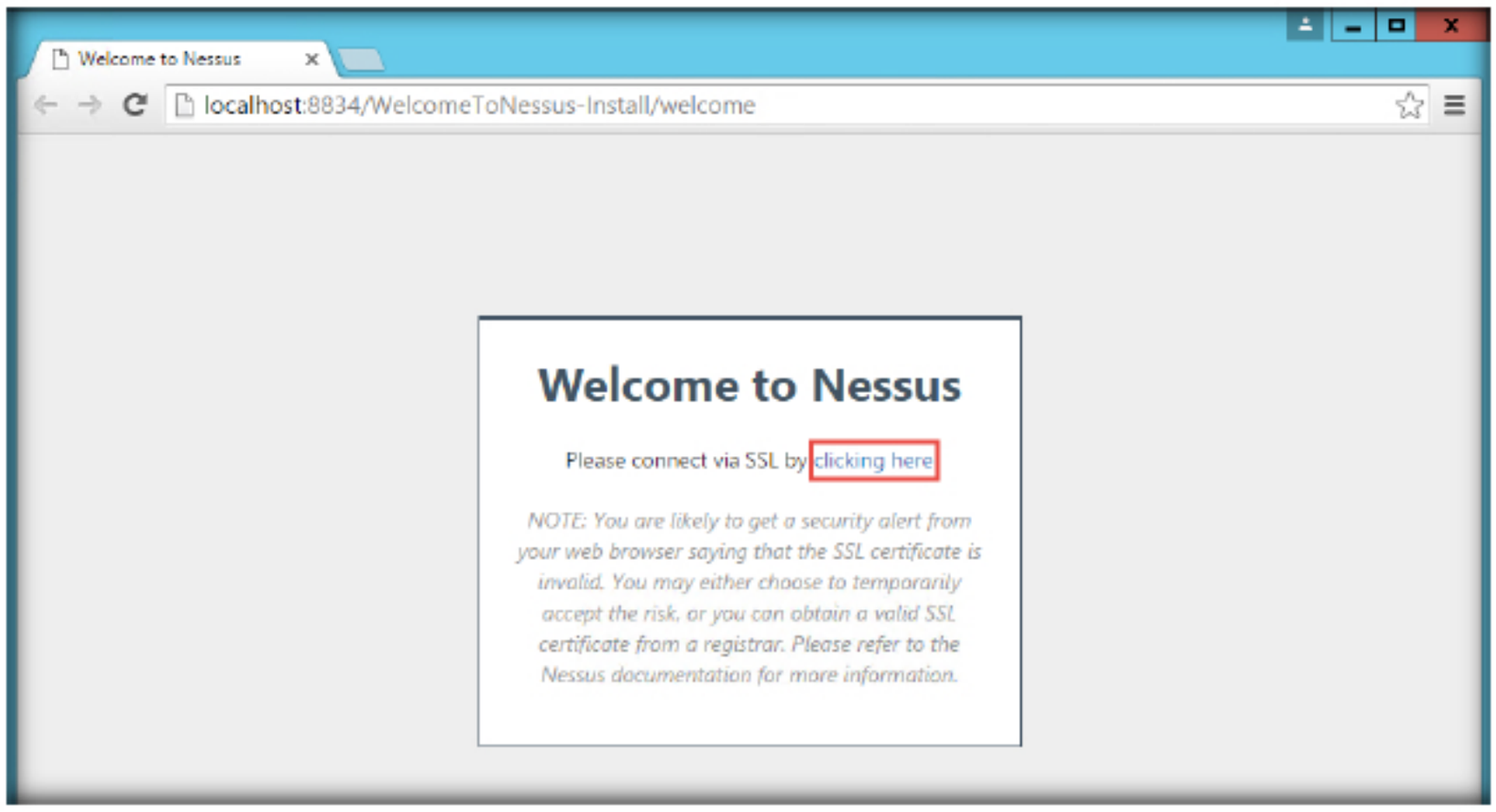


FIGURE 1.2: Welcome to Nessus window

8. The **Your connection is not private window appears**. Click the **ADVANCED** link.

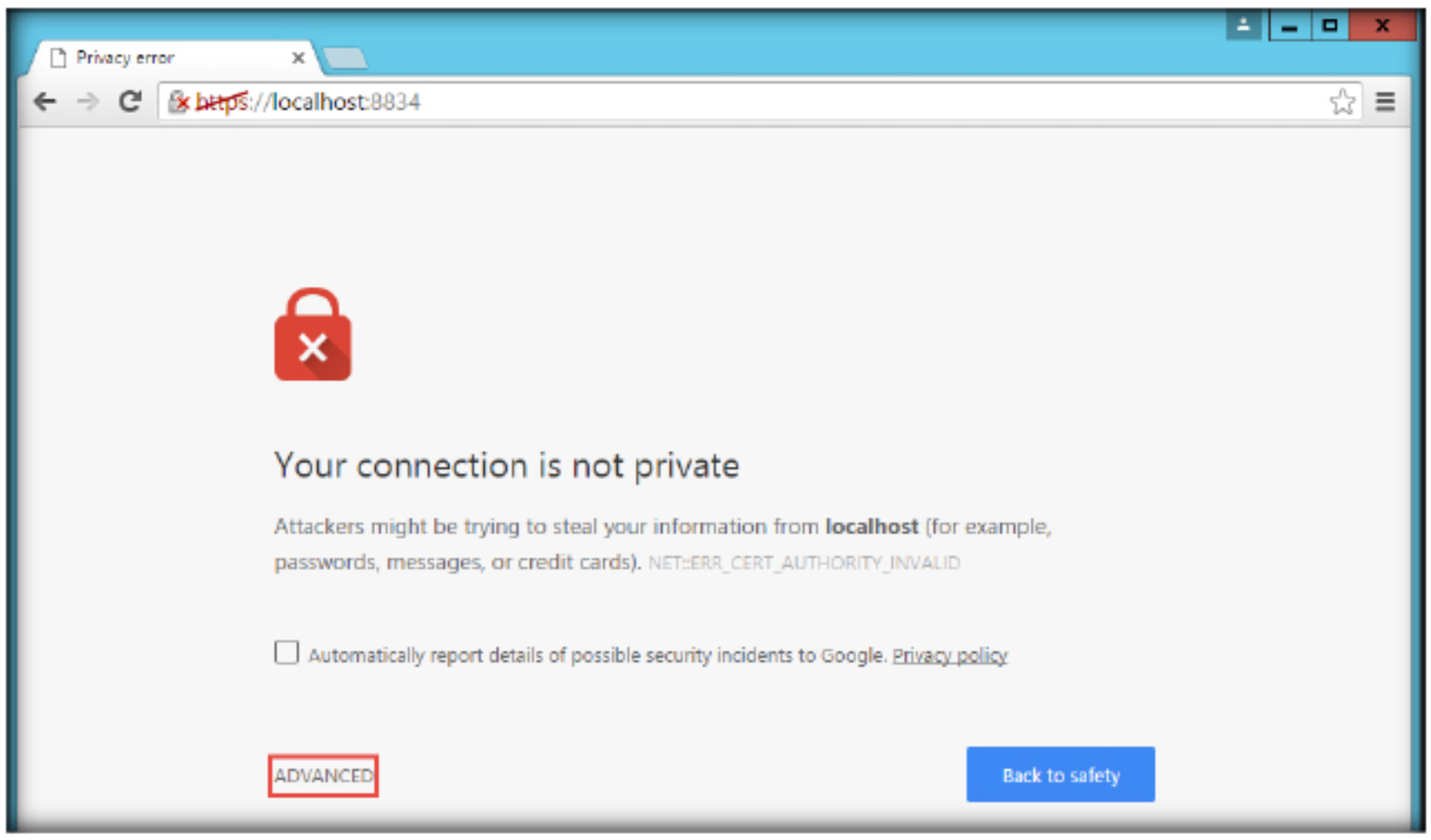


FIGURE 1.3: Browser Security Webpage

Nessus probes a range of addresses on a network to determine which hosts are alive.

During the installation and daily operation of Nessus, manipulating the Nessus service is generally not required

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

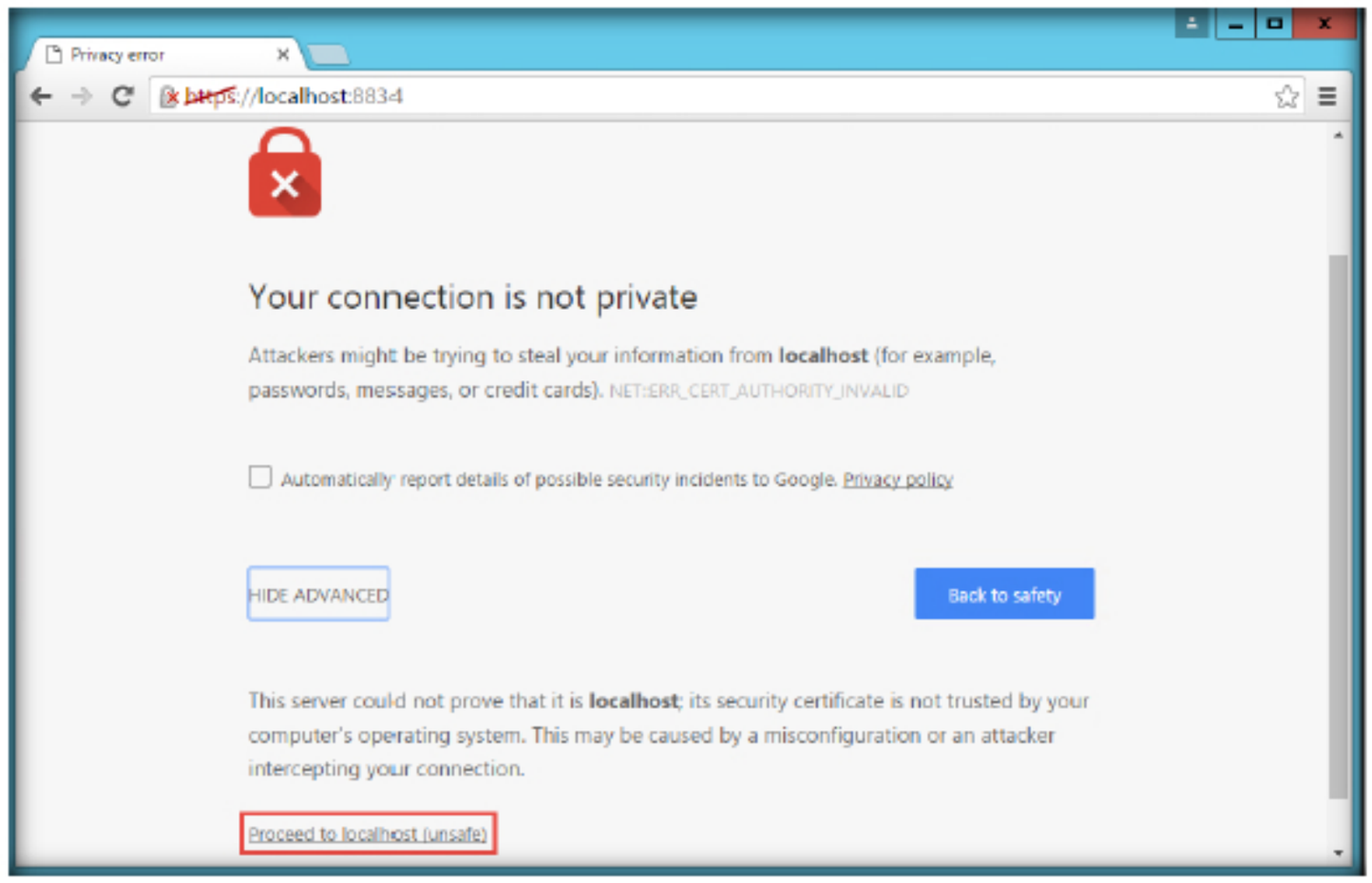


FIGURE 1.4: Browser Security Webpage

10. The **Welcome to Nessus 6** window appears. Click the **Continue** button.

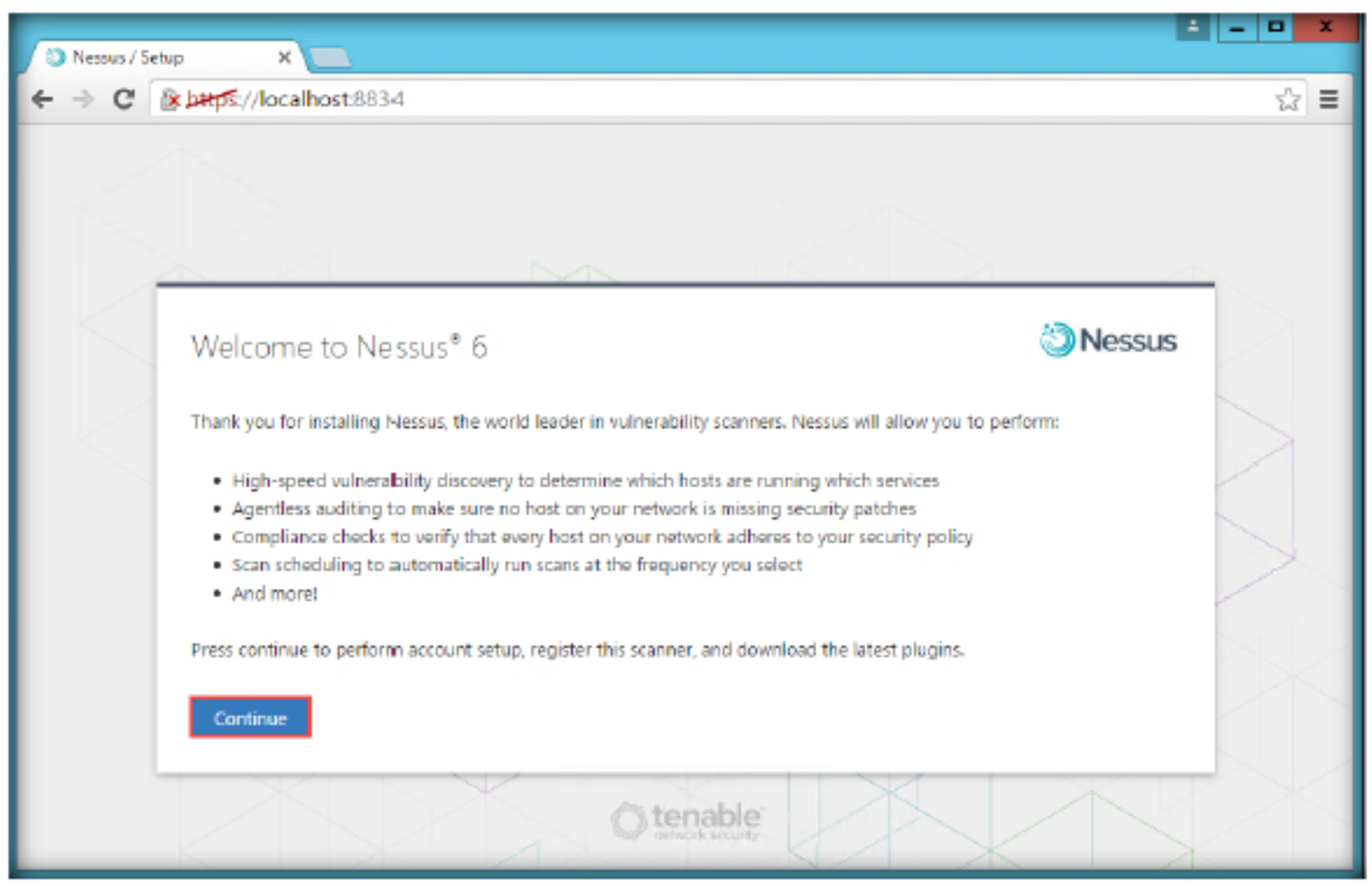


FIGURE 1.5: Welcome to Nessus window

Nessus is public Domain software licensed under the GPL.

11. The **Account Setup window** appears.
12. Create credentials for scanner administrative control. In this lab we have created the Username: **admin** and the Password: **test@123** then click **Continue**.

13. These credentials are used to log in to Nessus for the vulnerability scanning.

Nessus has the ability to test SSL services such as http, SMTPS, IMAPS and more.

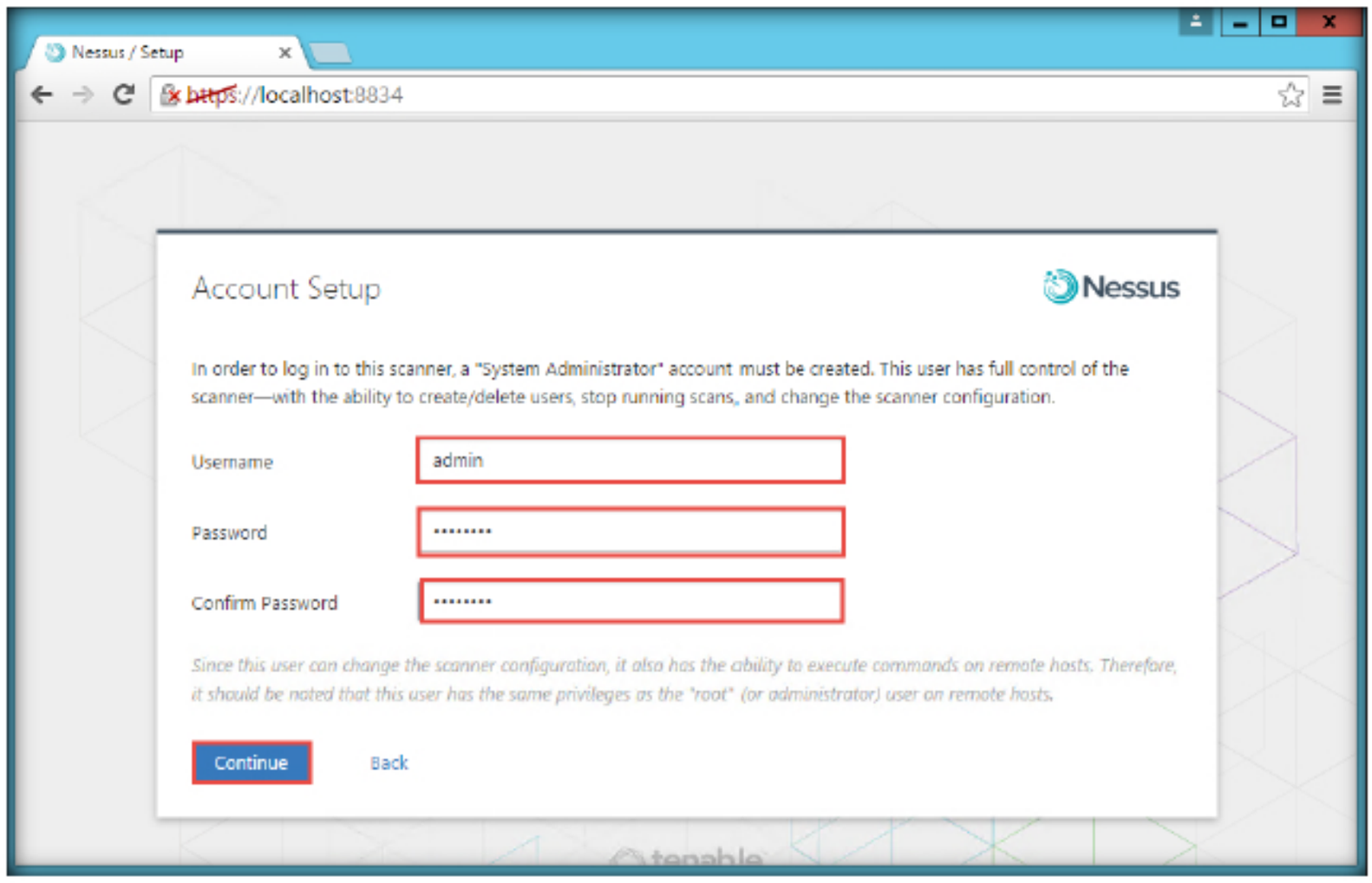


FIGURE 1.6: Account Setup window

14. The **Product Registration** window appears, in which you need to enter an Activation Code. Click the **Registering this scanner** link to obtain the Activation Code.

15. The **Obtain an Activation Code tab** opens. Scroll down and click the **Register Now** link under Nessus Home.

If you are using the Tenable Security Center, the Activation Code and plugin updates are managed from the Security Center. Nessus needs to be started to be able to communicate with the Security Center, which it will normally not do without a valid Activation Code and plugins.

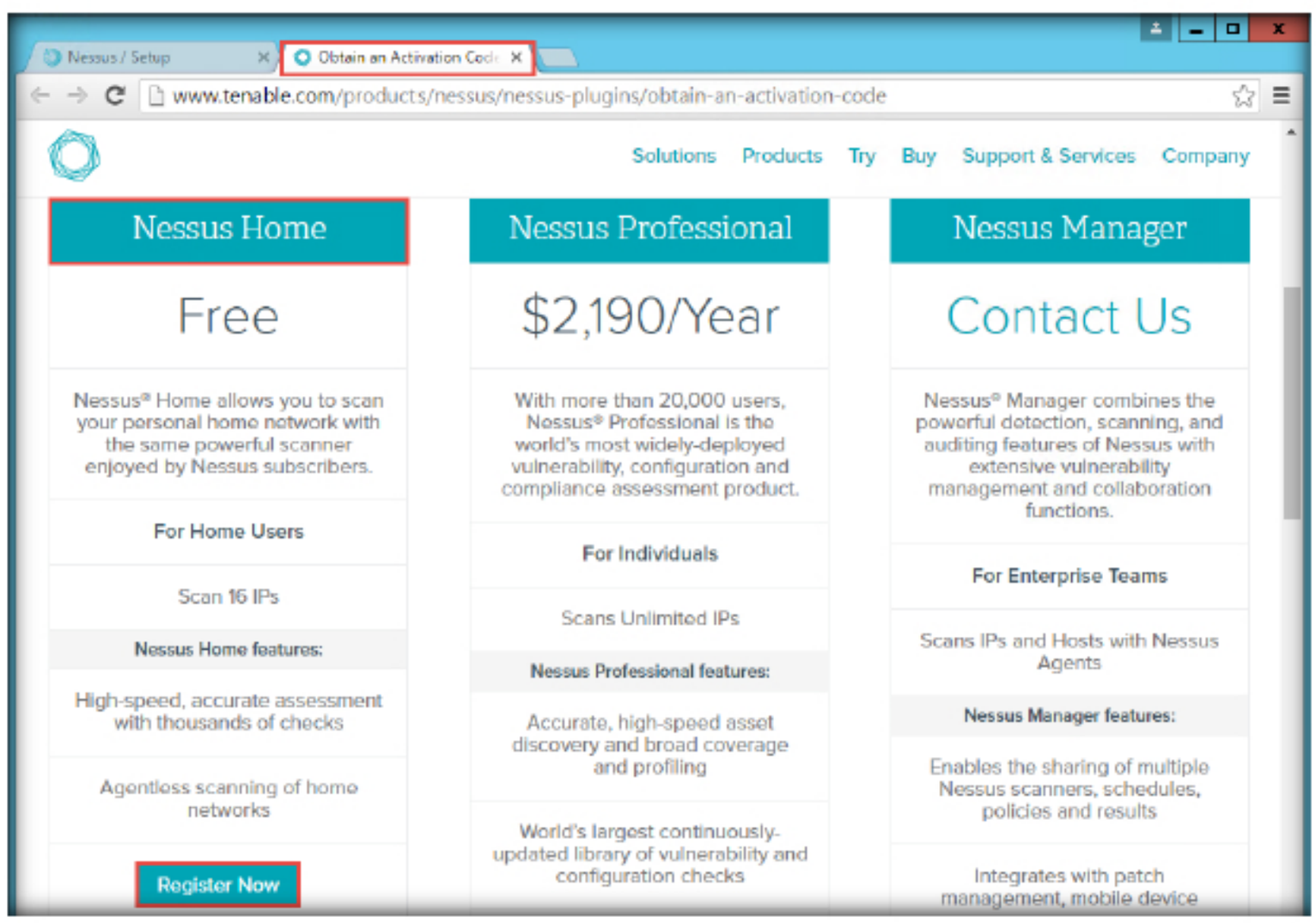


FIGURE 1.7: Activation Code Registration tab

16. The **Nessus Home** page appears. In the right pane under **Register for an Activation Code**, enter your details and click **Register**. Once you click the Register button you can close the newly opened tab.

Note: Provide a working email ID in the Email field, as Nessus will send you the activation code.

If you do not register your copy of Nessus, you will not receive any new plugins and will be unable to start the Nessus server. Note: The Activation Code is not case sensitive.

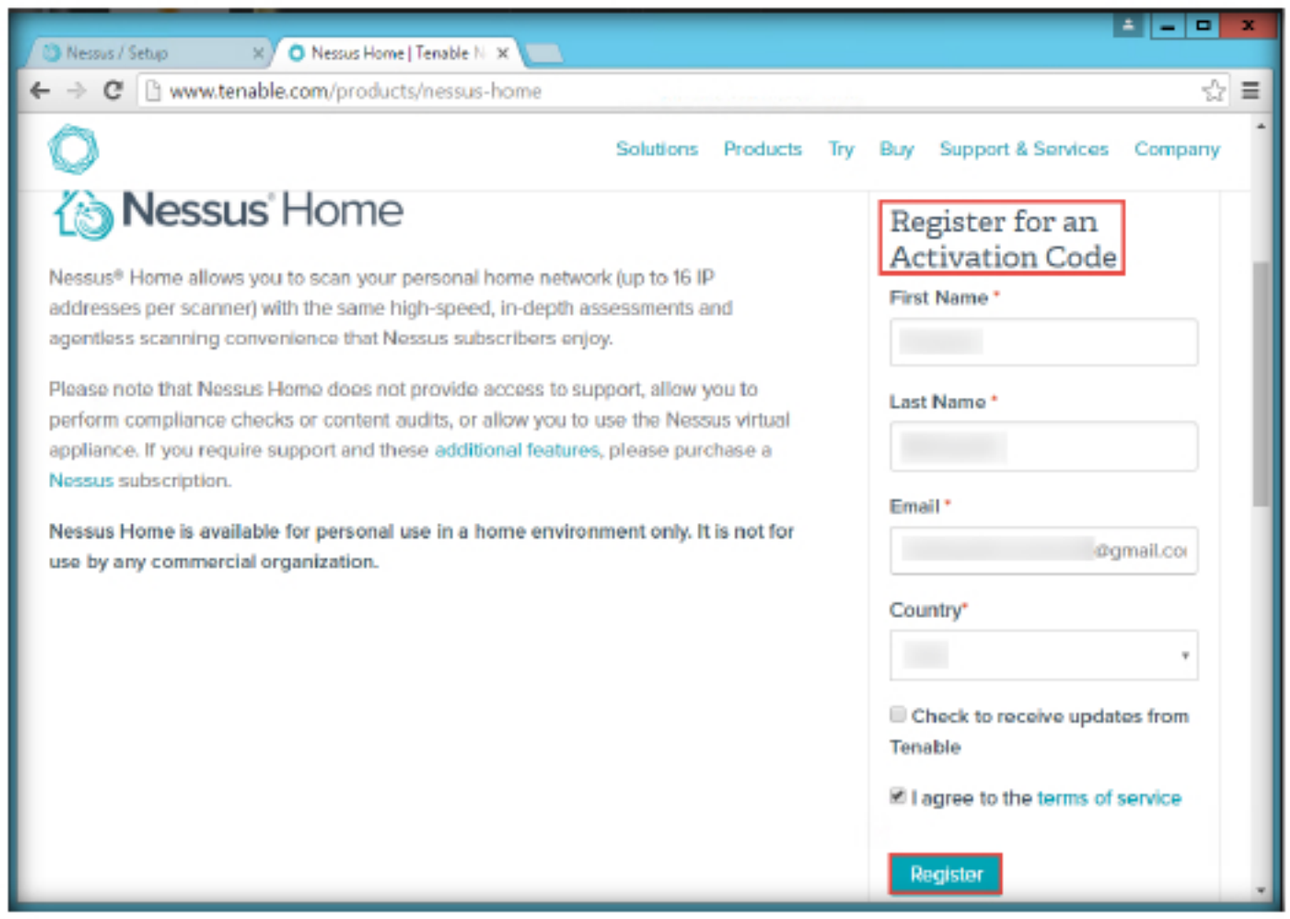


FIGURE 1.8: Registering for a Nessus activation code

17. Log in to your email and look for the activation code. The mail is from **Nessus Registration**, open it.

18. Look for activation code in the mail and note it down.

The updated Nessus security checks database is retrieved with the commands nessus-updated-plugins.

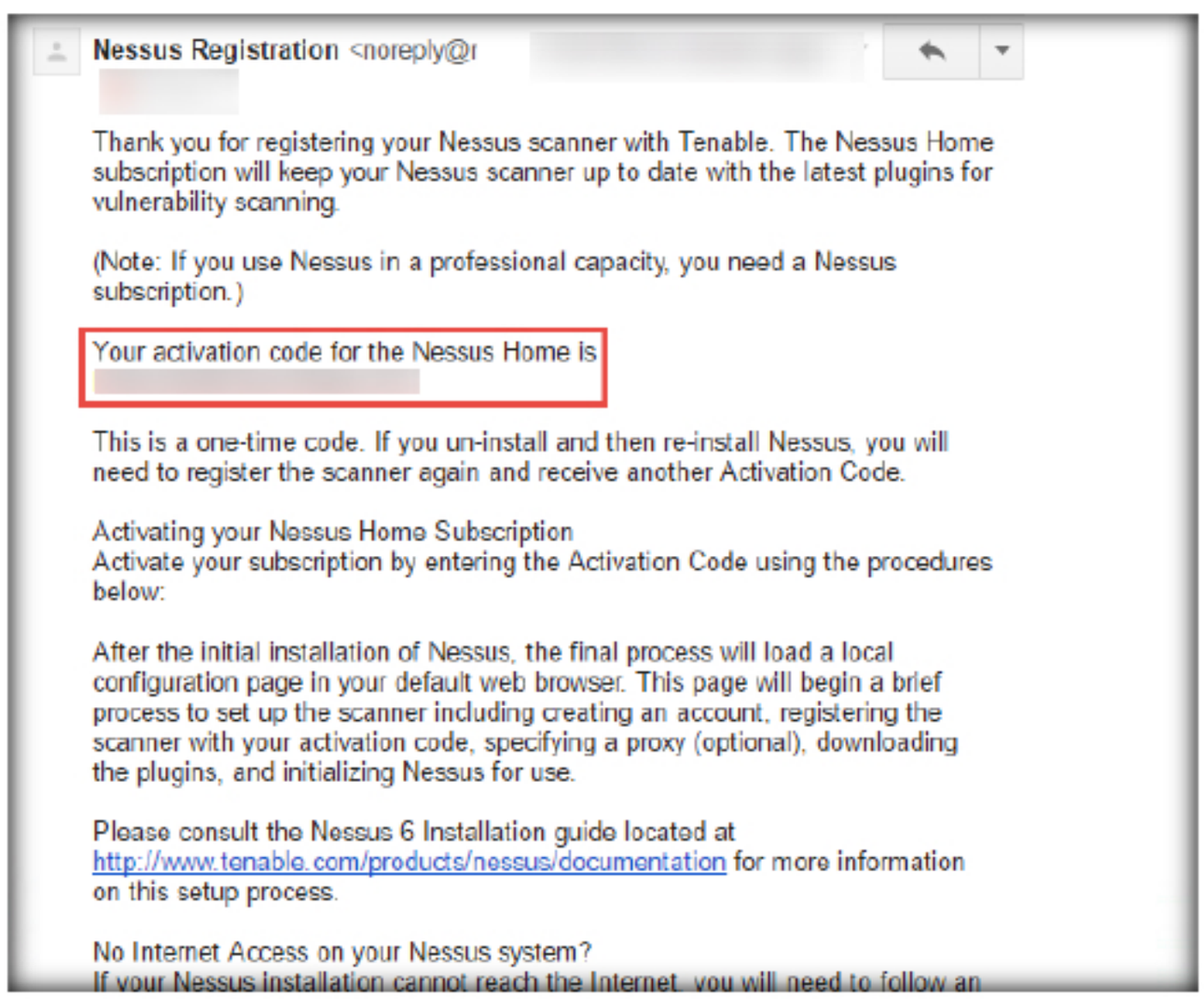


FIGURE 1.9: Activation code for Nessus

19. Switch to the **Product Registration** page and enter the Activation code in the **Activation code** section then click **Continue**.

Once the plugins have been downloaded and compiled, the Nessus GUI will initialize and the Nessus server will start.

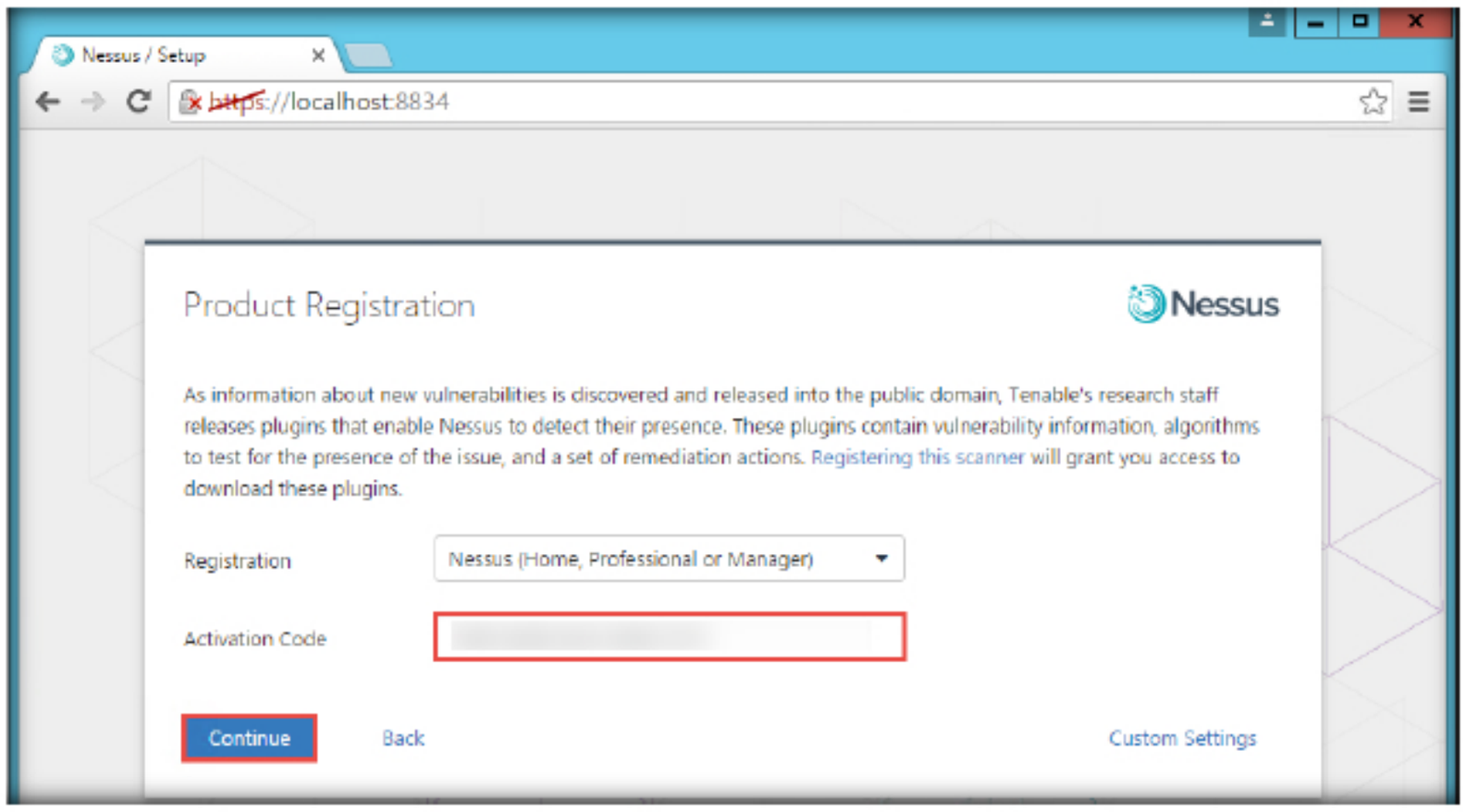


FIGURE 1.10: Activation code registration

20. The Nessus Download page appears. Wait for the download to complete.

The Nessus server configuration is managed via the GUI. The nessusd.conf file is deprecated. In addition, proxy settings, subscription feed registration, and offline updates are managed via the GUI

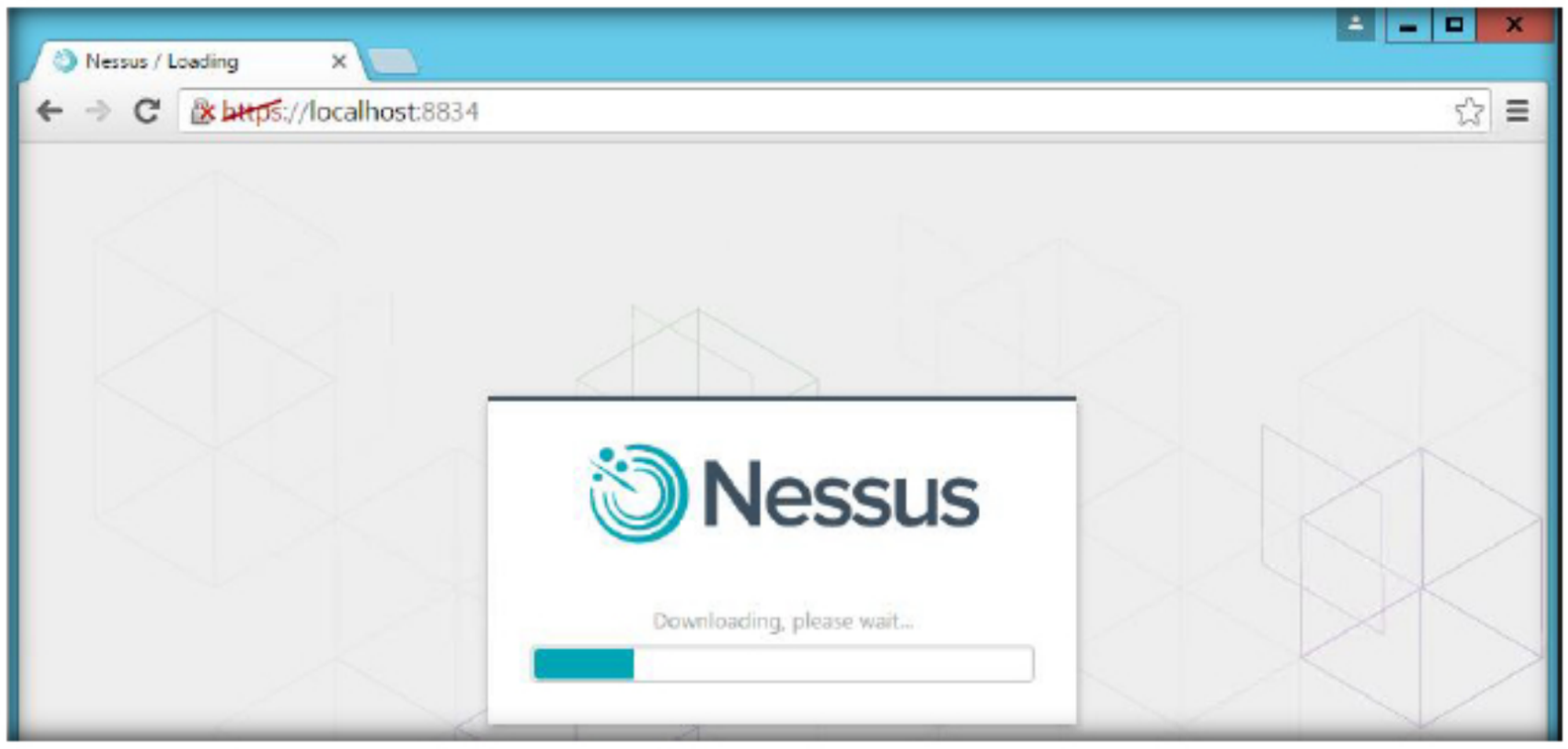


FIGURE 1.11: Nessus Download page

21. After downloading is complete, the **Initialization** page appears. Wait for the initialization process to complete (It will depend on ISP bandwidth).

For the item SSH user name, enter the name of the account that is dedicated to Nessus on each of the scan target systems.

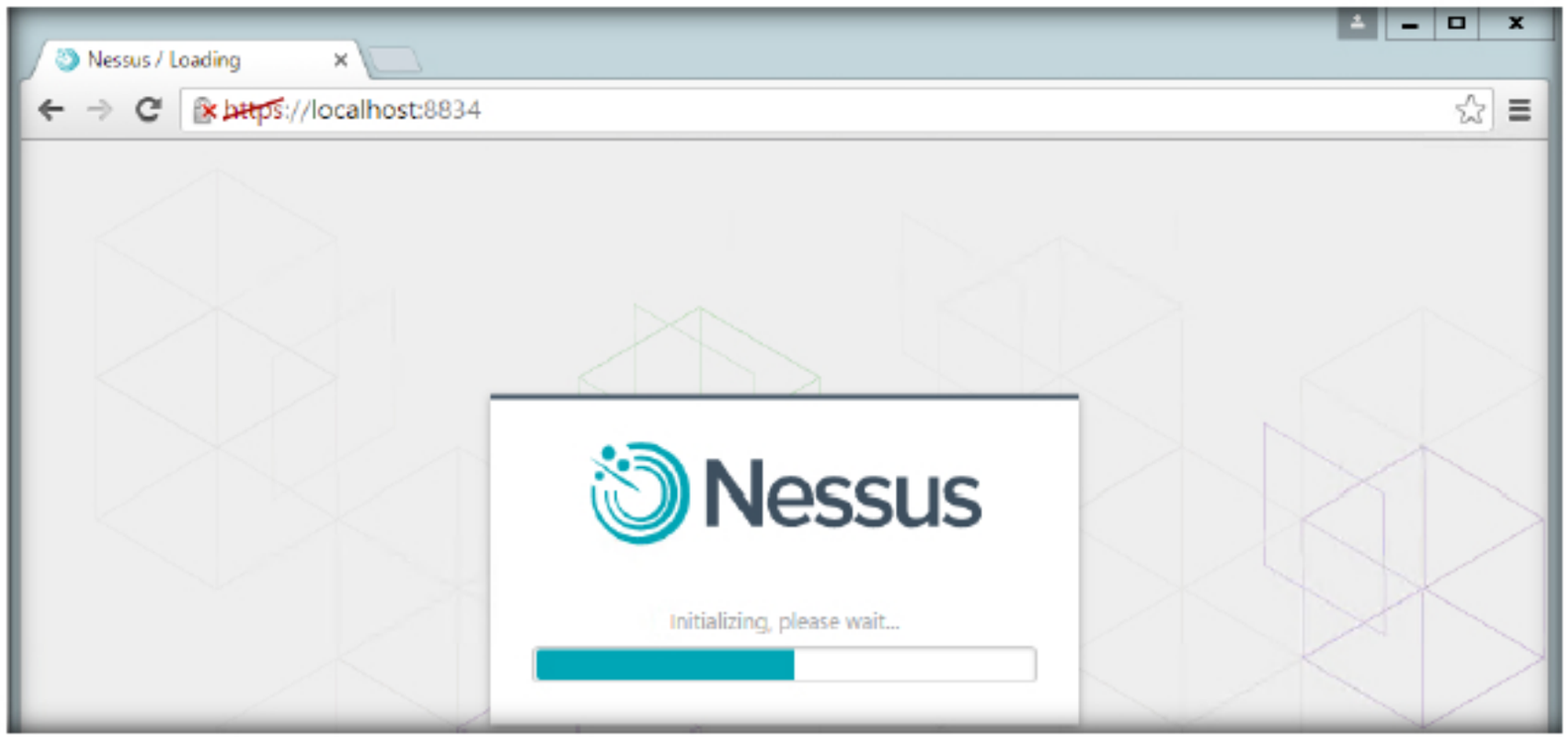


FIGURE 1.12: Nessus being initialized

22. On completion of the initialization, the **Nessus Login** page appears as shown in the screenshot.

23. Enter the **Username** and **Password** you created in Step 12 (Recommended User: admin; Password: password), then click **Sign In**.

Nessus probes network services on each host to obtain banners that contain software and OS version information.

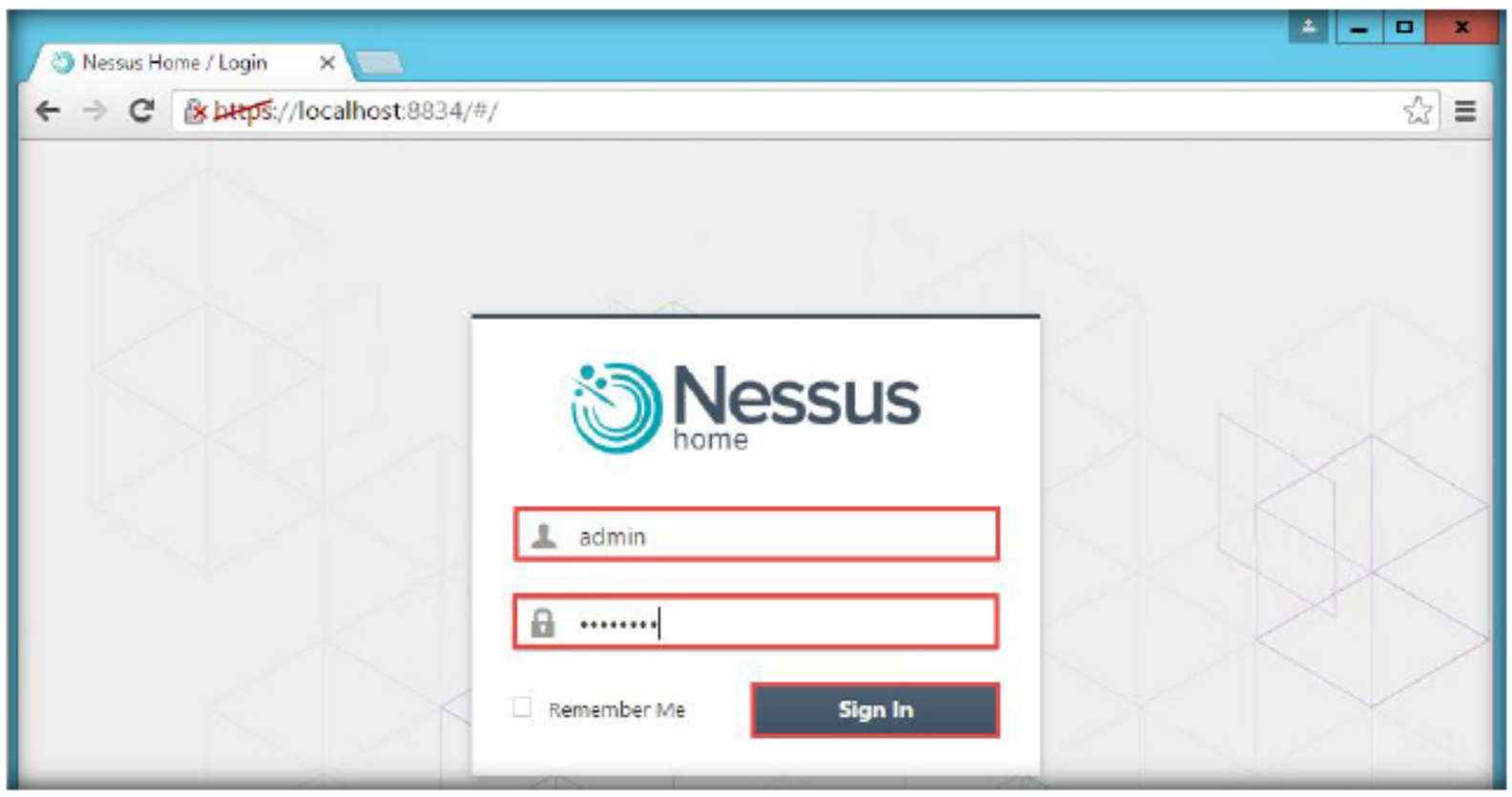


FIGURE 1.13: Signing into Nessus

24. The **Nessus/ Scans** window opens as shown.

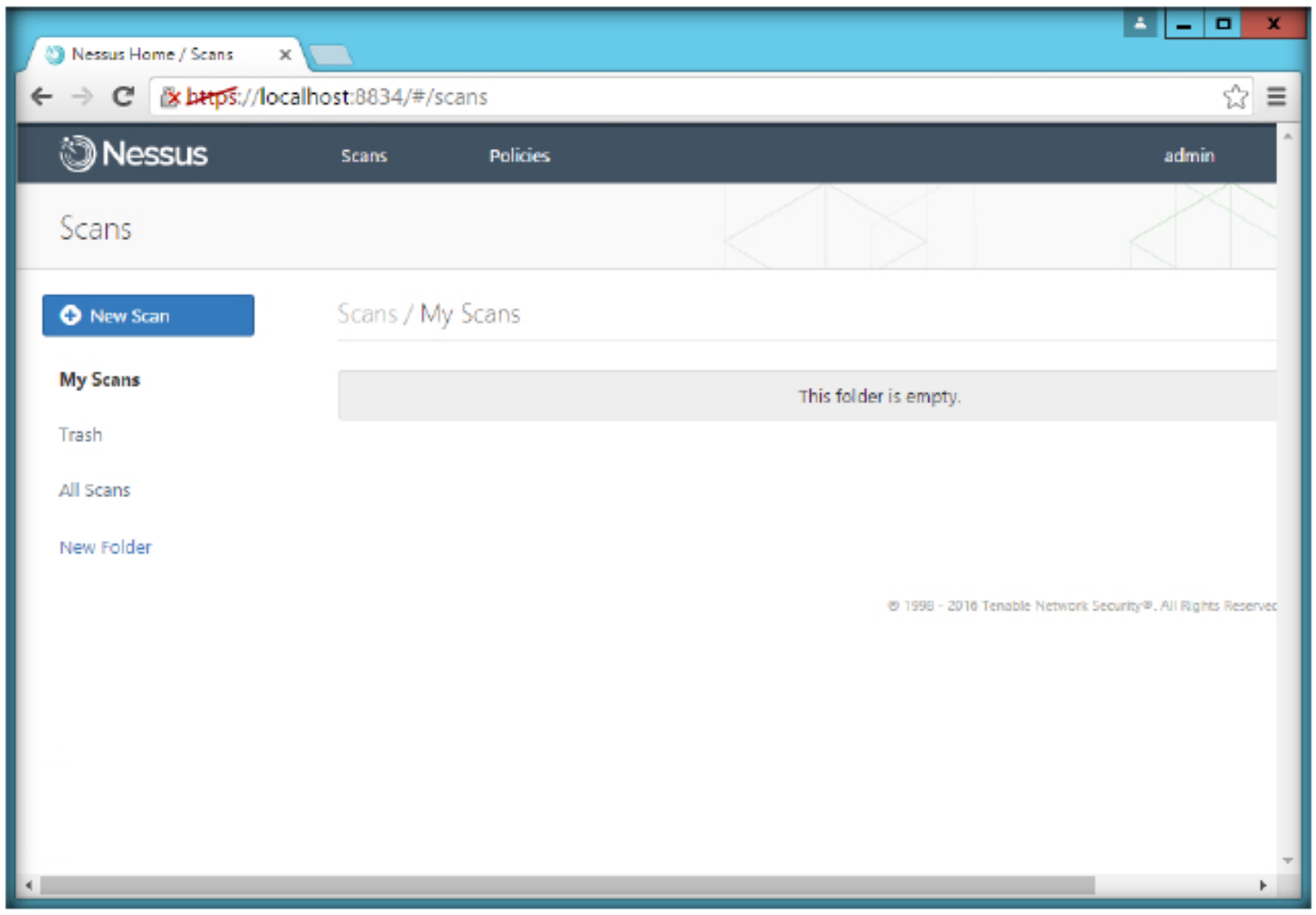


FIGURE: 1.14: The Nessus Scans window

TASK 2

Add a Network Policy

25. To add a new policy, click the **Policies** button in the menu bar.

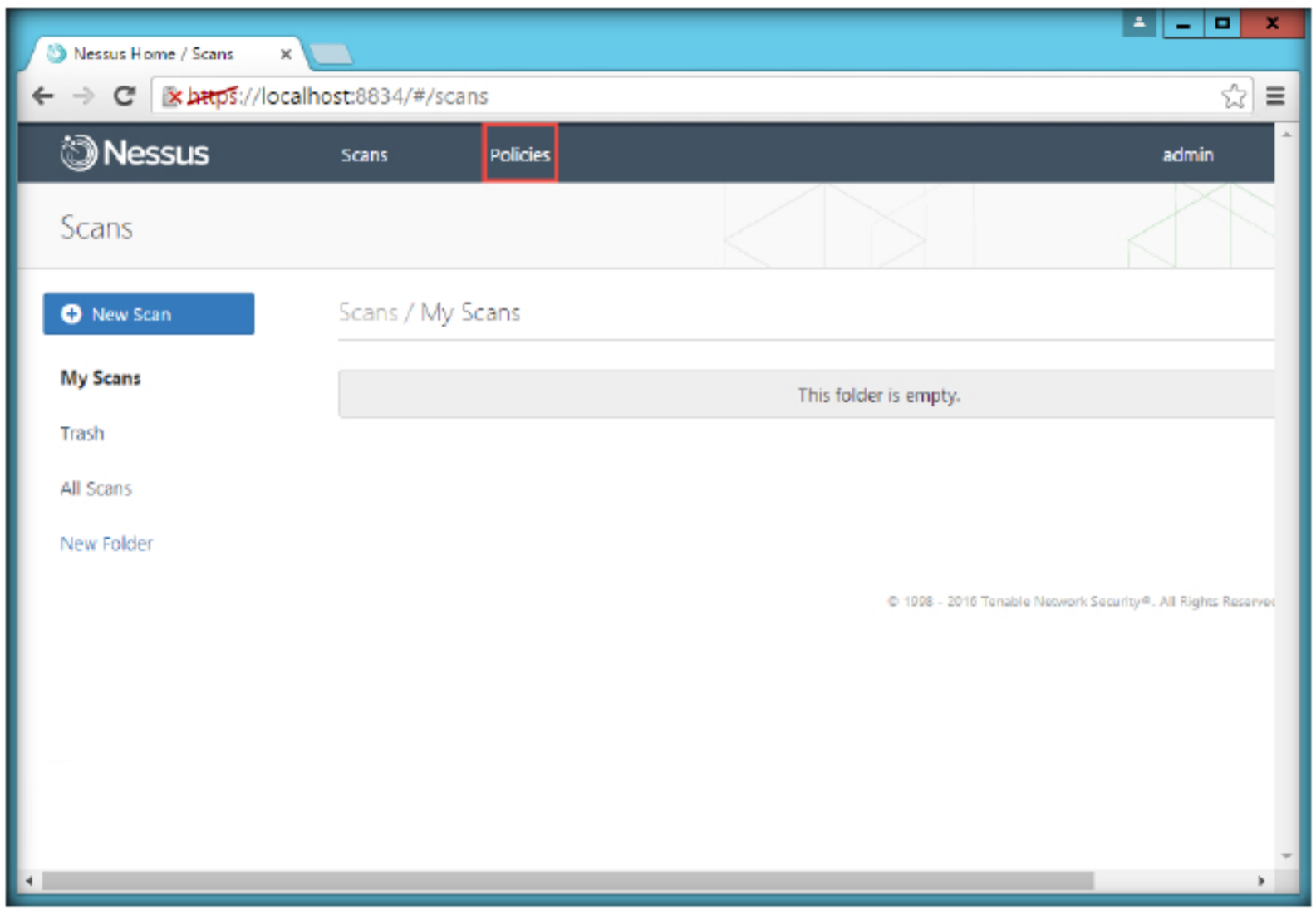


FIGURE 1.15: The Nessus Policies window

26. When the **Nessus/ Policies** window opens, click the **+ New Policy** button.

New policies are configured using the Credentials tab.

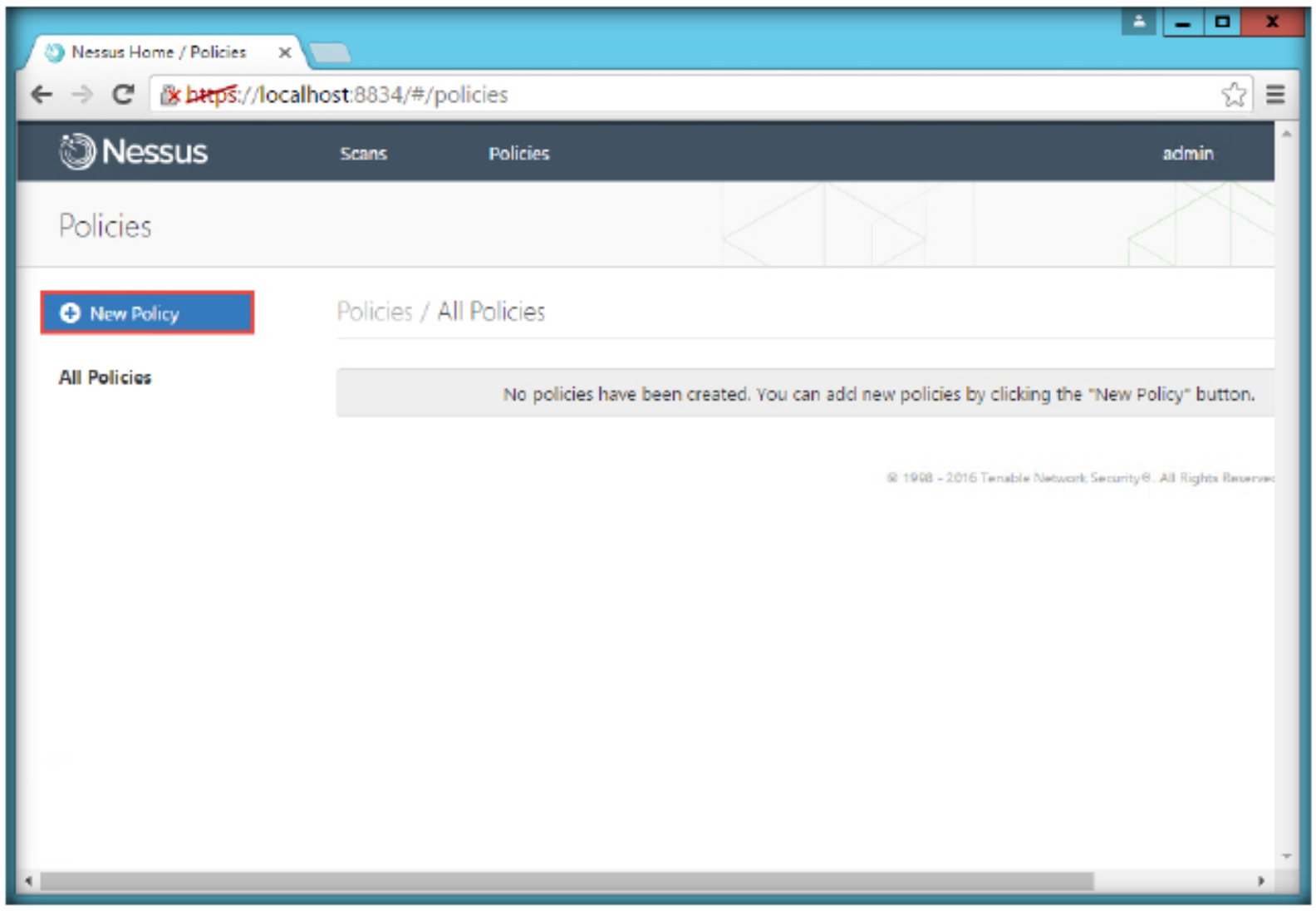


FIGURE 1.16: Adding a new policy in Nessus

27. The **Policy Library** window appears. Click **Advanced Scan**

warning, a custom certificate to your organization must be used.

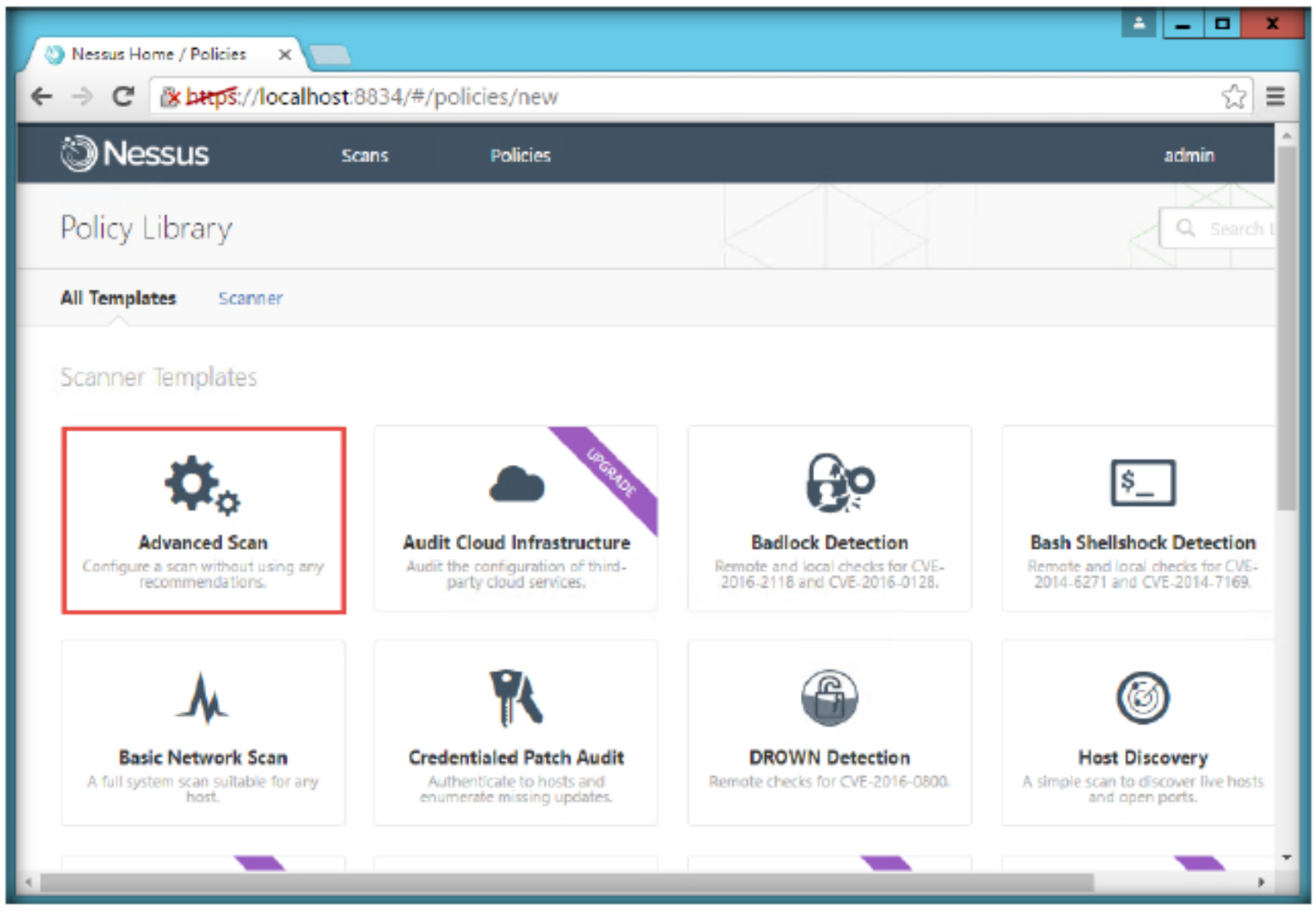


FIGURE 1.17: Choosing Advance scan from the Policy Library

28. The **New Policy / Advanced Scan** section with **General** settings appears under the **BASIC** tab.
29. Specify a policy name in the **Name** field (we are using **NetworkScan_Policy**), and give a **description** about the policy.

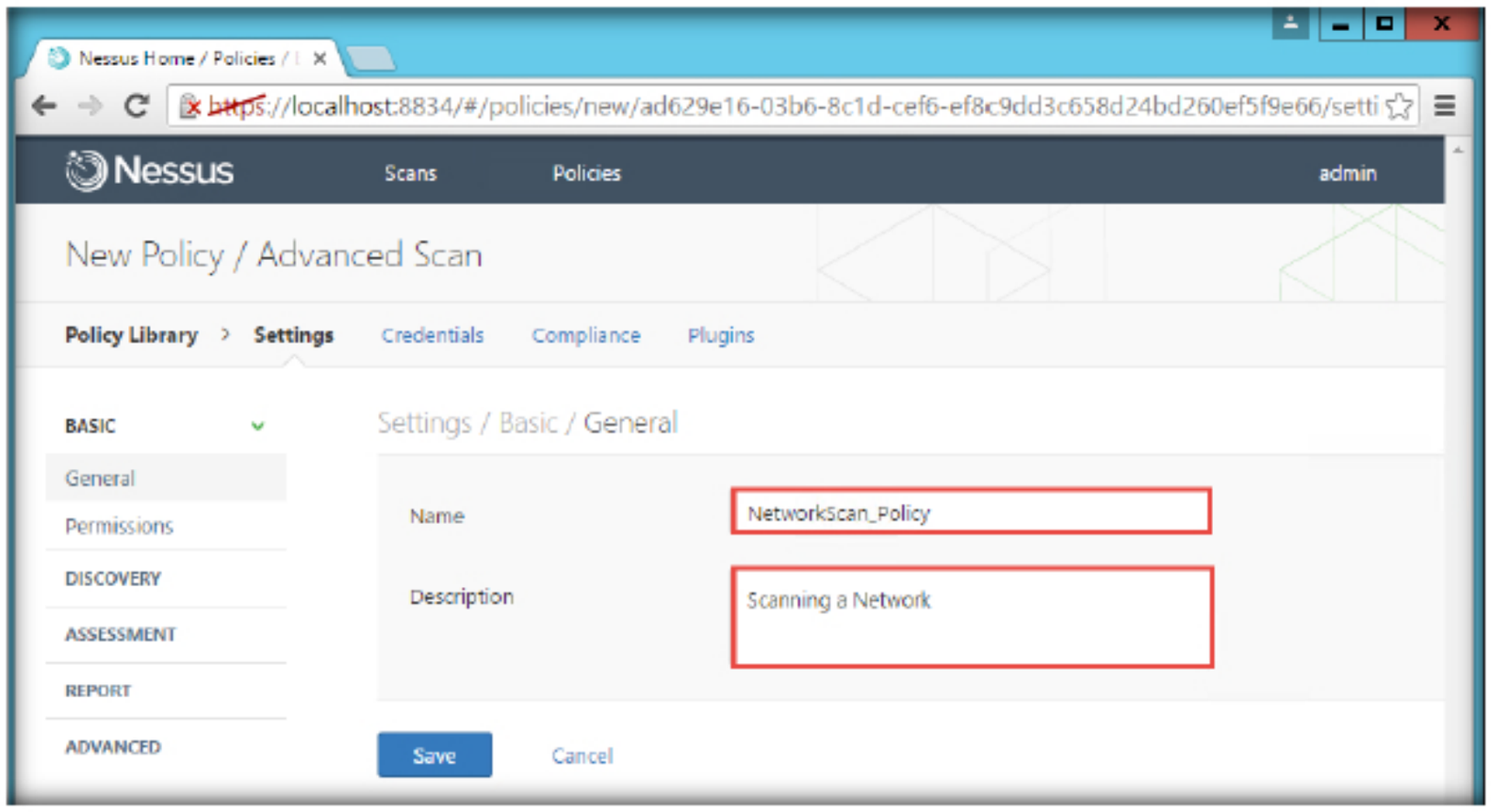


FIGURE 1.18: Customizing the general settings

TASK 3

Configure a Network Policy

30. Click the **DISCOVERY** tab in the left pane. **Host discovery** (which is a sub unit of Discovery) will appear.

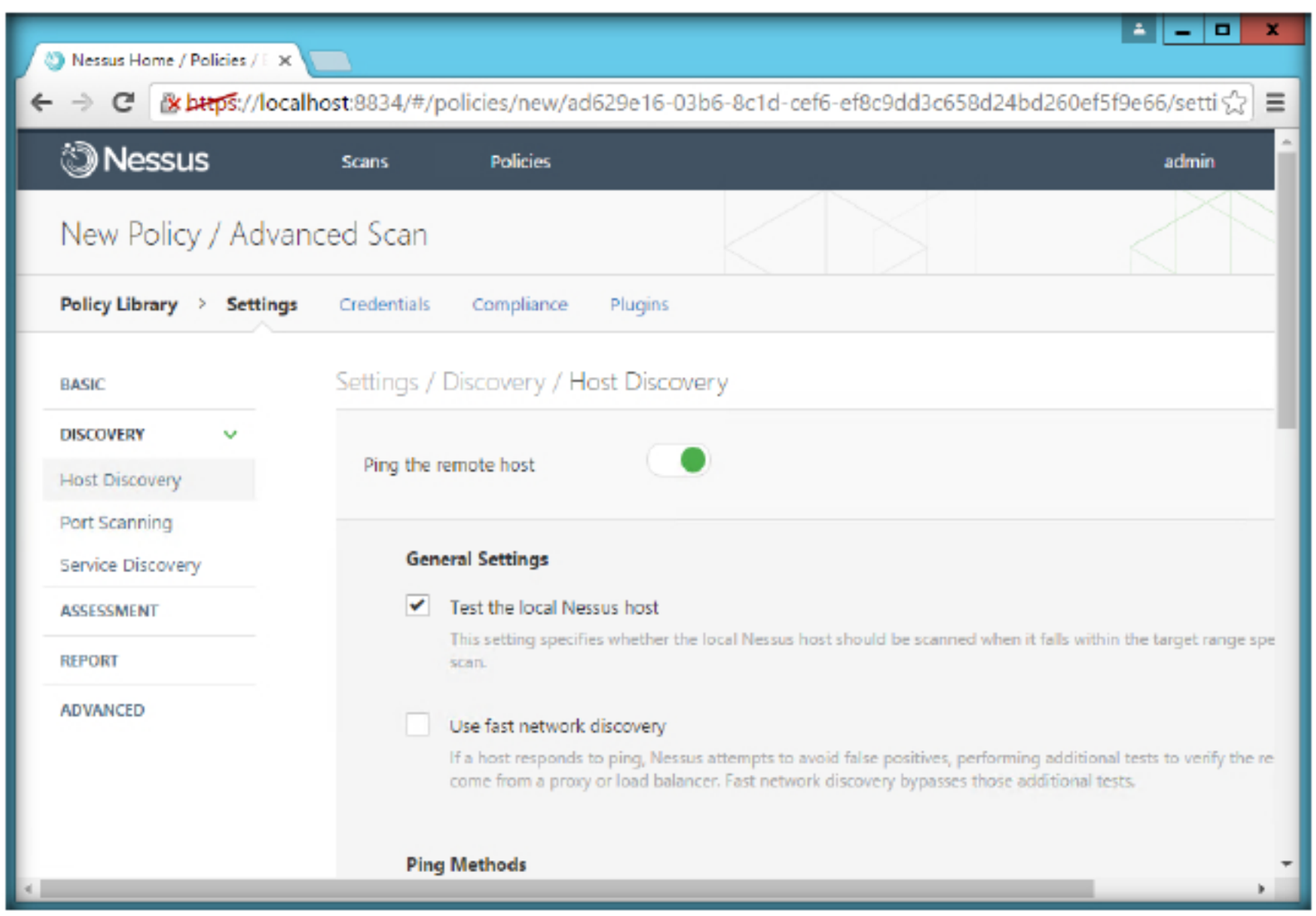


FIGURE 1.19: Host Discovery tab

31. Switch off the **Ping the remote host** button, check **Scan Network Printers** and **Scan Novell Netware hosts**. Next, click on the **Port Scanning** tab under Discovery.

The Nessus Server Manager used in Nessus 4 has been deprecated

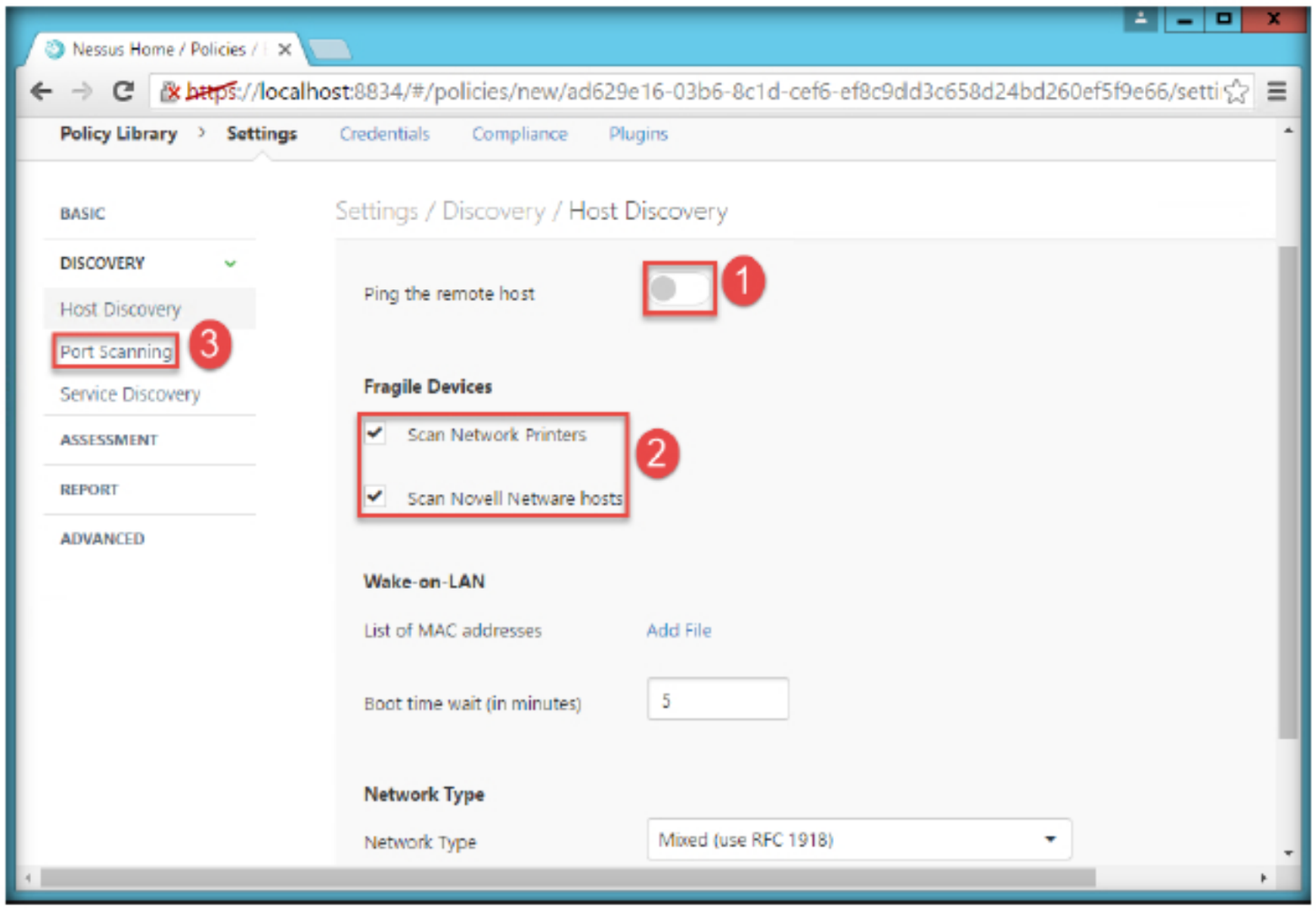


FIGURE 1.20: Customizing the Host Discovery tab

32. Click the checkbox to **Verify open TCP ports found by local port enumerators** and click on the **Service Discovery** tab.

Path of Nessus home directory for windows \programfiles\tenable\nessus

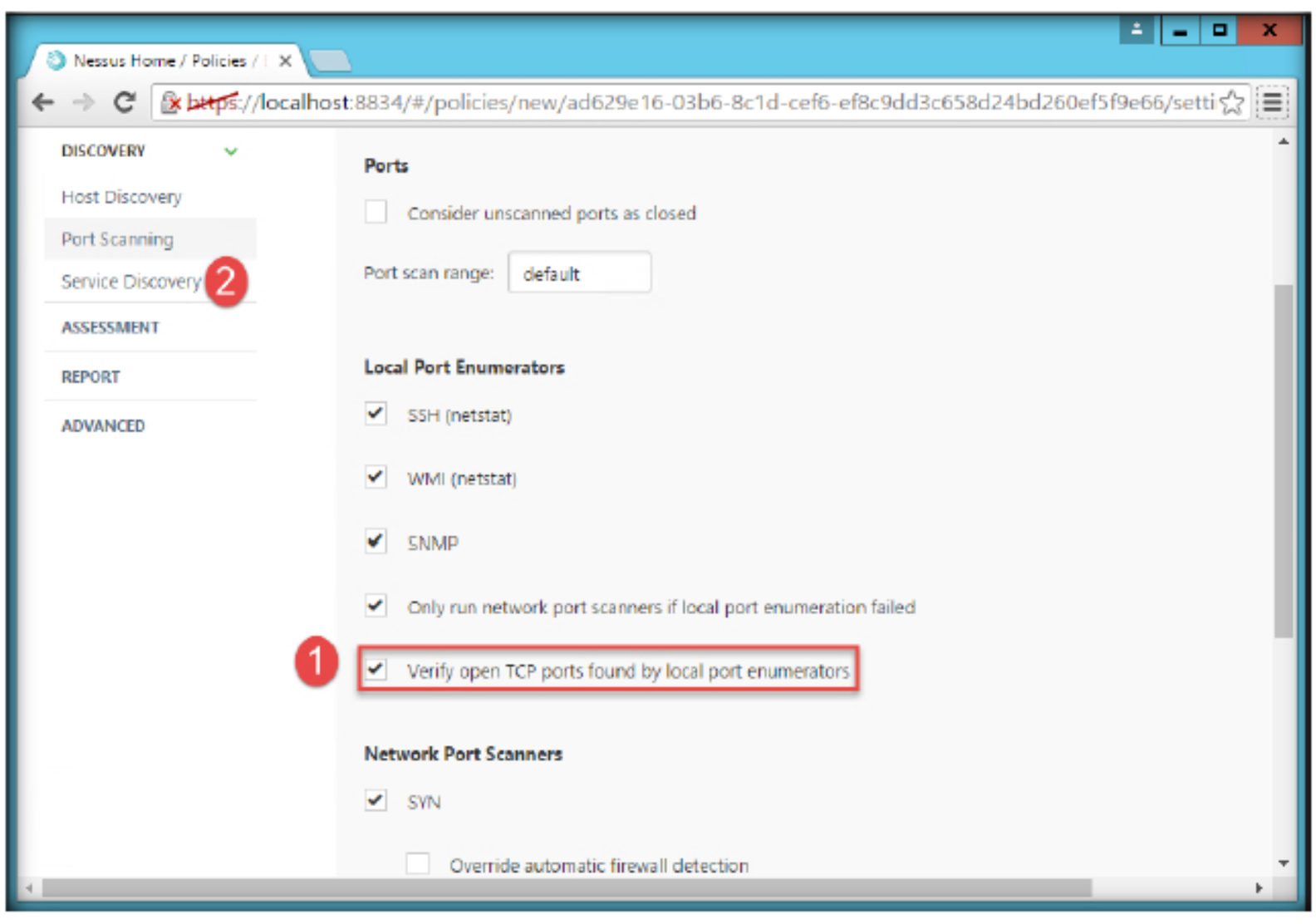


FIGURE 1.21: Customizing the Port scanning options

33. In the Service Discovery section, check the **Enable CRL checking** box then click **ASSESSMENT** in the left pane.

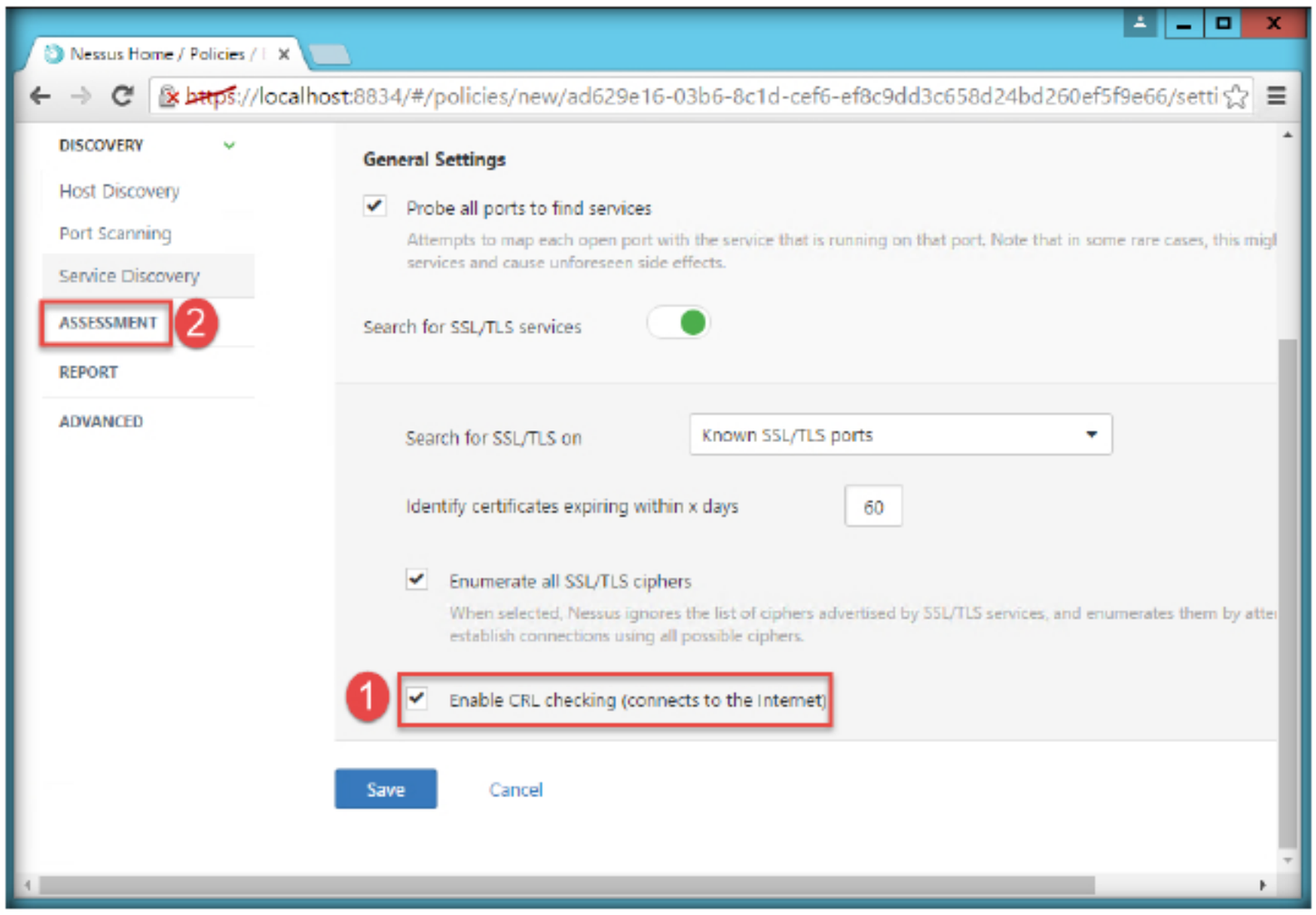


FIGURE 1.22: Customizing the Service Discovery tab

***WARNING:** Any changes to the Nessus scanner configuration will affect ALL Nessus users. Edit these options carefully*

34. In the ASSESSMENT section, click the **Web Applications** tab and turn on **Scan Web Applications**, this option will scan if you have any web applications running on the machine.

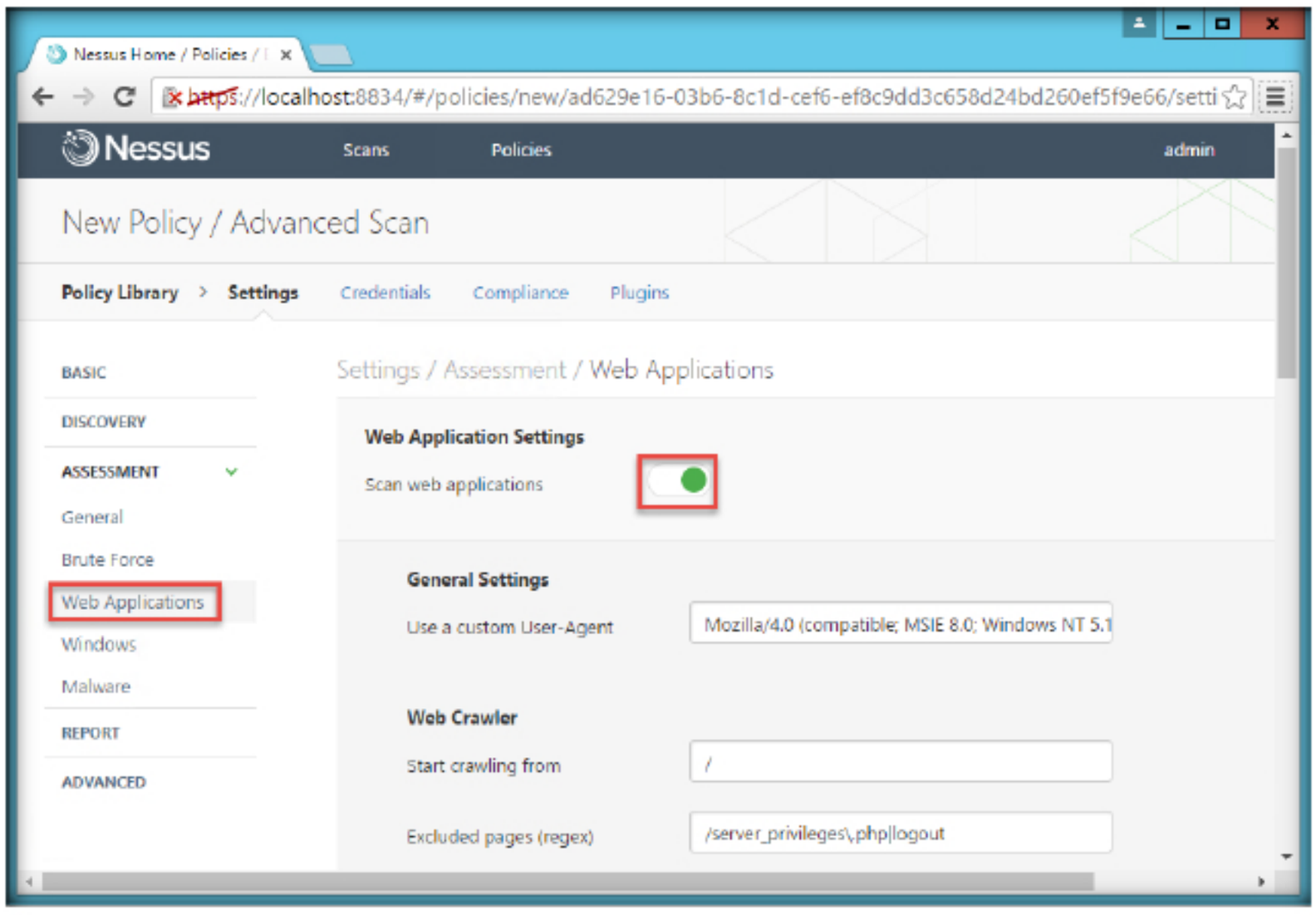


FIGURE 1.23: Customizing the Web Applications tab

35. Click on the Advanced tab and set the **Max number of concurrent TCP sessions per host** and the **Max number of concurrent TCP sessions per scan** as 10000.

Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments. Nessus prevents network attacks by identifying the vulnerabilities and configuration issues that hackers use to penetrate your network.

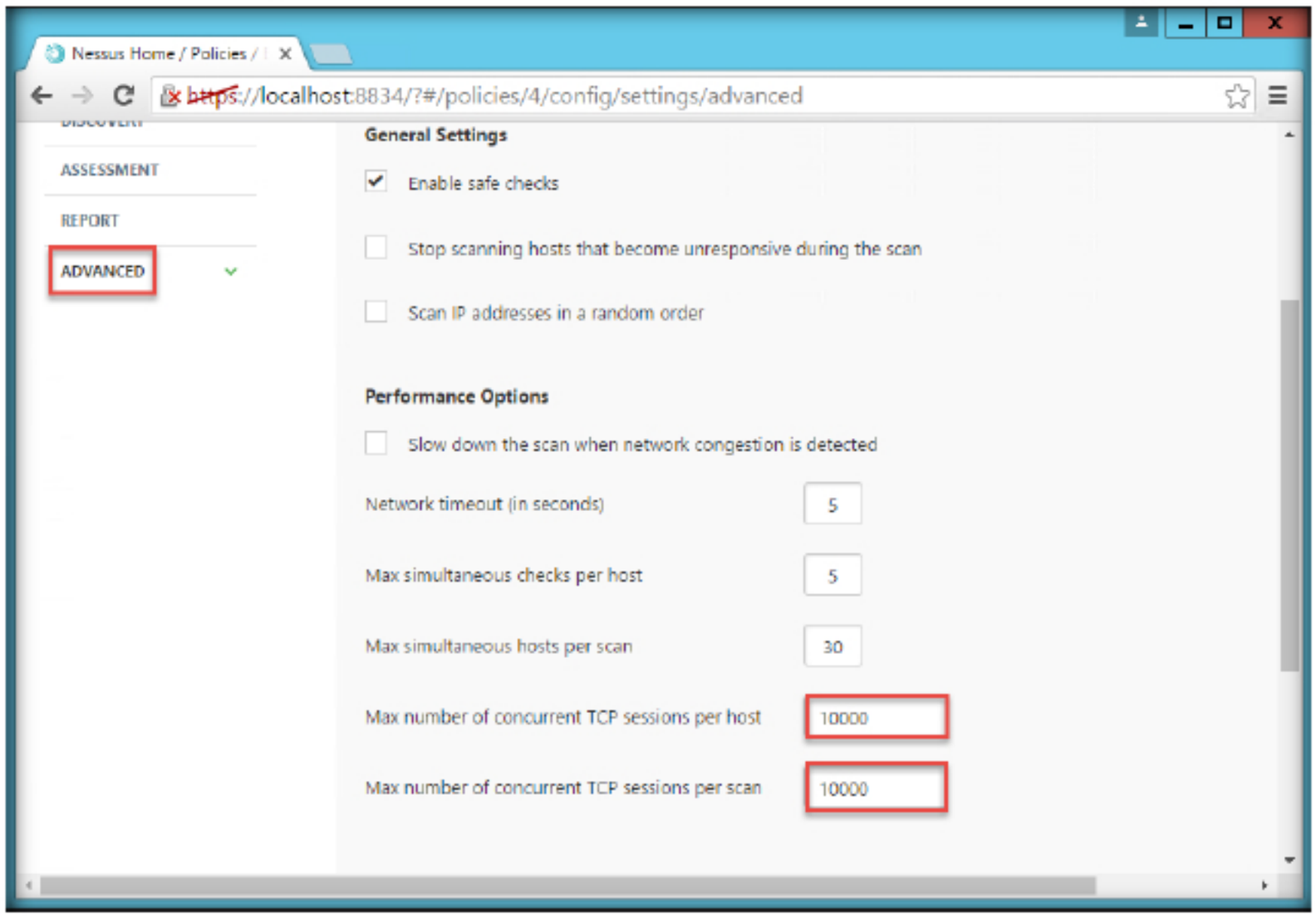


FIGURE 1.24: Customizing the Advanced tab

36. Click **Credentials** on the **menu** bar. Expand the **Host** tab in the left pane.

Nessus supports the widest range of network devices, operating systems, databases, applications in physical, virtual and cloud infrastructures.

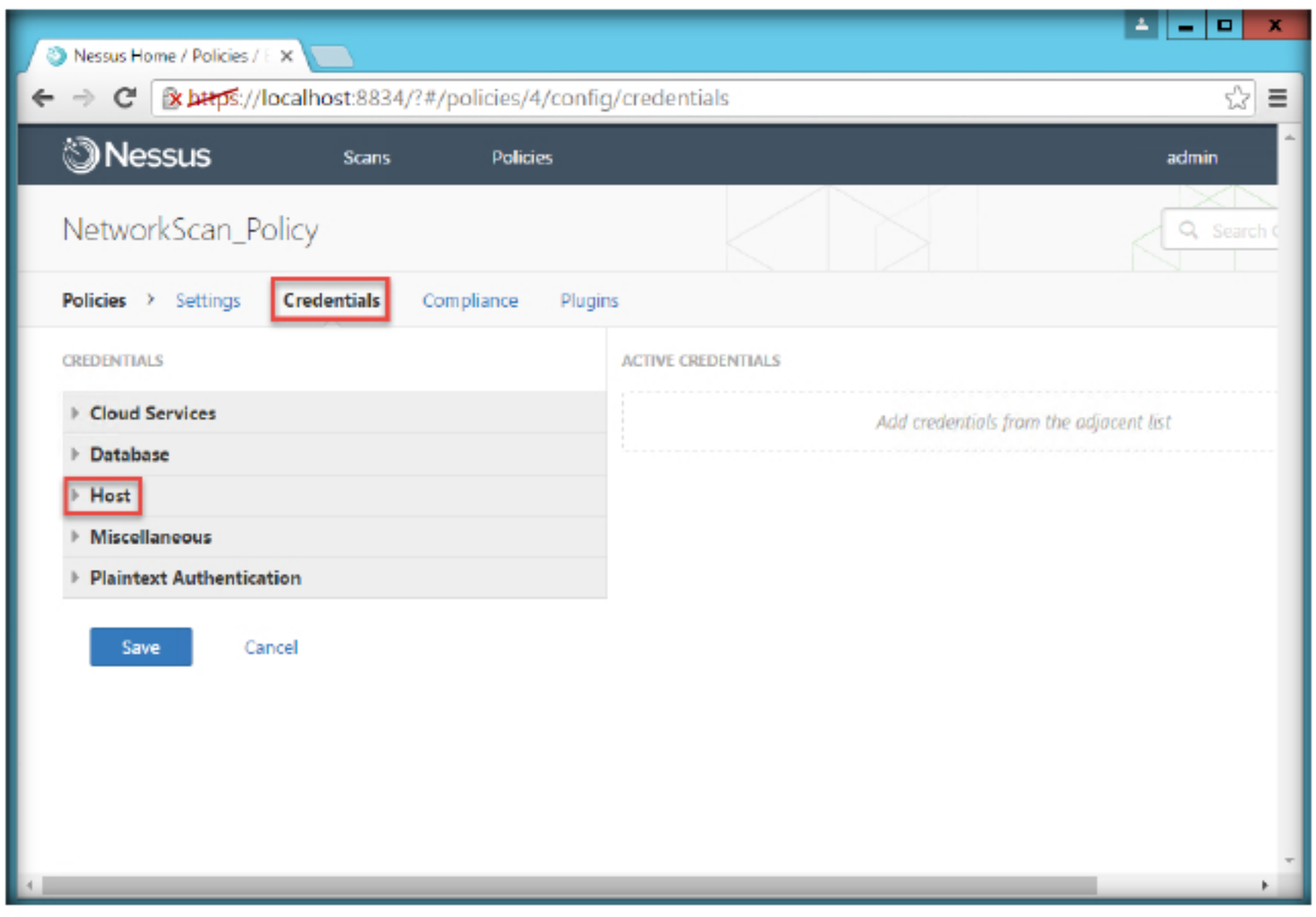


FIGURE 1.25: Customizing the credentials

37. After expanding Hosts, a Windows tab appears below Hosts. Click on the **Windows** tab. A **Windows Active Credential** appears on the right.

The most effective credential scans are those for which the supplied credentials have root privileges.

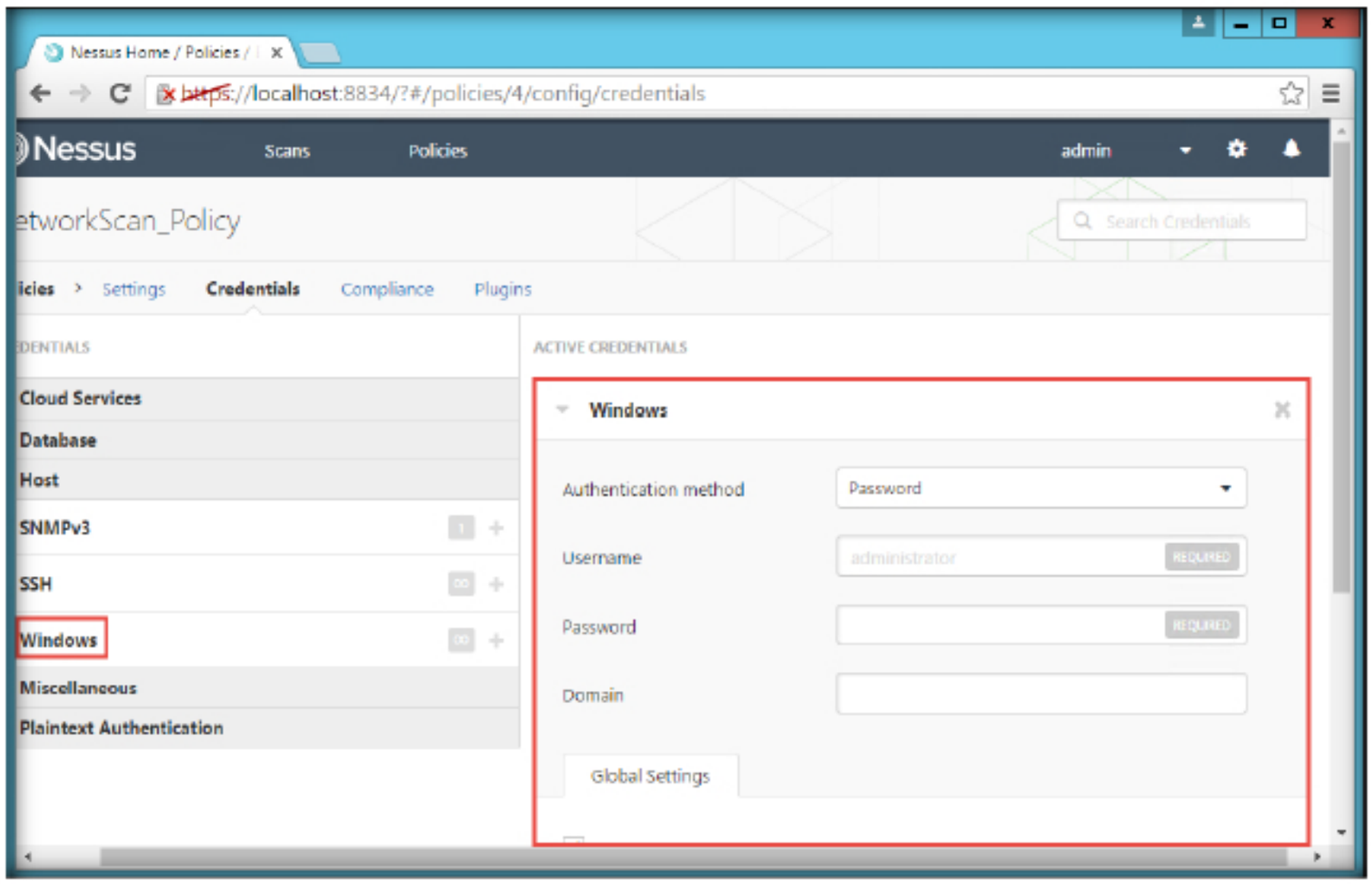
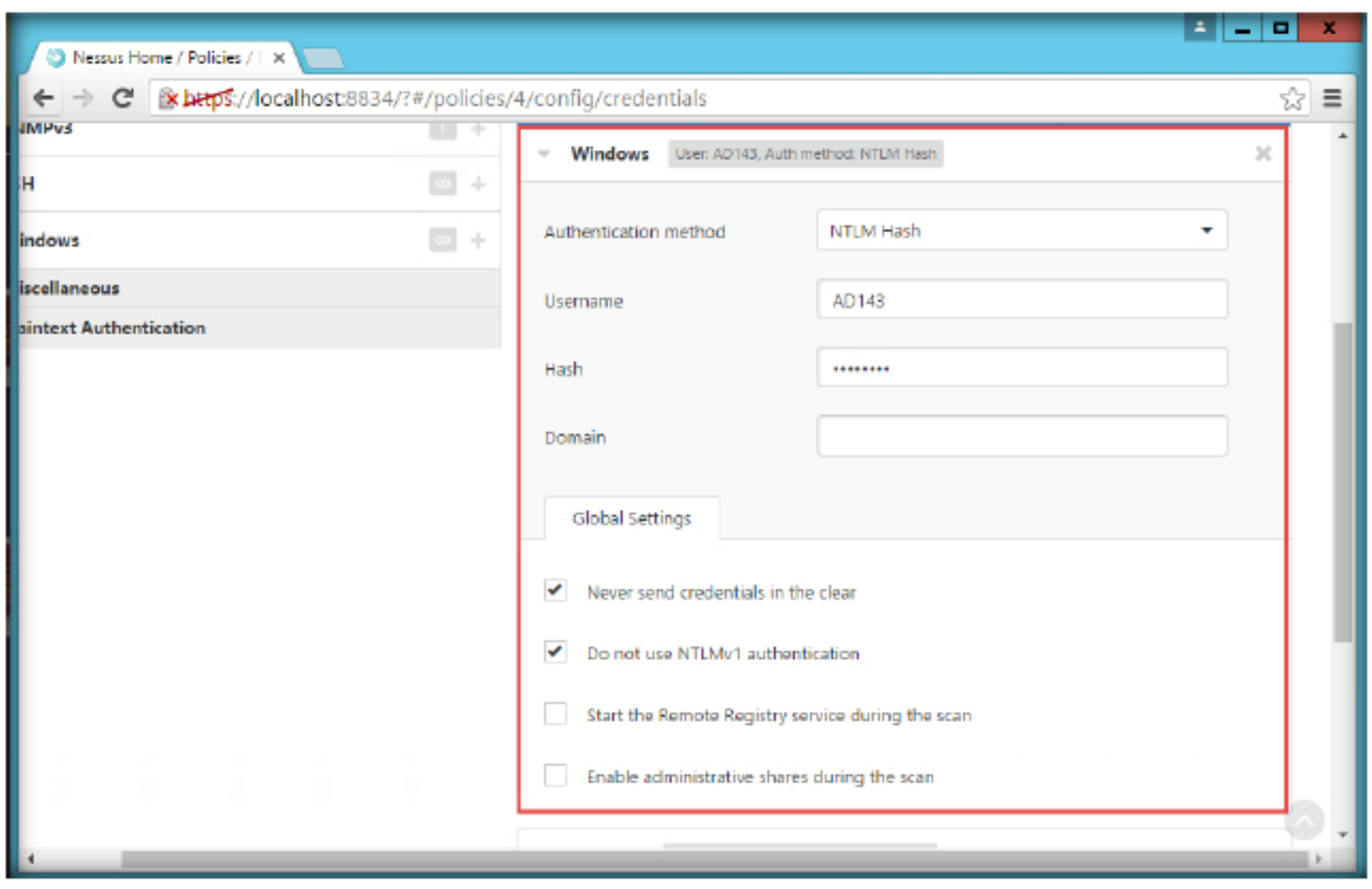


FIGURE 1.26: Adding Windows hosts

38. Select **NTLM hash** as the **Authentication method** from the drop down. The username will be **AD143** and the hash is **qwerty@123**.



If the policy is successfully added, then the Nessus server displays a confirmation message.

FIGURE 1.27: Adding Windows credentials

39. Add another three Windows hosts by following the same steps as above. The Username will be **AD144, AD145 and AD146** respectively and the hash value is common for all three. It is **qwerty@123**.

40. Now, expand the **Database** tab which is above the Host tab. Under the Database tab click **Database** to add a New Database.

If you are using Kerberos, you must configure a Nessus scanner to authenticate a KDC.

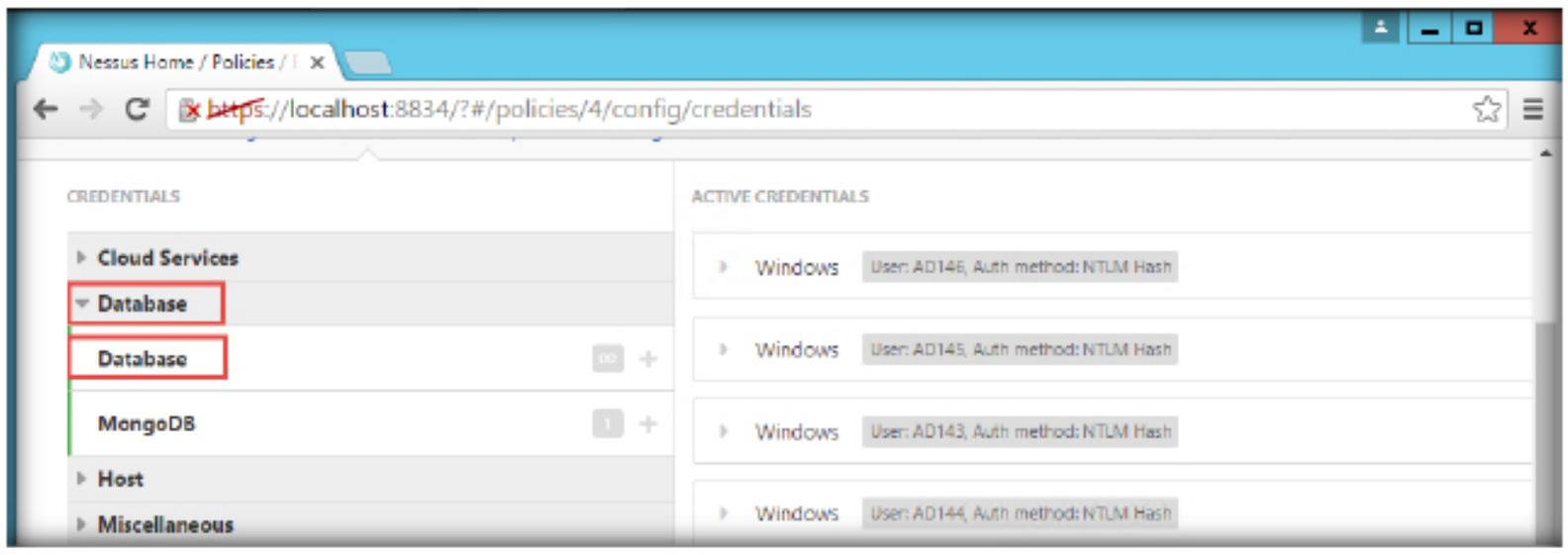


FIGURE 1.28: Adding a Database

41. A new Database window opens in the right pane. Enter the Admin **Login** details created in Step 12.

42. Enter the Database SID: **4587**; Database port to use: **124**; and select the Oracle Auth type: **SYSDBA**.

To scan the window, input the field name, type, policy, scan target, and target file.

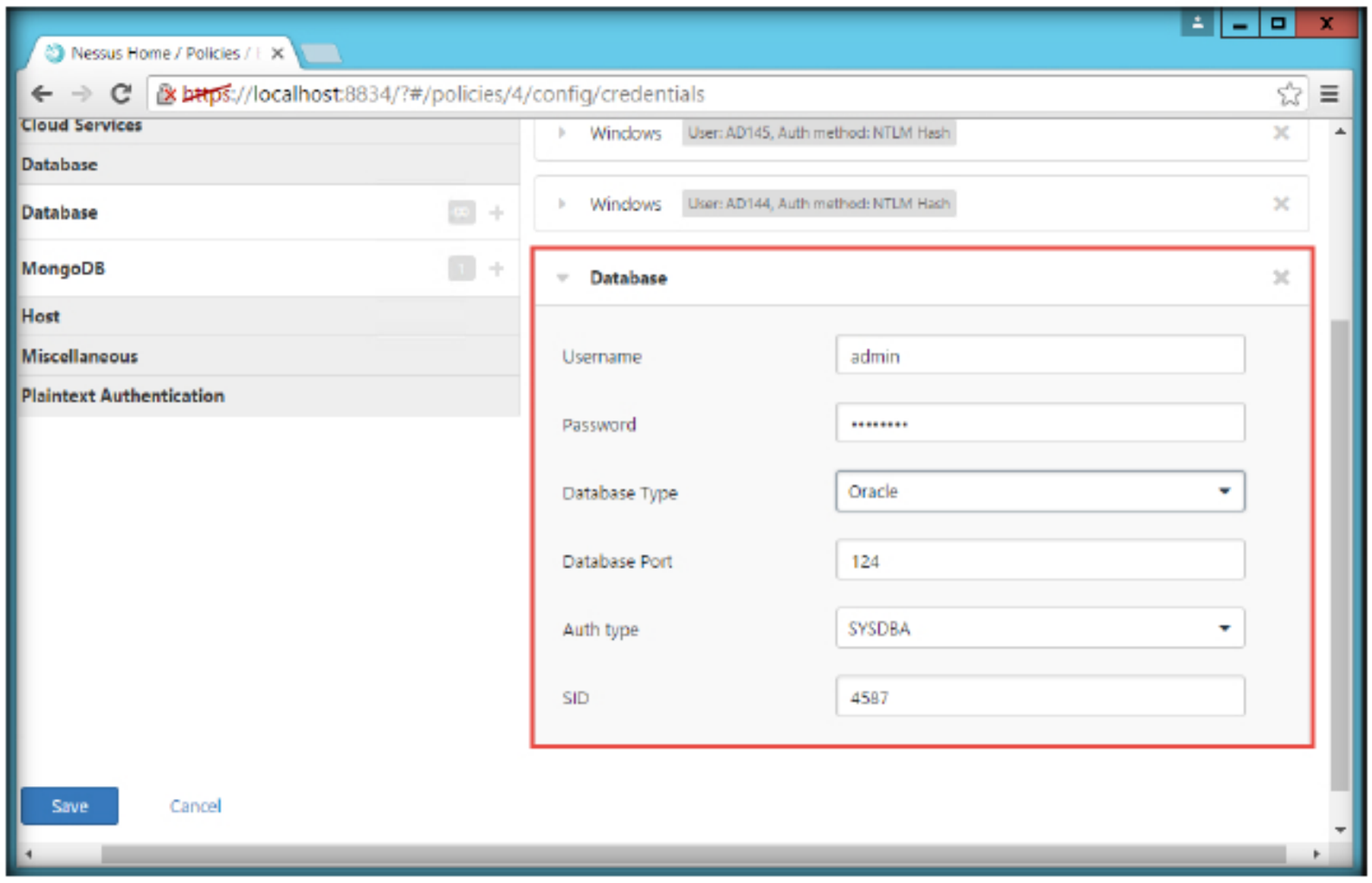


FIGURE 1.29: Adding Database credentials

43. Click **Save**.

Nessus has the ability to save configured scan policies, network targets, and reports as a Nessus file.

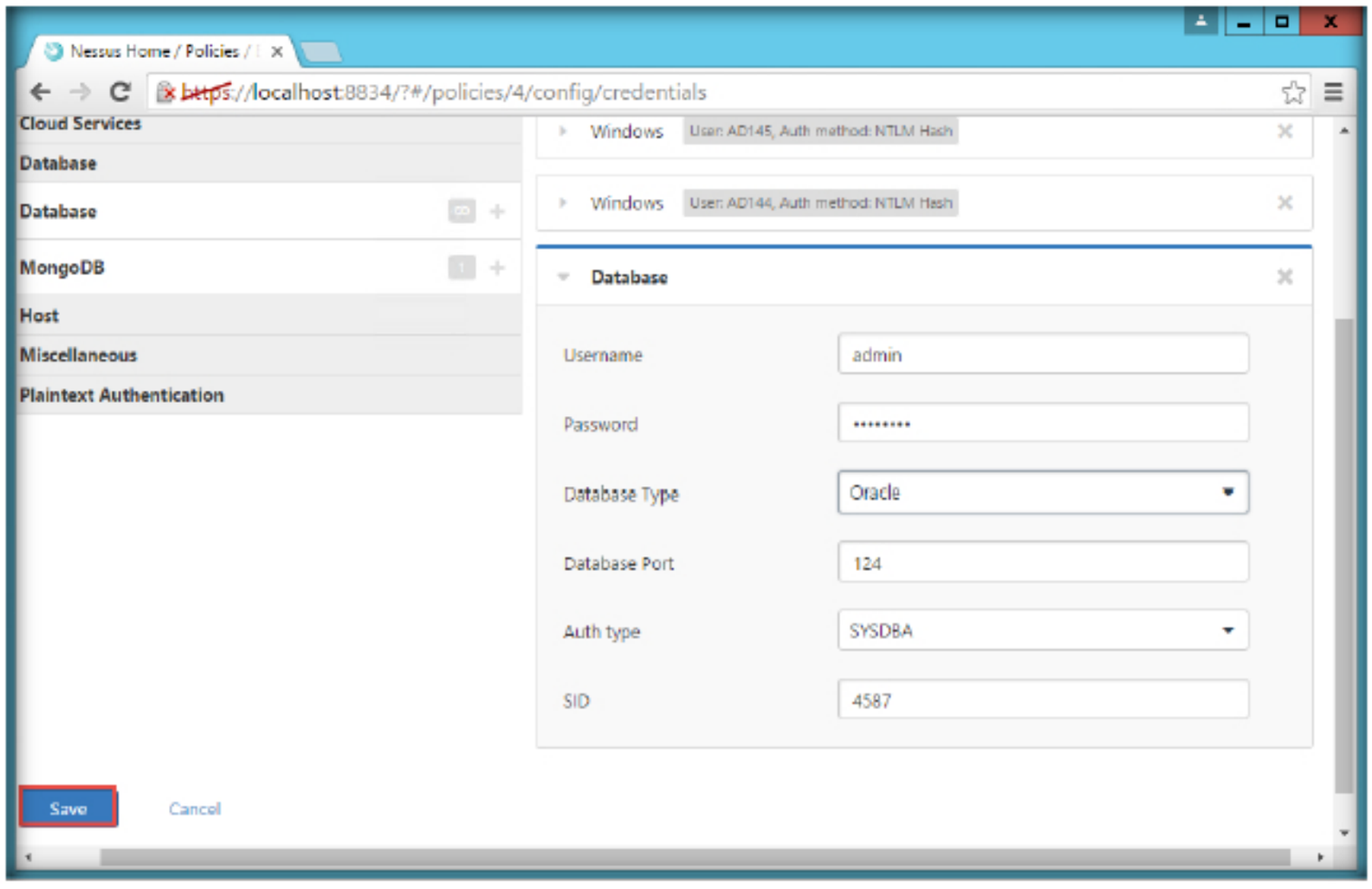


FIGURE 1.30: Saving the settings

44. A **Policy updated successfully** notification appears, and the policy is added as in the Nessus/ Policies window, as shown.

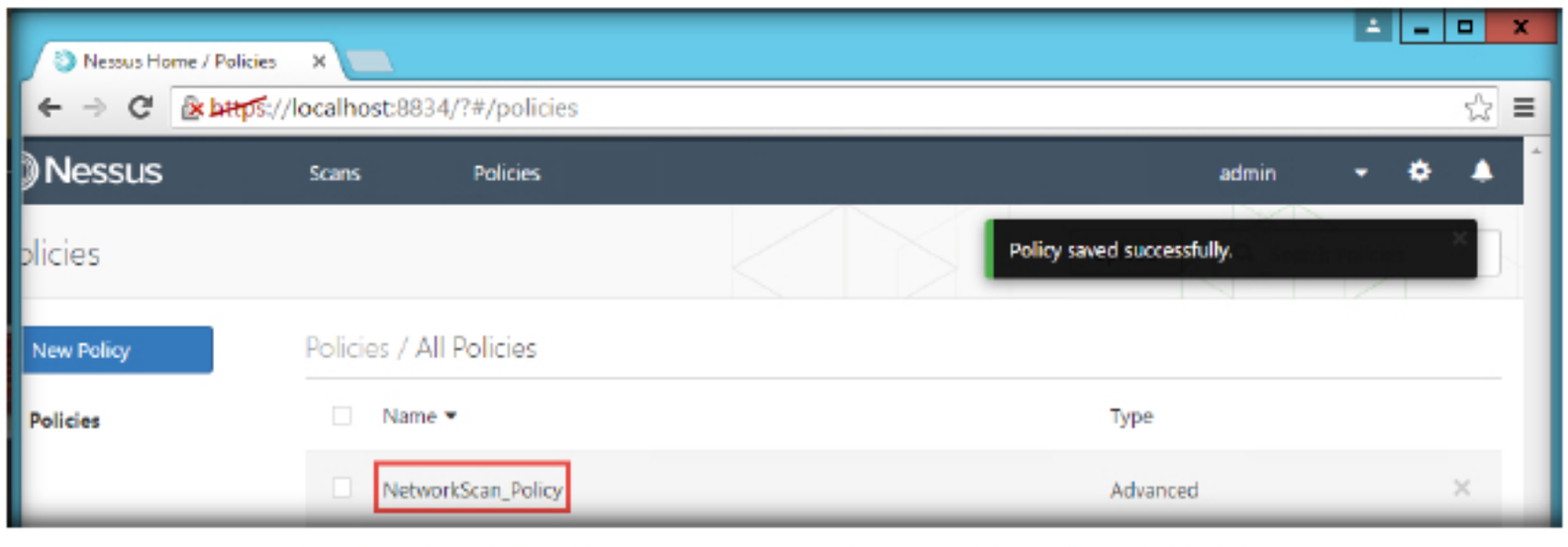


FIGURE 1.31: The Nessus - Policies window with the newly added policy

TASK 4

Launch a Network Scan

45. Now, click **Scans** → **+ New Scan** to open the **New Scan Template** window.

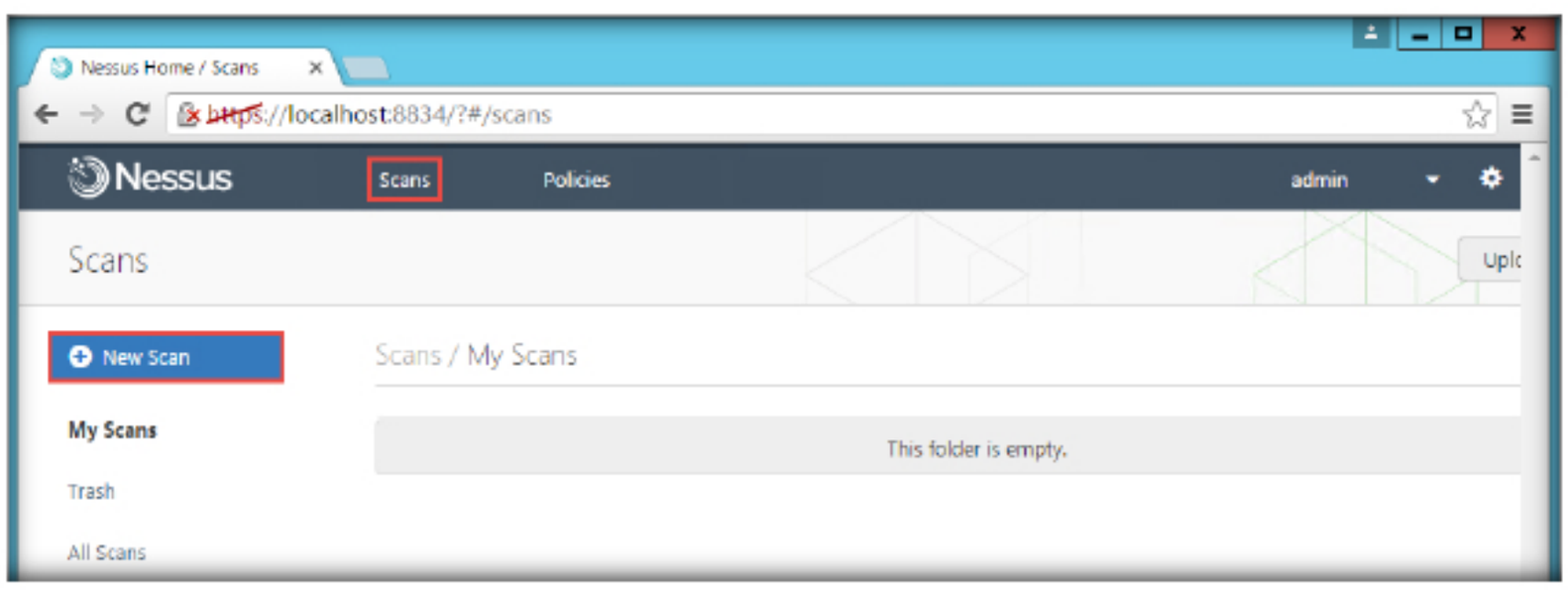


FIGURE 1.32: Adding a New Scan

46. Click on the **User** tab on the menu bar.

Nessus supports non-credentialed, remote scans; credentialed, local scans for deeper, granular analysis of assets; and offline auditing on a network device's configuration.

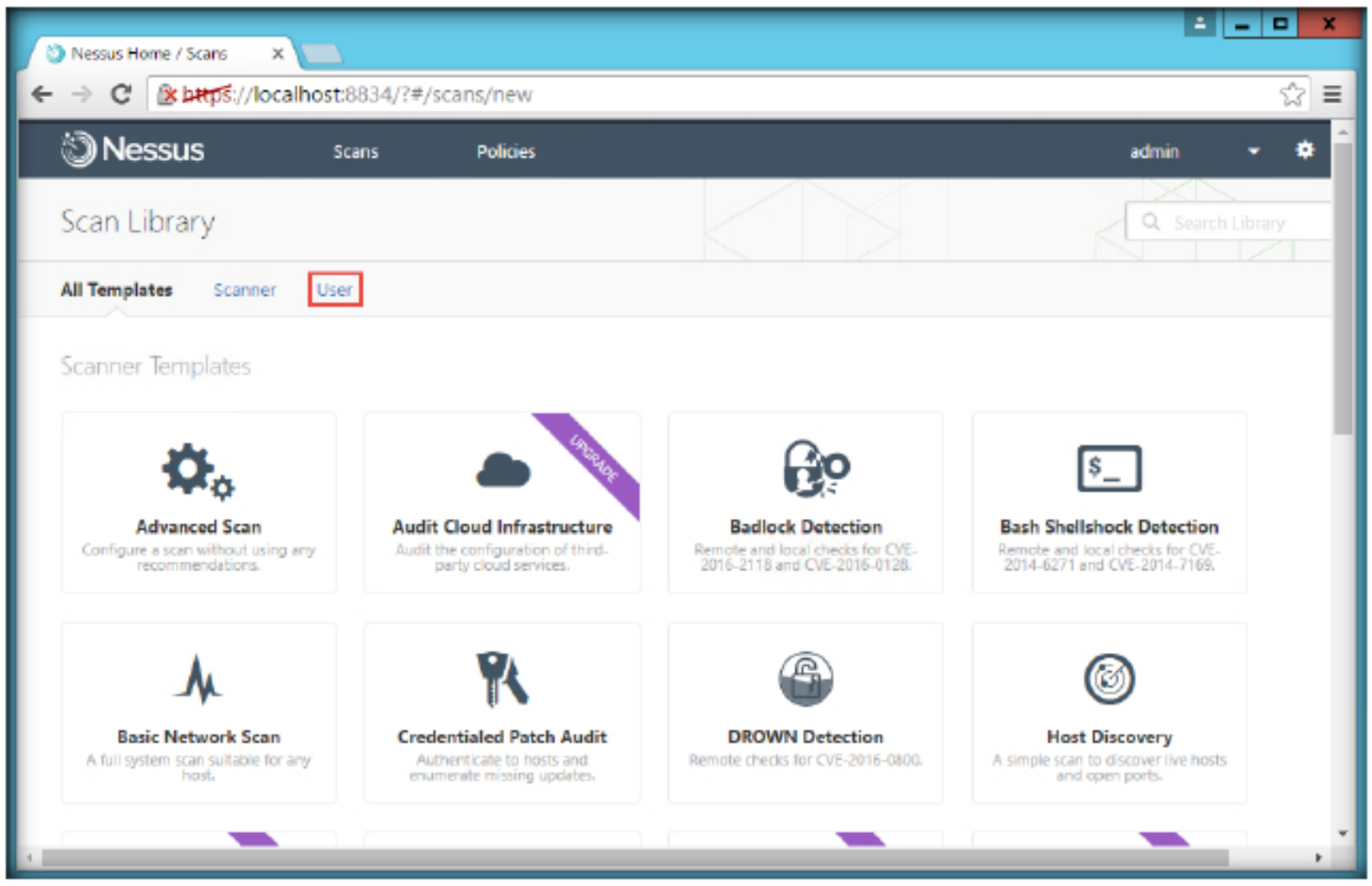


FIGURE 1.33: Selecting the user tab

47. Click on the policy created. (**NetworkScan_Policy**)

Nessus has more than 450 templates are available for compliance (e.g., FFIEC, HIPAA, NERC, PCI, more) and configuration (e.g., CERT, CIS, COBIT/ITIL, DISA STIGs) auditing.

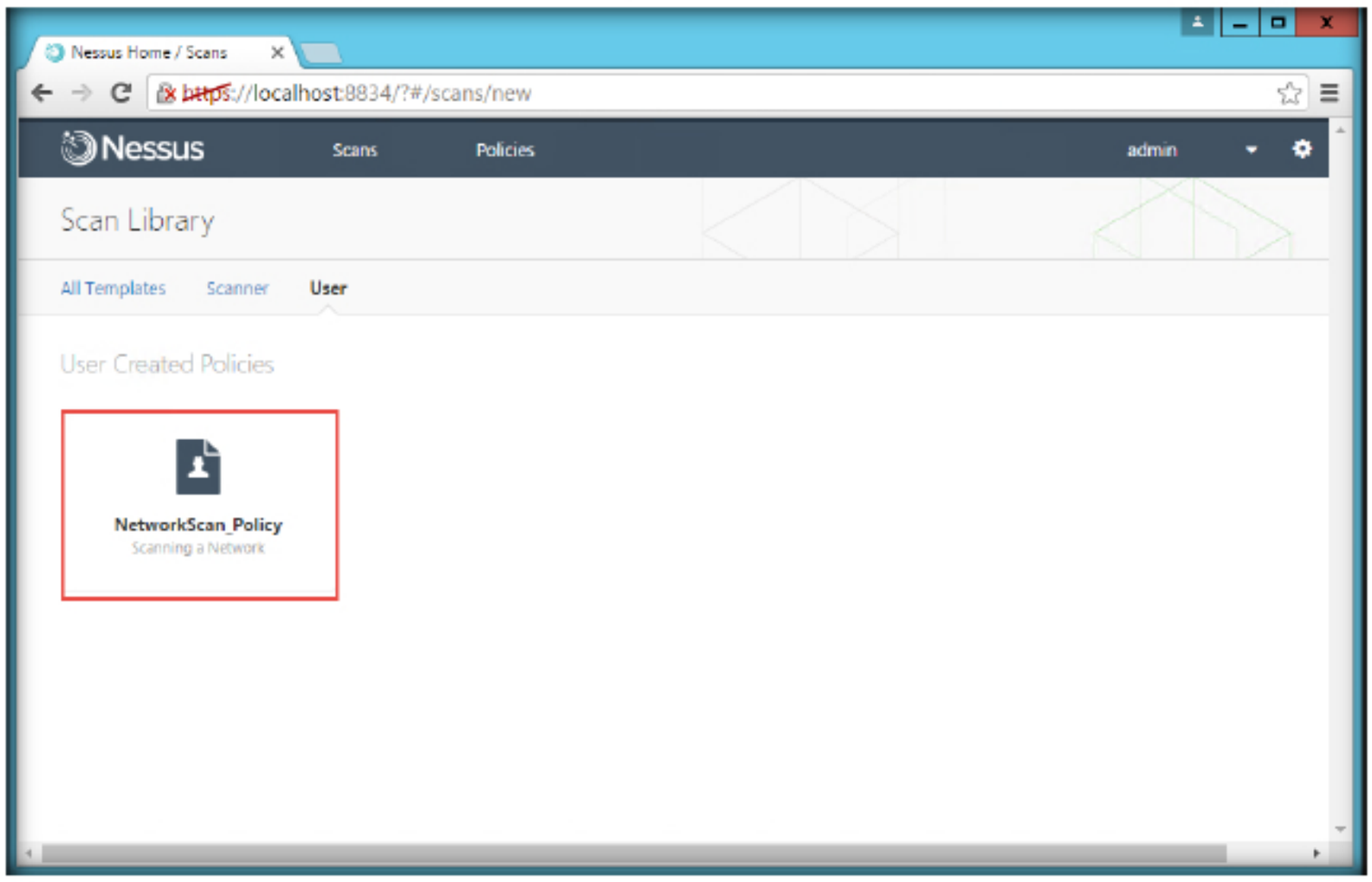


FIGURE 1.34: Selecting the created policy

Nessus scans for viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes as well as web services linking to malicious content.

48. Input the **Name** of the scan (for this lab use Local Network), then enter the **Description** for the scan.
49. In **Scan Targets**, enter the IP address of the target on which you want to perform the vulnerability assessment. In this lab, it is the **Windows 10** virtual machine and the IP address is **10.10.10.10**.

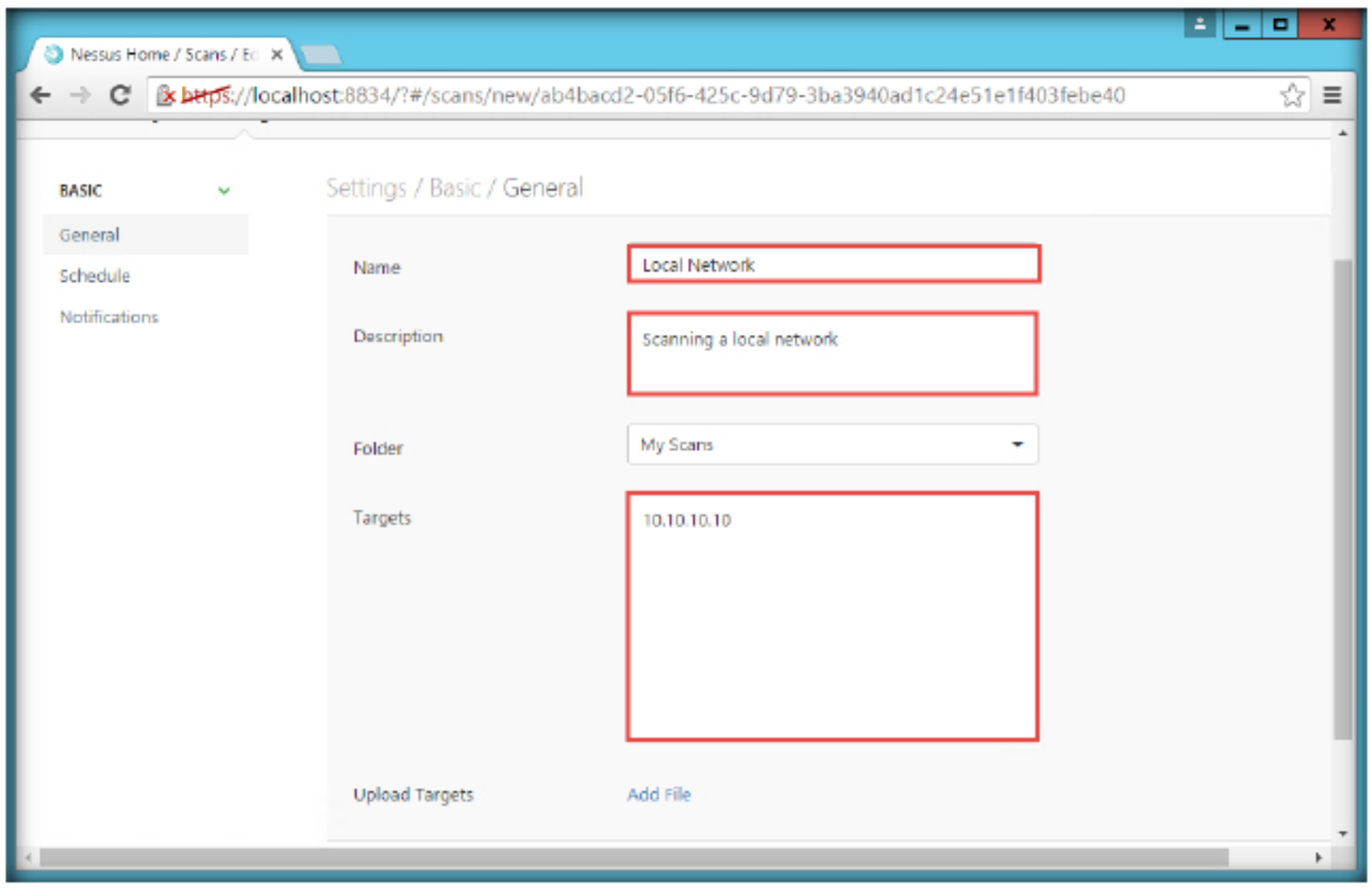


FIGURE 1.35: Configuring the basic settings in the scans window

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

50. Click **Save**.

Report what matters to responsible parties with exploitability, severity modification, scan scheduling and deliver remediation reports via targeted emails.

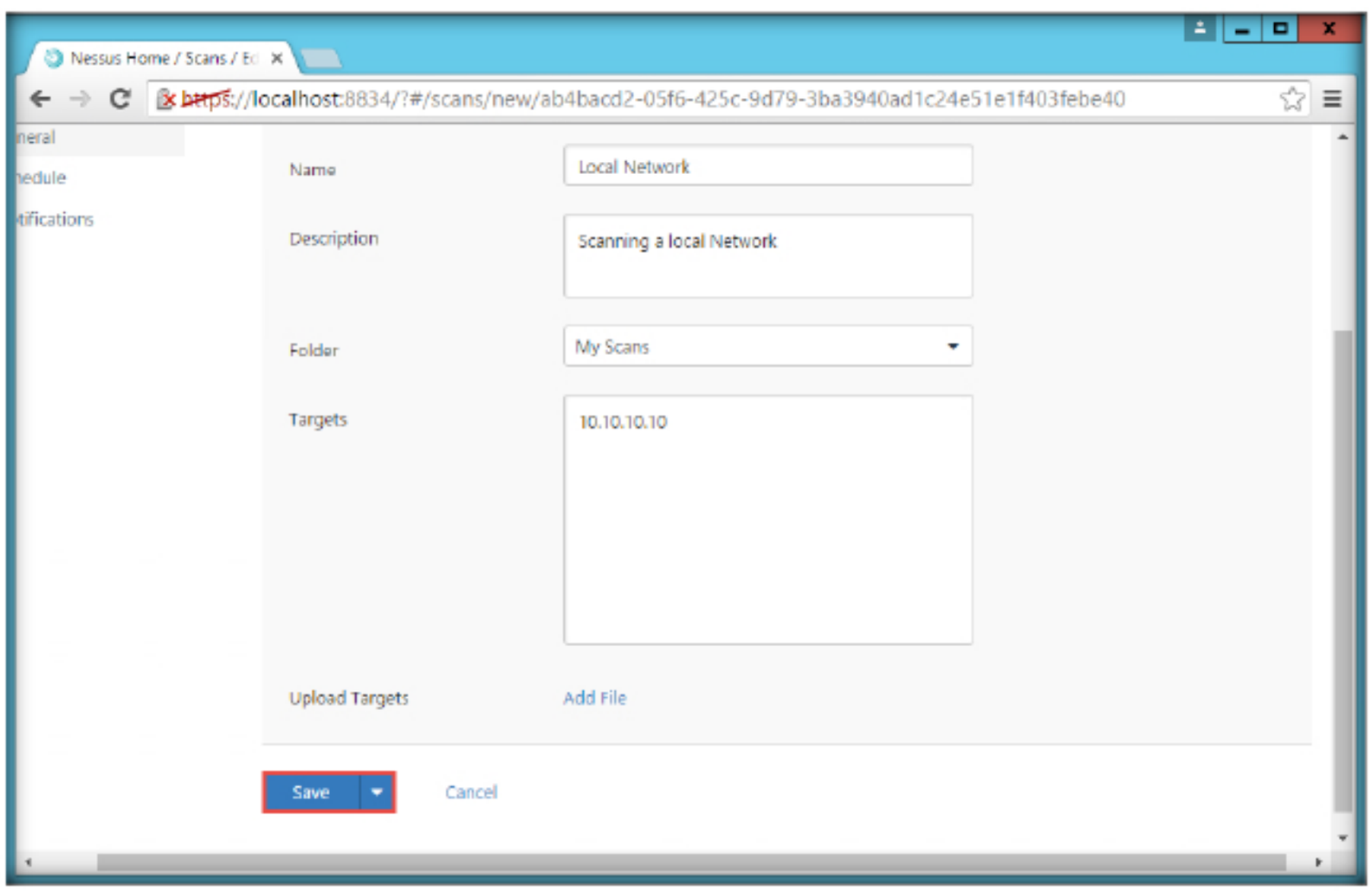


FIGURE 1.36: Saving the scan settings

51. You can view the new scan file created. The **Scan saved Successfully** message appears.

Every audit in the Tenable Nessus vulnerability scanner is coded as a plugin: a simple program which checks for a given flaw. Nessus uses more than 60,000+ different plugins, covering local and remote flaws.

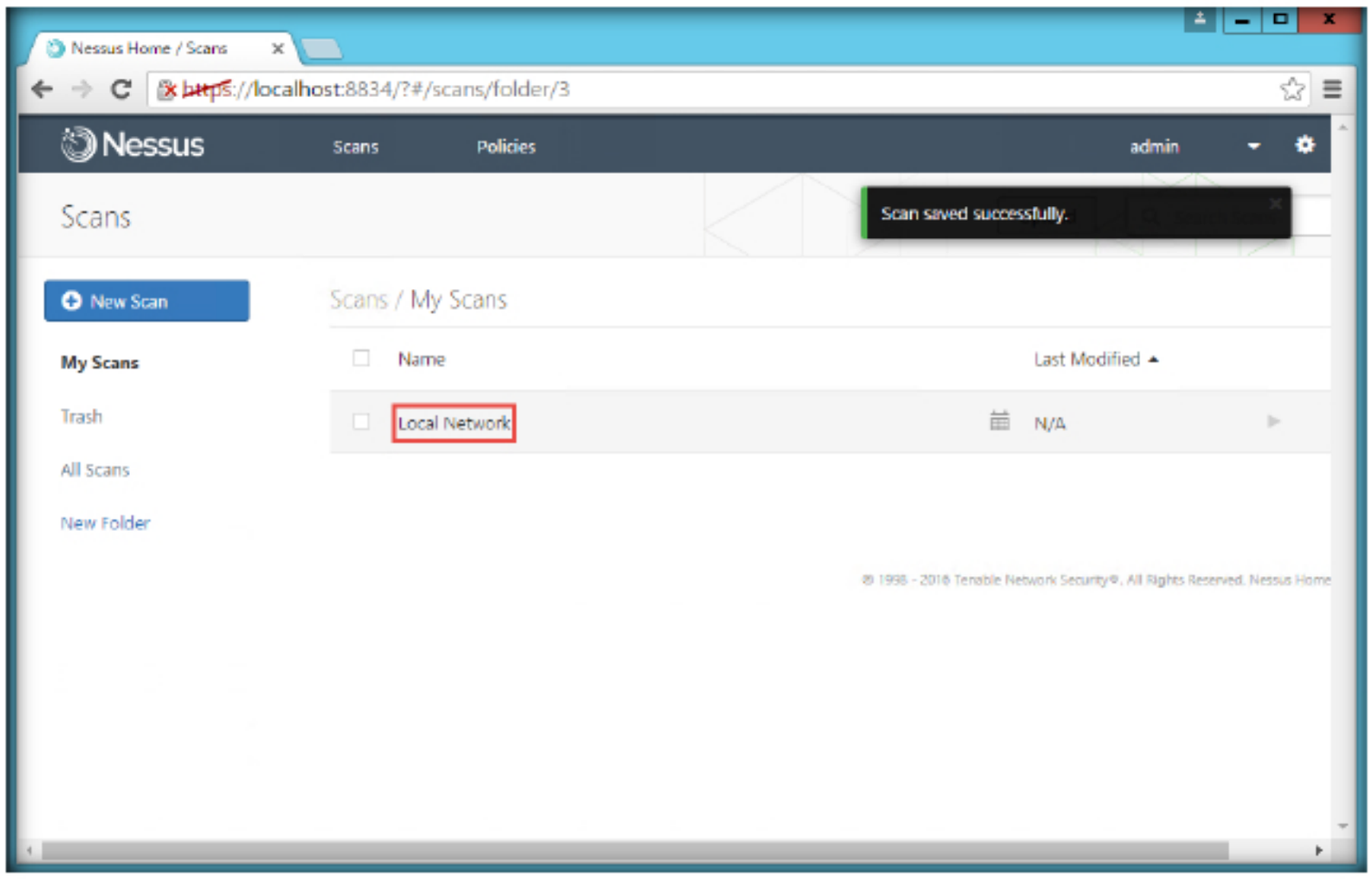


FIGURE 1.37: Scan settings saved successfully

52. Click on the **Launch** symbol to start the scan.

Badlock Detection

This policy is used to perform remote and local checks for the Badlock vulnerability (CVE-2016-2118 and CVE-2016-0128).

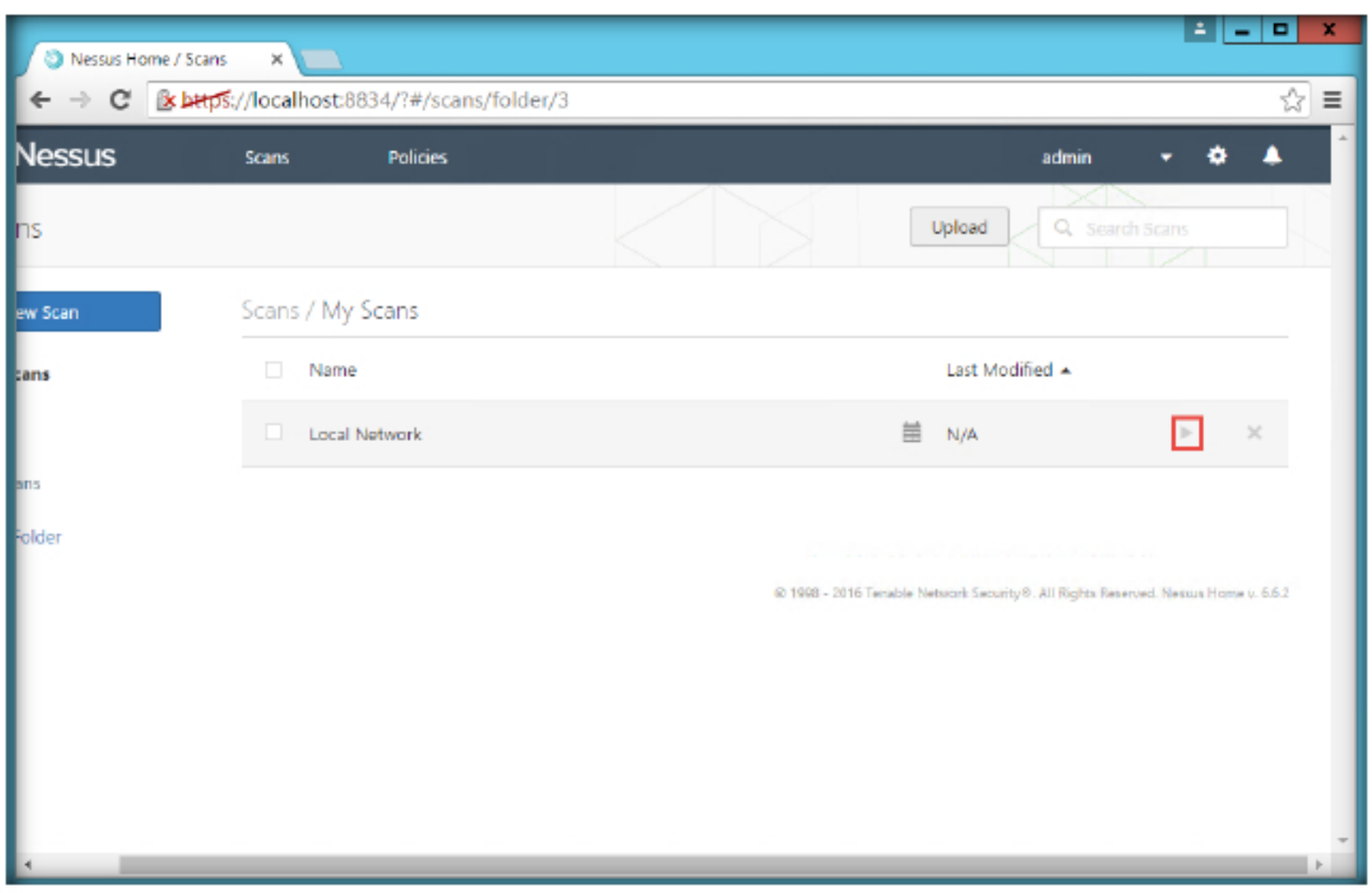


FIGURE 1.38: Launching the scan

53. Click on the scan name (**Local Network**) to view the status. Wait for the scan to complete.

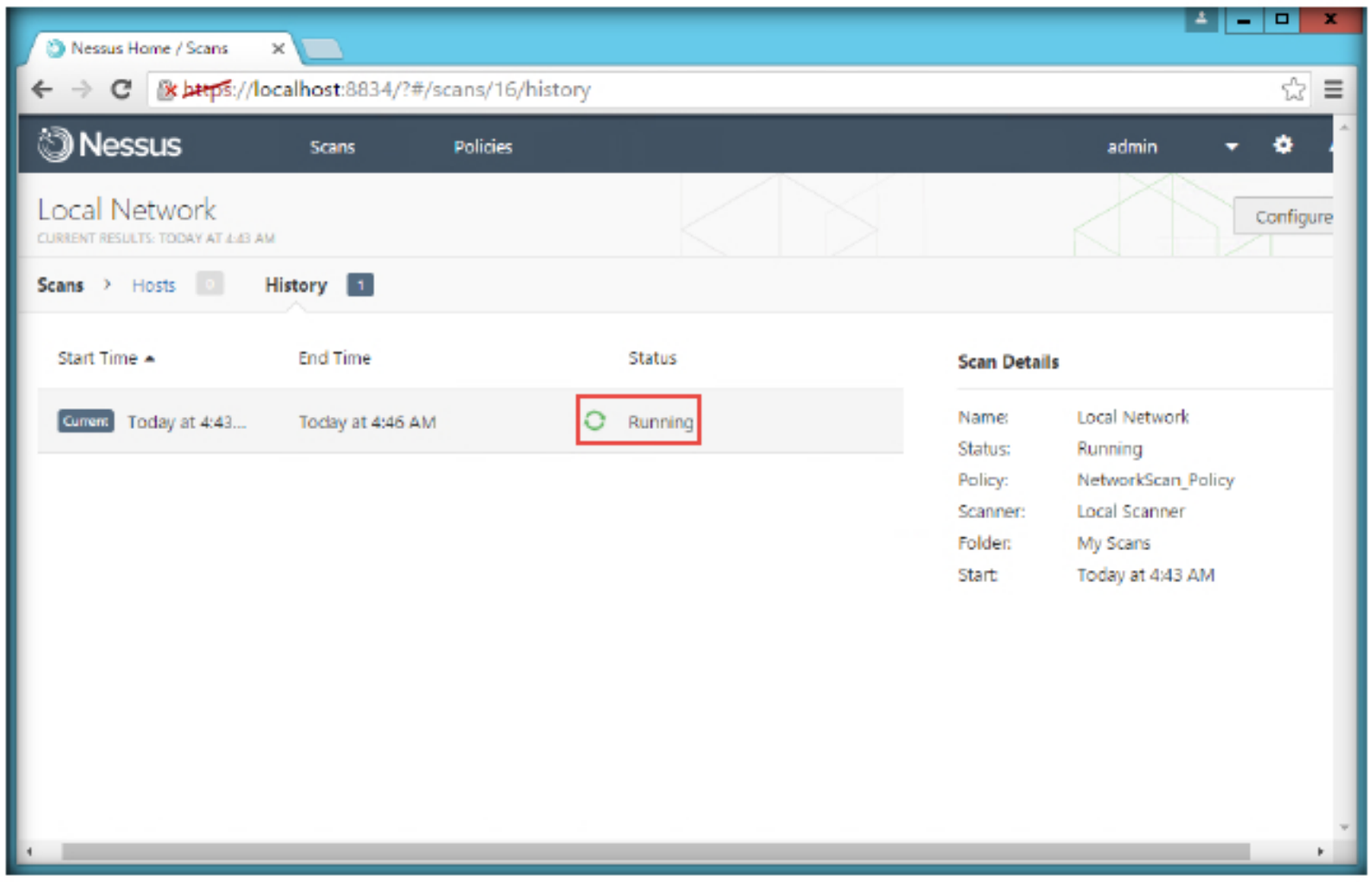


FIGURE 1.39: Scanning the Device

Bash Shellshock Detection

This policy is used to perform remote checks for the Shellshock vulnerability (CVE-2014-6271) via HTTP, FTP, SMTP, telnet, and SIP. SSH credentials can optionally be provided to test for CVE-2014-6271 via SSH and enumerate missing software updates for CVE-2014-6271 and CVE-2014-7291.

54. Once the scan is complete, the status changes to **Completed**.

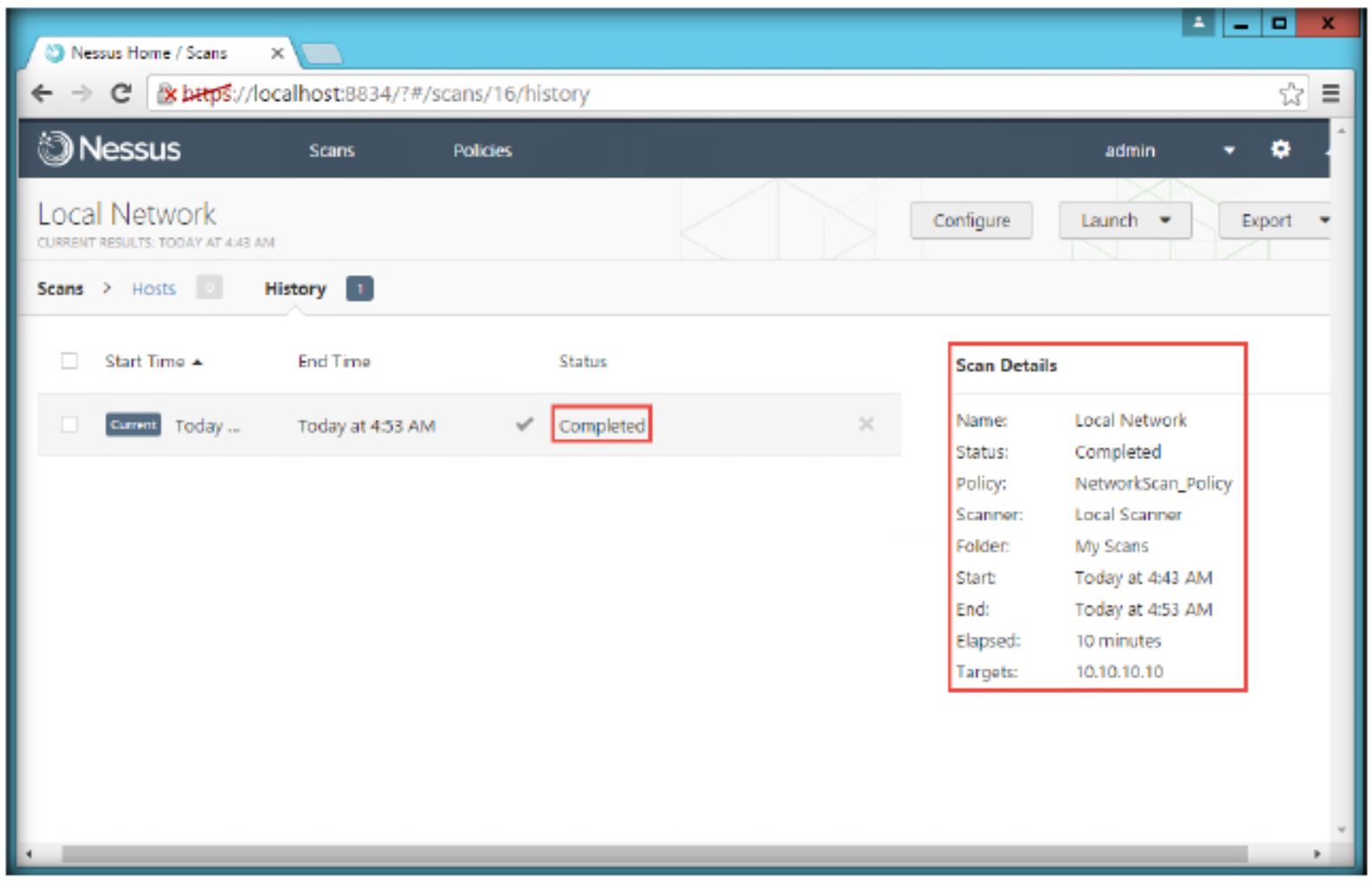


FIGURE 1.40: Scan completed successfully

55. No vulnerabilities are found in the **Windows 10 machine**. Now we are going to scan the **Windows Server 2008** machine.
56. Click **Scans → + New scan**.

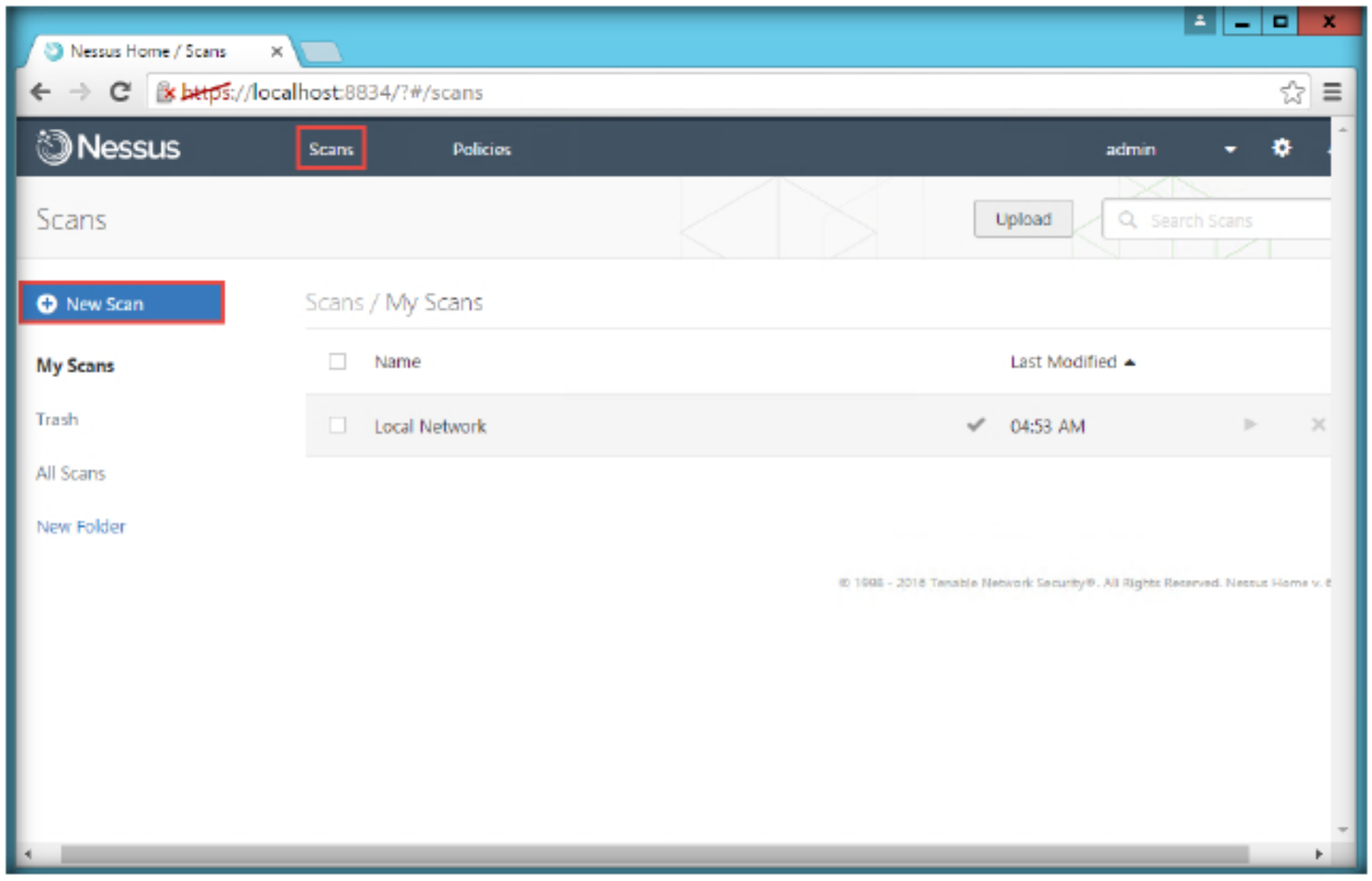


FIGURE 1.41: Adding a new scan

DROWN Detection

This policy is used to perform remote checks for the DROWN vulnerability (CVE-2016-0800).

57. Click on **User**.

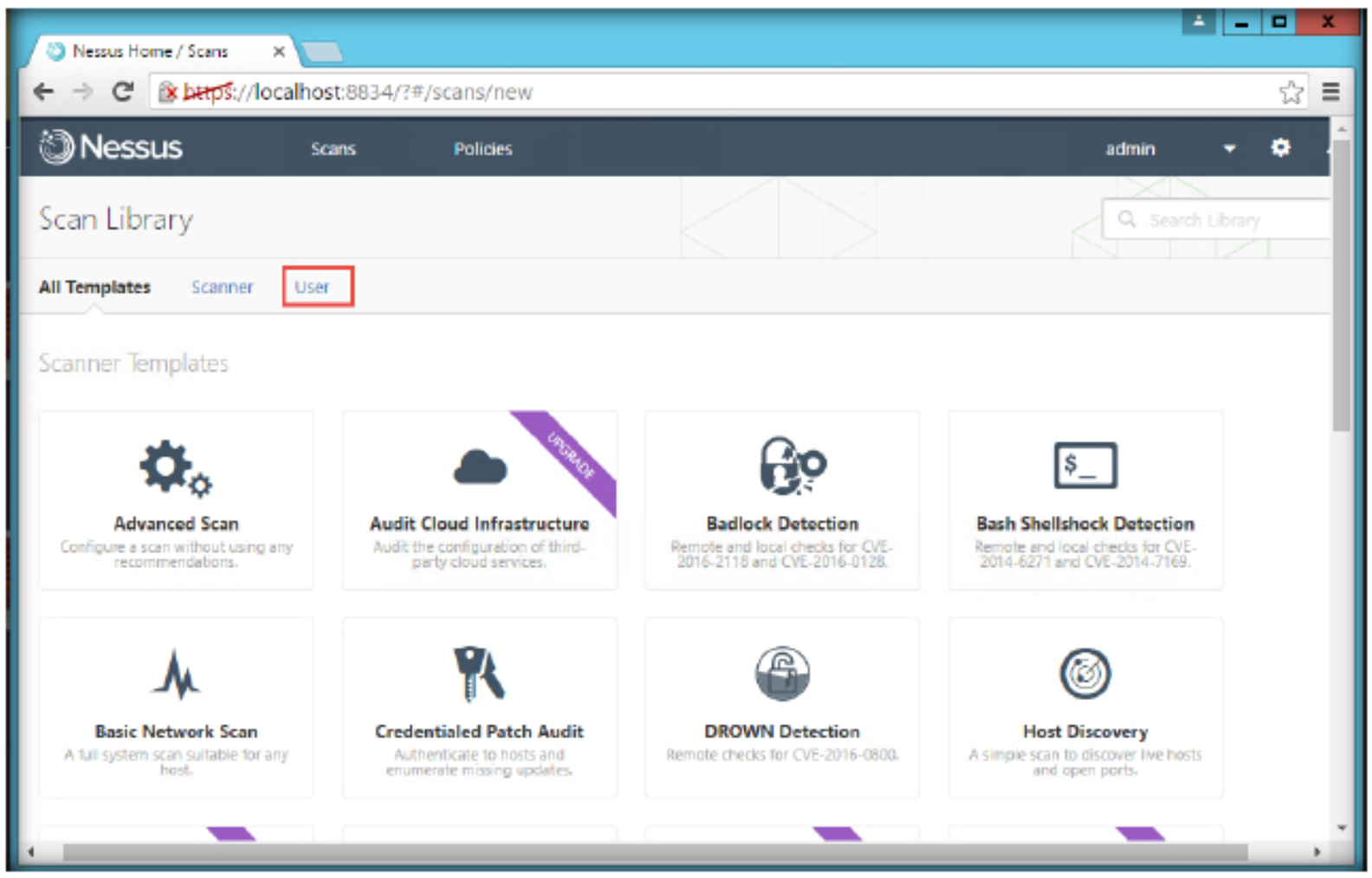


FIGURE 1.42: Selecting the policy for scan

58. Select the **NetworkScan_Policy**.

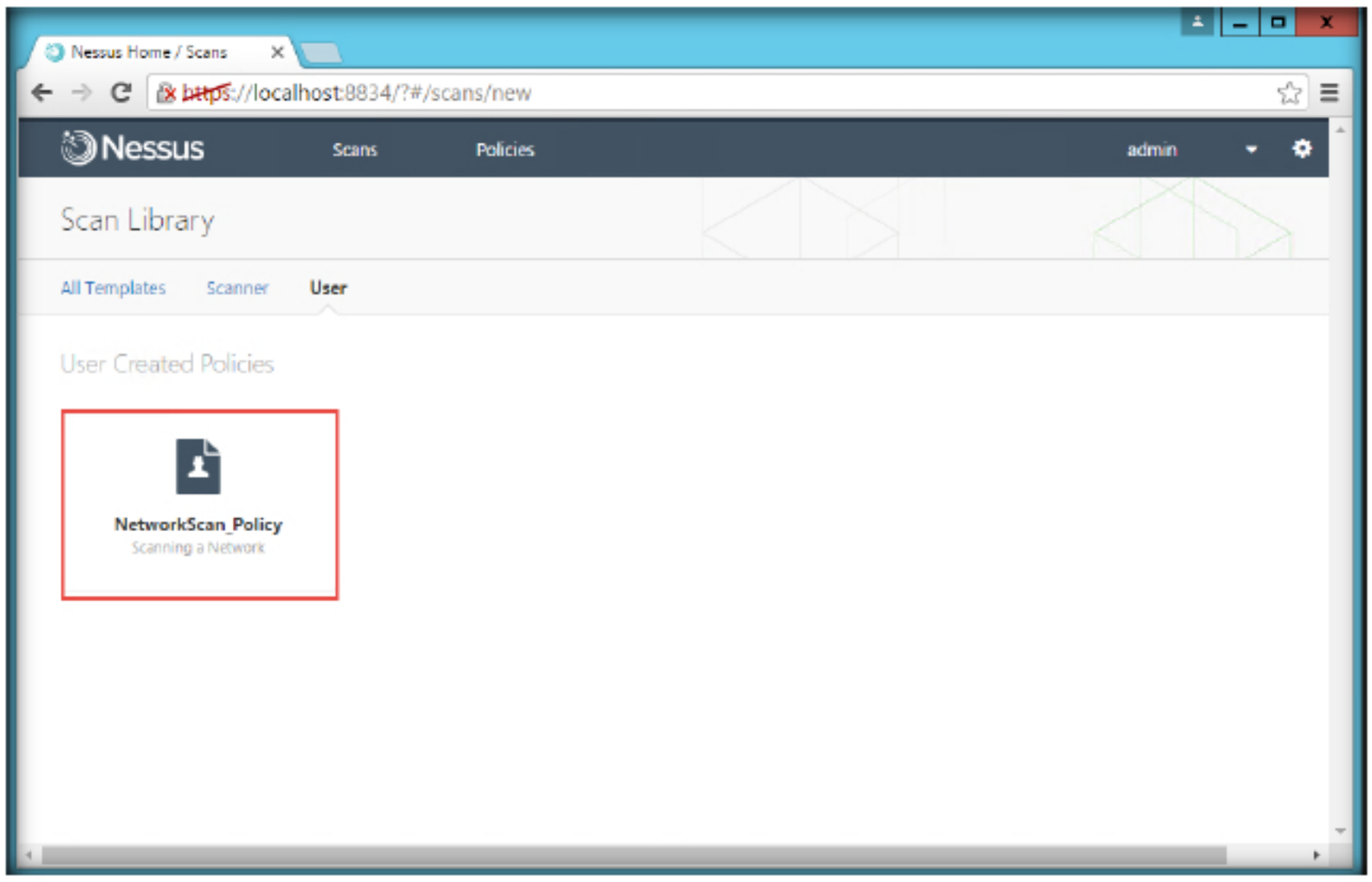


FIGURE 1.43: Selecting the created policy

Nessus summarizes the actions to take for the address with the largest quantity of vulnerabilities on the network. For example, Nessus will recommend that "Taking the following actions across 2 hosts would resolve 42% of the vulnerabilities on the network" and proceed to list the details of those specific vulnerabilities.

59. Enter the Name, Description, and Target IP address as 10.10.10.8 (**Windows Server 2008** machine) then click **Save**.

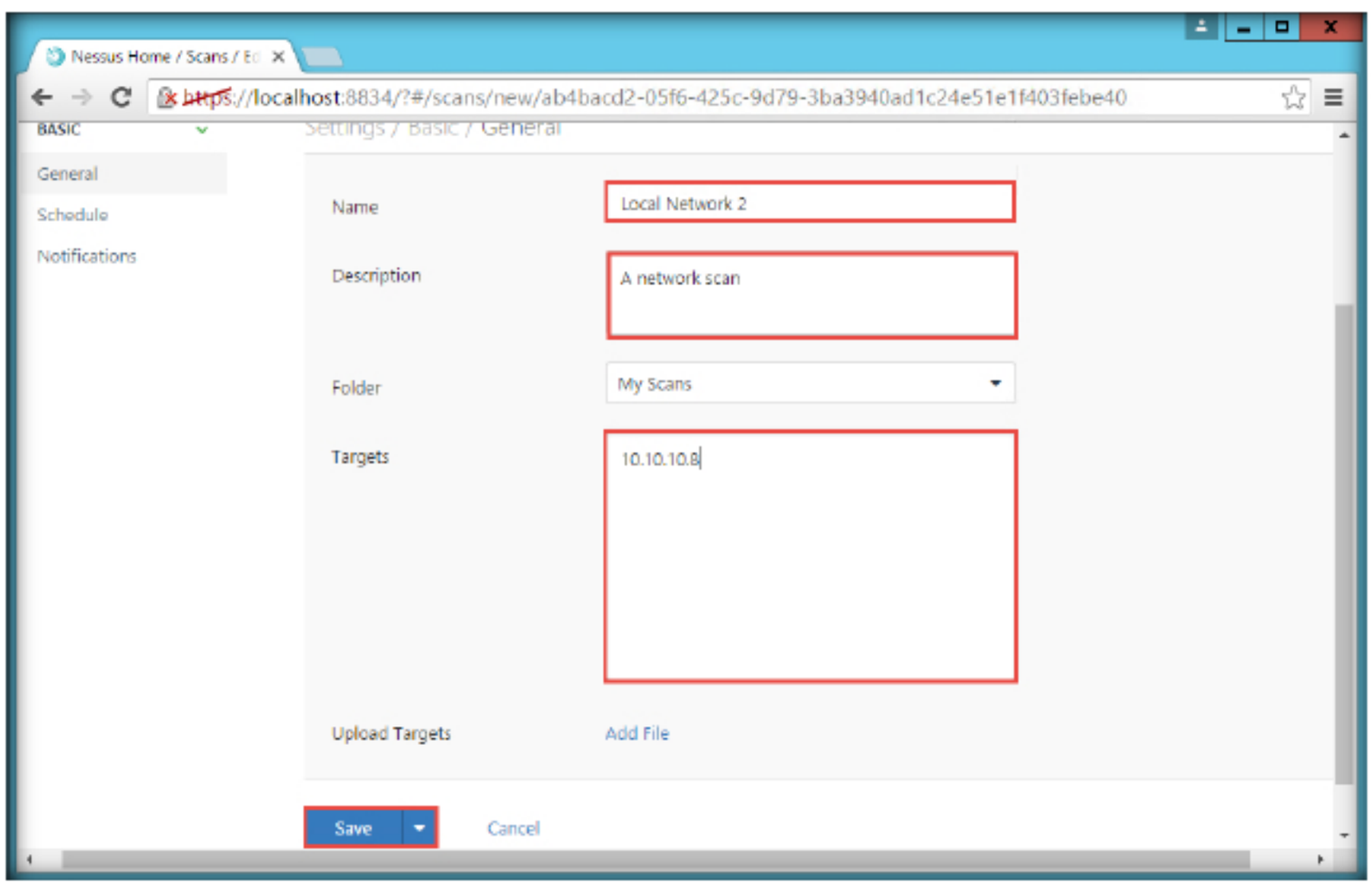


FIGURE 1.44: Entering details of the scan

60. You can see the new scan created and the **Scan saved Successfully** message appears.

Nessus lists each vulnerability found during your scan and the affected hosts. System administrators will find it easy to read this report and fix the problems that have been identified.

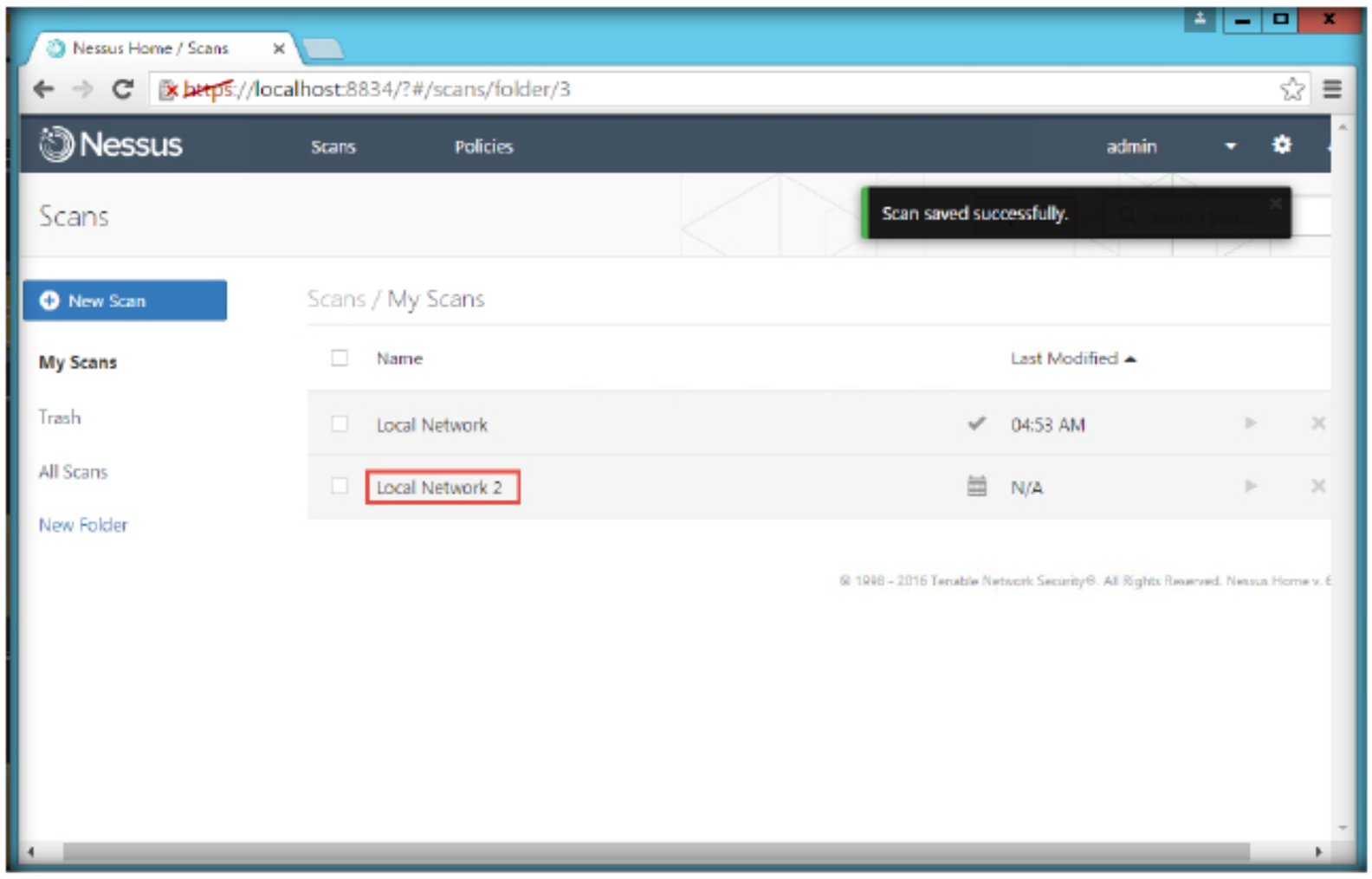


FIGURE 1.45: New scan created

61. Click on the **Scan** icon to start the scan then click on **Local Network 2**.

Nessus lists each host found during the scan and its associated vulnerabilities. Systems administrators will often use this report to address specific issues with certain hosts, follow-up scans, PCI scans, and targeted assessments.

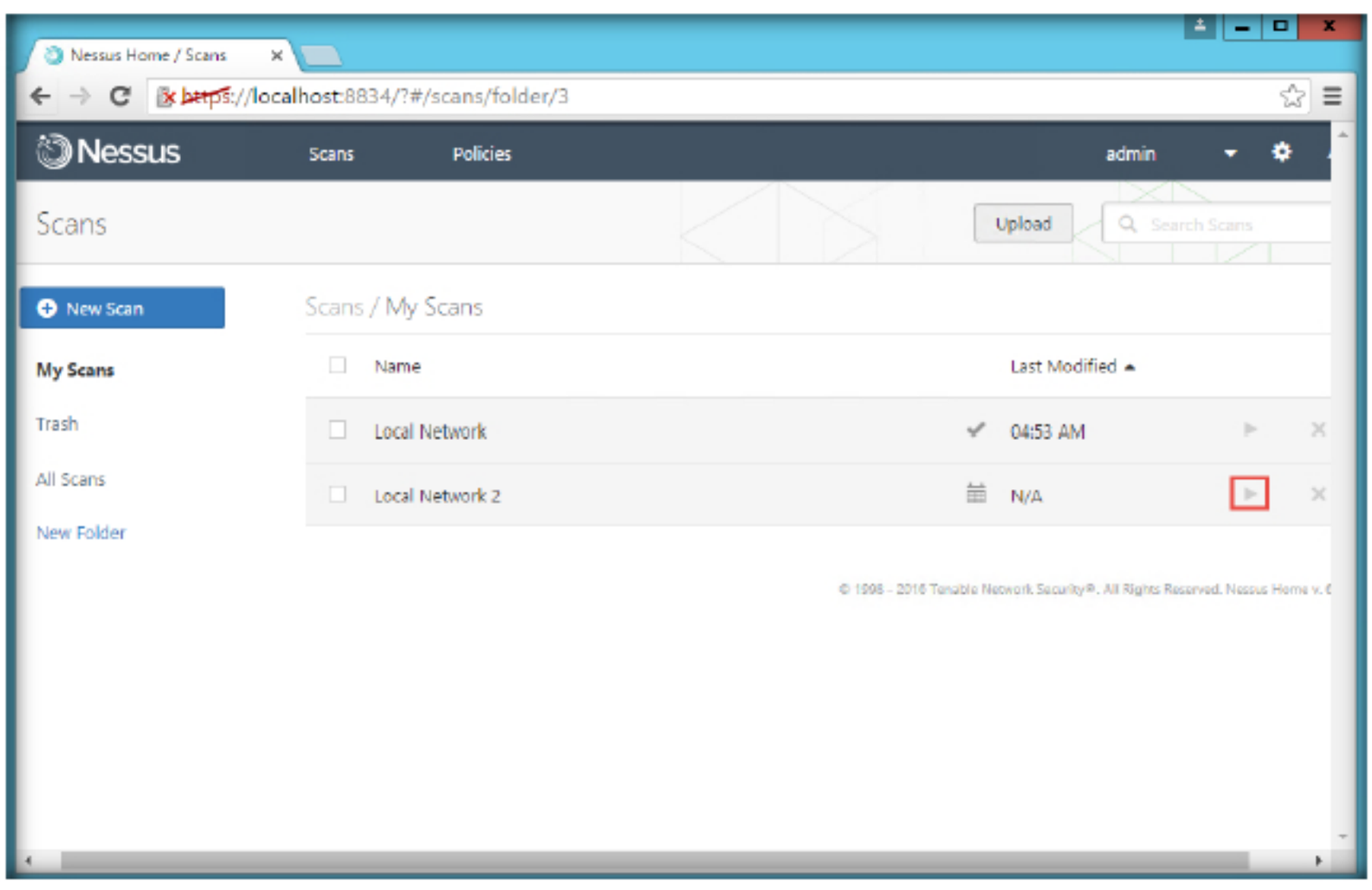


FIGURE 1.46: Starting the scan

62. You can see the status of the scan as **Running**. Wait for the scan to be completed.

Using result filtering, Nessus can generate a report that lists only vulnerabilities for which there is an associated exploit. The following reports are from network scans showing exploitable vulnerabilities grouped by plugin and by host.

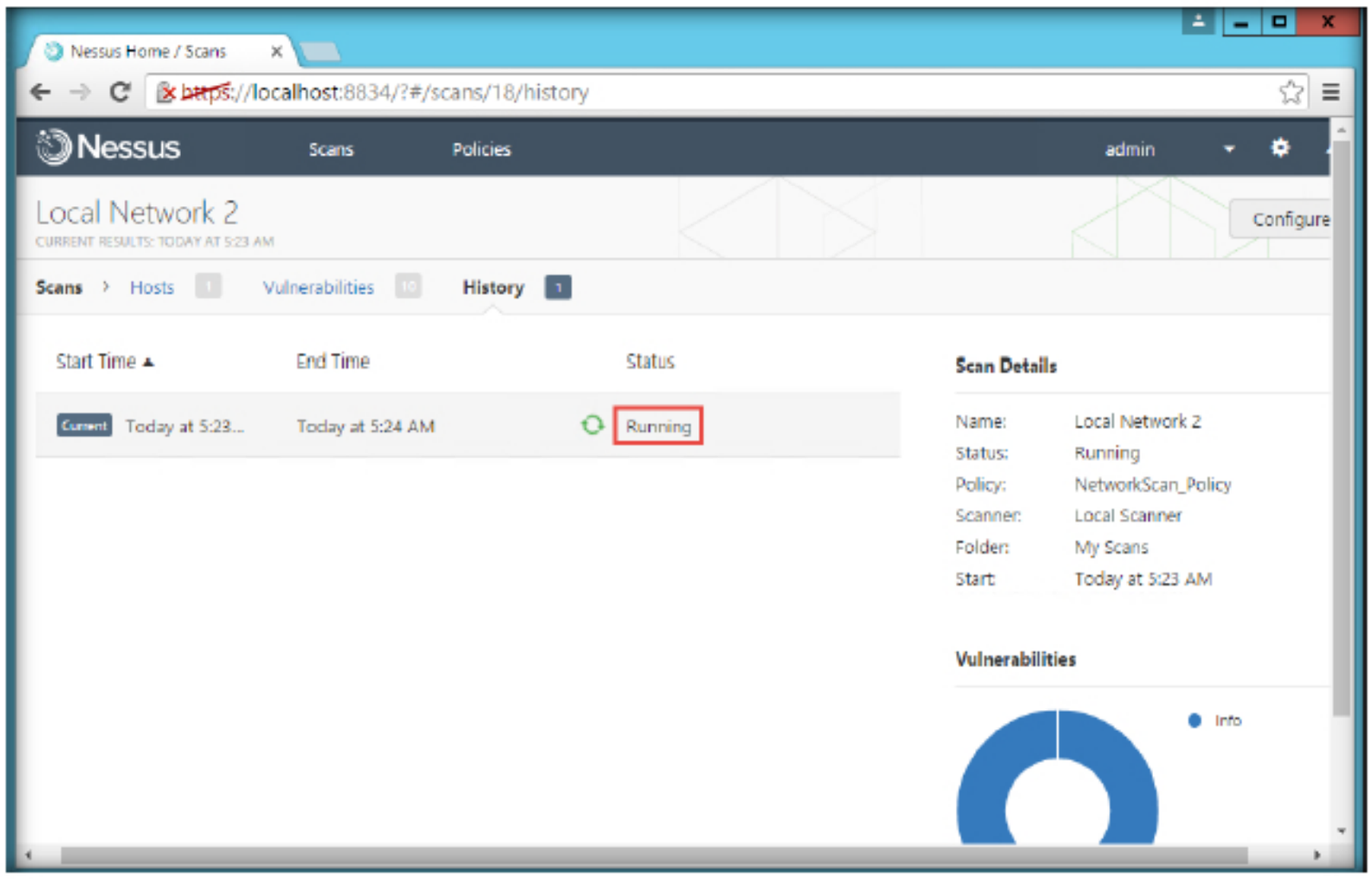


FIGURE 1.47: Scanning in progress

63. After the scan is completed the status changes to **Completed**. Now, there are vulnerabilities found in the Windows Server 2008 machine. Click on the **Vulnerabilities** tab to view the vulnerabilities in more detail.

The Nessus Scan Report presents extensive data about vulnerabilities detected on the network. The report can be especially useful to security teams that are new to Security Center but are familiar with the format and content of reports generated by Nessus.

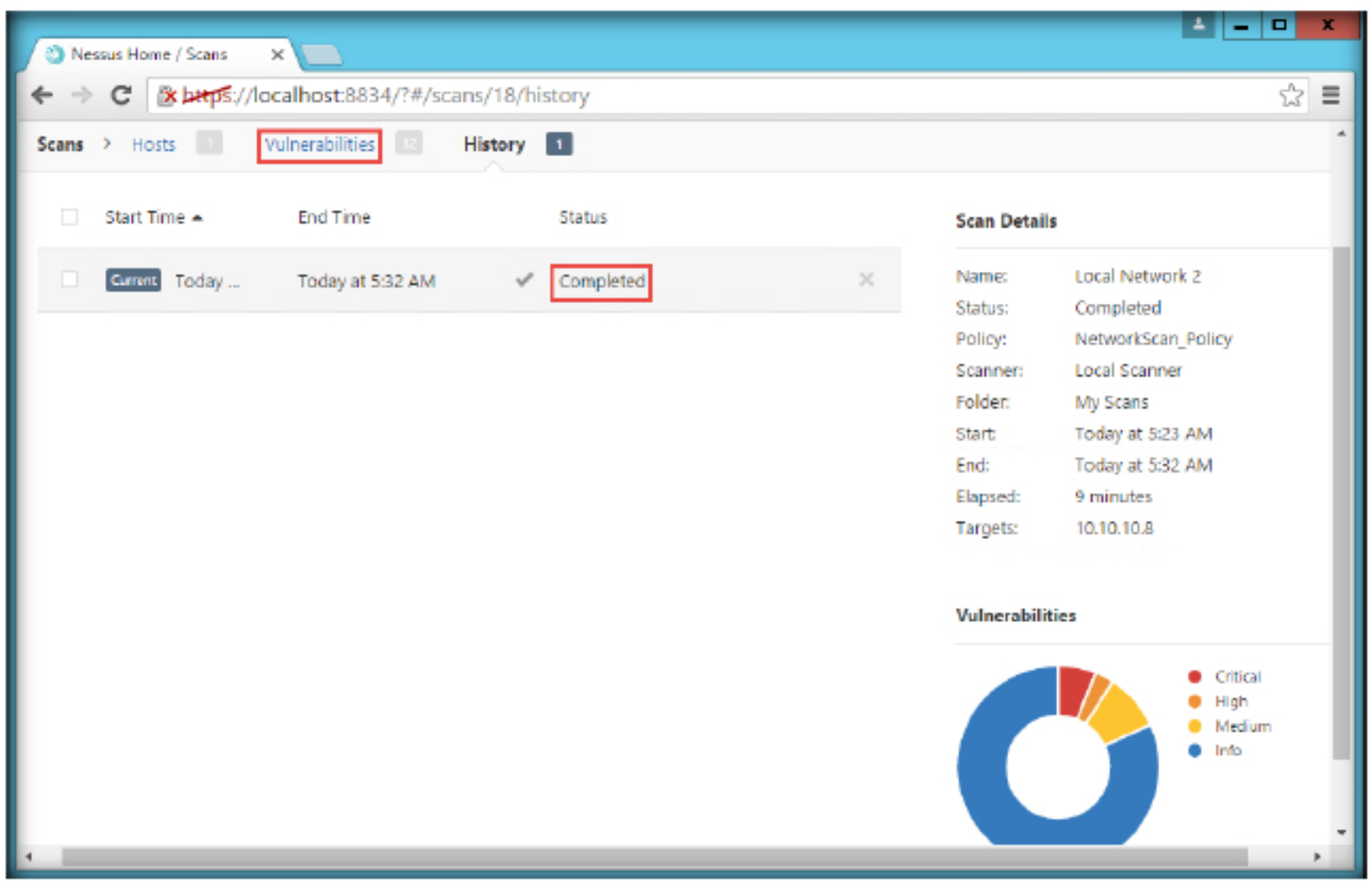


FIGURE 1.48: Scan completed Successfully

TASK 5

Examine the Vulnerabilities

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

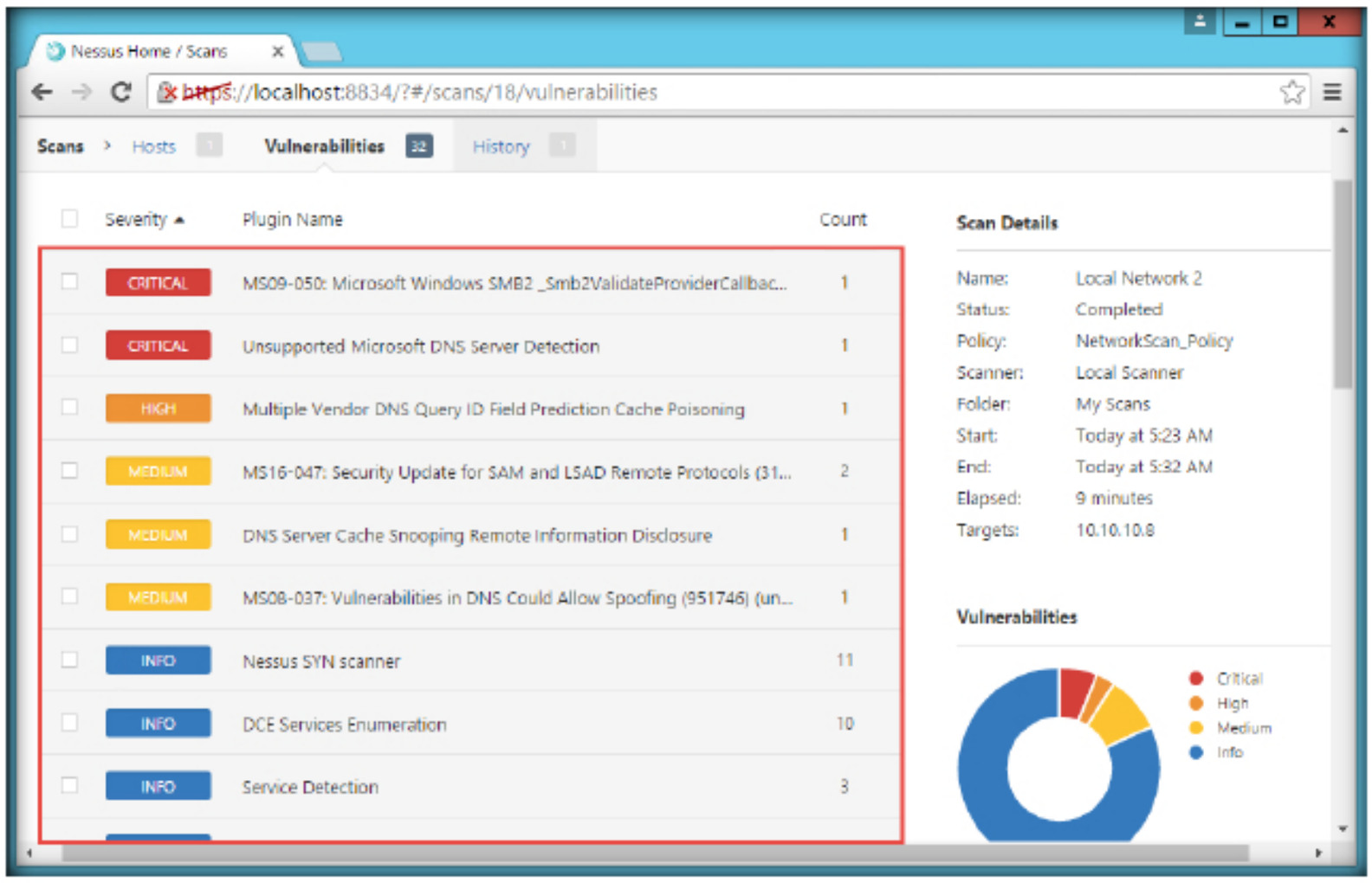


FIGURE 1.49: Vulnerability Summary window

65. Click on these vulnerabilities to view a detailed report about each of them. For instance, in this lab, **MS09-050: Microsoft Windows SMB2ValidateProviderCallback()** vulnerability is selected.

Nessus will provide the detailed information about the vulnerabilities detected on every host scanned. Security teams use this report to easily identify vulnerabilities and the affected hosts in their network.

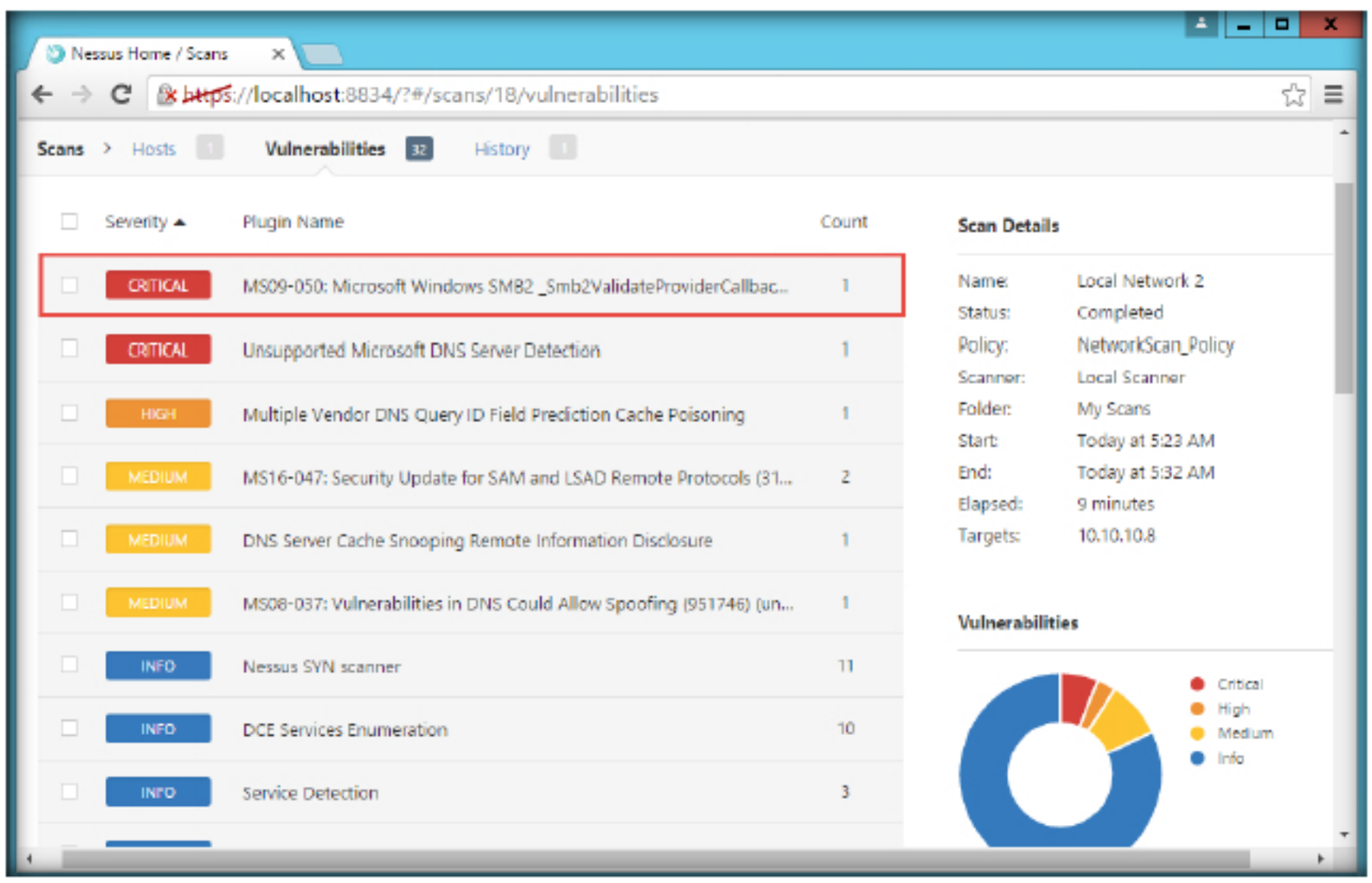


FIGURE 1.50: Selecting vulnerability

66. The report appears, as shown in the following screenshot

If you are manually creating ".nessusrc" files, there are several parameters that can be configured to specify SSH authentications.

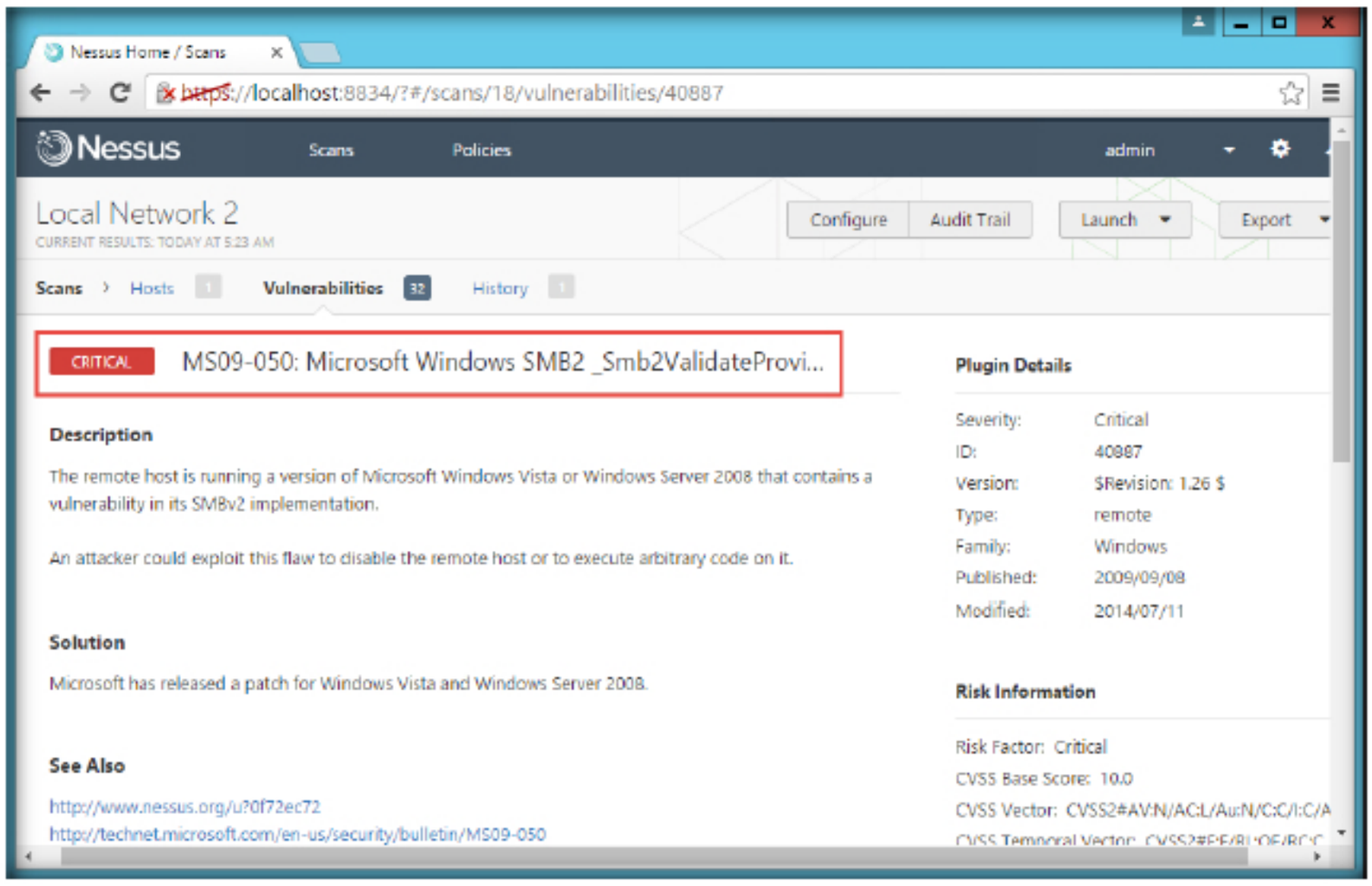


FIGURE 1.51: Vulnerability report

67. If you wish to save a detailed Report, switch to the **Nessus** tab and click **Export - HTML**.

TASK 6

Generate a Vulnerability Report

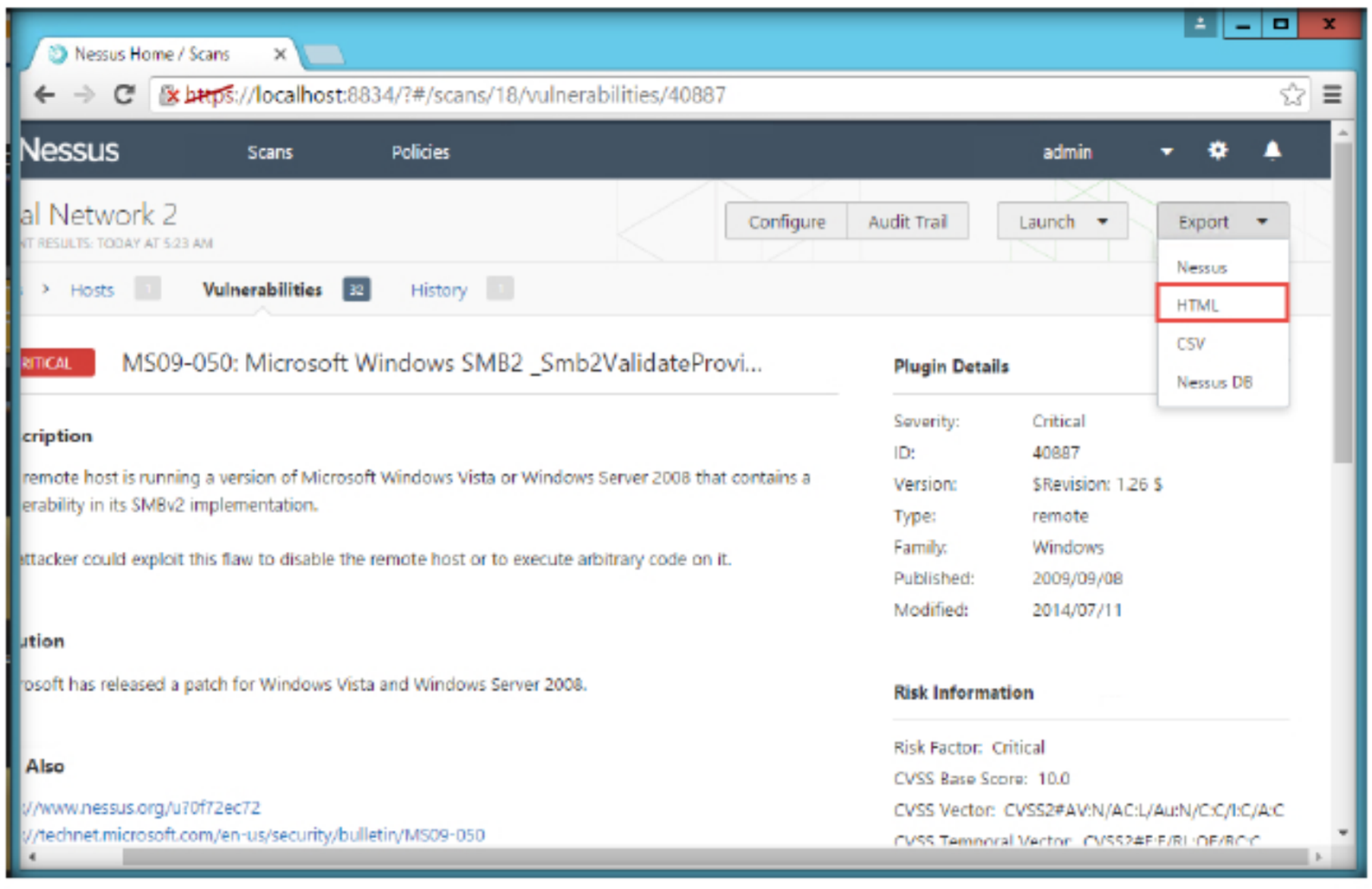


FIGURE 1.52: Exporting Report to HTML Format

68. Select **Custom** from the **Report** drop down menu.

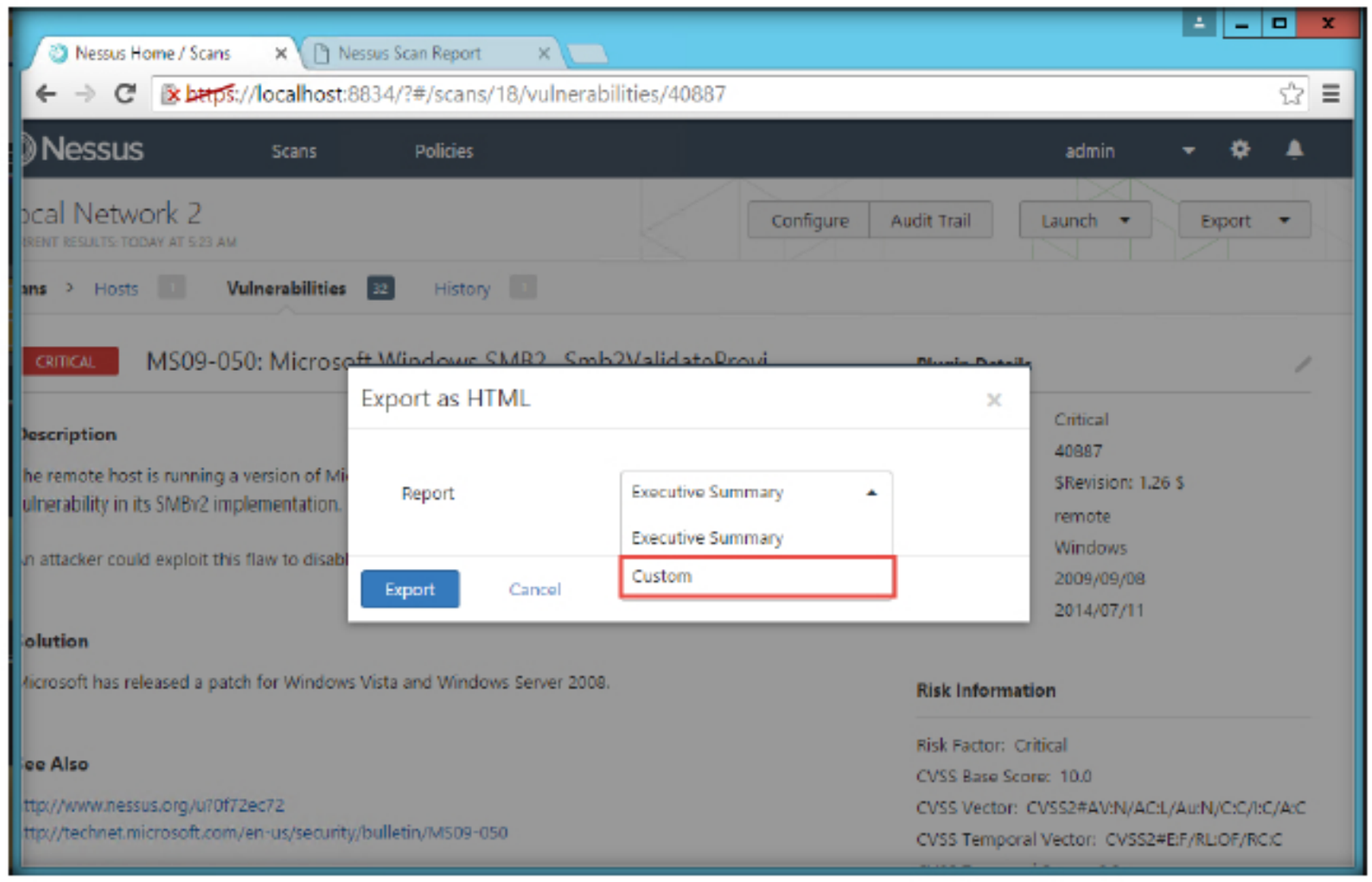


FIGURE 1.53: Selecting the Custom Report

To stop the Nessus server, open the Nessus Server Manager, and click the Stop Nessus Server button.

69. Click **Export**.

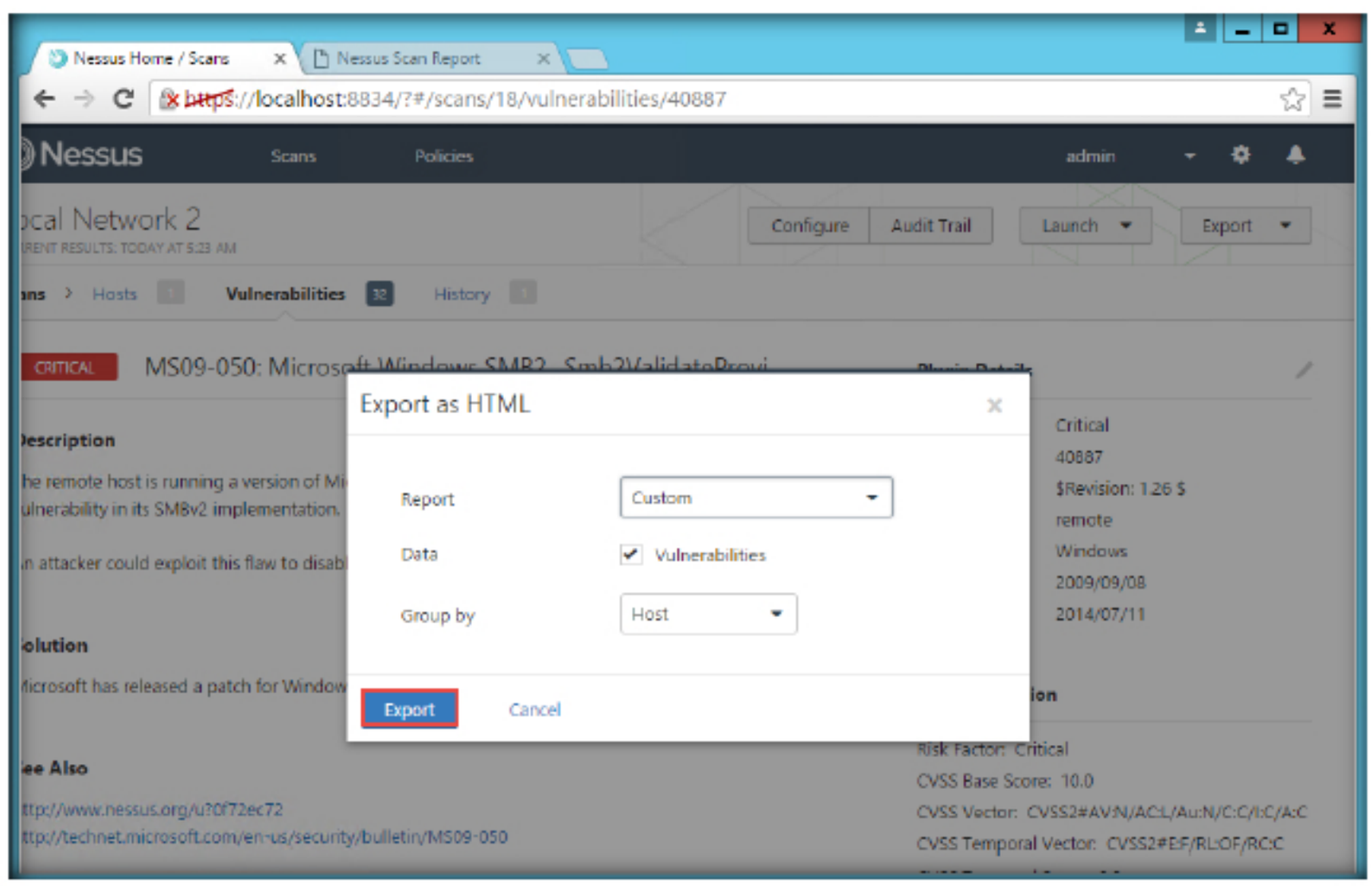


FIGURE 1.54: Saving the HTML file

70. Now the report appears on the bottom left side of your browser. Click on the downloaded file. (If you are using a different browser, the downloads appear in different places)

Nessus has implemented new features to help users combat mobile threats. Network-based scanning is not the right approach to identify vulnerabilities on mobile devices, due in large part to the fact that most devices are in "sleep" mode and/or using a 3G/4G network.

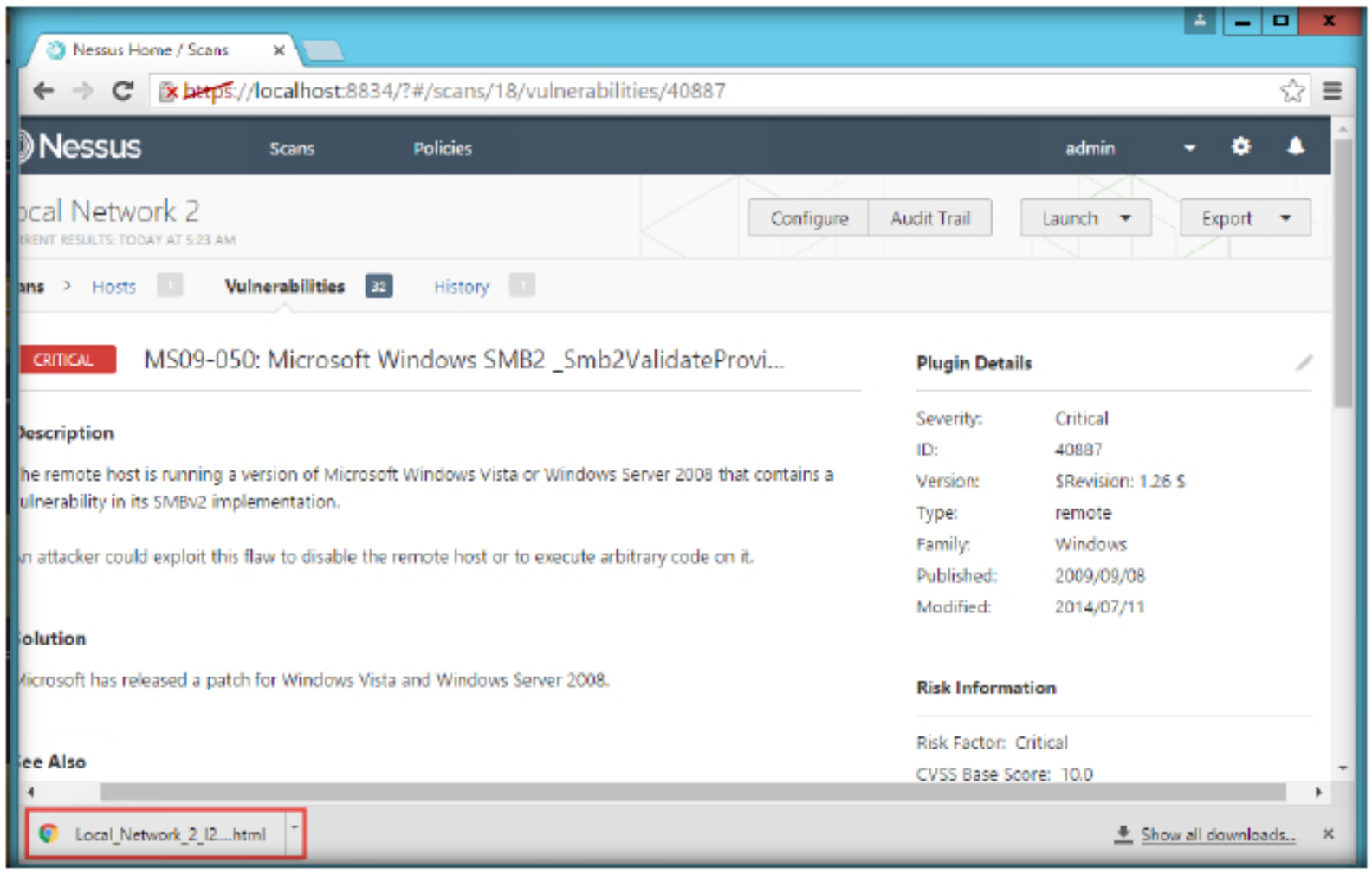


FIGURE 1.55: HTML report file saved

71. You can **scroll down** to view all the vulnerabilities. Click on any vulnerability to view its detail report.

Nessus report filtering features show information for a specific type of device, for example the following feature displays information about iPads.

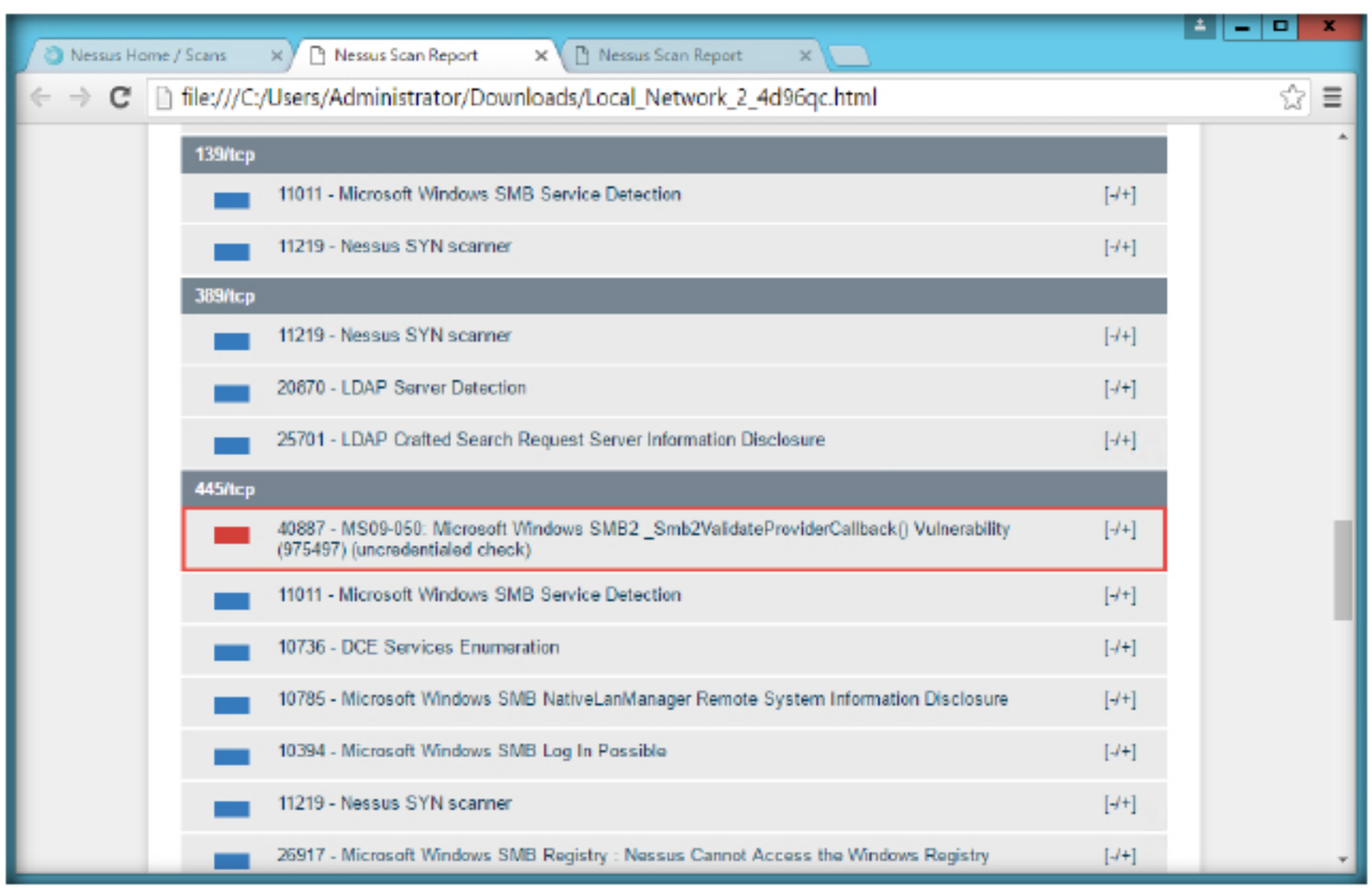


FIGURE 1.56: Selecting a vulnerability for detailed view

72. Now, you can view the detailed report including the **Solution** for the Vulnerability.

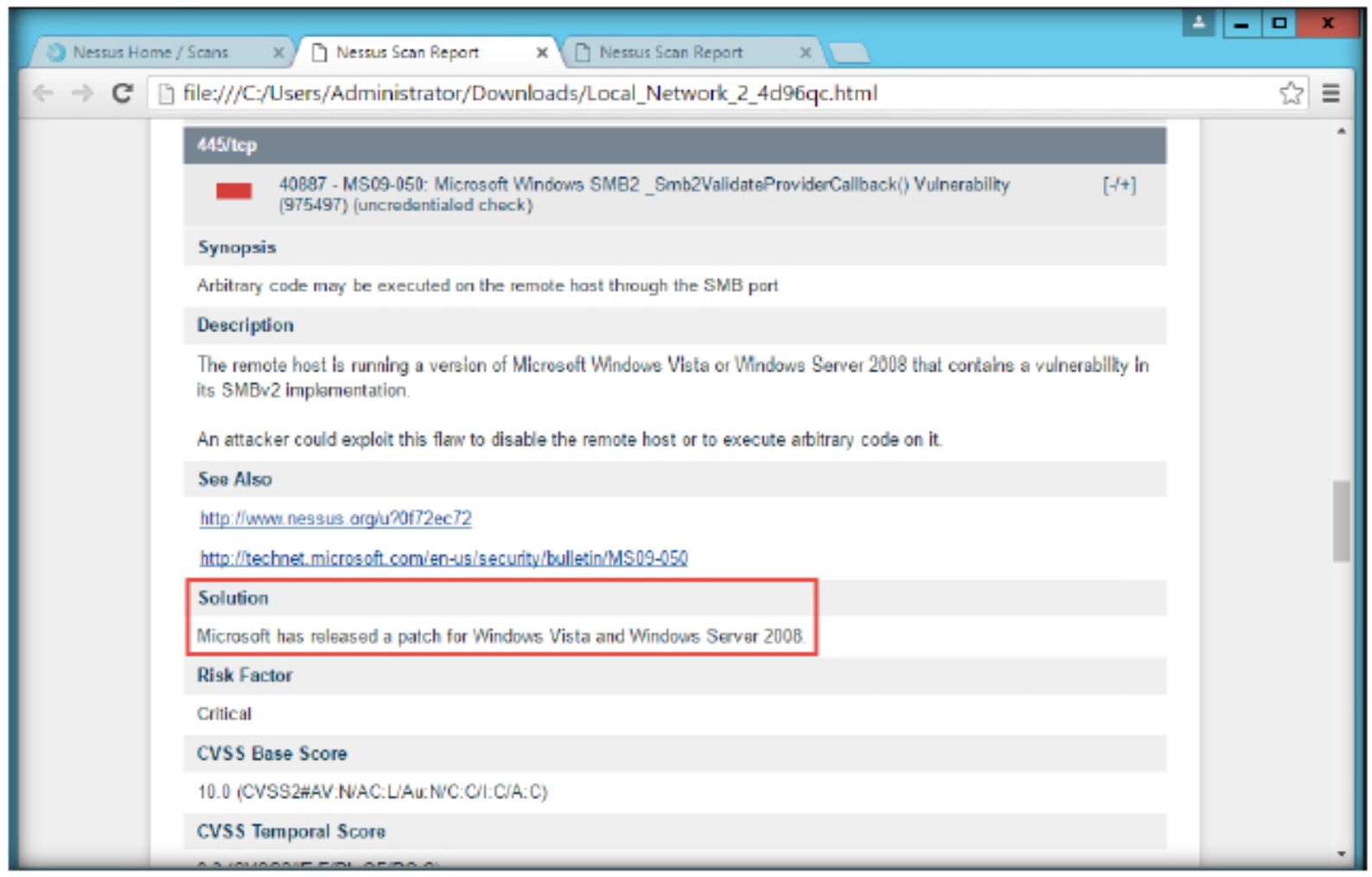


FIGURE 1.57: Detailed Vulnerability report

73. To **Sign out** of Nessus, Switch to the Nessus Home tab, click on **admin – Sign Out**.

Nessus External Network Scan - This policy is tuned to scan externally facing hosts, which typically present fewer services to the network. The plugins associated with known web application vulnerabilities (CGI Abuses and CGI Abuses: XSS plugin families) are enabled in this policy. Also, all 65,535 ports are scanned for each target.

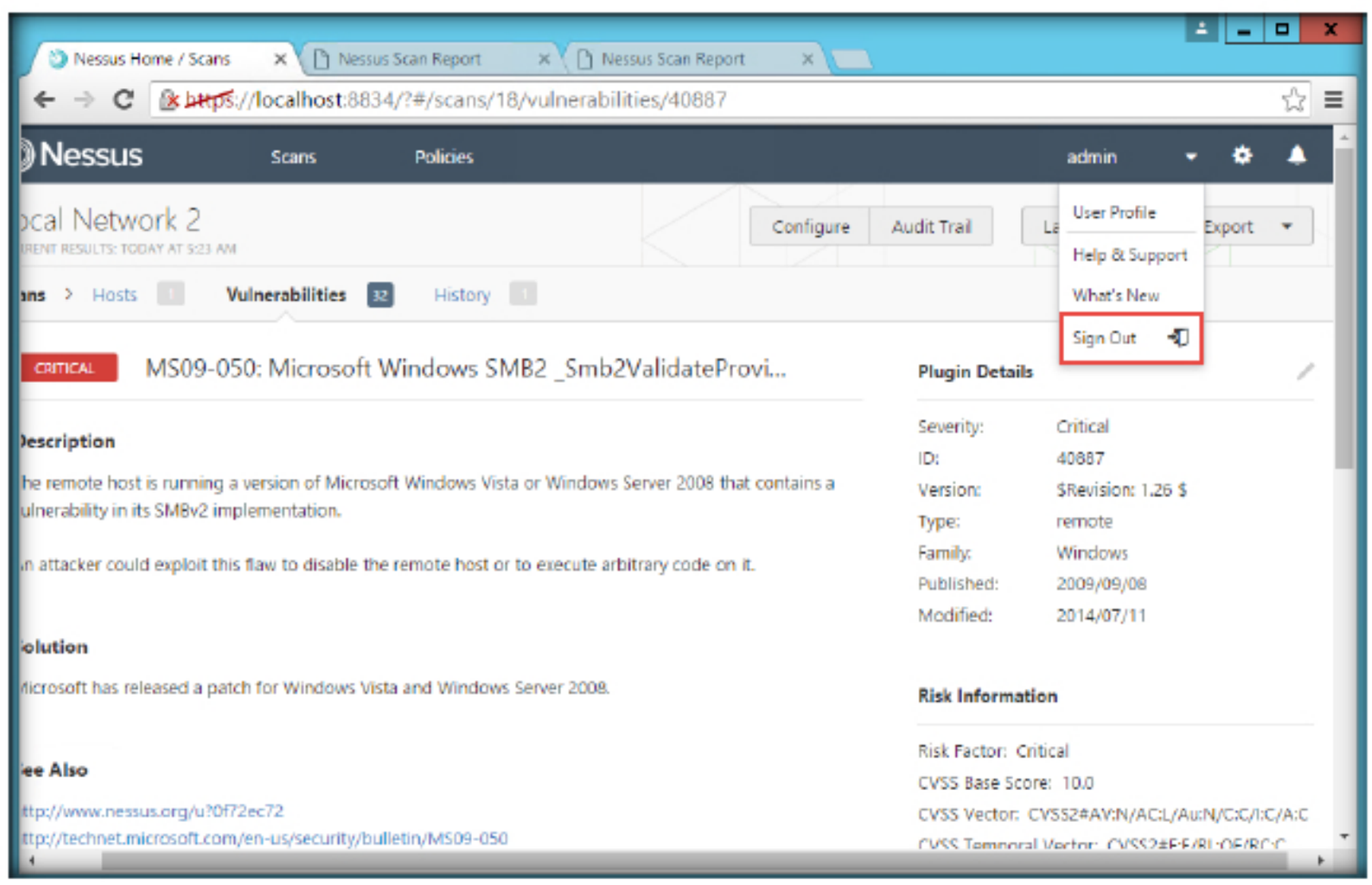


FIGURE 1.58: Signing out of Nessus

74. You get the signed out successfully, Goodbye, admin message upon successful log out.

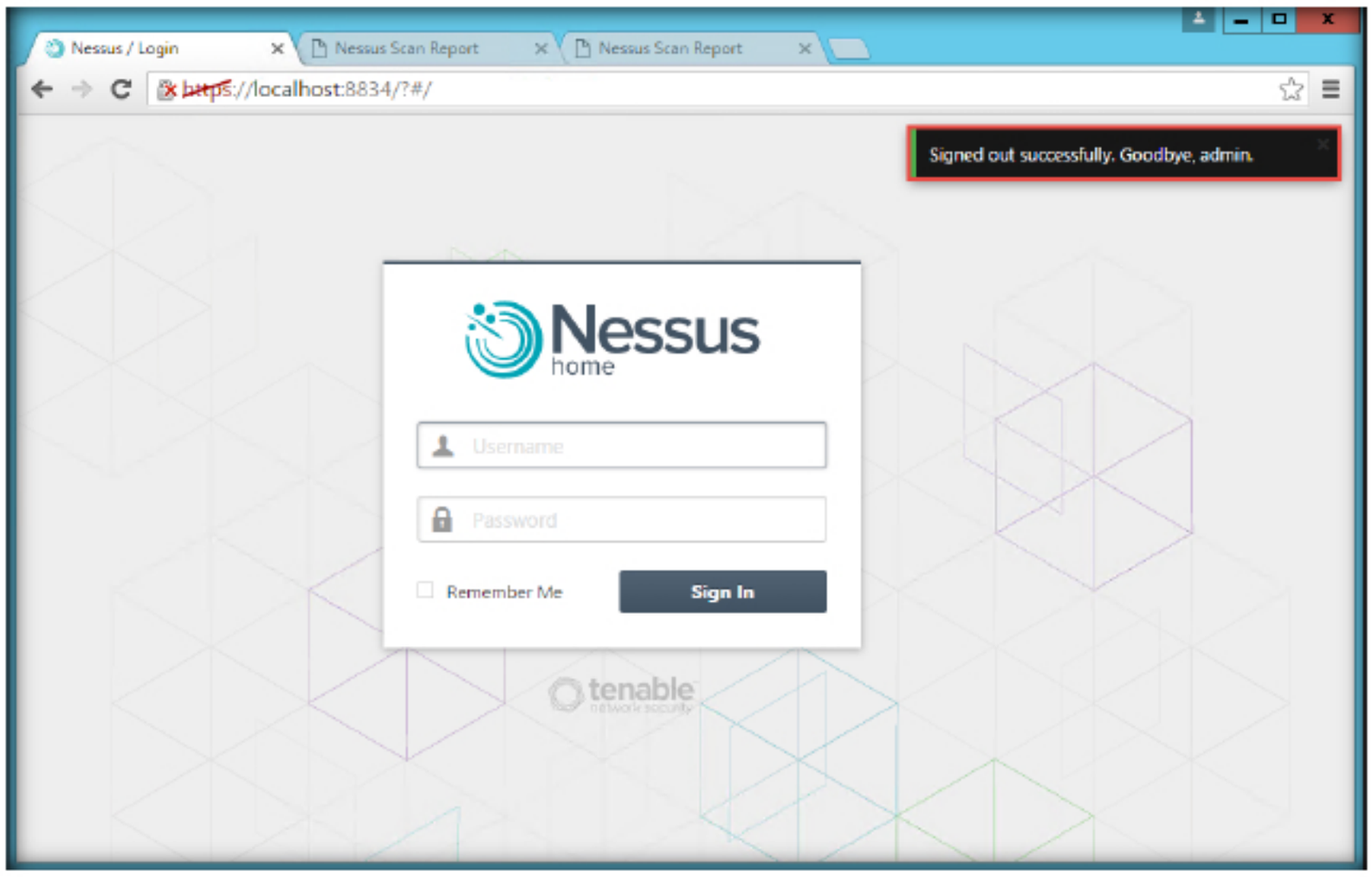


FIGURE 1.59: Successfully Signed out of Nessus

TASK 7

Removing a Vulnerability

75. Let's see how to remove a vulnerability. Select the critical vulnerability **MS09-050: Microsoft Windows SMB2ValidateProviderCallback()** and resolve it.

76. To resolve the issue, we need to **install the updates** on the Windows Server 2008. Launch the **Windows Server 2008** machine

77. Navigate to the **Control panel** and click **Windows Update**

Vulnerabilities in SMBv2 Could Allow Remote Code Execution

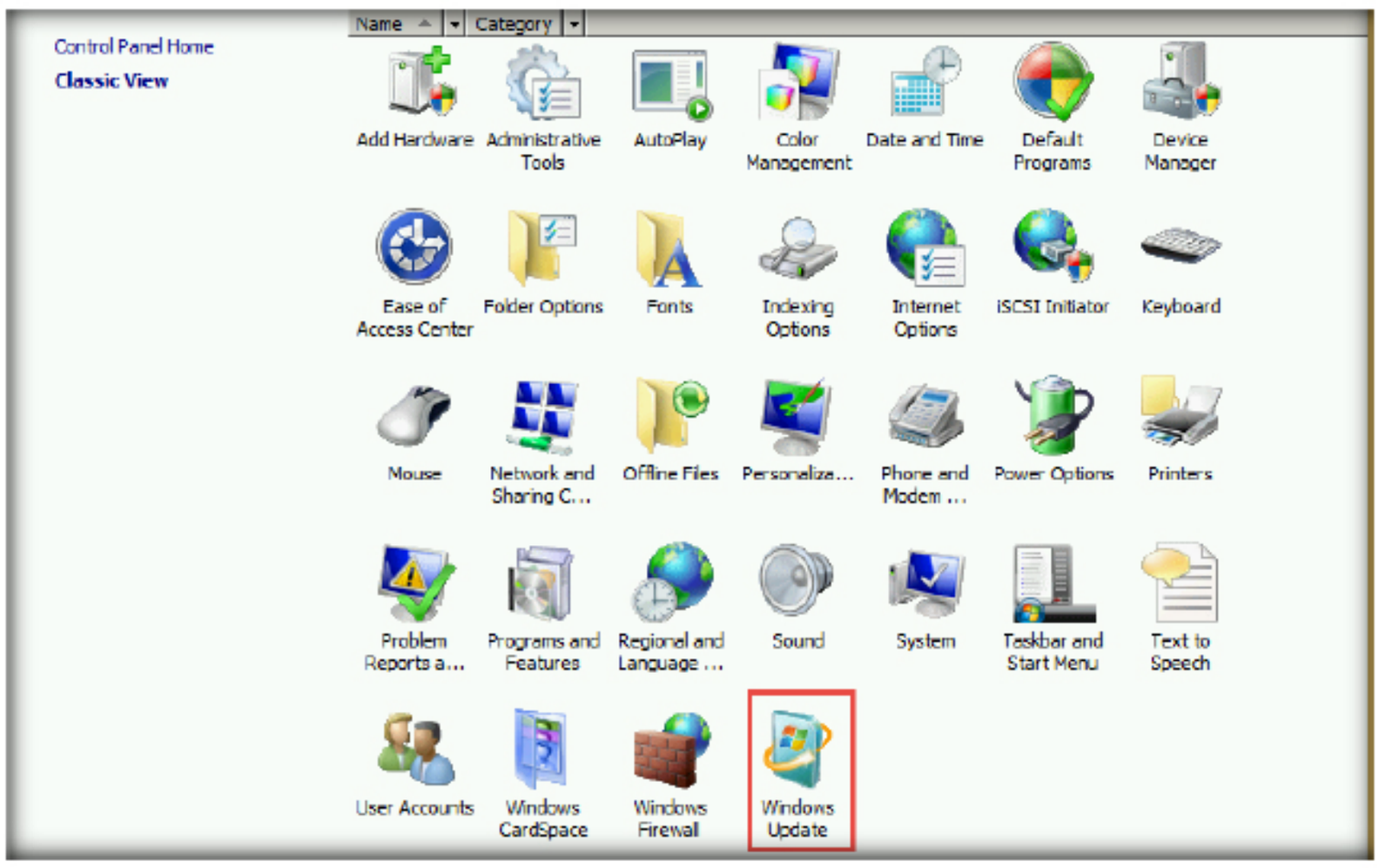


FIGURE 1.60: Navigating to Windows Update

78. Windows Update was turned off per the Lab Tasks in the beginning of this lab exercise. Turn Windows Update on, then click **Install Updates**.

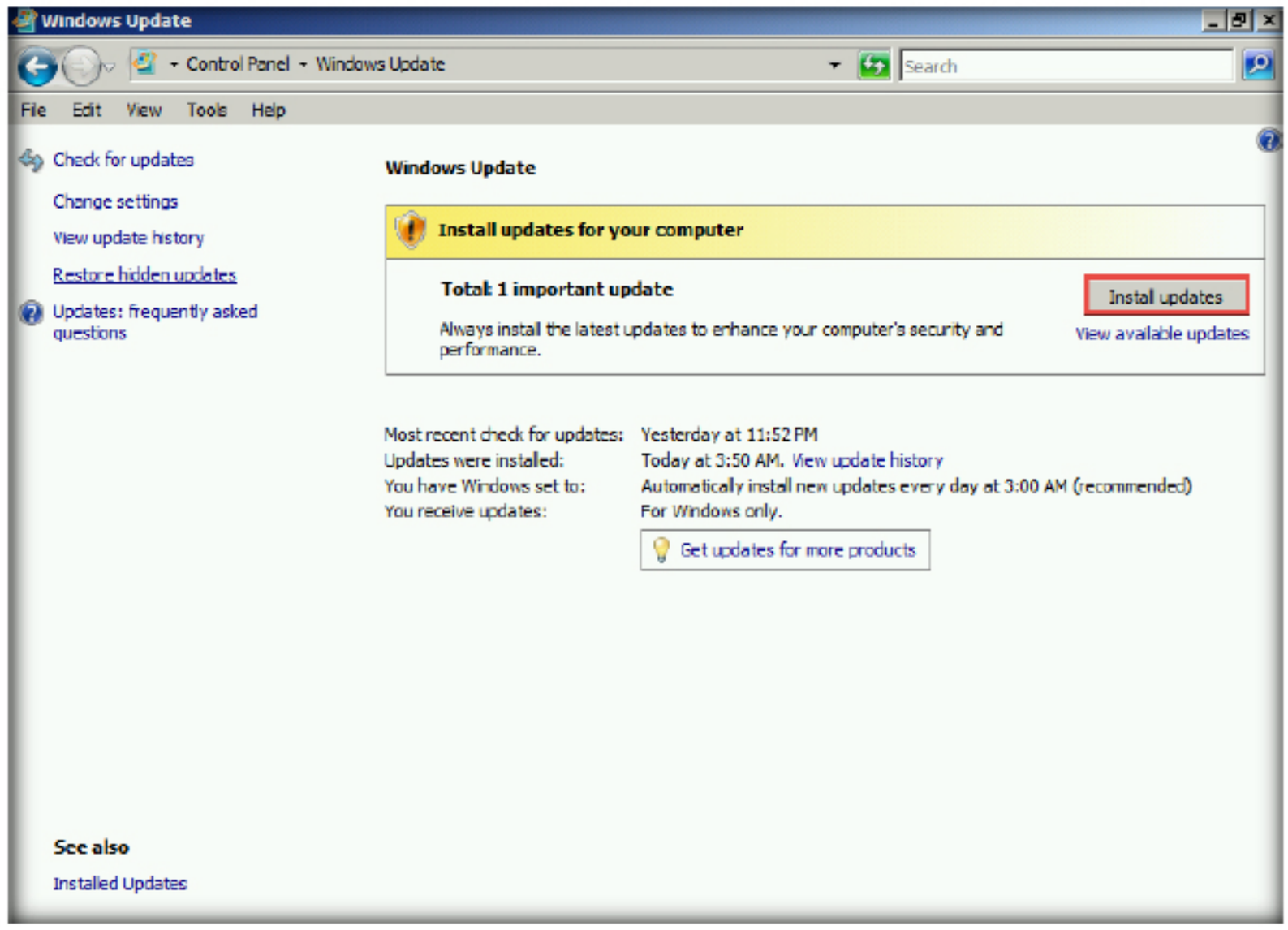


FIGURE 1.61: Installing an update

79. Wait for all the updates to be installed.

Windows is installing the available updates

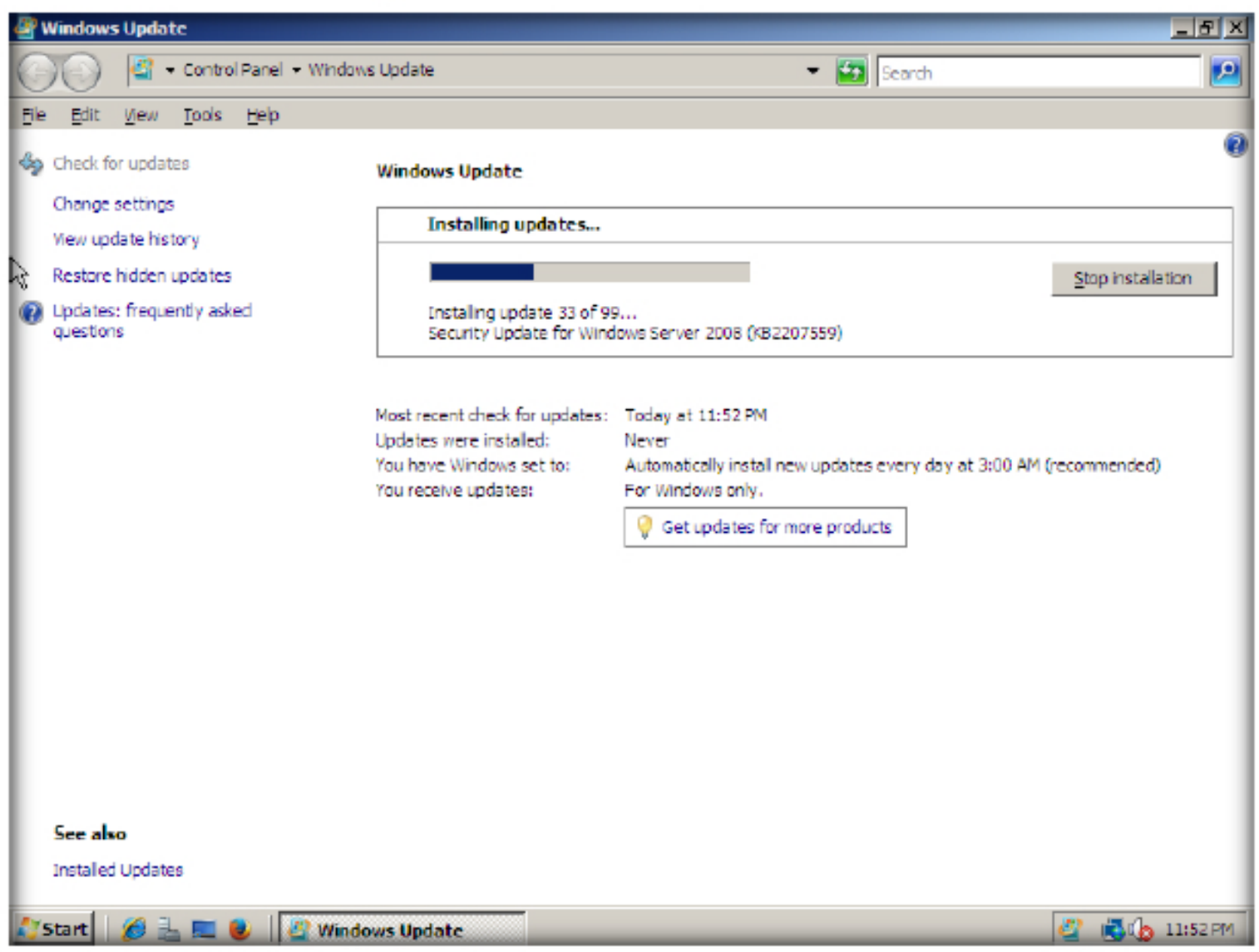


FIGURE 1.62: Update installation in progress

80. After all updates are installed, click **Restart now**. Wait for the restart to complete. It takes some time

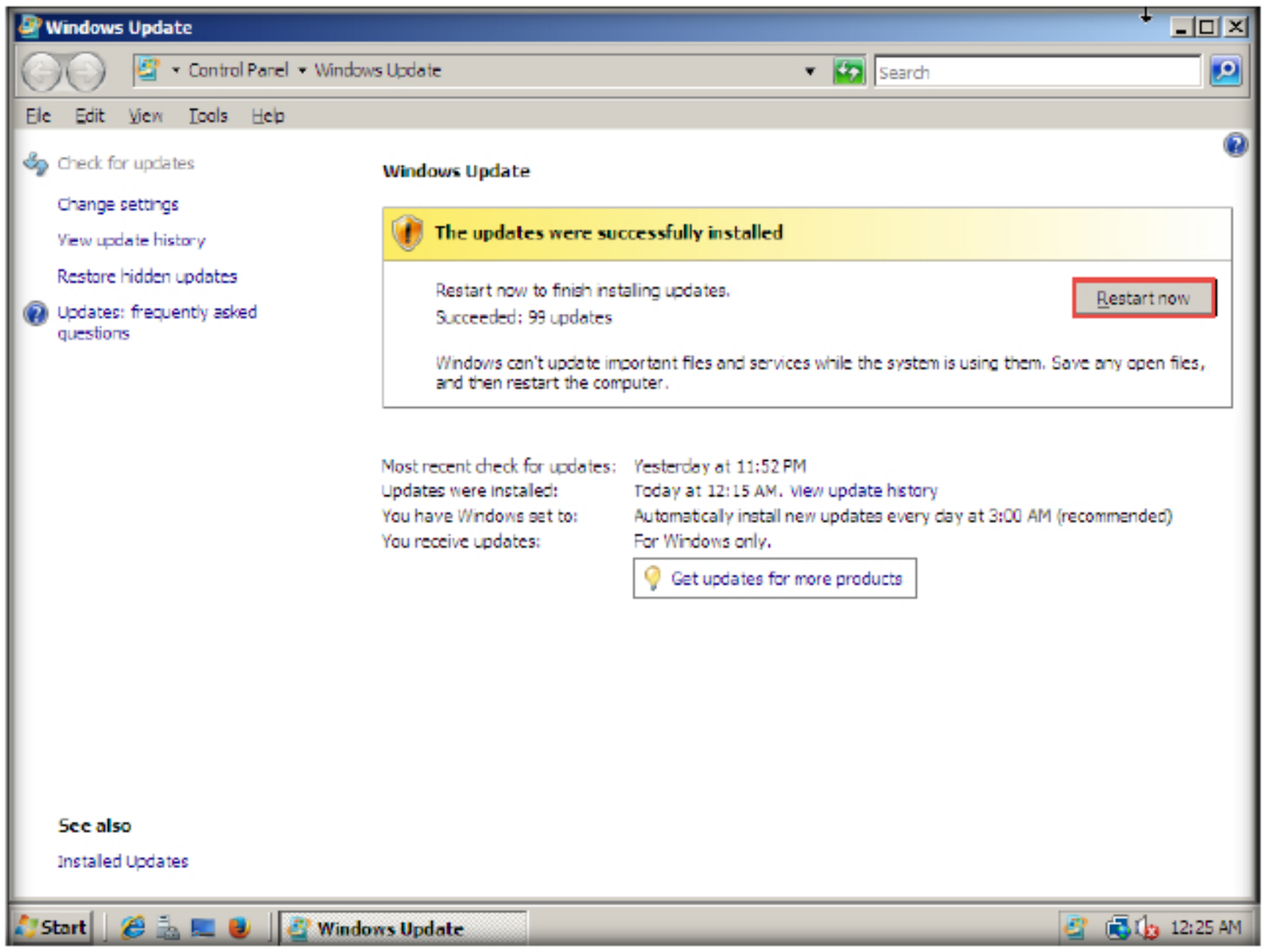


FIGURE 1.63: Restarting the system after update is installed

81. Switch to the Windows Server 2012 machine and run the vulnerability scan again on Windows Server 2008, by following the steps mentioned above using Nessus.

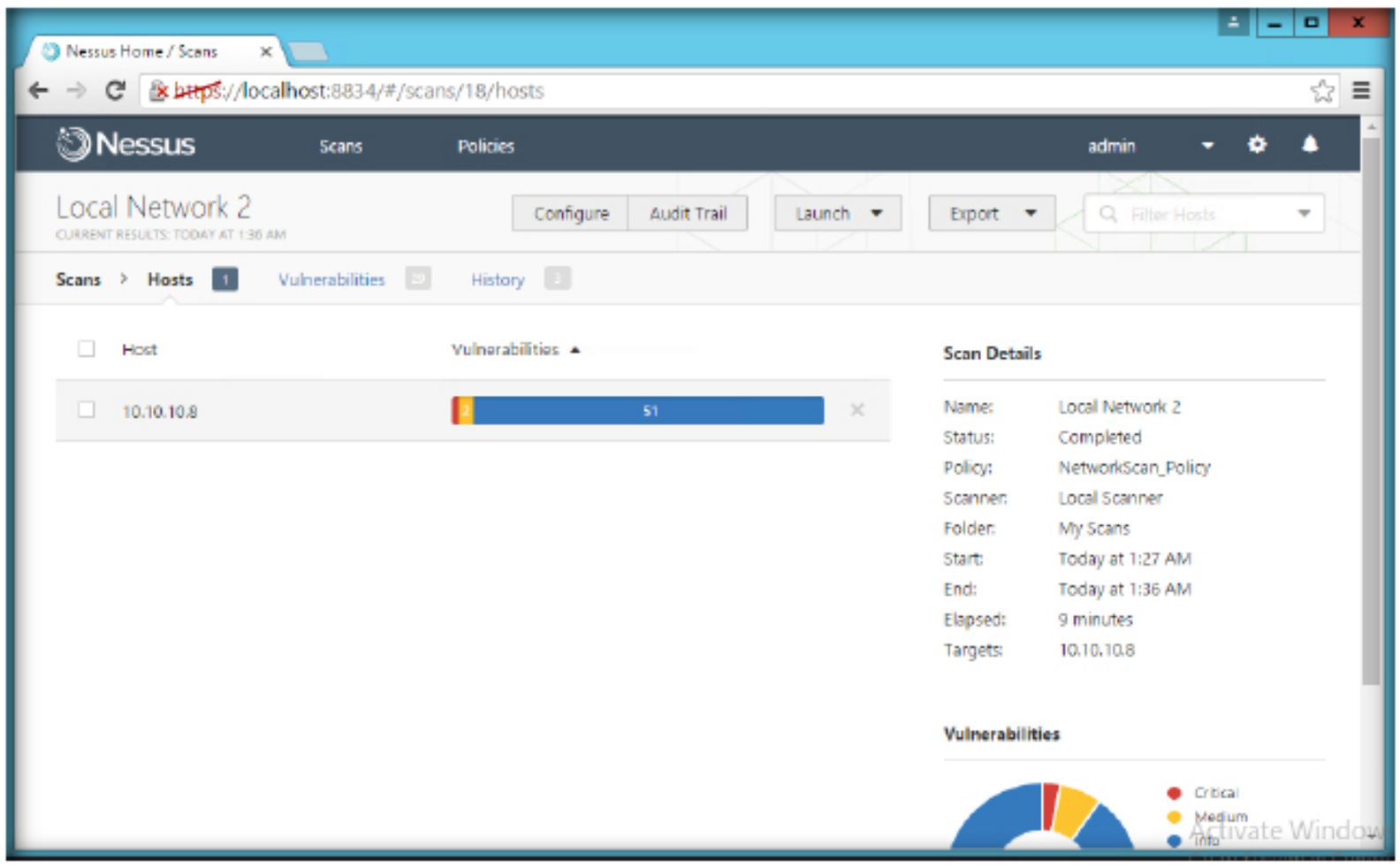


FIGURE 1.64: Scanning vulnerabilities after Windows server 2008 update

82. Now click **Vulnerabilities** from the menu bar.

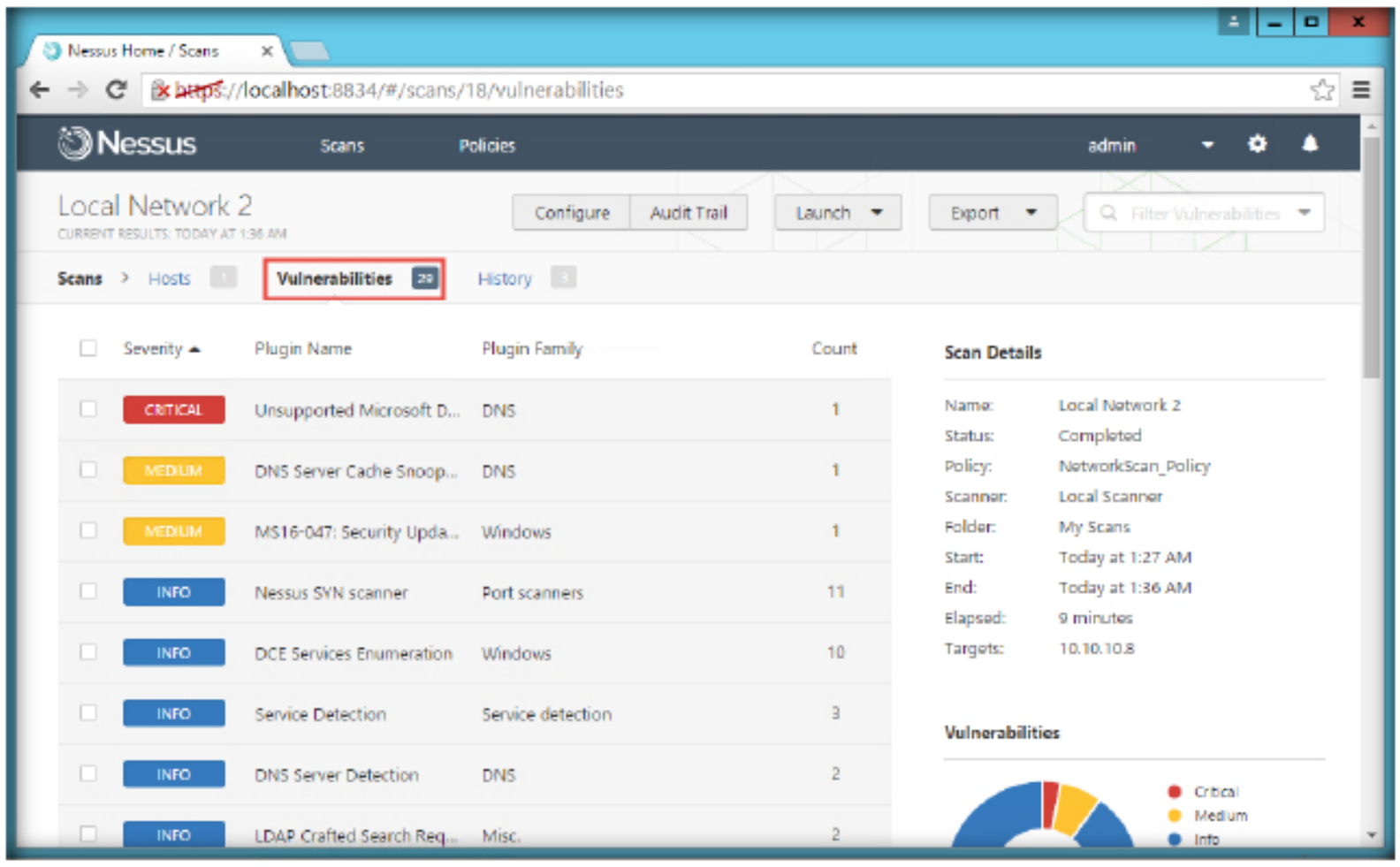


FIGURE 1.65: Vulnerabilities in the system after update

83. The vulnerabilities are arranged in order of severity levels. **CRITICAL, MEDIUM, INFO**.
84. You can see in the CRITICAL field only one vulnerability is present related to DNS. The earlier vulnerability related to SMB is removed.
85. By following this same procedure for every vulnerability you can remove them all.

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Using one vulnerability-scanning tool may not be sufficient. As a network administrator you should know different tools used for scanning network vulnerabilities. You should always try to perform a vulnerability scanning with different kinds of vulnerability scanning tools.

Lab Objectives

The objective of this lab is to demonstrate vulnerability scanning with the GFI LanGuard network vulnerability scanner.

Lab Environment

To perform this lab, you need:

- Register at the GFI website http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download to obtain a license key.
- Complete the registration to receive an activation code. You will then receive an email containing the code.
- If you download the latest version, then screenshots shown in the lab might differ.
- A virtual machine running Windows 2012 Server.
- A virtual machine running Windows 10.
- Administrator privileges to run the GFI LanGuard Network Security Scanner.

You can download GFI LanGuard from http://www.gfi.com.

Lab Duration

Time: 35 Minutes

Overview of GFI LanGuard

GFI LanGuard helps discover and list all vulnerabilities for the operating system on remote computers (missing security patches), as well as vulnerabilities of installed software, system configurations, and so on.

Lab Tasks

TASK 1

Register and Download GFI LanGuard

Note: Before starting this lab, turn on the Windows 10 virtual machine, and login with the domain user credentials or with the local admin credentials and leave the machine running.

1. Launch a web browser in the Windows Server 2012 virtual machine, 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 registration page for GFI LanGuard appears. Enter your details, and click **GET MY FREE TRIAL**.

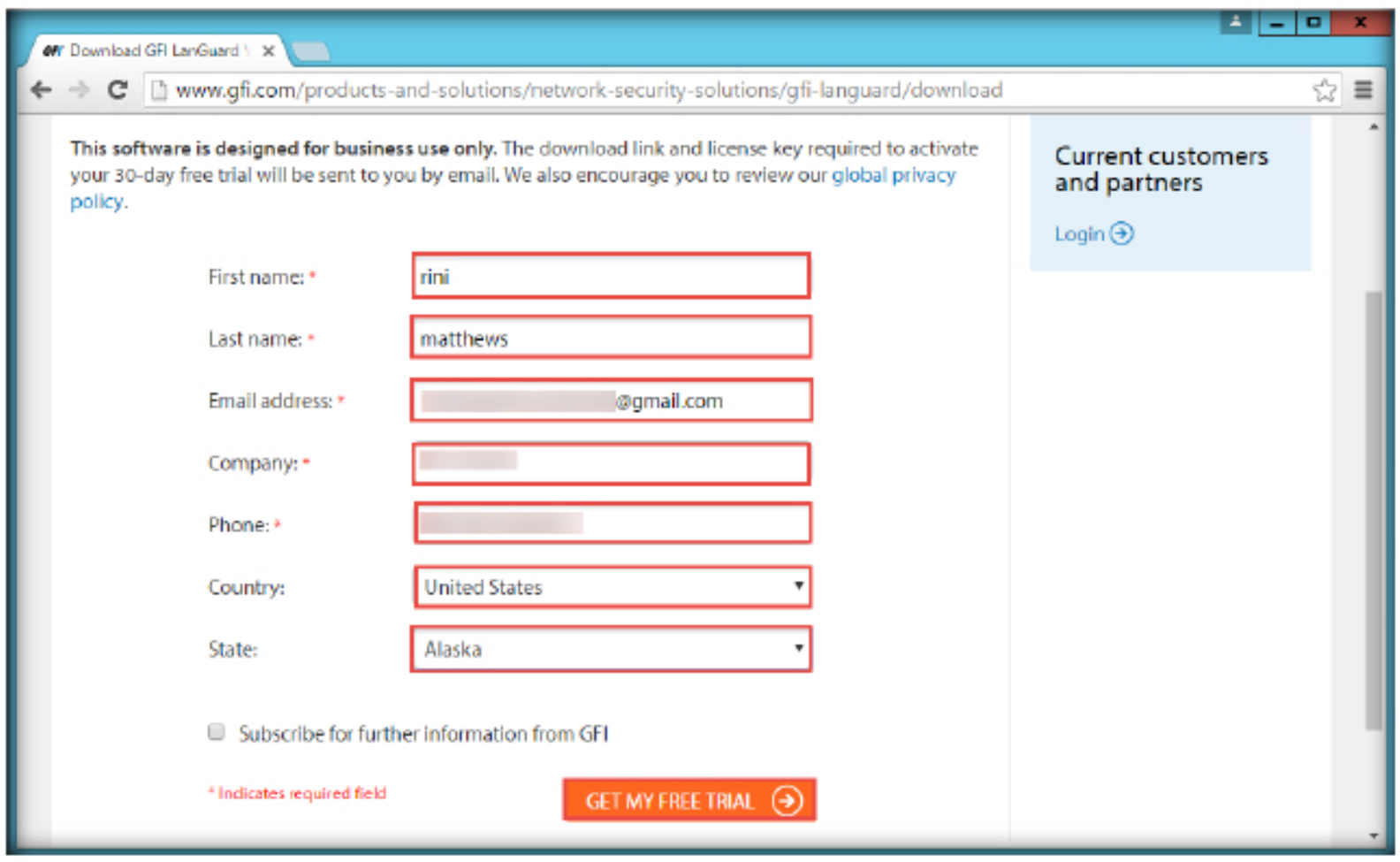


FIGURE 2.1: GFI LanGuard Registration page

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

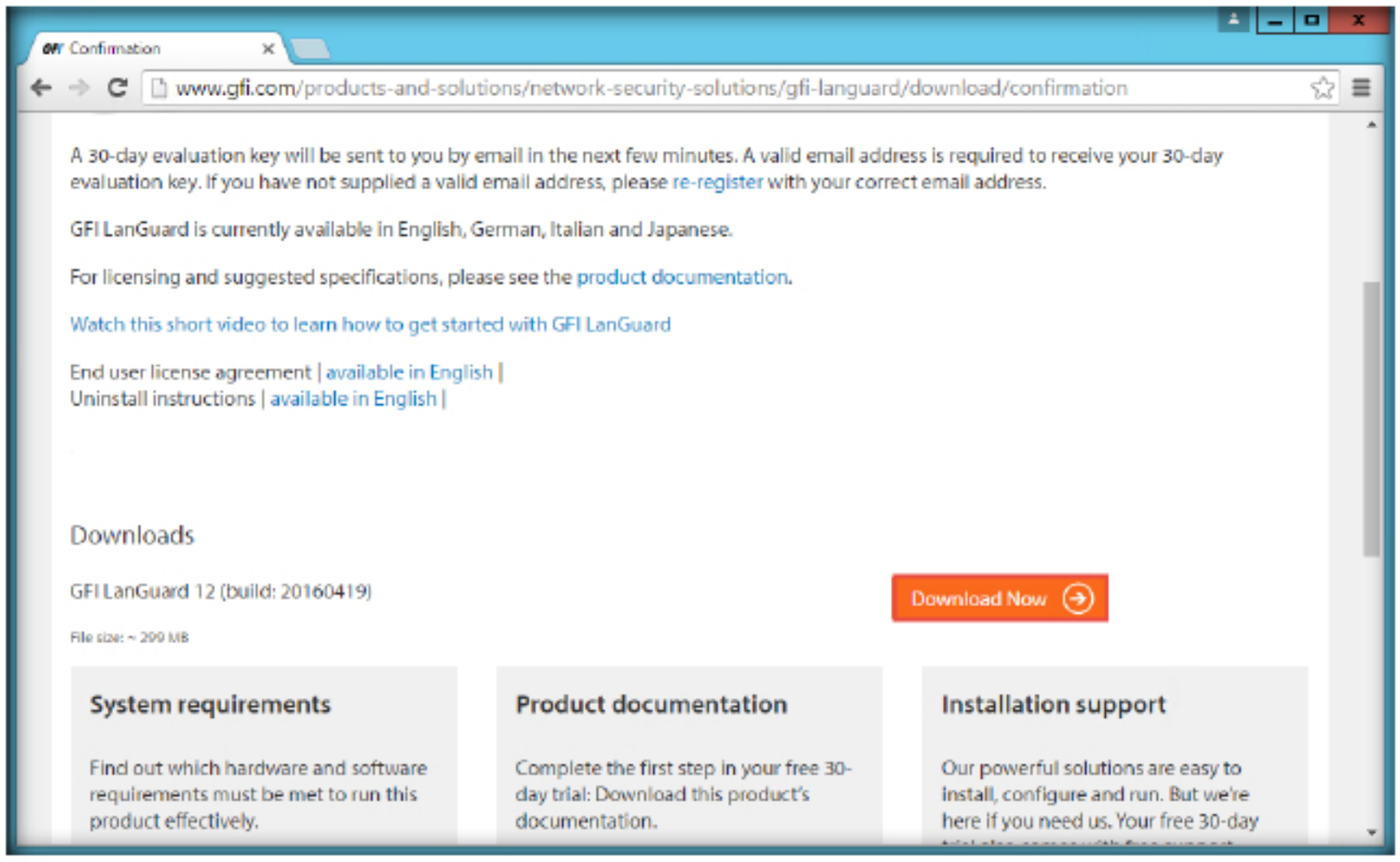


FIGURE 2.2: GFI LanGuard Download page

TASK 2

Install GFI LanGuard

4. Navigate to the download location for your browser and double-click **languard.exe** to begin the installation.

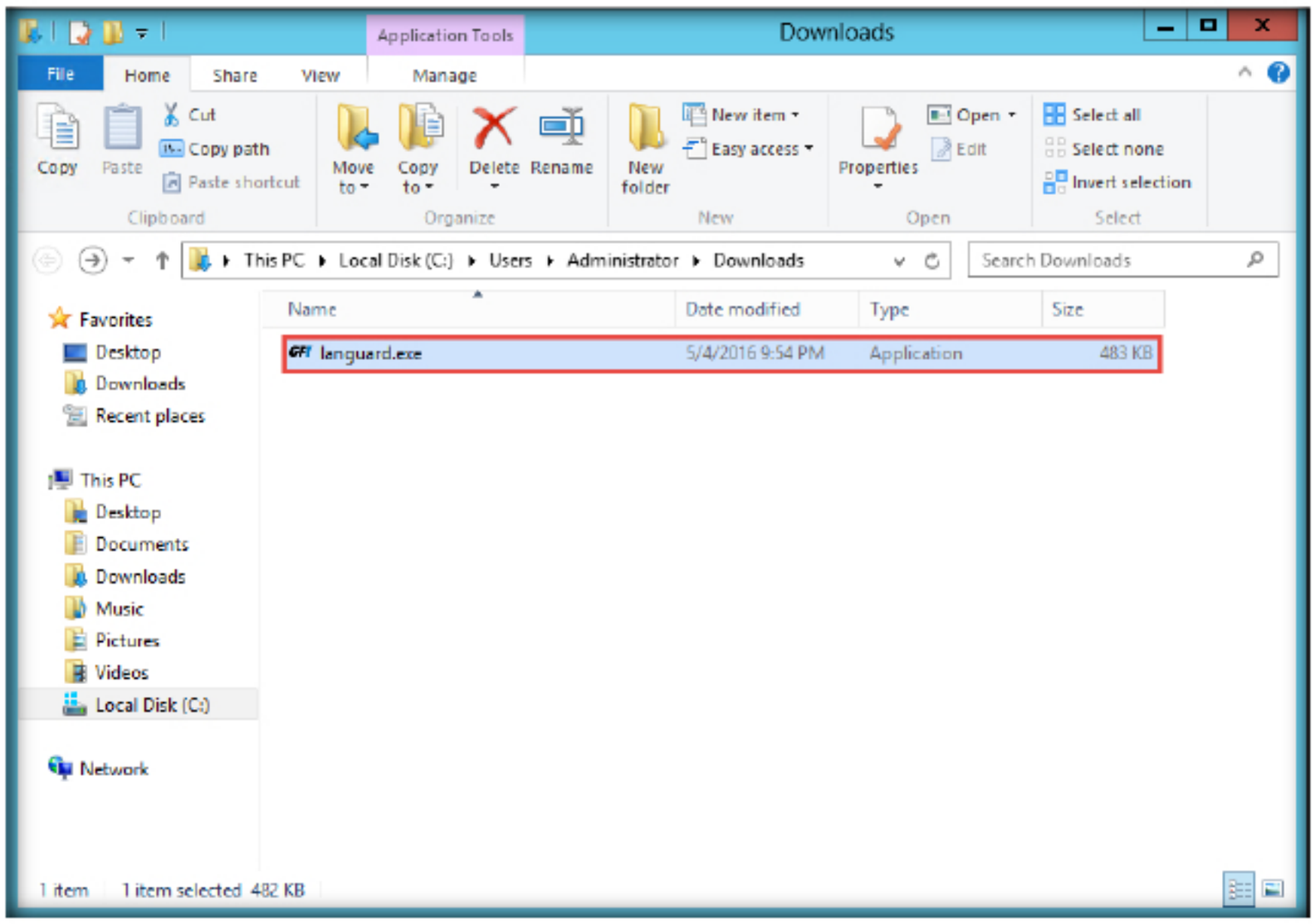


FIGURE 2.3: GFI LanGuard exe file

5. If the **Open File - Security Warning** pop-up appears, click **Run**.
6. When the **GFI LanGuard Installer** dialog box appears, click **I Agree**.

FIGURE 2.4: GFI LanGuard License Agreement Window

GFI LanGuard works on Microsoft Windows Server 2008 Standard/Enterprise, Windows Server 2003 Standard/Enterprise, Windows 7 Ultimate, Microsoft Small Business Server 2008 Standard, Small Business Server 2003 (SP1), and Small Business Server 2000 (SP2).

7. The GFI LanGuard product installer begins to download. Wait until the download is completed. Once the download is finished click **Next**.
8. The **GFI LanGuard** dialog box appears. Select a preferred language, then click **OK**.

FIGURE 2.5: Selecting a language

9. The **GFI LanGuard** installation window opens. Click **Next**.

The GFI LanGuard Computers by operating system -
This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by the installed operating system.

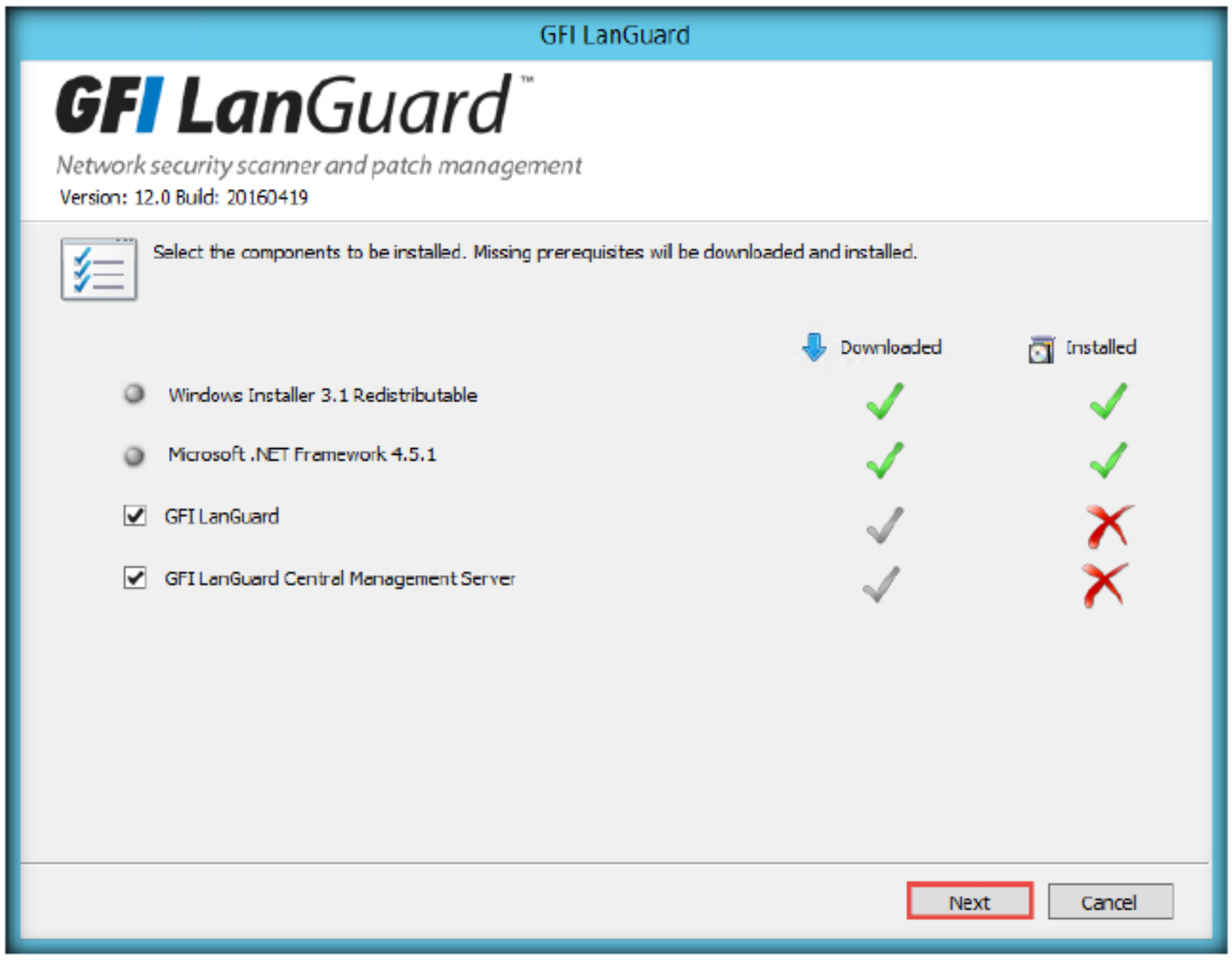


FIGURE 2.6: GFI LanGuard 2014 installation window

10. The **Database Configuration** window pops up. Click **Install Microsoft SQL Server Express (free)**.

The GFI LanGuard Computers by network role

This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by network role. Amongst other roles, this graph identifies the number of servers and workstations per selected domain.

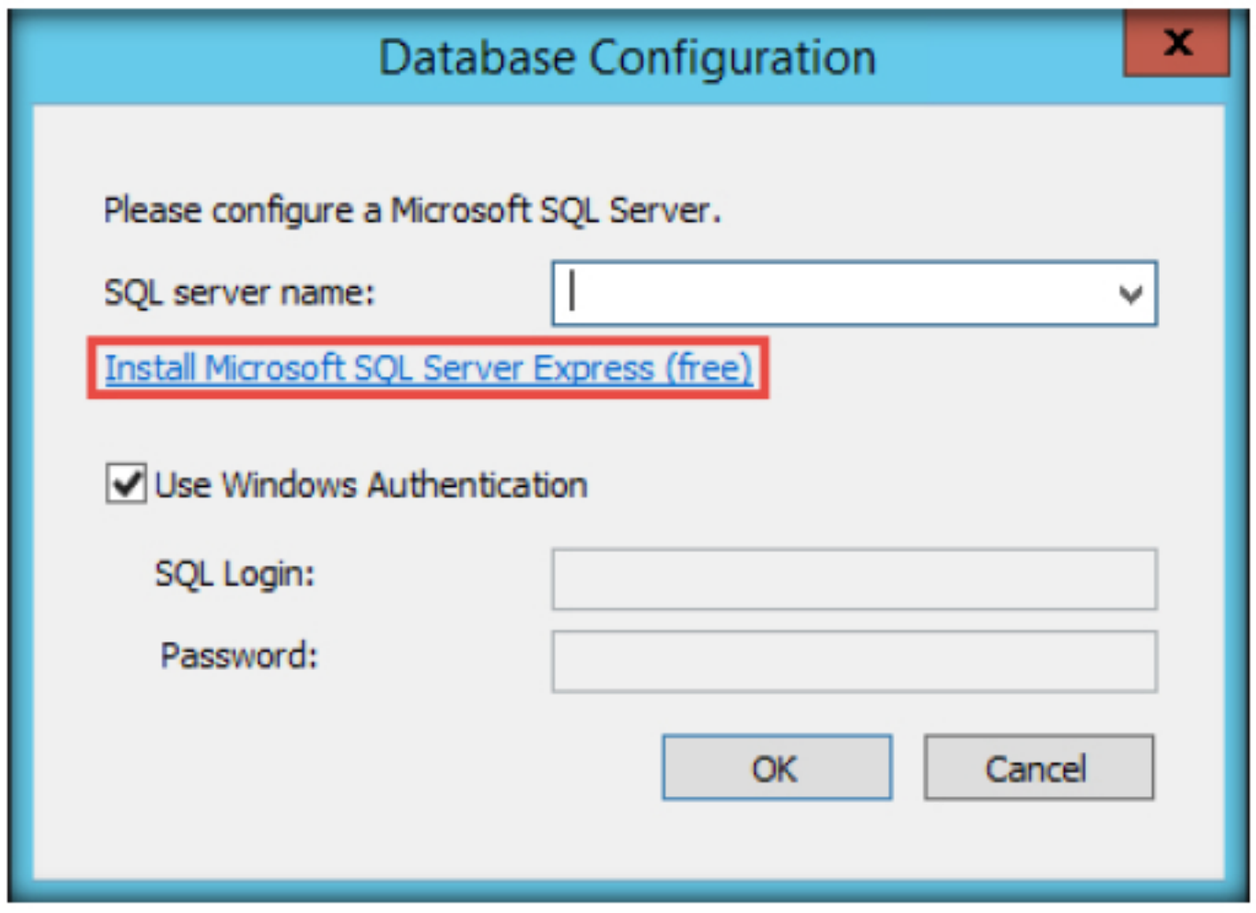


FIGURE 2.7: Database Installation

The GFI LanGuard Audit status
This chart is available only when selecting a domain or workgroup and enables you to identify how many audits have been performed on your network grouped by time.

11. The SQL Server 2012 Setup window appears. Wait for the rule check to complete.
12. In the License terms page click the checkbox **I accept the license terms** then click **Next**.

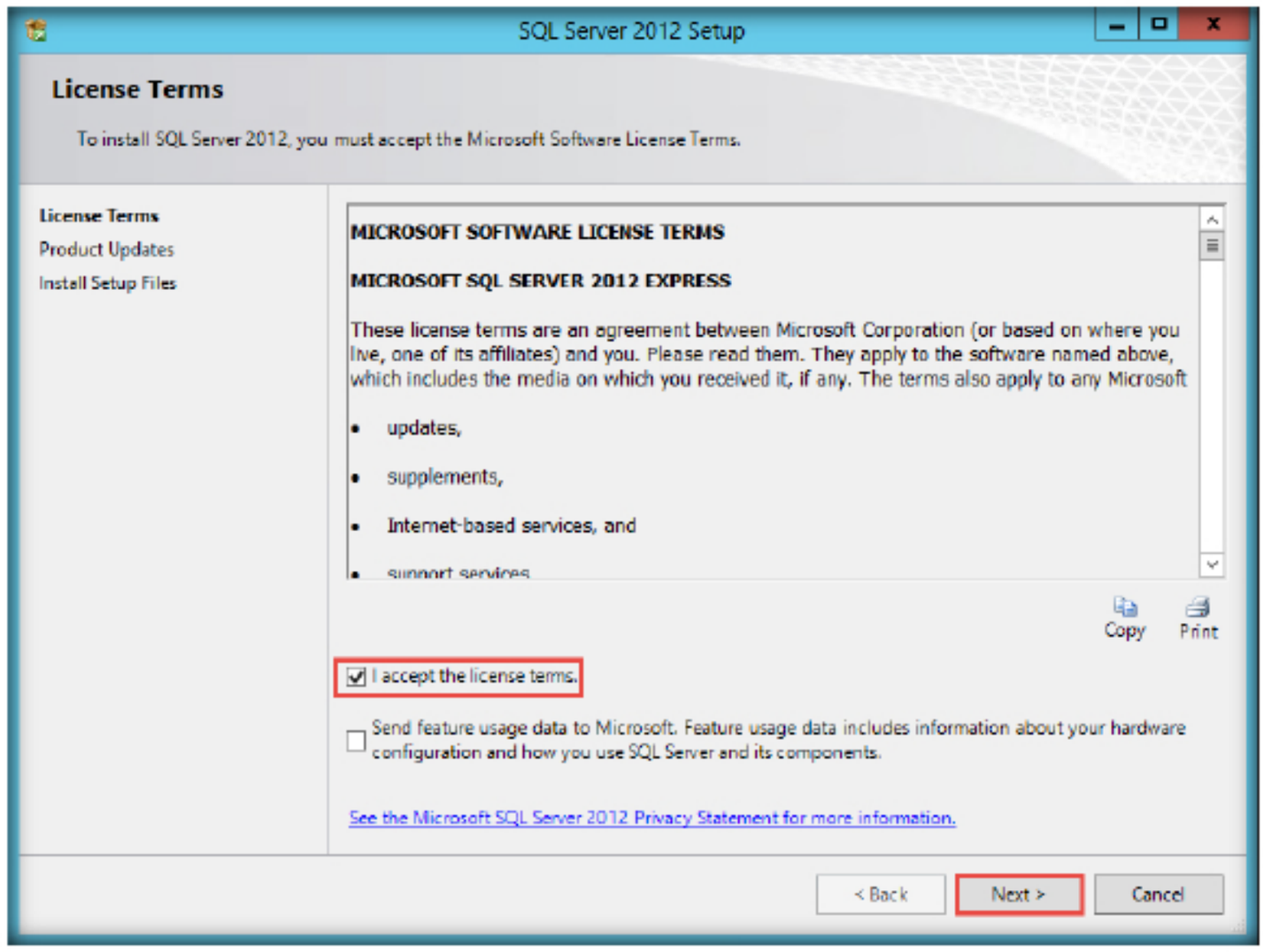


FIGURE 2.8: Accepting the license terms

13. The **Product Update** page appears. Click **Next**.

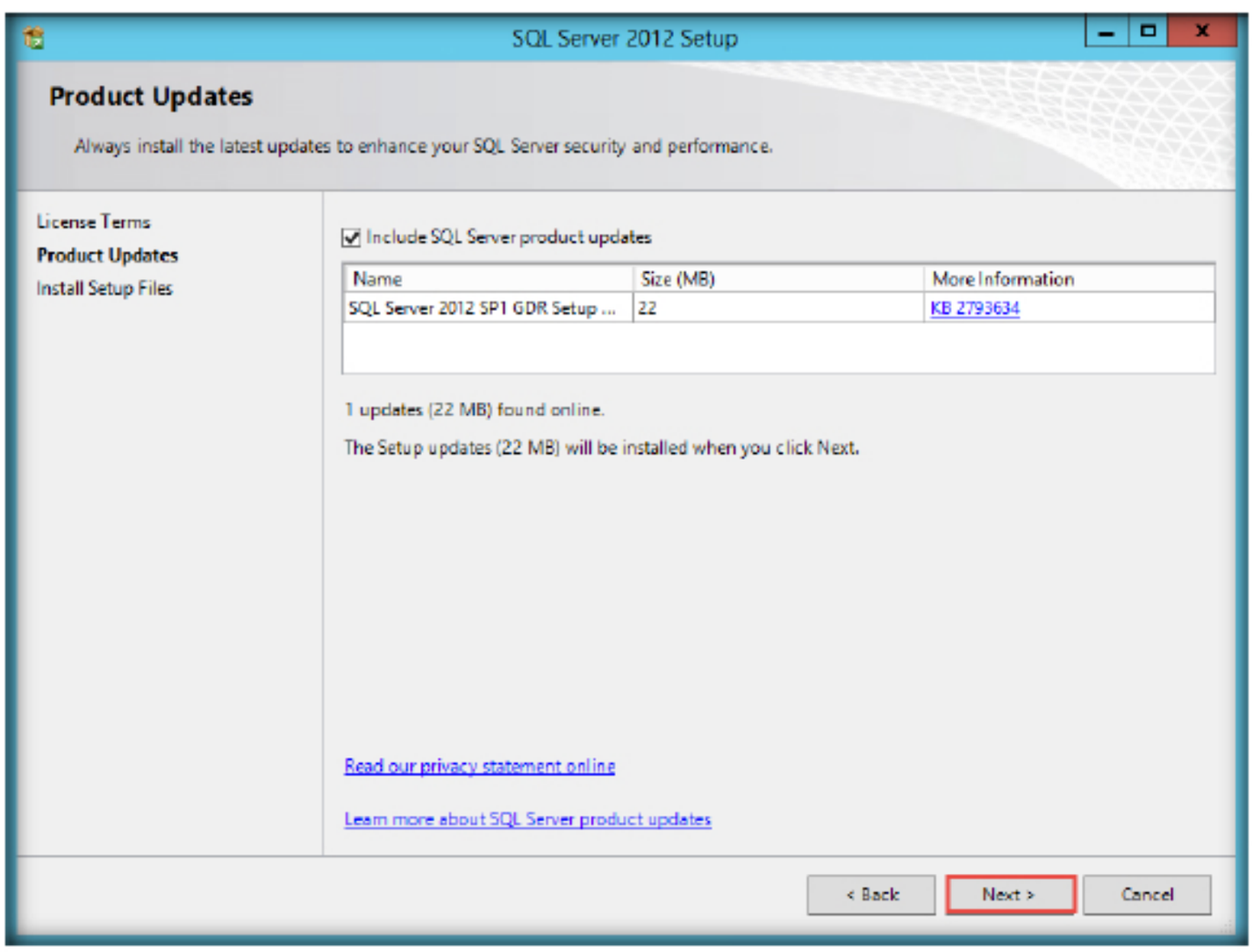


FIGURE 2.9: Accepting the license terms

The GFI LanGuard Vulnerability trends over time -
When a domain or workgroup is selected, this section displays a line graph showing the change of vulnerability level over time grouped by computer count. When a single computer is selected, this section displays a graph showing the change of vulnerability level over time for the selected computer.

14. The **Install Setup Files** appears. Wait for all tasks to download and be installed.

The GFI LanGuard Computer vulnerability distribution - This chart is available only when selecting a domain or a workgroup, and displays the distribution of vulnerabilities on your network. This chart enables you to determine how many computers have high, medium and low vulnerability rating.

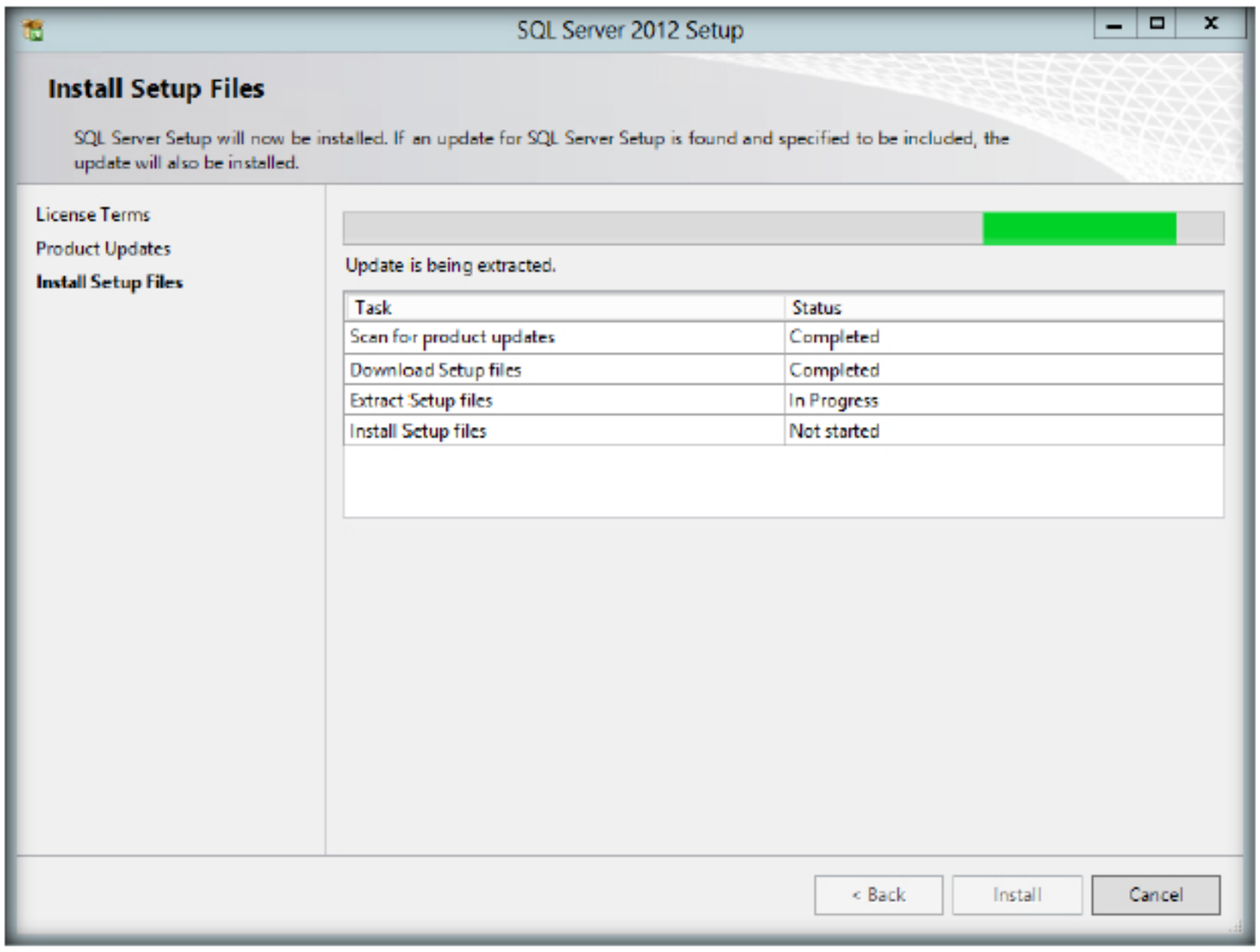


FIGURE 2.10: Install files download

15. Next, the **SQL Server 2012 Setup** with Feature Selection wizard, leave the settings as default then click **Next**.

The GFI LanGuard: Most vulnerable computers

This list is available only when selecting a domain or a workgroup, and shows the most vulnerable computers discovered during the scan. The icon color on the left indicates the vulnerability level.

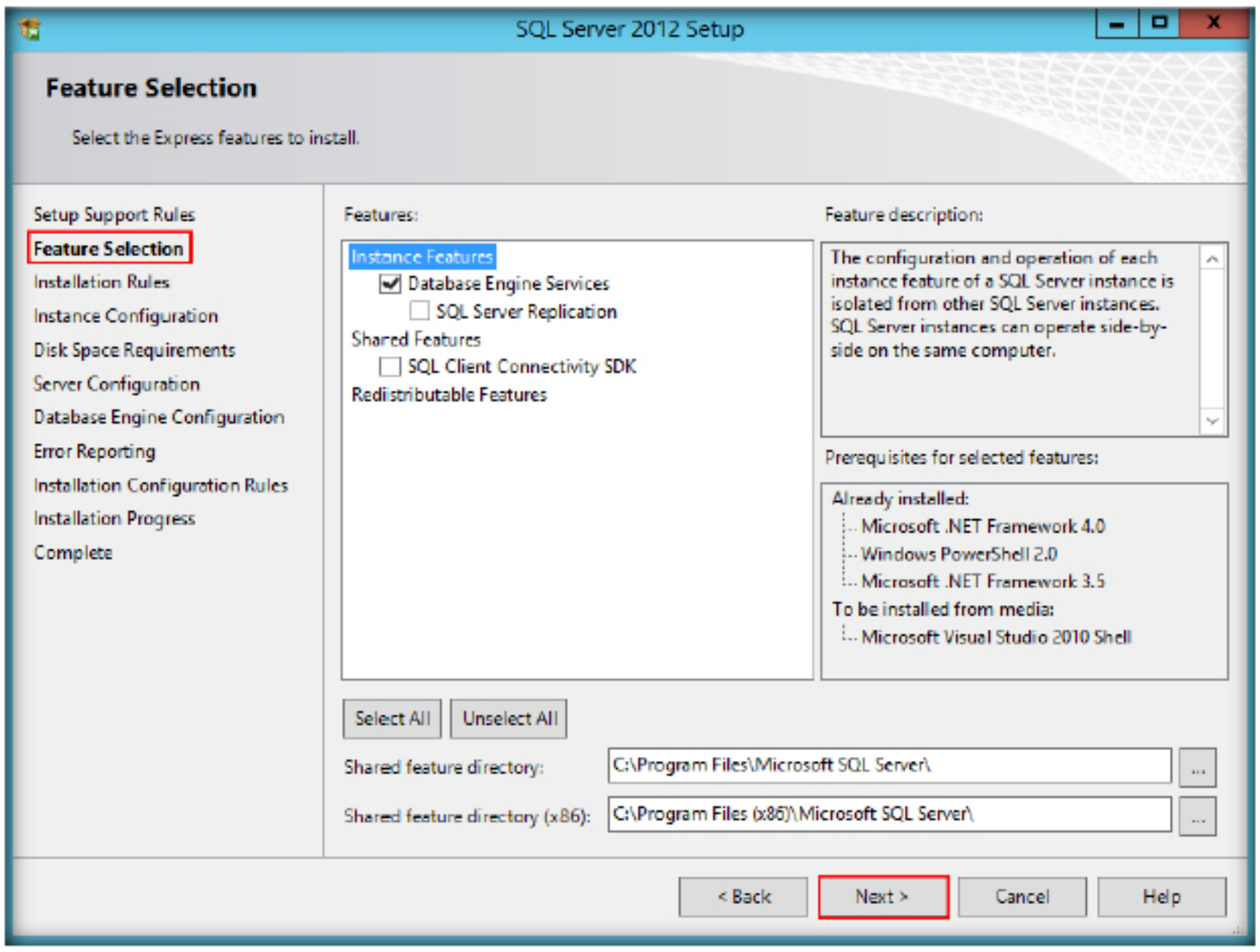


FIGURE 2.11: SQL Server Feature Selection

16. In the Instance Configuration option, change the name to SQL under the **Named Instance** radio button, then click **Next**.

The GFI LanGuard dashboard Overview is a graphical representation of the security level/vulnerability level of a single computer, domain or entire network.

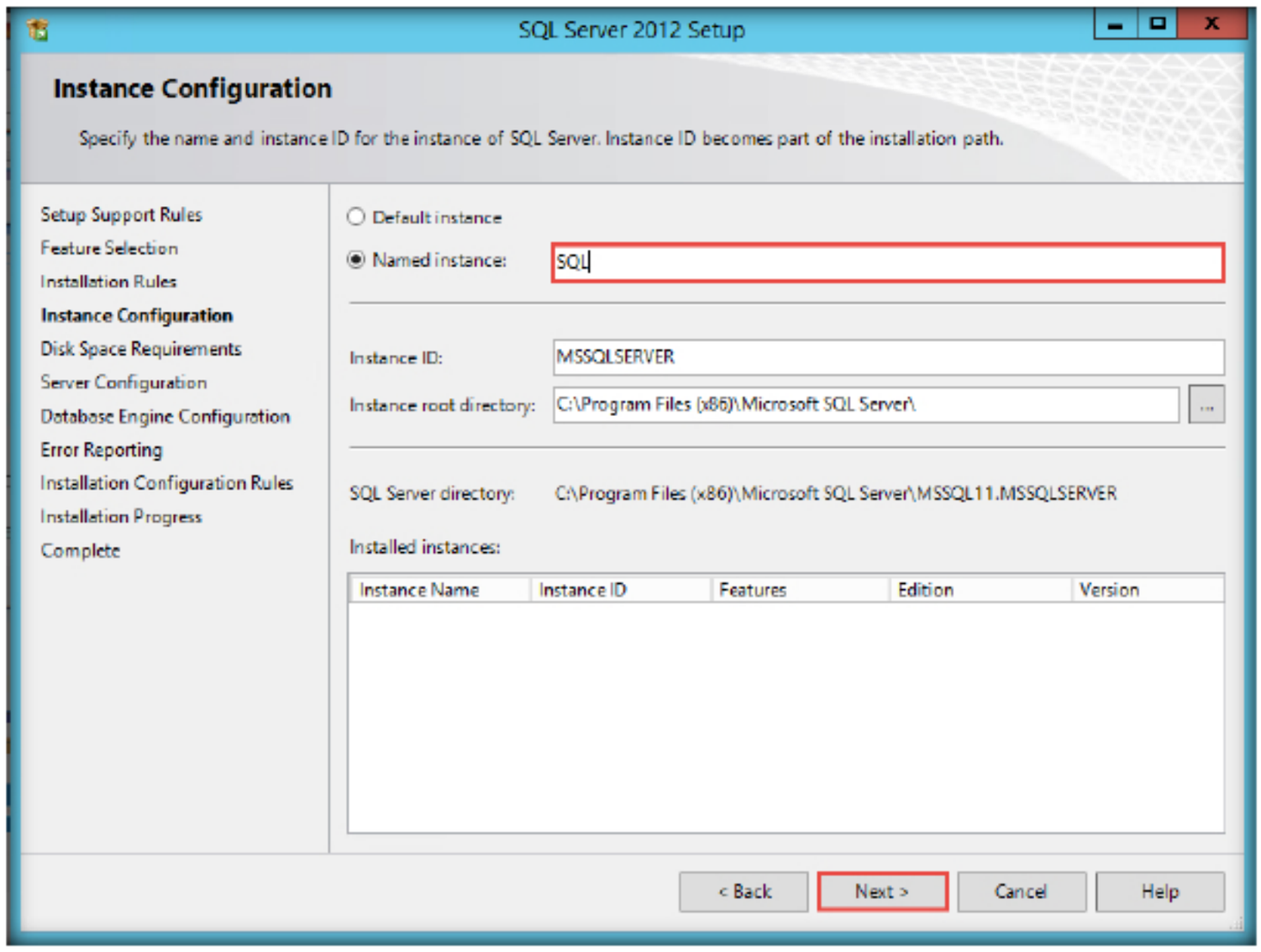


FIGURE 2.12: Instance configuration option setup

17. Install the SQL Server 2012 Setup with the default options, after completing the installation, you are prompted for a System restart. Click **OK**. Then, click the Close button to exit the SQL Server Setup window

18. The Database Configuration window appears. Select **.\SQL** from the **SQL Server Name** drop down list then click **Next**.

The GFI LanGuard: Network security level This rating indicates the vulnerability level of a computer/network, depending on the number and type of vulnerabilities and/or missing patches found. A high vulnerability level is a result of vulnerabilities and/or missing patches which average severity is categorized as high.

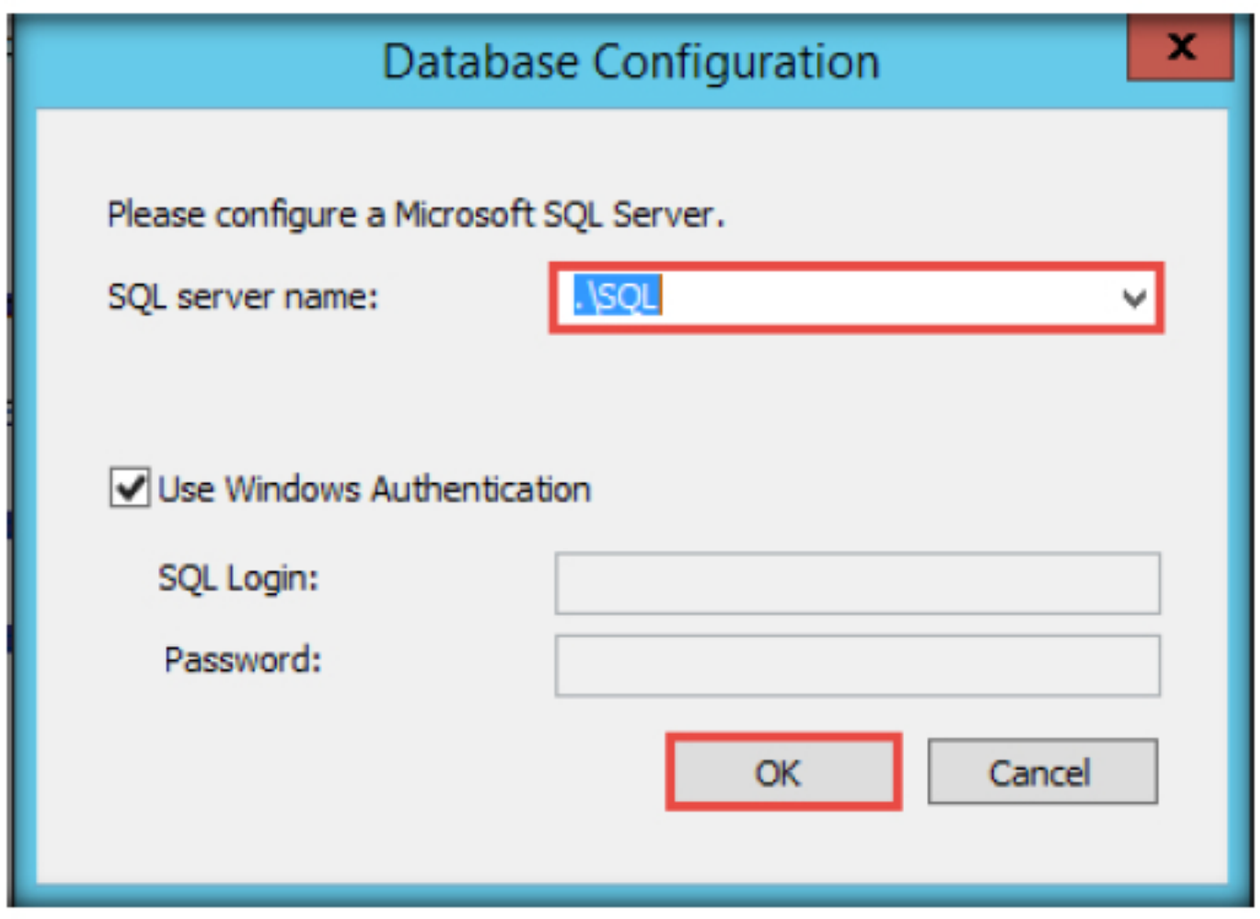


FIGURE 2.13: Database Configuration window

19. Wait until the necessary files are downloaded.

FIGURE 2.14: GFI LanGuard 2014 dialog-box

20. The **GFI LanGuard Setup** window opens, click **Next**

The GFI LanGuard dashboard is made up of multiple views. These different views enable real-time monitoring of your scan targets and allow you to perform instant remedial and reporting operations.

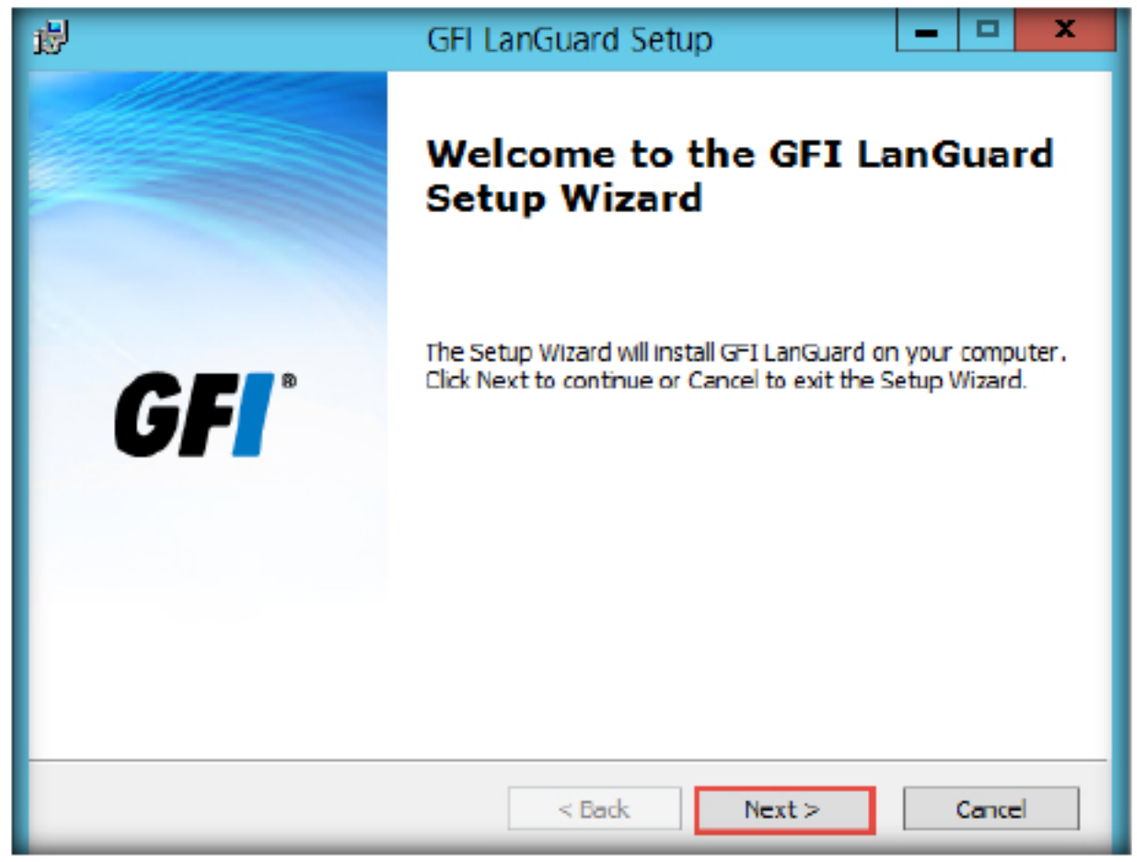


FIGURE 2.15: GFI LanGuard dialog-box

21. The **Customer Information** section of the Setup wizard appears with the **License Key** then click **Next**

Full Scan (Active)Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with LAN environments.

FIGURE 2.16: GFI LanGuard 2014 dialog-box

22. In the **Attendant service credentials** section, leave the **Name** field set to its default, and enter the **Password** for the machine where **GFI LanGuard** is installed, then click **Next**.

FIGURE 2.17: GFI LanGuard Attendant service credentials section

23. In the **Choose Destination Location** section, choose the location where you want to install the application, then click **Install**.

GFI LanGuard ships with the default scanning profiles described in the sections below. To create your own custom scanning profiles, refer to creating a new Scanning Profile.

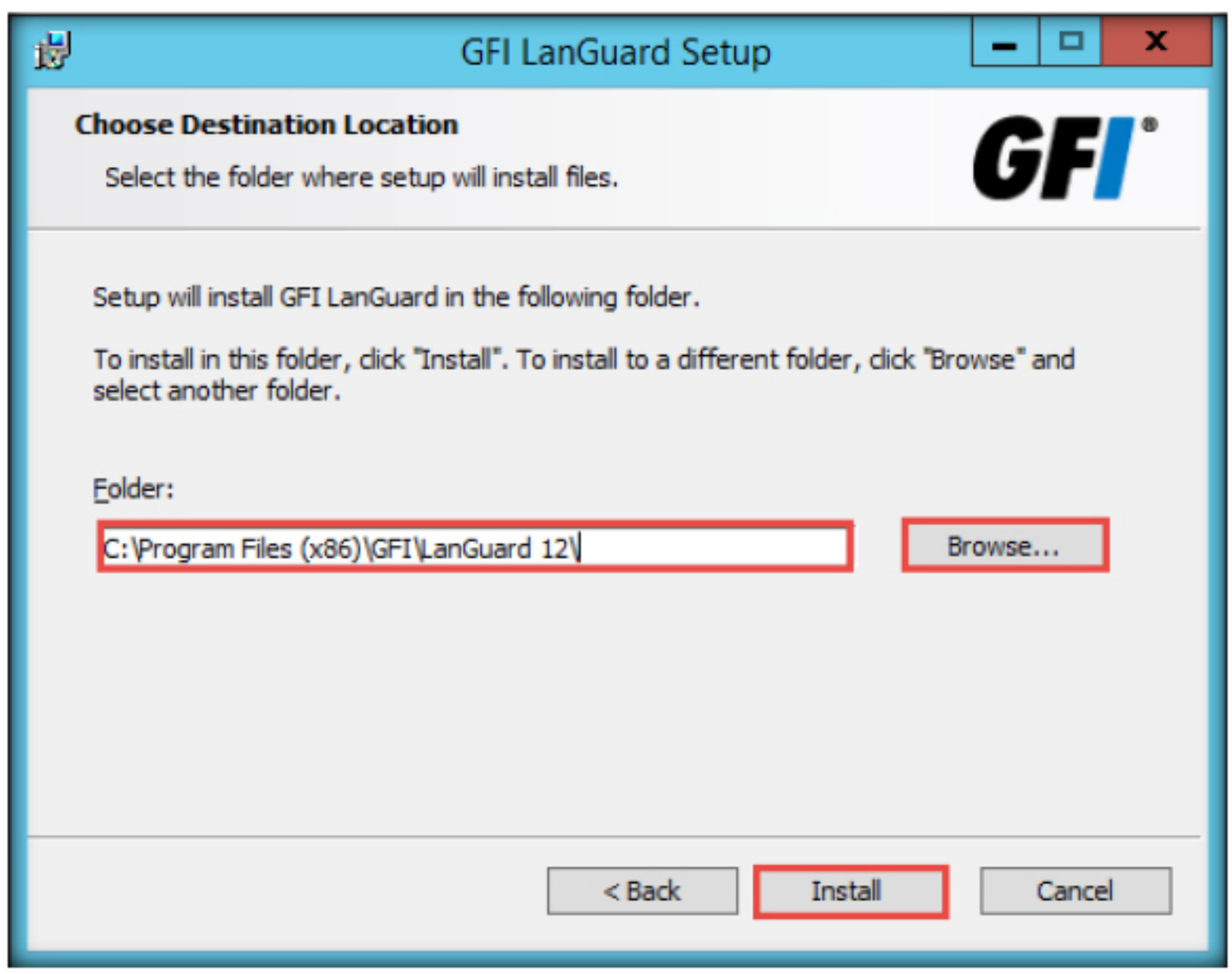


FIGURE 2.18: GFI LanGuard Attendant service credentials section

24. The application begins to install. Wait for the process to complete.

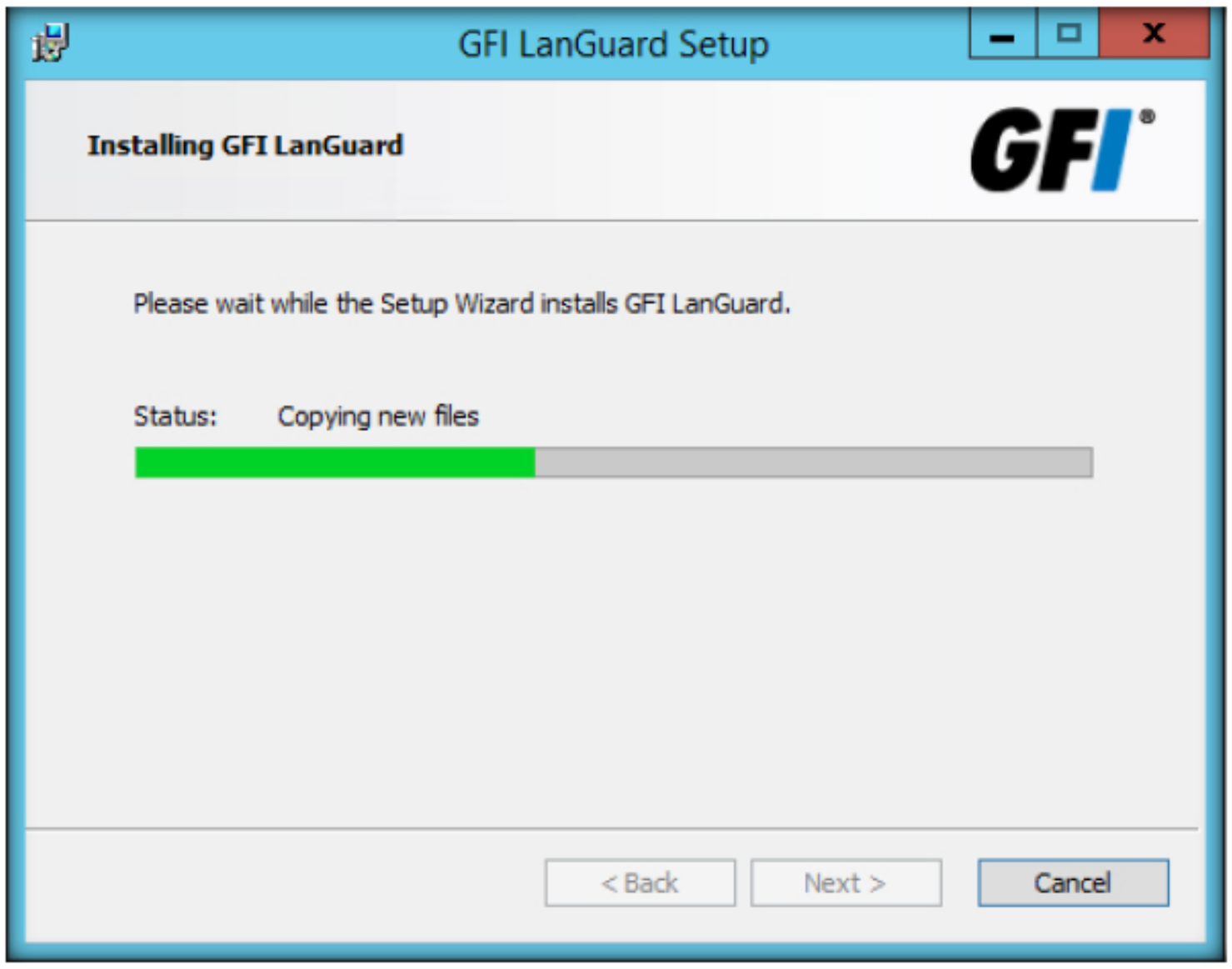


FIGURE 2.19: GFI LanGuard Installation window

25. The **GFI LanGuard Central Management Server Setup** page appears. Click **Next**.

GFI LanGuard enables you to scan your IT infrastructure for particular vulnerabilities using pre–configured sets of checks known as scanning profiles. Scanning profiles enable you to scan your network targets and enumerate only specific information.

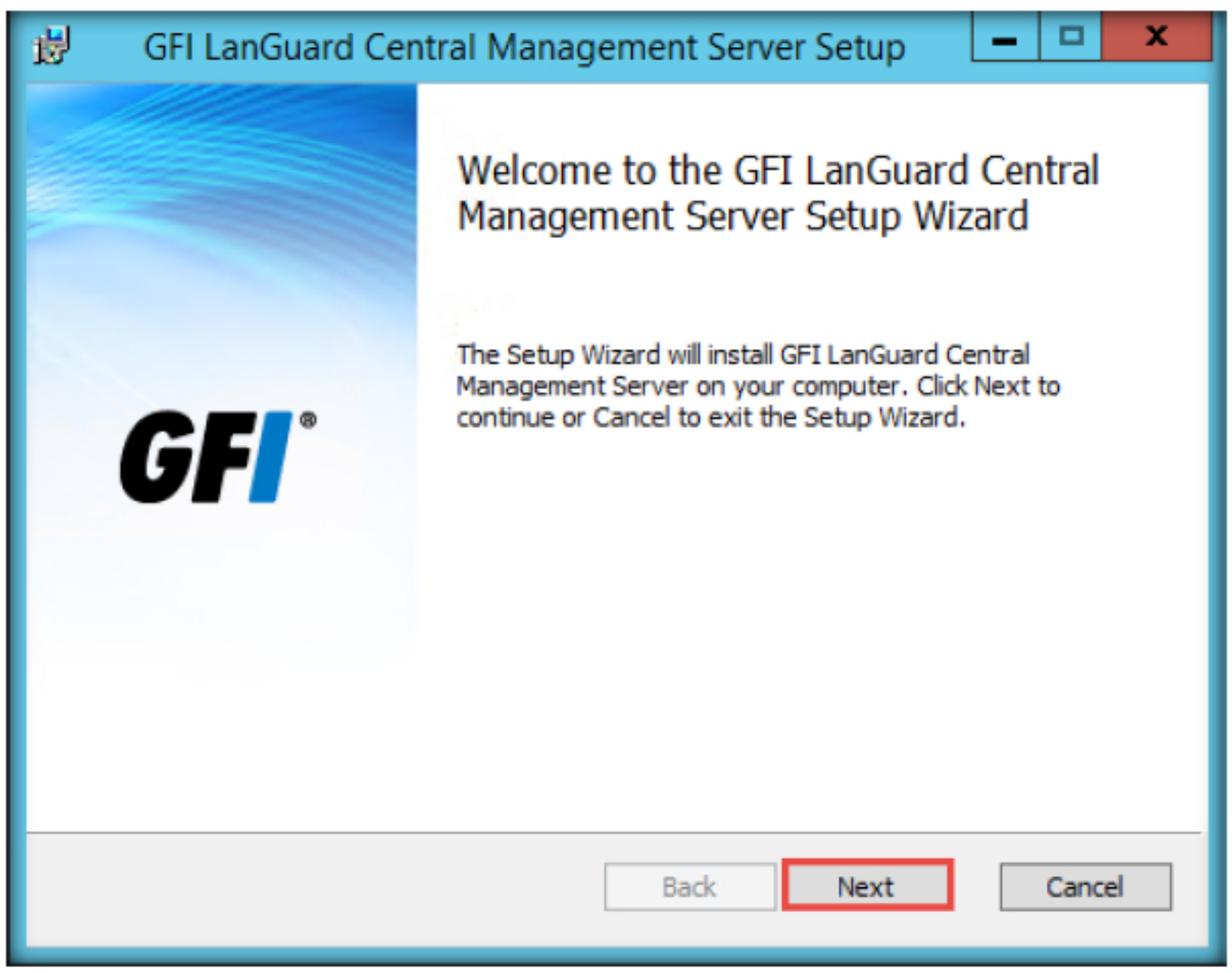


FIGURE 2.20: GFI LanGuard Central management server

26. In the **Service logon information** section, leave the **Name** field set to its default, and enter the **Password** for the machine where **GFI LanGuard** is installed then click **Next**.

In practice, scanning profiles enable you to focus your vulnerability scanning efforts on to a specific area of your IT infrastructure, such as identifying only missing security updates. The benefit is that you have less scan results data to analyze; tightening up the scope of your investigation and helping you quickly and easily locate the information you require.

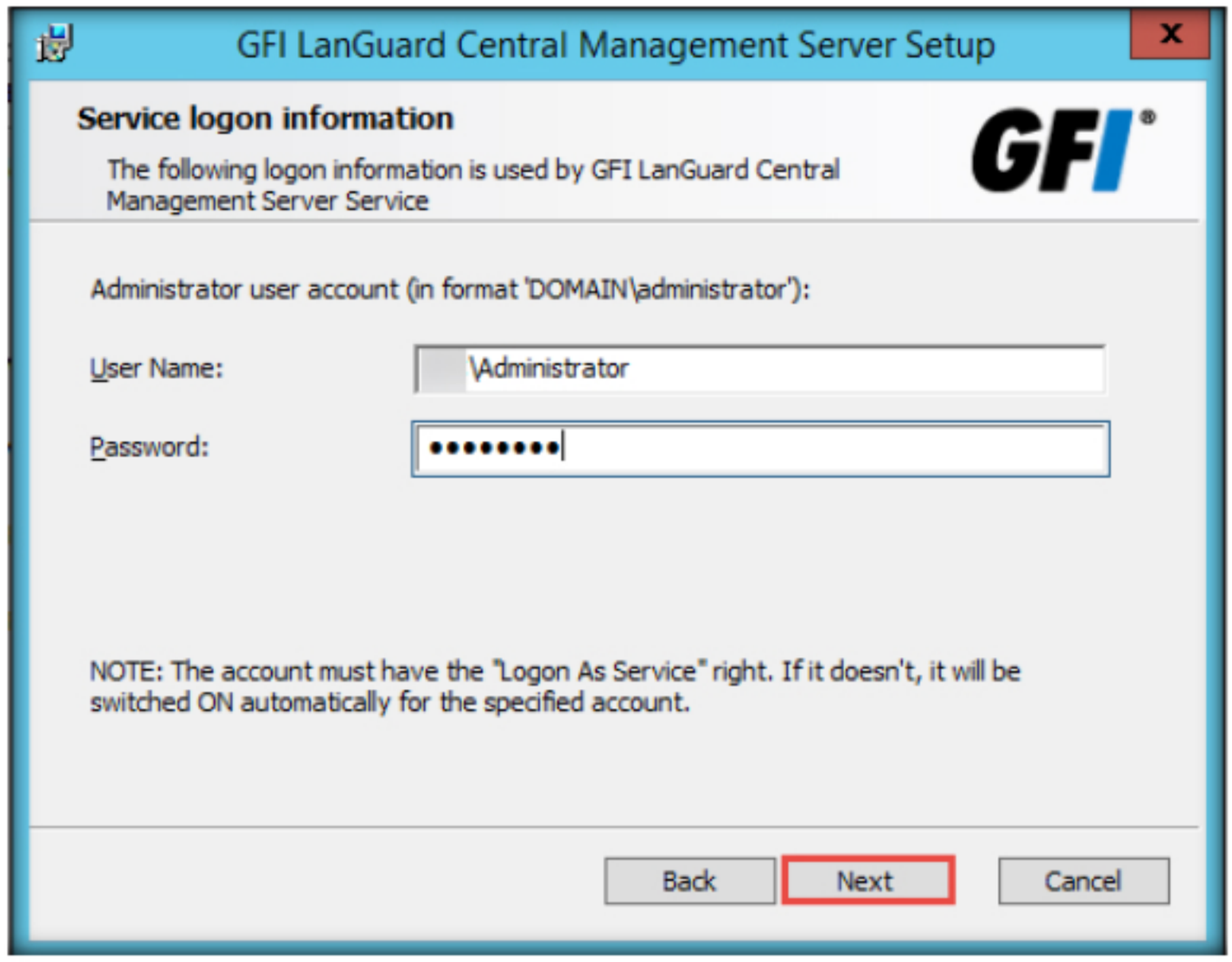


FIGURE 2.21: GFI LanGuard Service logon information section

27. The **HTTPS settings** page appears. Do not make any changes. Click **Next**

GFI LanGuard Central Management Server is aimed at very large networks that want to monitor the operation of multiple GFI LanGuard instances in one central console. It offers administrators a view of the security and vulnerability status for all computers, networks or domains managed by the different GFI LanGuard instances.

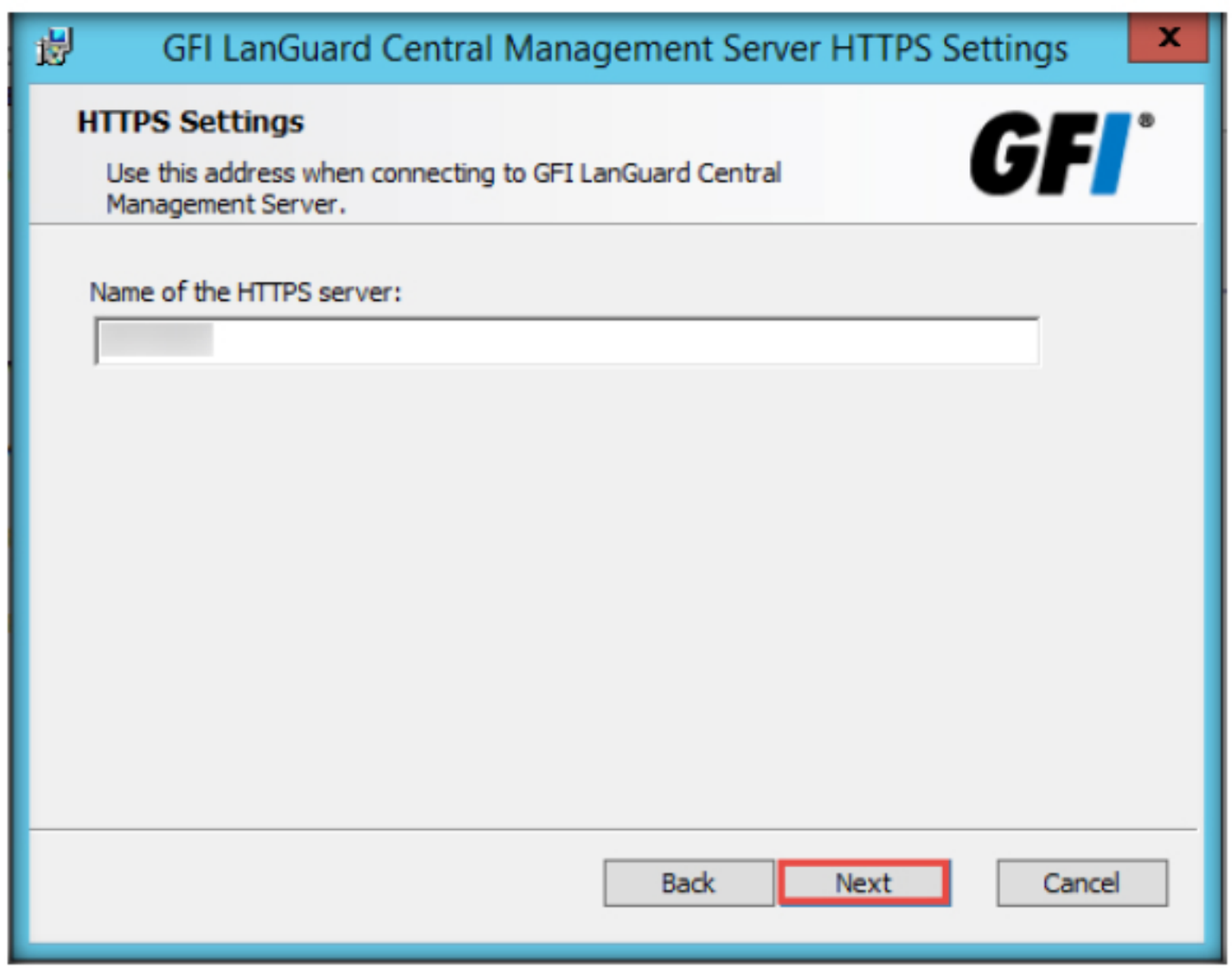


FIGURE 2.22: GFI LanGuard HTTPS settings section

28. The **Destination Folder** section appears. If you want to change the default location click **Change...** and select new location. Otherwise, click **Next**.

The GFI LanGuard Central Management Server is used for reporting only. Scans and remediation take place within each individual GFI LanGuard instance. Information is centralized to the GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard, depending on the network size and amount of data being transferred.

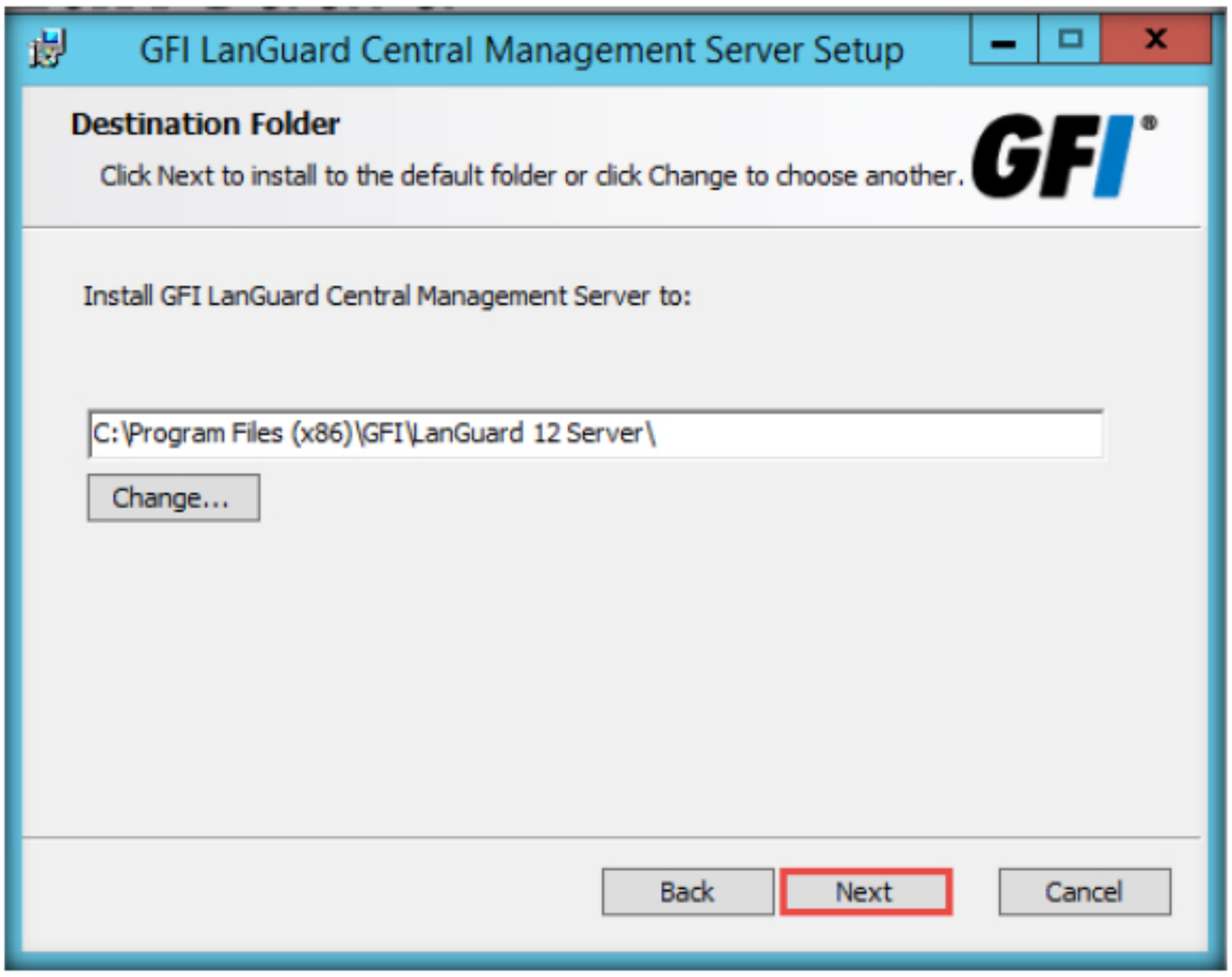


FIGURE 2.23: GFI LanGuard Destination Folder section

29. The **Ready to install** section appears. Click **Install**.

Agents send scan data to GFI LanGuard through TCP port 1070. This port is opened by default when installing GFI LanGuard. Agents do not consume resources on the scan target unless the agent is performing a scan or a remediation operation.

Note that agents can only be deployed on computers running a Microsoft Windows operating system and they require approximately 25 MB of memory and 350 MB of hard disk space.

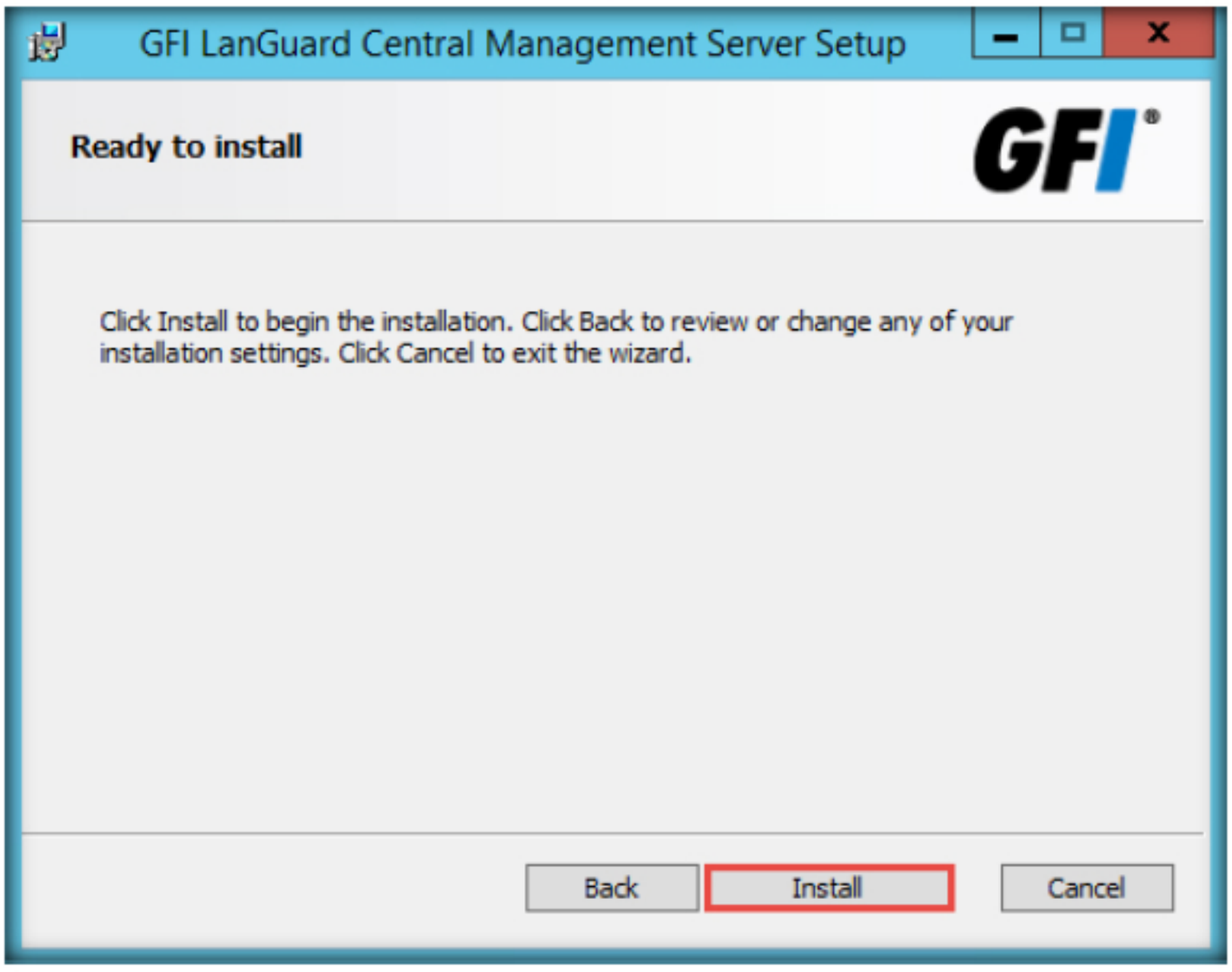


FIGURE 2.24: GFI LanGuard Ready to install section

30. Wait for the installation process to complete.

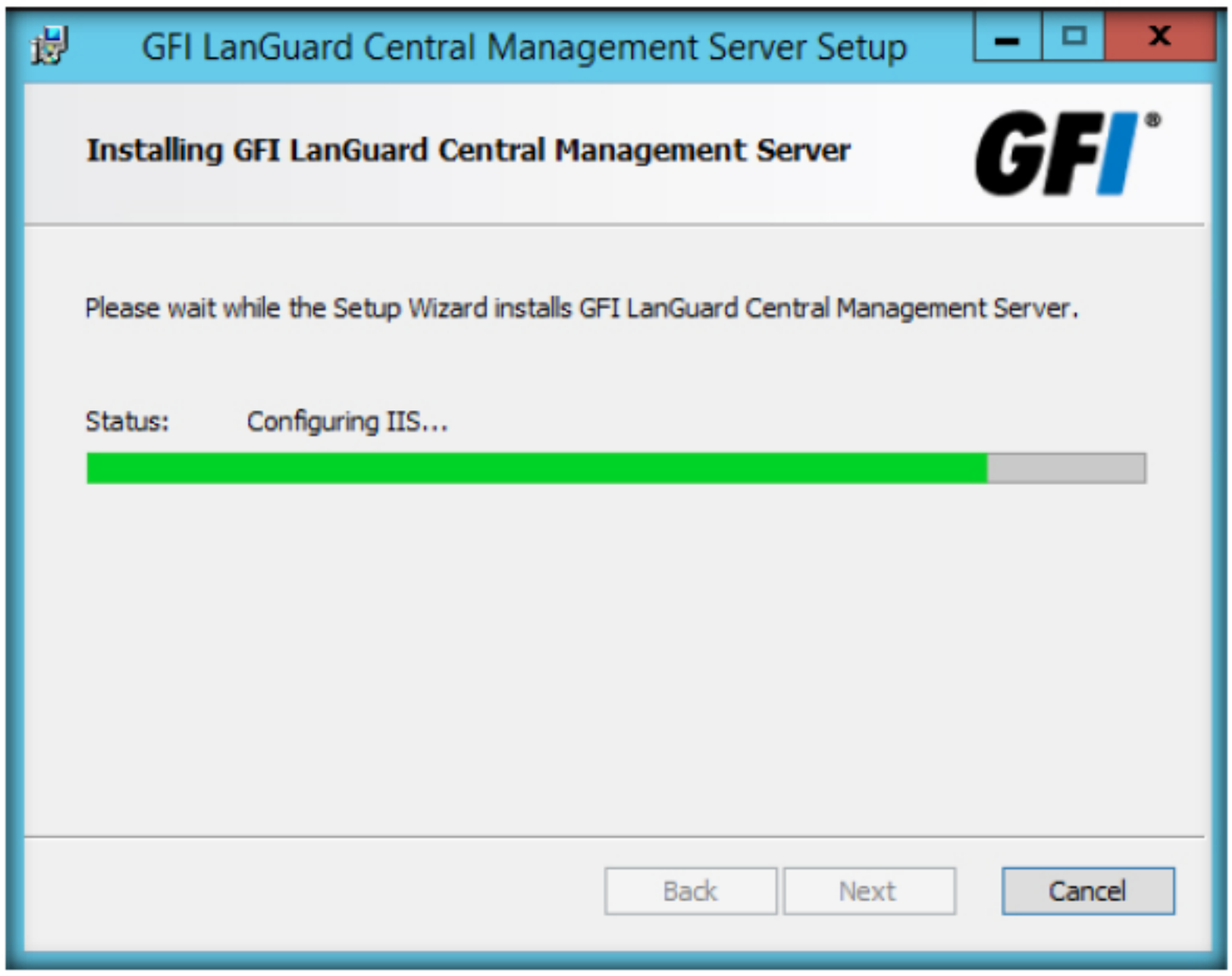


FIGURE 2.25: Central Management Server installation in progress

Relay agents reduce the load from the server where GFI LanGuard is installed to increase server performance and to apply bandwidth load balancing techniques. Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers.

31. Click **Finish** once the installation is completed.

FIGURE 2.26: Central Management Server installation completed

GFI LanGuard can be deployed in a number of ways, depending on the number and type of computers and devices you want to monitor network bandwidth usage during normal operation times and the network topology.

32. The **GFI LanGuard page** appears. Click **Finish** to launch **GFI LanGuard** and the **GFI LanGuard Central Management Server**.

GFI LanGuard can be configured to automatically deploy agents on computers. Agents minimize network bandwidth utilization because audits are done using the scan target's resources and only a result XML file is transferred over the network. Devices that have a GFI LanGuard agent installed will be scanned even if the device is not connected to the company network and are more accurate than agent-less scans because agents can access more information on the local host.

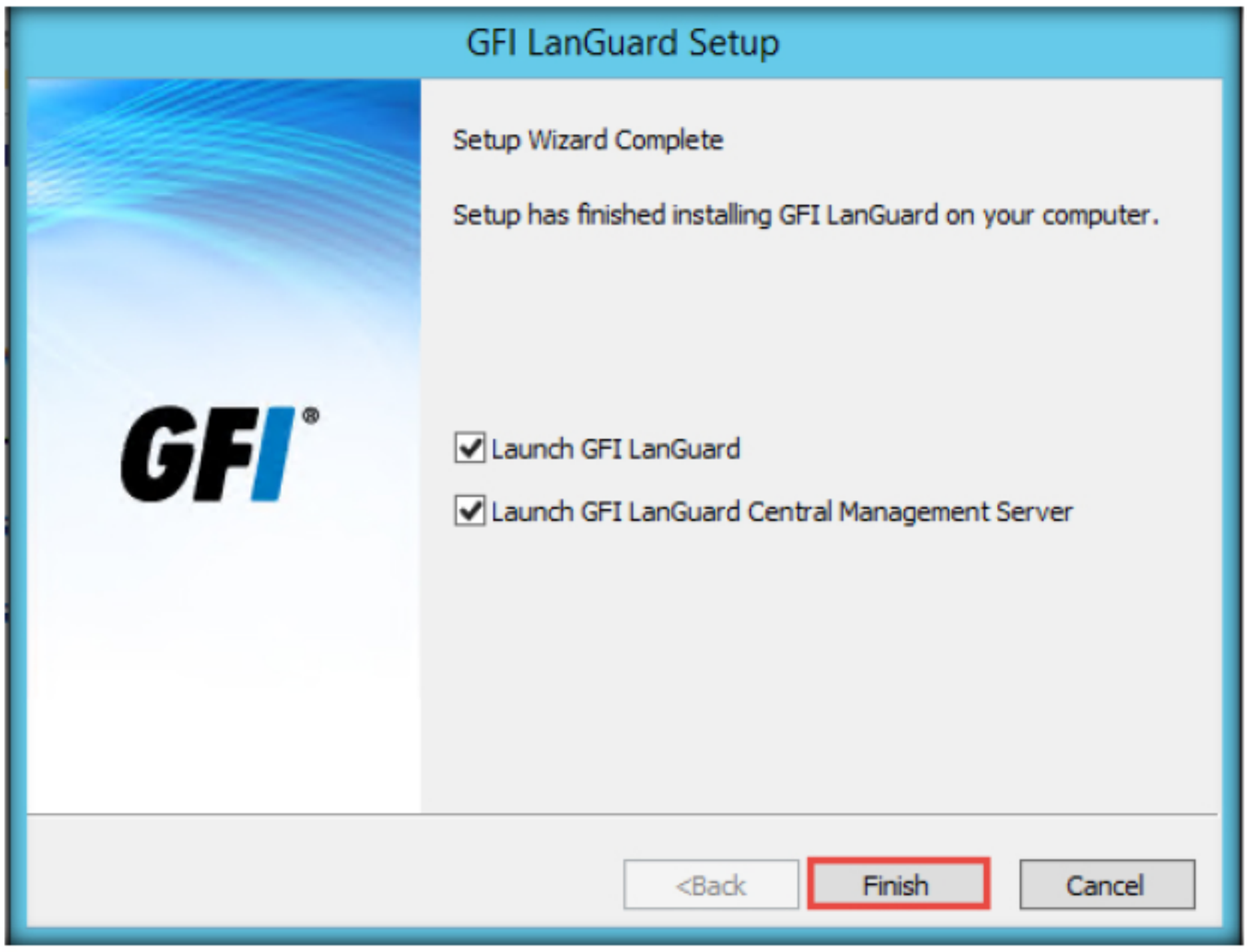


FIGURE 2.27: Launching GFI LanGuard and GFI Central Management Server

33. If the **GFI Central Management Server** appears in the browser minimize or close the browser.

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

If intrusion detection software (IDS) is running during scans, GFI LanGuard sets off a multitude of IDS warnings and intrusion alerts in these applications.

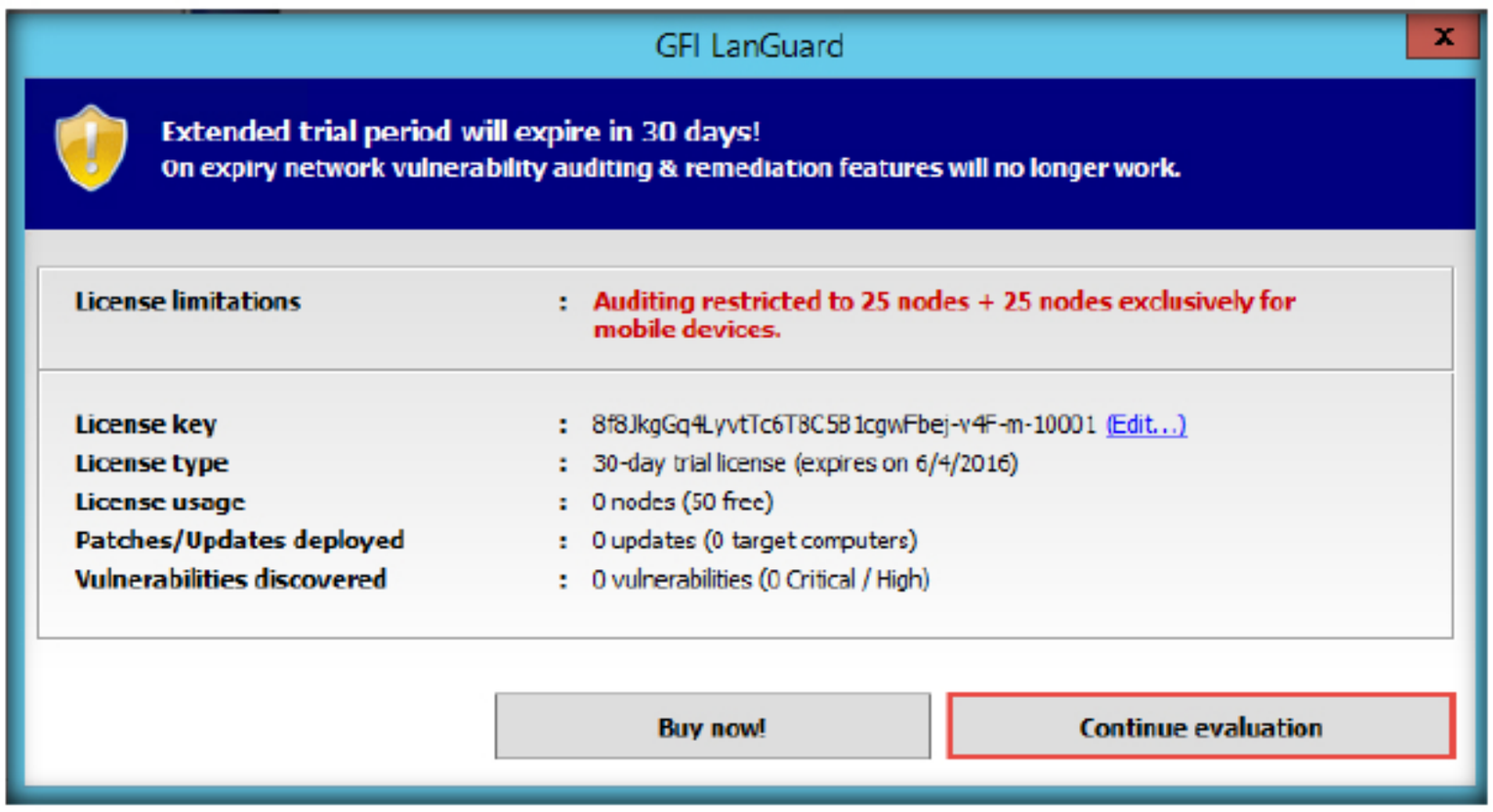


FIGURE 2.28: GFI LanGuard 2014 pop-up

TASK 3

Configure GFI LanGuard

35. The **GFI LanGuard** main window opens with the Network Audit tab contents.
36. GFI LanGuard begins to inspect the security status of the local computer.
37. Click **Launch a Scan**.

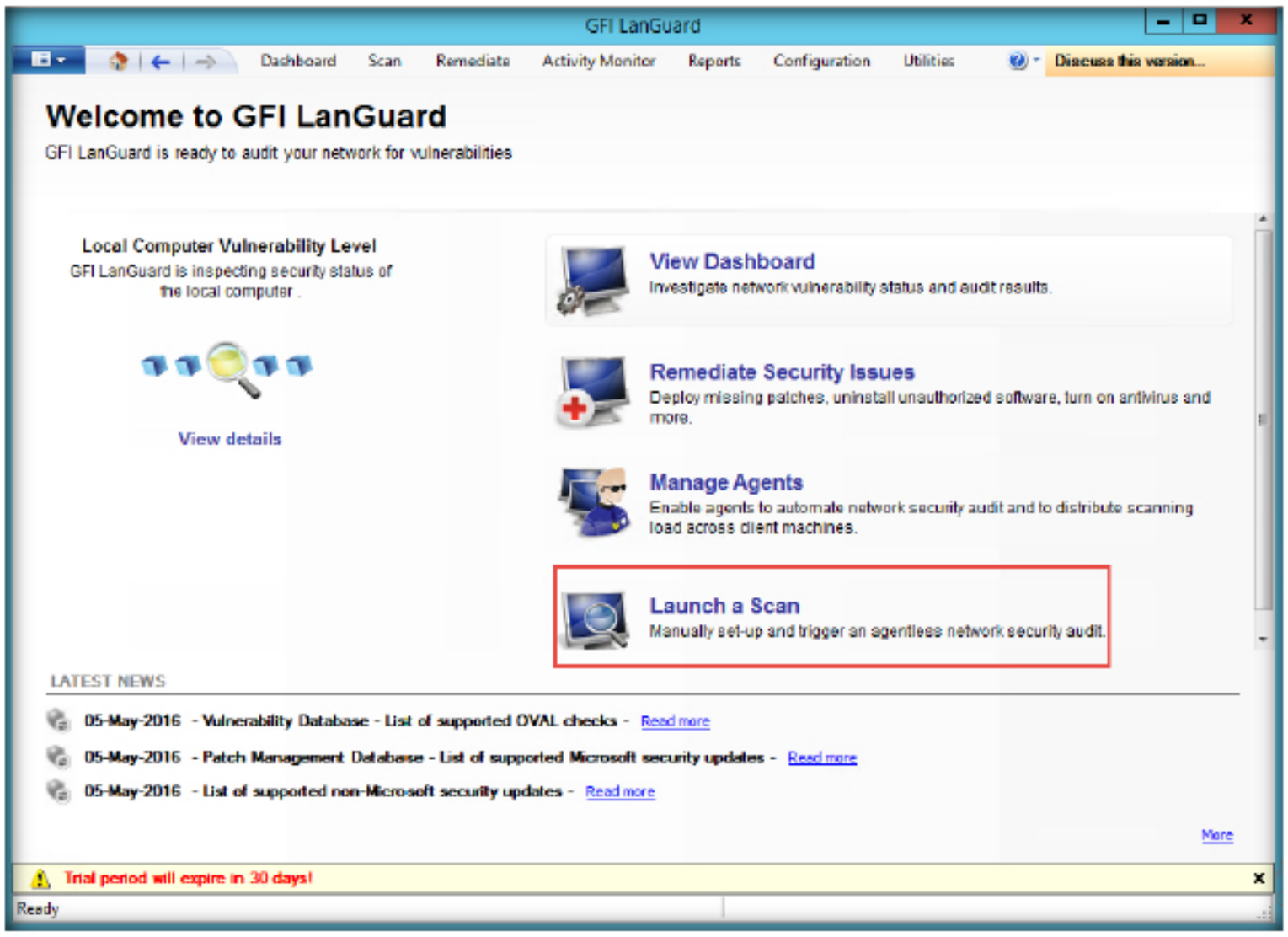


FIGURE 2.29: Launching a scan in GFI Languard

GFI LanGuard identifies reachable machines within your network. It collects information sets from the network machines as part of its Network Discovery operations and performs a deep scan to enumerate all the information related to target computers.

38. The **Launch a New scan** window appears, by default it will start scanning the local machine. This scan can be stopped by clicking on the **Stop** button or by waiting until the scan is completed.

Custom scans are recommended:

- When performing a onetime scan with particular scanning parameters/profiles
- When performing a scan for particular network threats and/or system information
- To perform a target computer scan using a specific scan profile

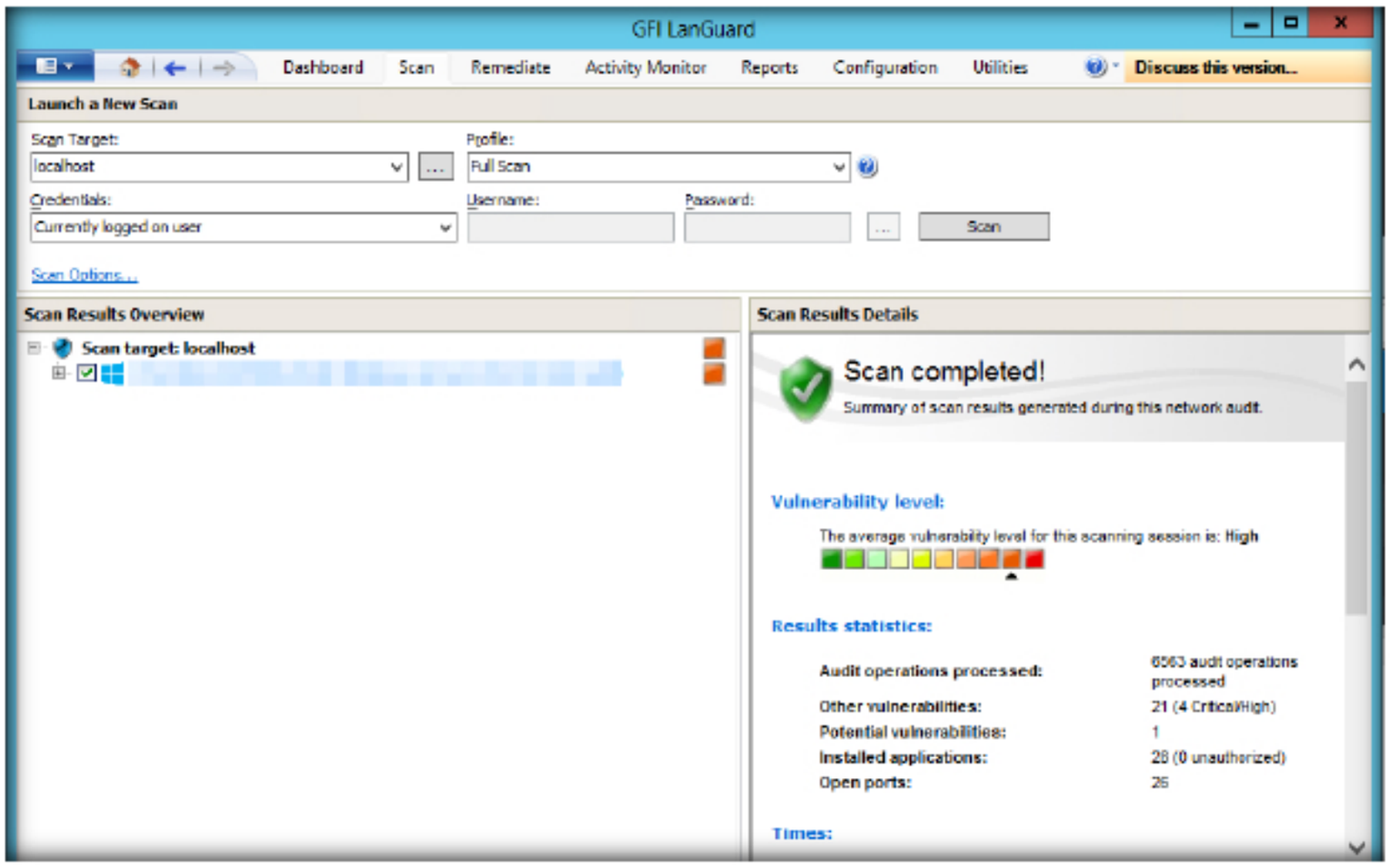


FIGURE 2.30: Launch a new scan window

TASK 4

Scan a Target

39. Enter the IP address of the virtual machine in the **Scan Target** field, select **Full Scan** from the **Profile** drop-down list. Next, select the **Currently logged on user** from the **Credentials** drop-down list then click **Scan**.

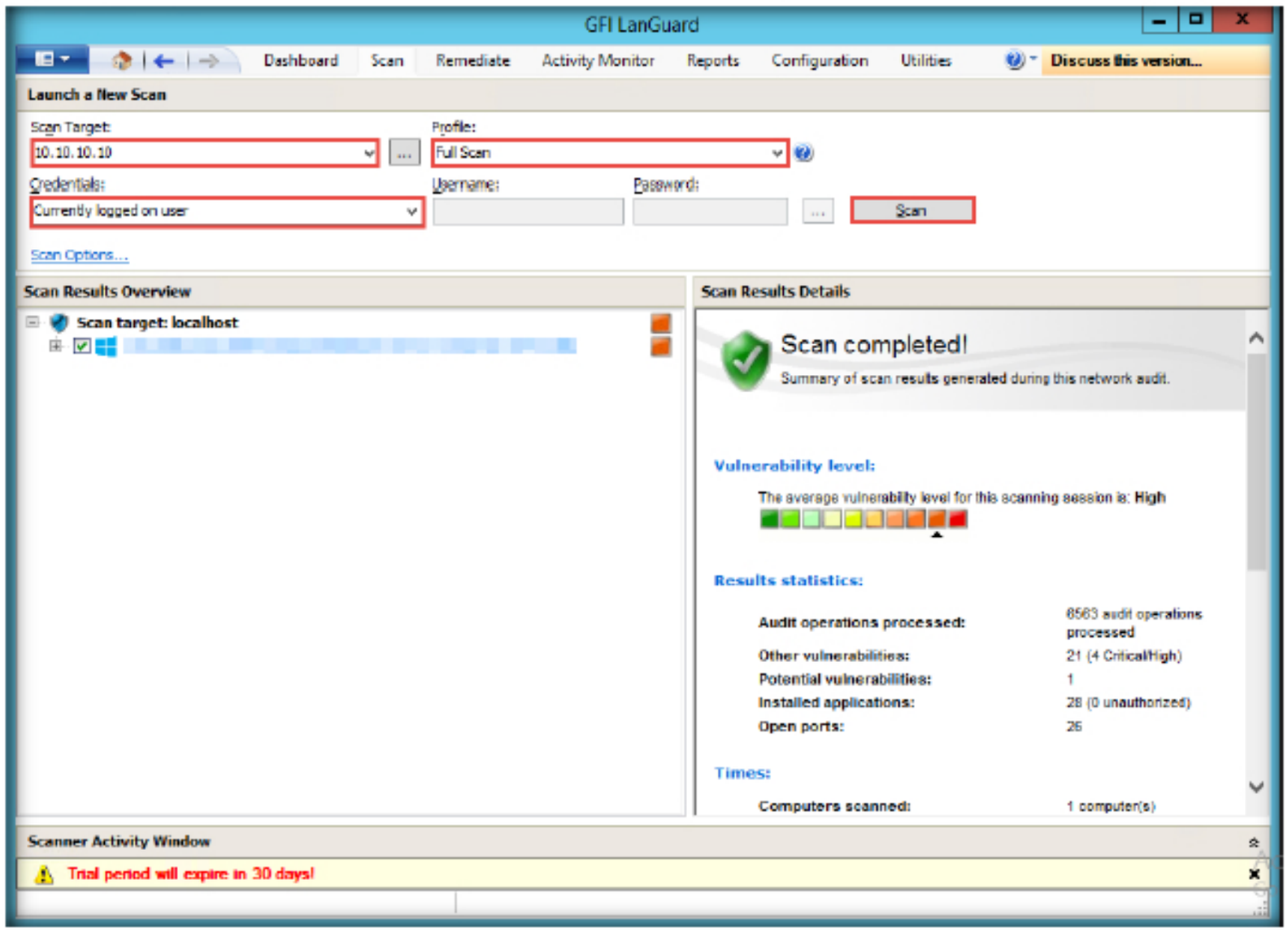


FIGURE 2.31: Customizing the scan settings

Use GFI LanGuard to scan, analyze and remediate the health of your network devices. Install GFI LanGuard on a server within your network.

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

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

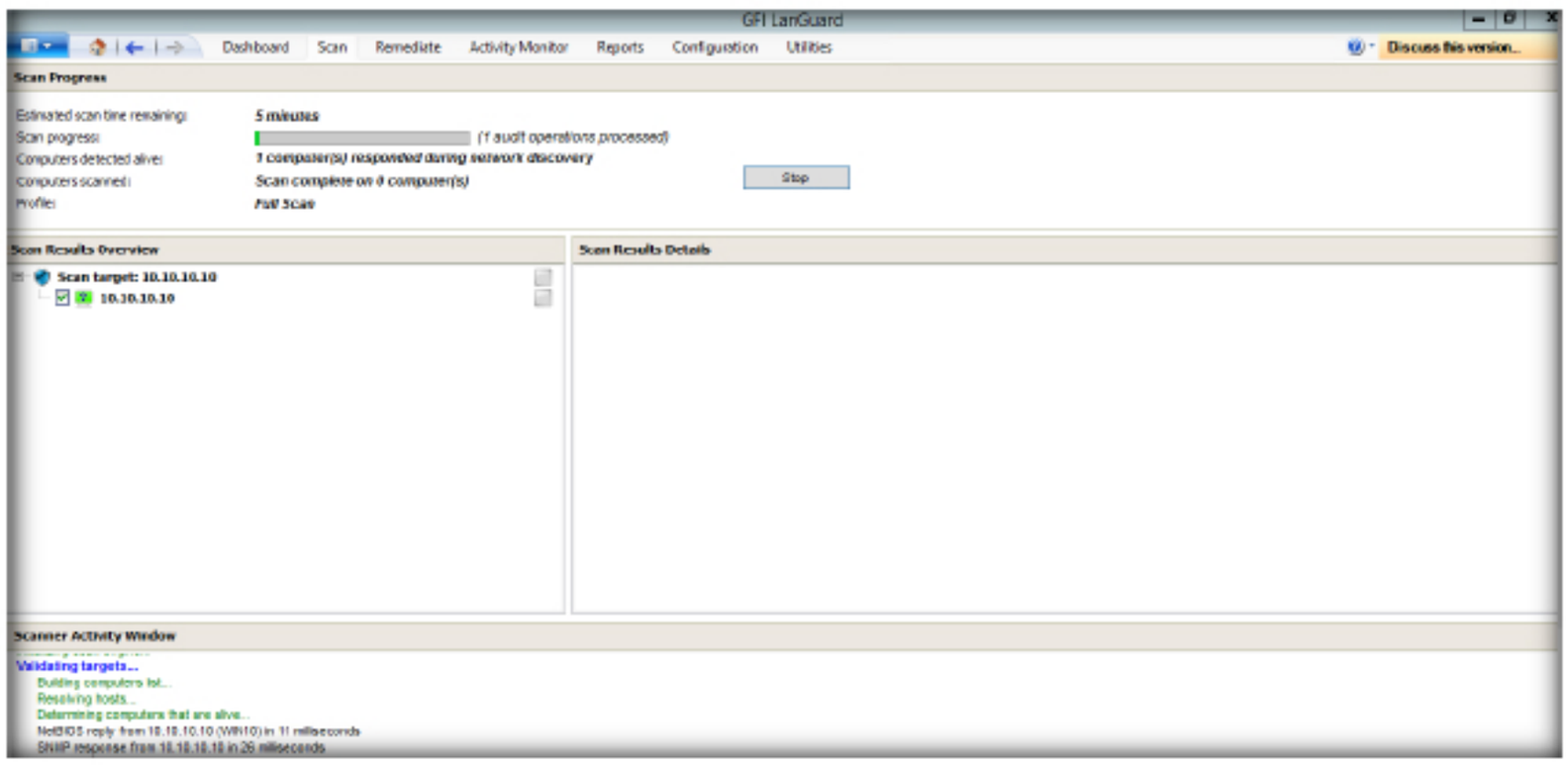


FIGURE 2.32: Vulnerability assessment being performed

During a full scan, GFI LanGuard scans target computers to retrieve the setup information and to identify all security vulnerabilities, including:

Missing Microsoft updates

System software information, including unauthorized applications, incorrect antivirus settings and outdated signatures.

System hardware information, including connected modems and USB devices.

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

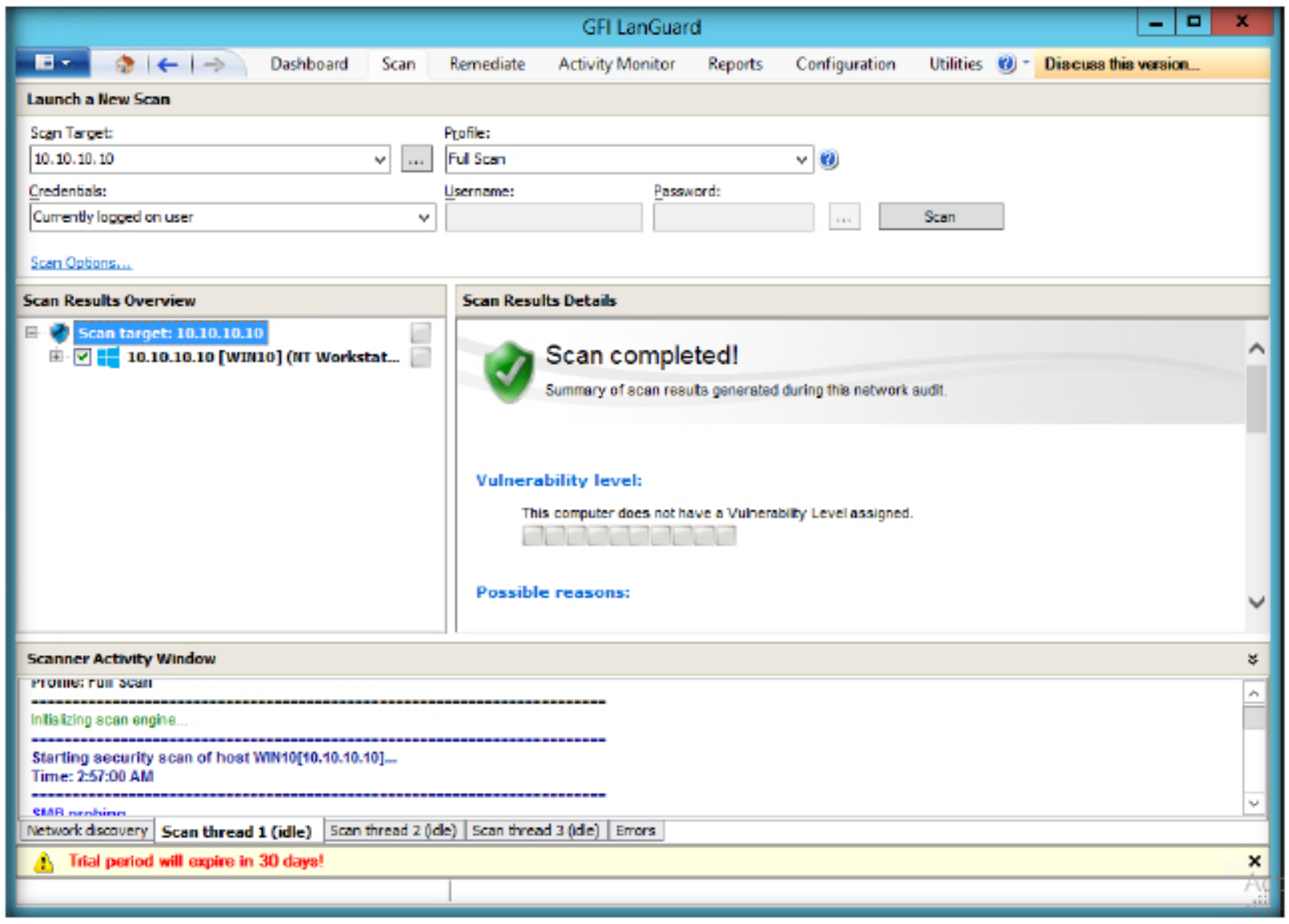


FIGURE 2.33: Scan Results displayed in GFI LanGuard

TASK 5

Examine the Scan Results

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

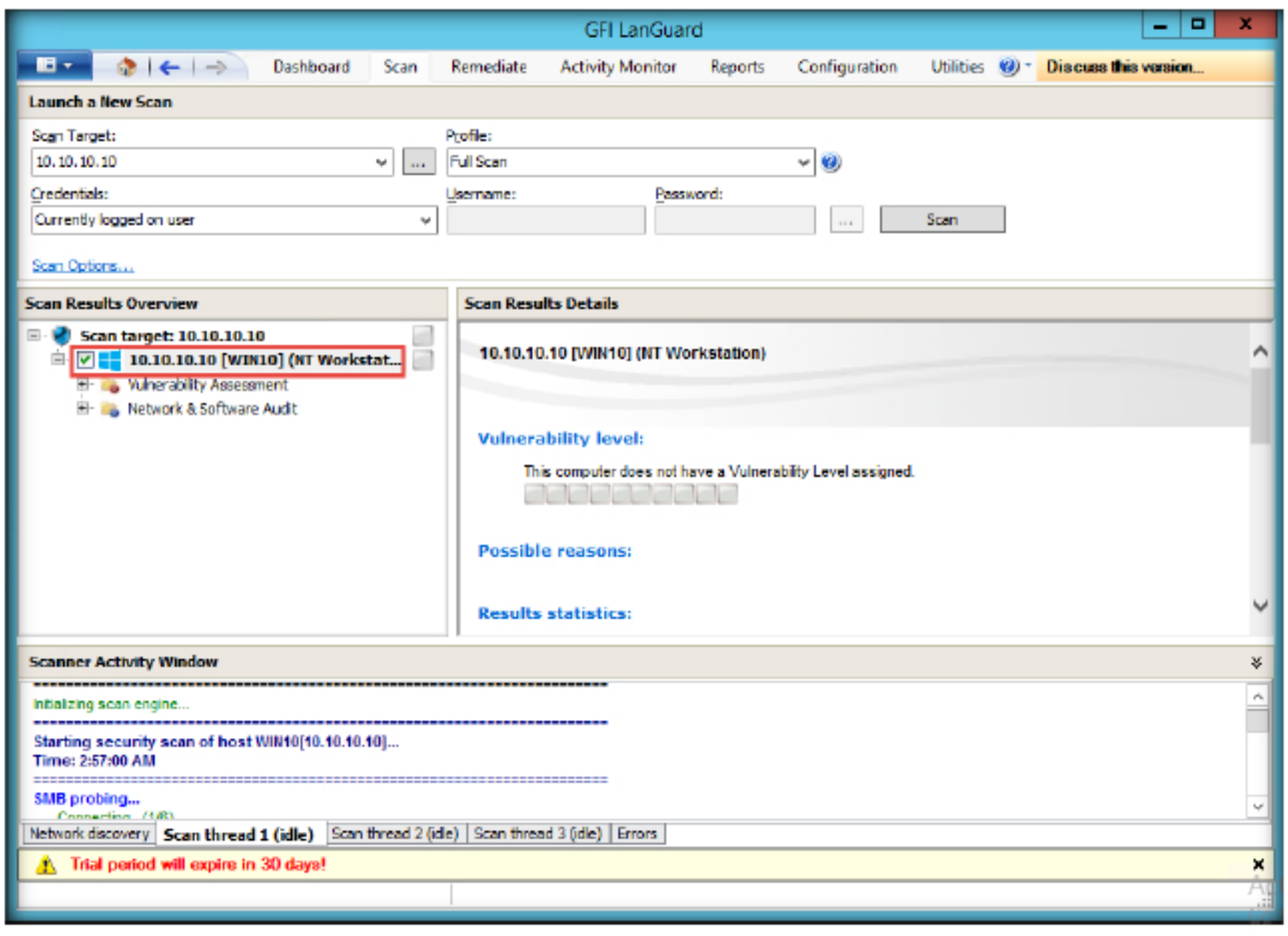


FIGURE 2.34: Viewing the scan results

43. It displays the **Vulnerability Assessment** and the **Network & Software Audit** nodes. Click on **Vulnerability Assessment**.

Note: The results may vary in your lab environment according to the vulnerabilities recorded.

Due to the large amount of information retrieved from scanned targets, full scans often tend to be lengthy. It is recommended to run a full scan at least once every two weeks.

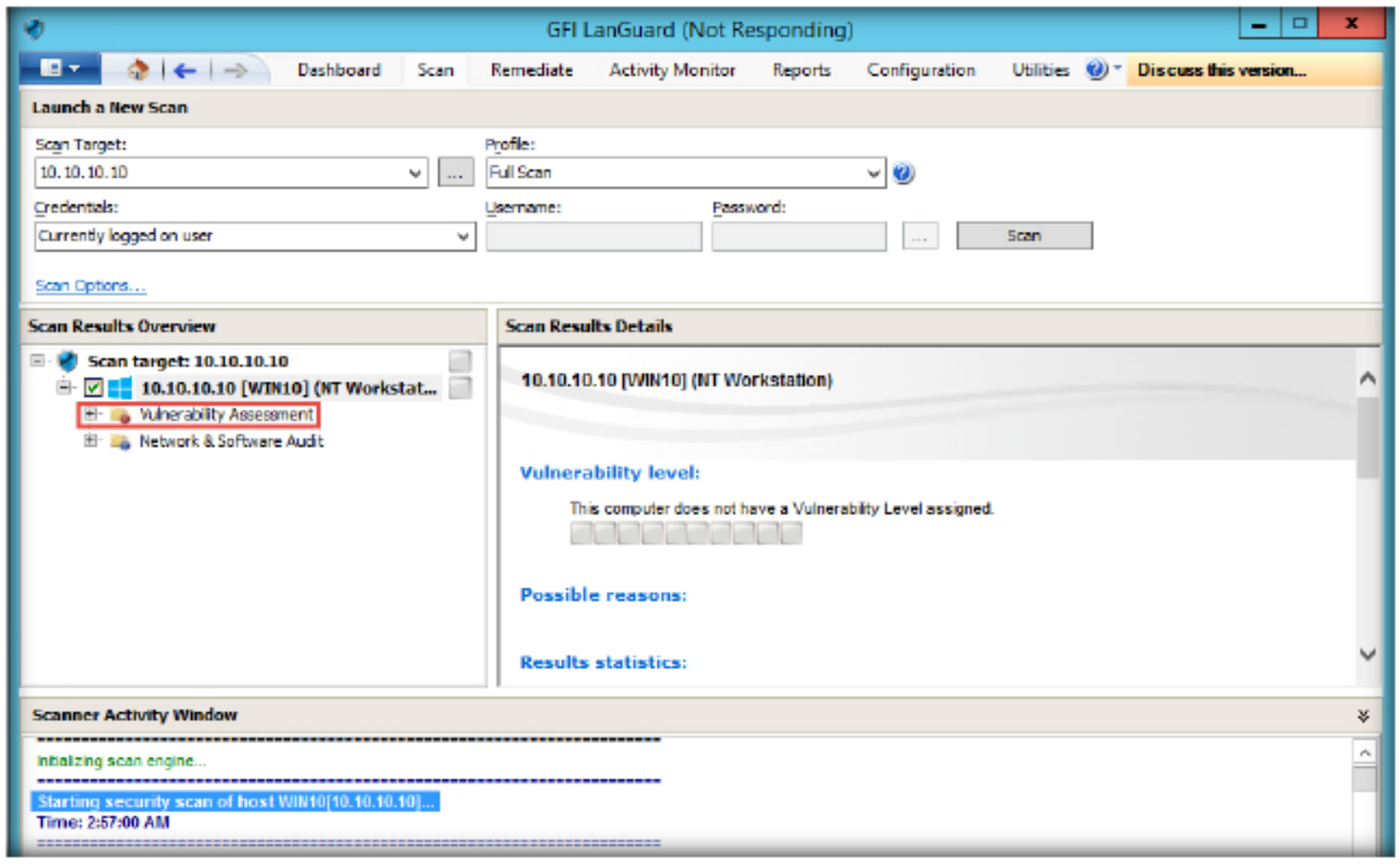


FIGURE 2.35: Viewing the scan results

44. The details of the **Vulnerability Assessment** by category. Click each category to view all the vulnerabilities in the virtual machine.

A scheduled scan is a network audit scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically.

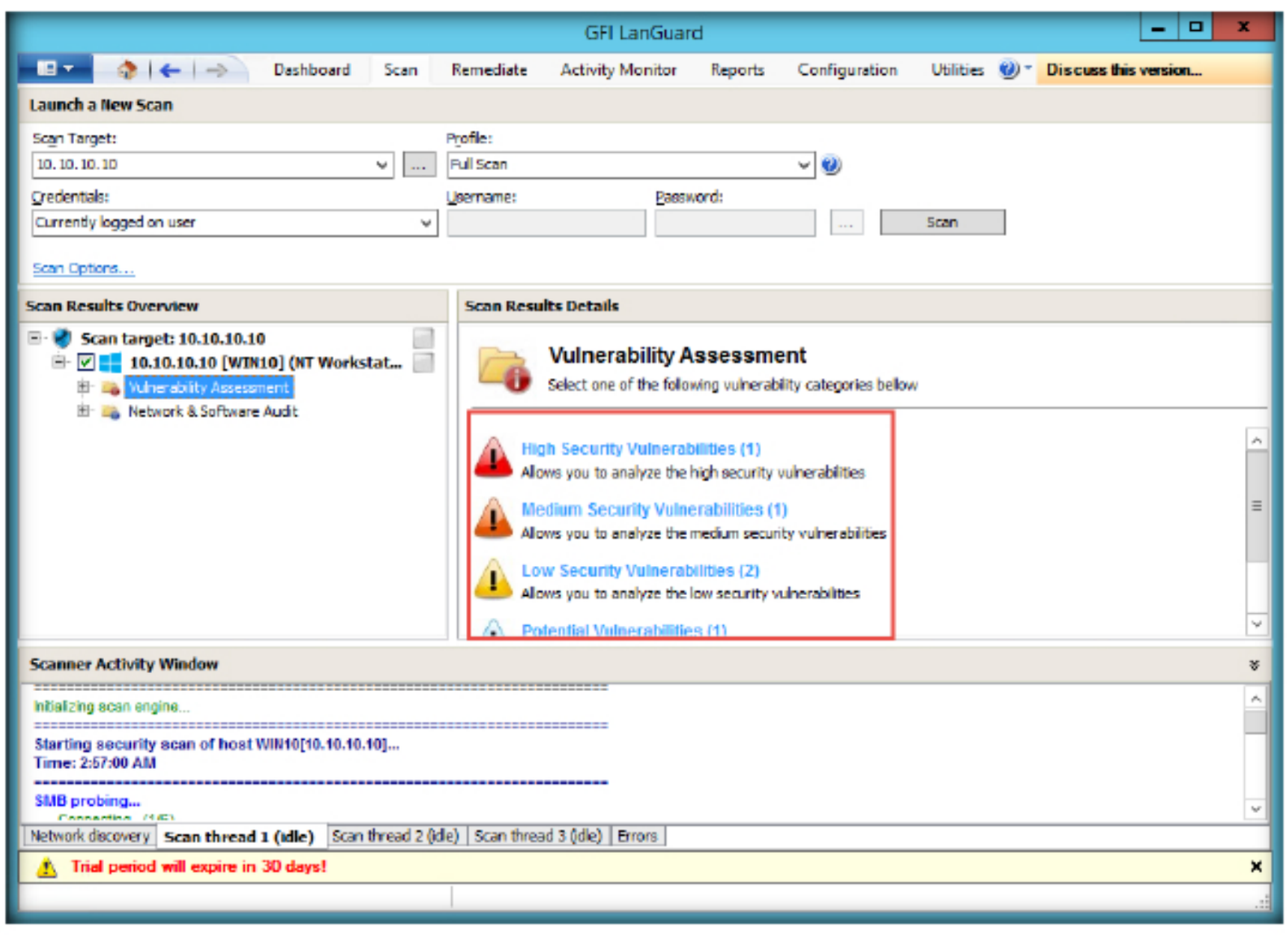


FIGURE 2.36: Vulnerability Assessment categories

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

Following a network security scan, the next job is to identify which areas and systems require your immediate attention. Do this by analyzing and correctly interpreting the information collected and generated during the security scan.

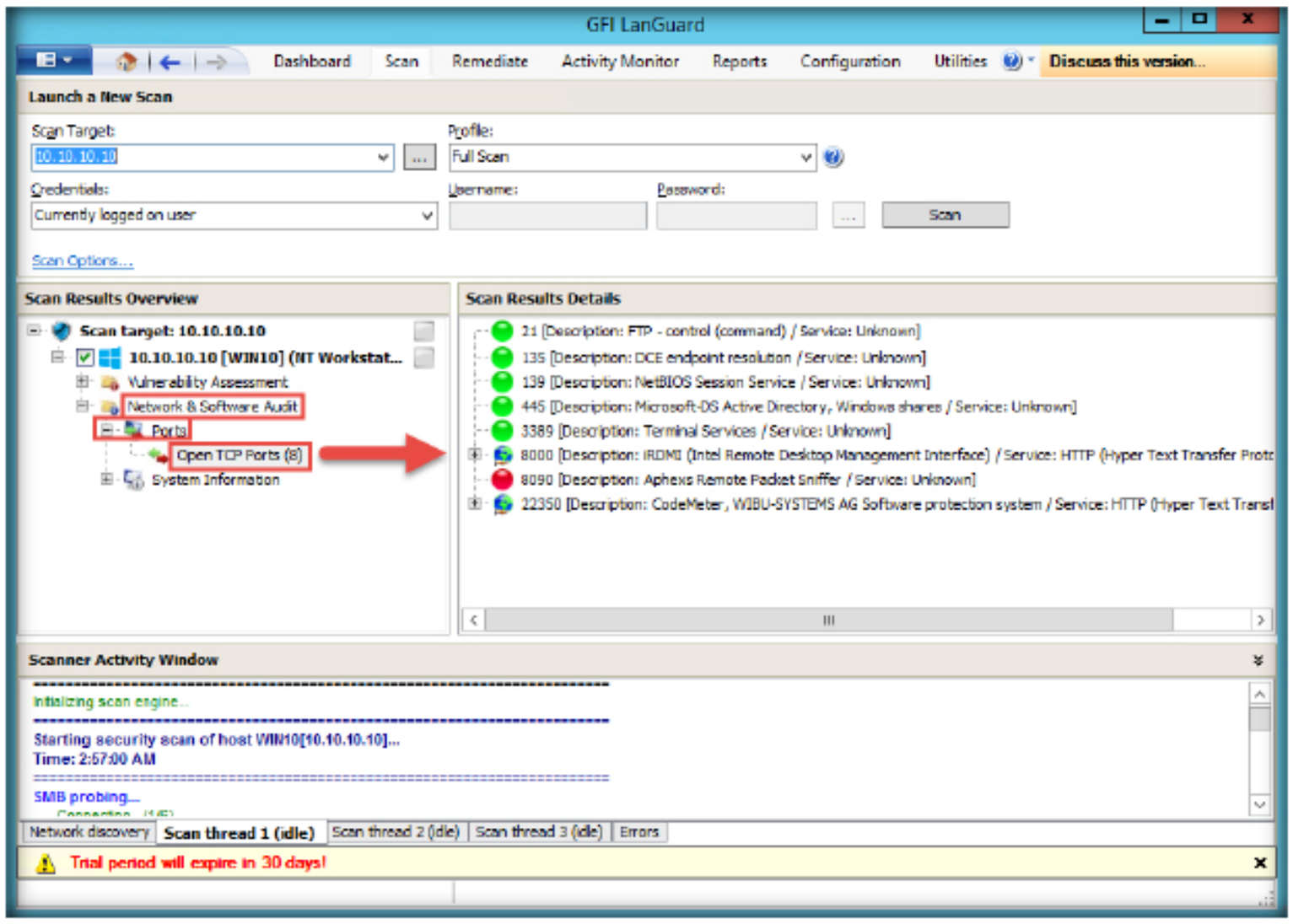


FIGURE 2.37: Scan results for open TCP Ports

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

47. Click the **NETBIOS names** to view the name and description of all the systems in the network.

A high vulnerability level is the result of vulnerabilities or missing patches whose average severity is categorized as "high."

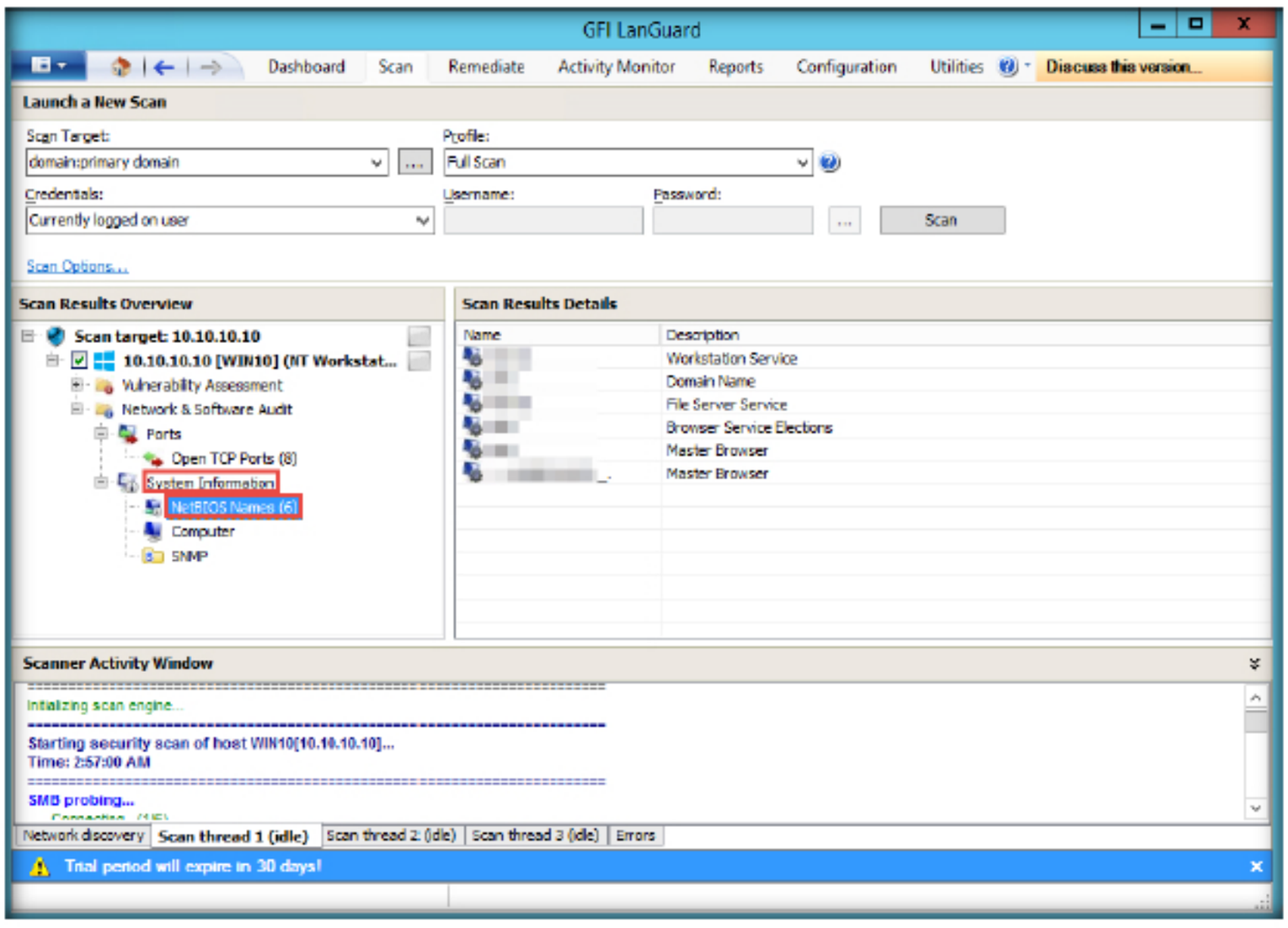


FIGURE 2.38: Viewing the NETBIOS names

48. Click the **Computer** tab to view various details about the target machine.

It is recommended to use scheduled scans:

- To perform periodical/regular network vulnerability scans automatically and using the same scanning profiles and parameters
- To trigger scans automatically after office hours and to generate alerts and auto-distribution of scan results via email
- To automatically trigger auto-remediation options, (e.g., Auto download and deploy missing updates)

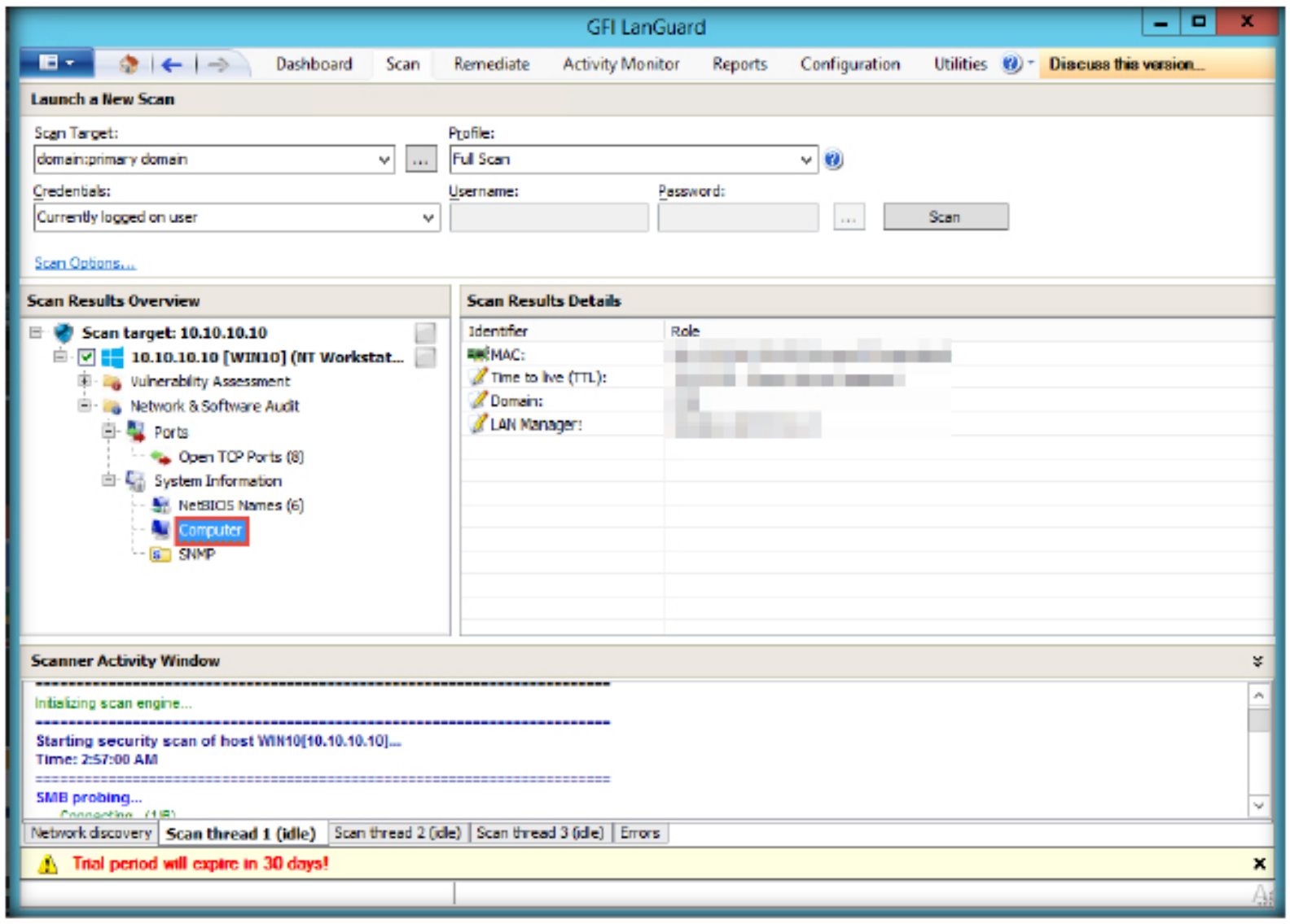


FIGURE 2.39: Viewing Computer results

49. Click on **SNMP** to view the SNMP details of the target system.

GFI LanGuard includes a reporting module which enables you to generate text and graphical reports based on information obtained from network security scans. This topic provides you with an overview of the available reports as well as how to create your own reports for a tailored solution. Through the Reports tab, you are able to generate technical activity reports for IT staff and also executive reports that normally contain less technical details and focus more on overall statistics.

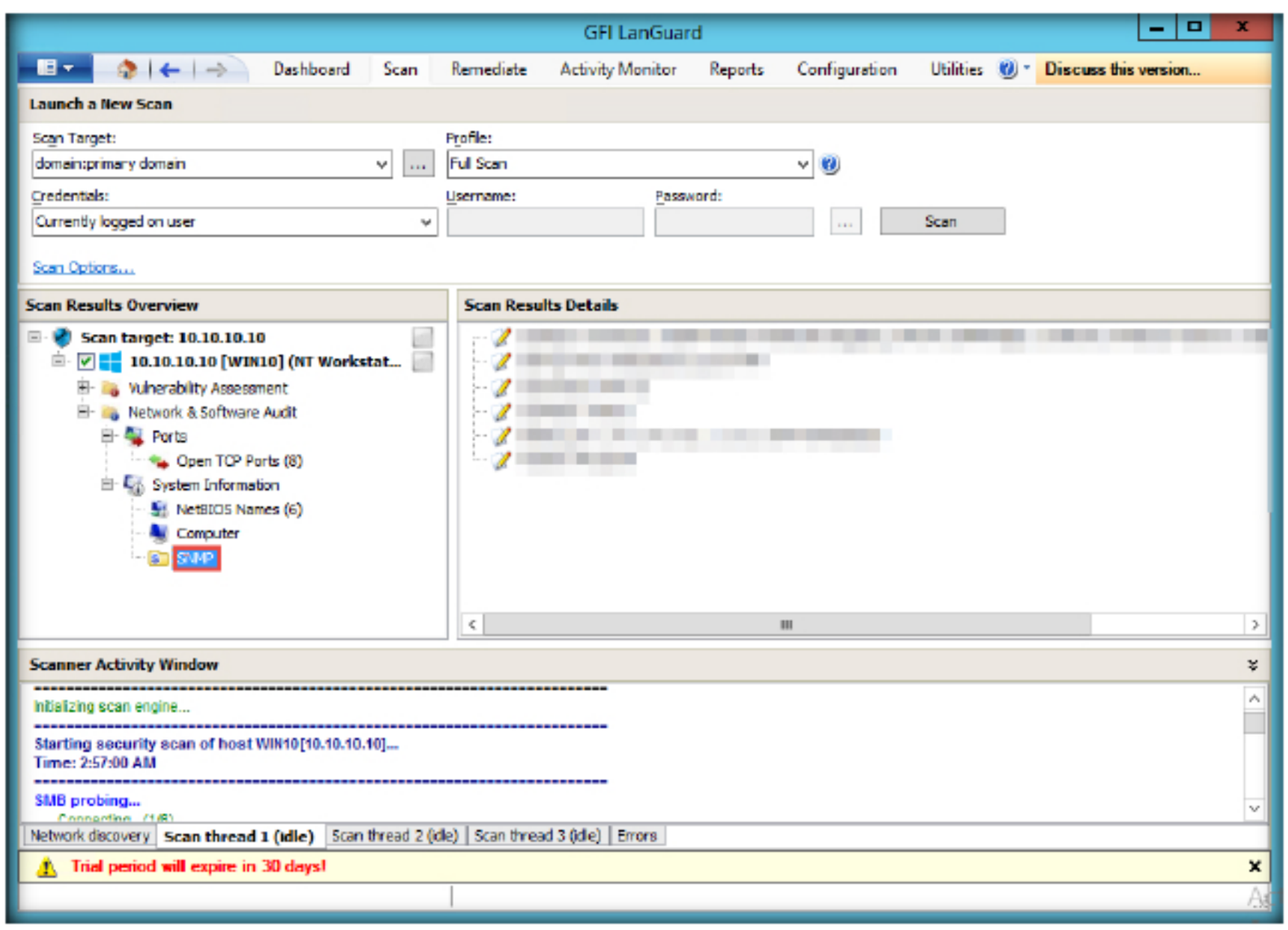


FIGURE 2.40: Viewing SNMP results

50. Click the **Dashboard** tab to display all the scanned network information.

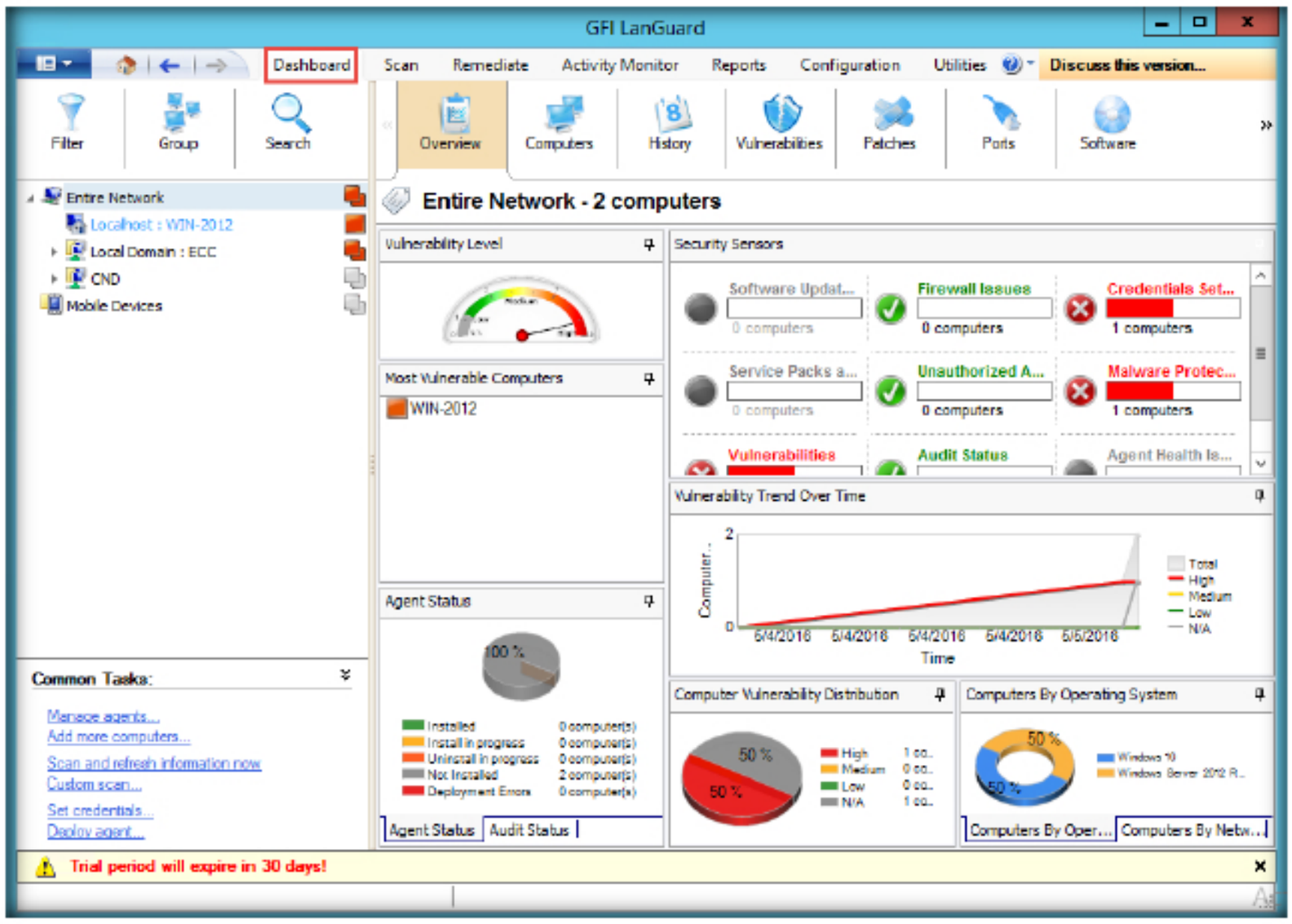


FIGURE 2.41: Overview of the Scan in Dashboard

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

Auditing the Network Security with Nsauditor

Nsauditor Network Security Auditor is used to scan networks and hosts for vulnerabilities, and to provide security alerts.

Lab Scenario

Network auditing is an important task of any network security operation where an administrator ensures their network security by conducting various checks against the network. As a network administrator, you should be able audit your network to find security loopholes.

ICON KEY
Valuable information
Test your knowledge
Web exercise
Workbook review

Lab Objectives

This lab will demonstrate how to audit your network using Nsauditor.

Lab Environment

To carry out the lab, you need:

- Nsauditor, located at **D:\CND-Tools\CND Module 12 Network Risk and Vulnerability Management\Vulnerability Assessment Tools\Nsauditor Network Security Auditor**
- A virtual machine running Windows Server 2012
- A virtual machine running Windows 10
- A Web browser with an Internet connection
- **Administrative** privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Nsauditor

Nsauditor will check the network for all potential methods a hacker will use to attack it and then create a report of any potential problems found. Nsauditor provides insight into the services running locally, with additional options to dig down into each connection and analyze the remote system, terminate connections and view data.

Lab Tasks

TASK 1

Launching Nsauditor

1. Launch **Windows Server 2012**
2. Navigate to **D:\CND-Tools\CND Module 12 Network Risk and Vulnerability Management\Vulnerability Assessment Tools\Nsauditor Network Security Auditor** then double click **nsauditor_setup.exe** to start the installation.
3. The **Open File – Security Warning** window appears. Click **Run**.

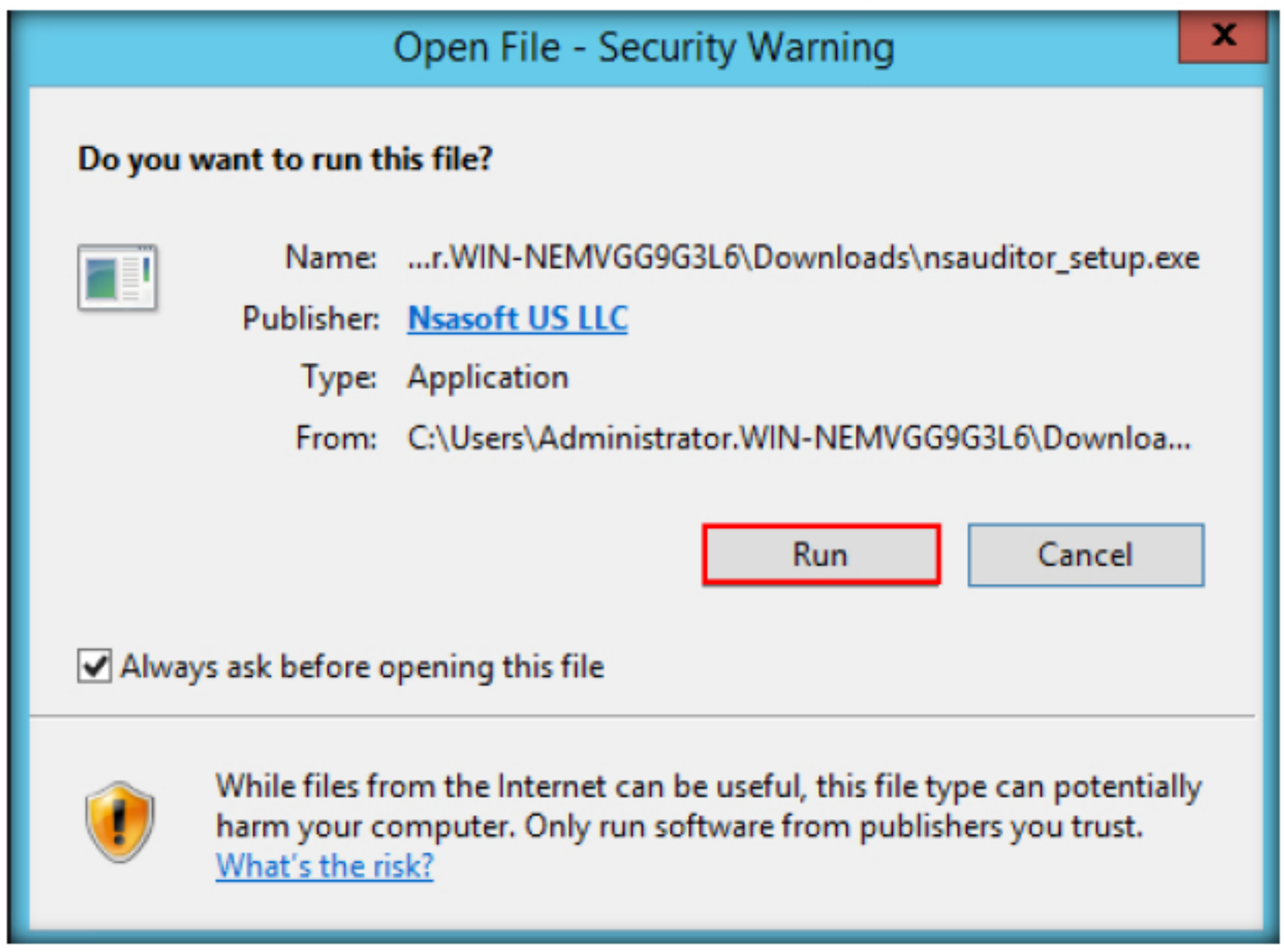


FIGURE 3.1: Windows security warning file

4. Follow the onscreen instructions and complete the installation of **Nsauditor**.

5. Click the **Start** button and navigate to **Apps** and click **Nsauditor** to launch it.

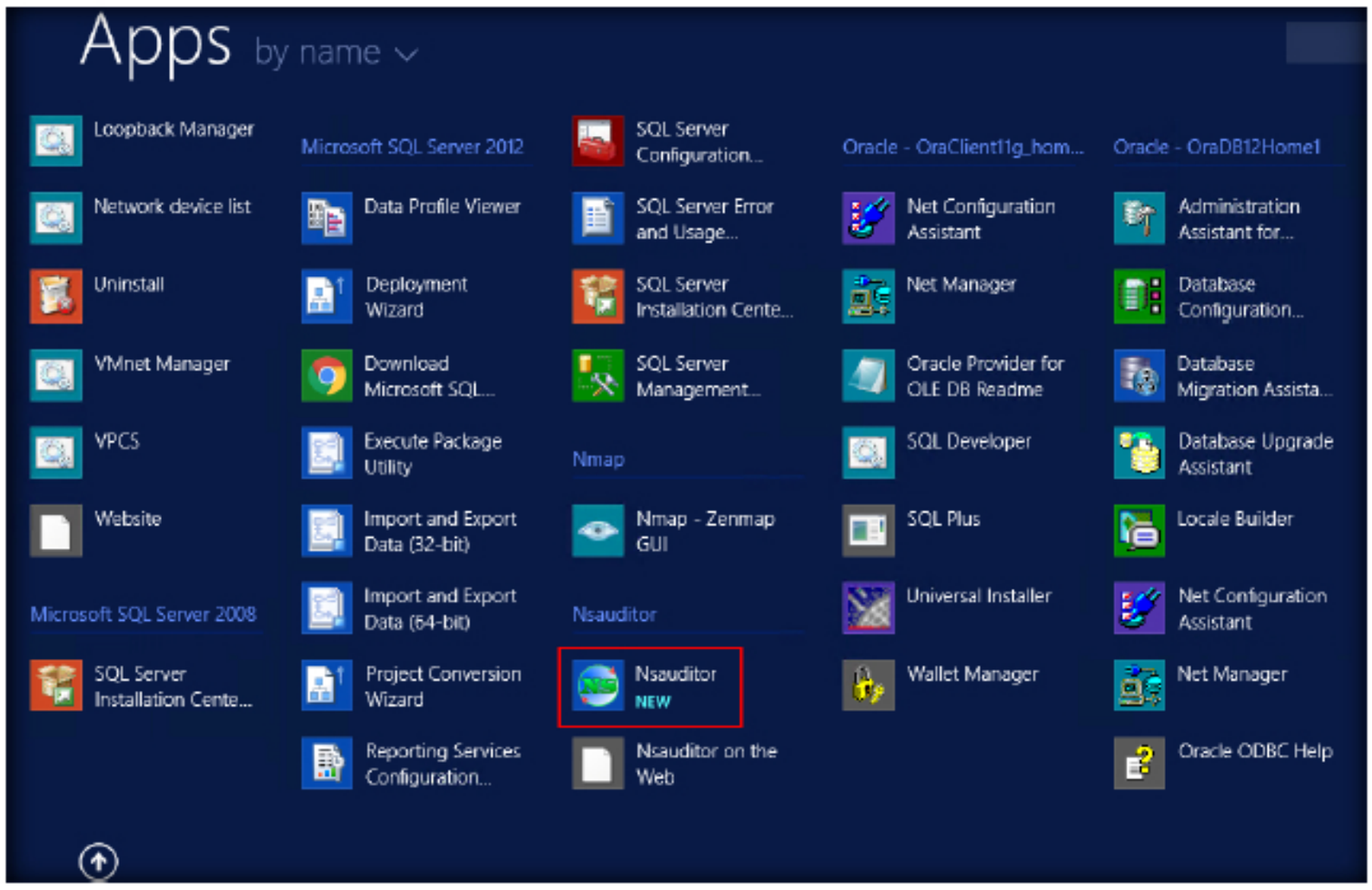


FIGURE 3.2: Launching Nsauditor

6. The **Nsauditor** main window will appear as shown in the following screenshot.

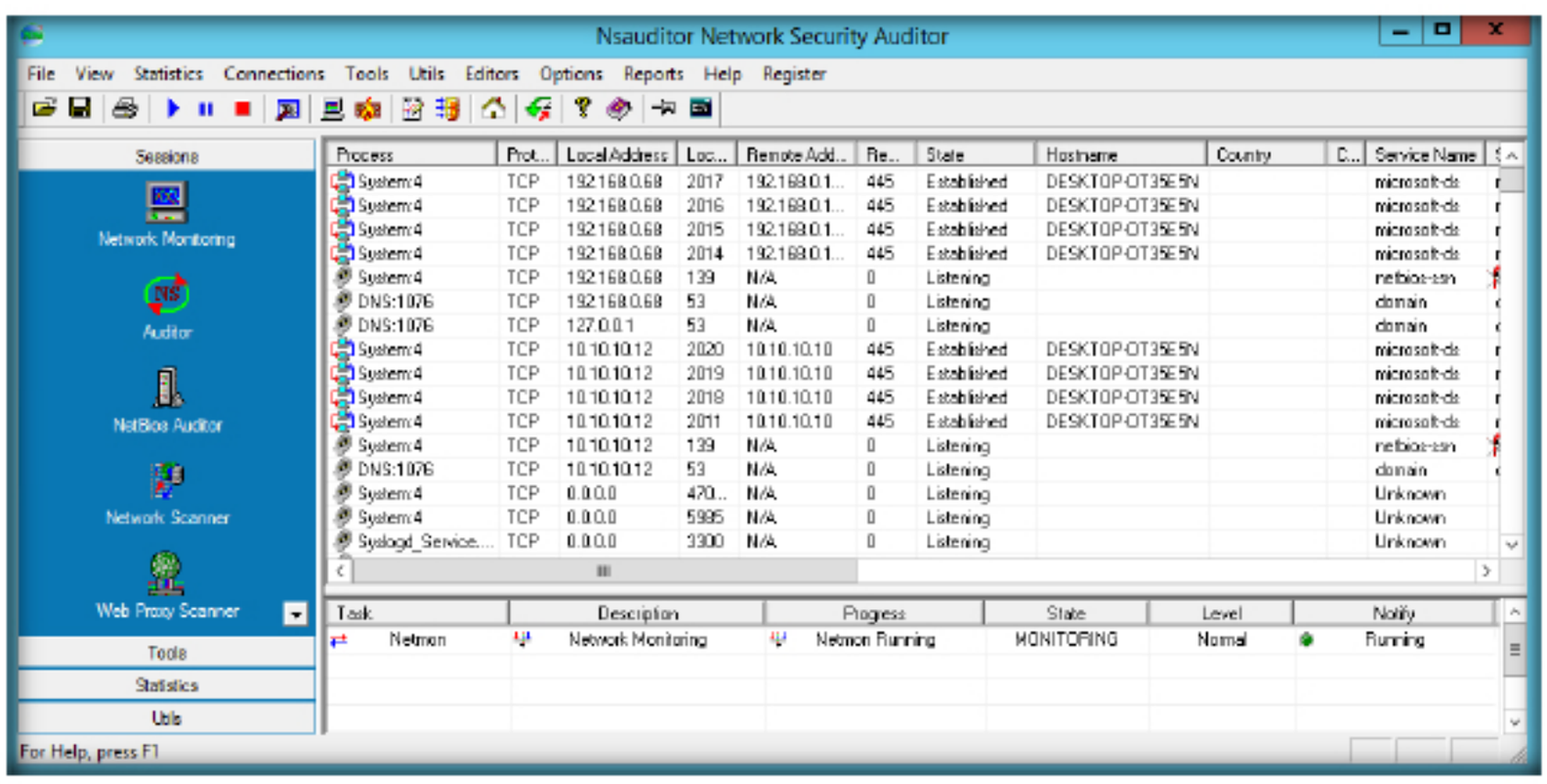


FIGURE 3.3: Nsauditor GUI

TASK 2

Turn On User Machine

7. Launch the **Windows 10** user machine and login as a local administrator.

(**Note**: You need to turn off the firewall on the user machine before auditing it with Nsauditor.)

8. Navigate to the Control Panel and click **System and Security**.

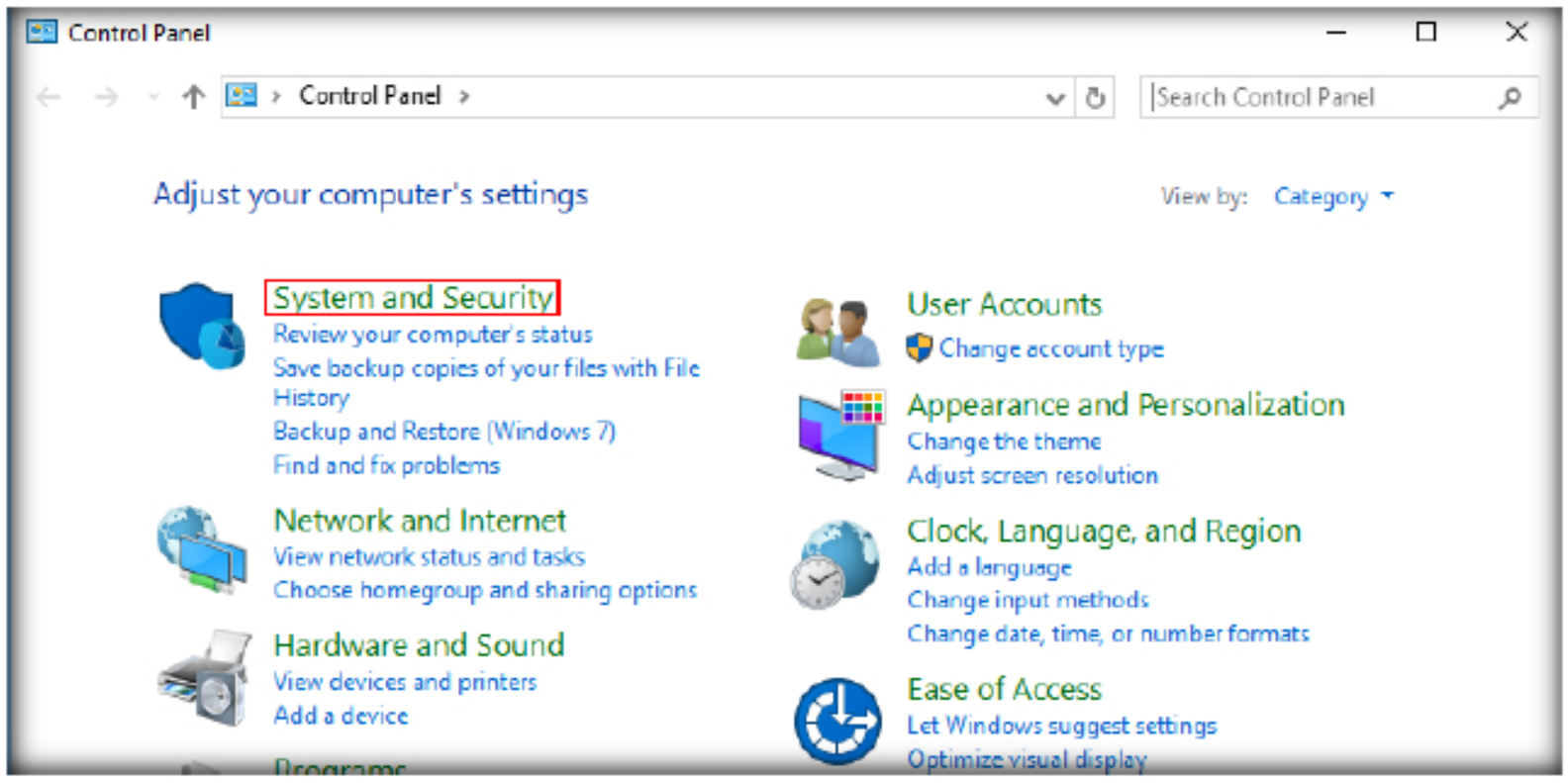


FIGURE 3.4: Navigating to System and Security

9. The **System and Security** window appears. Click on the **Windows Firewall**.

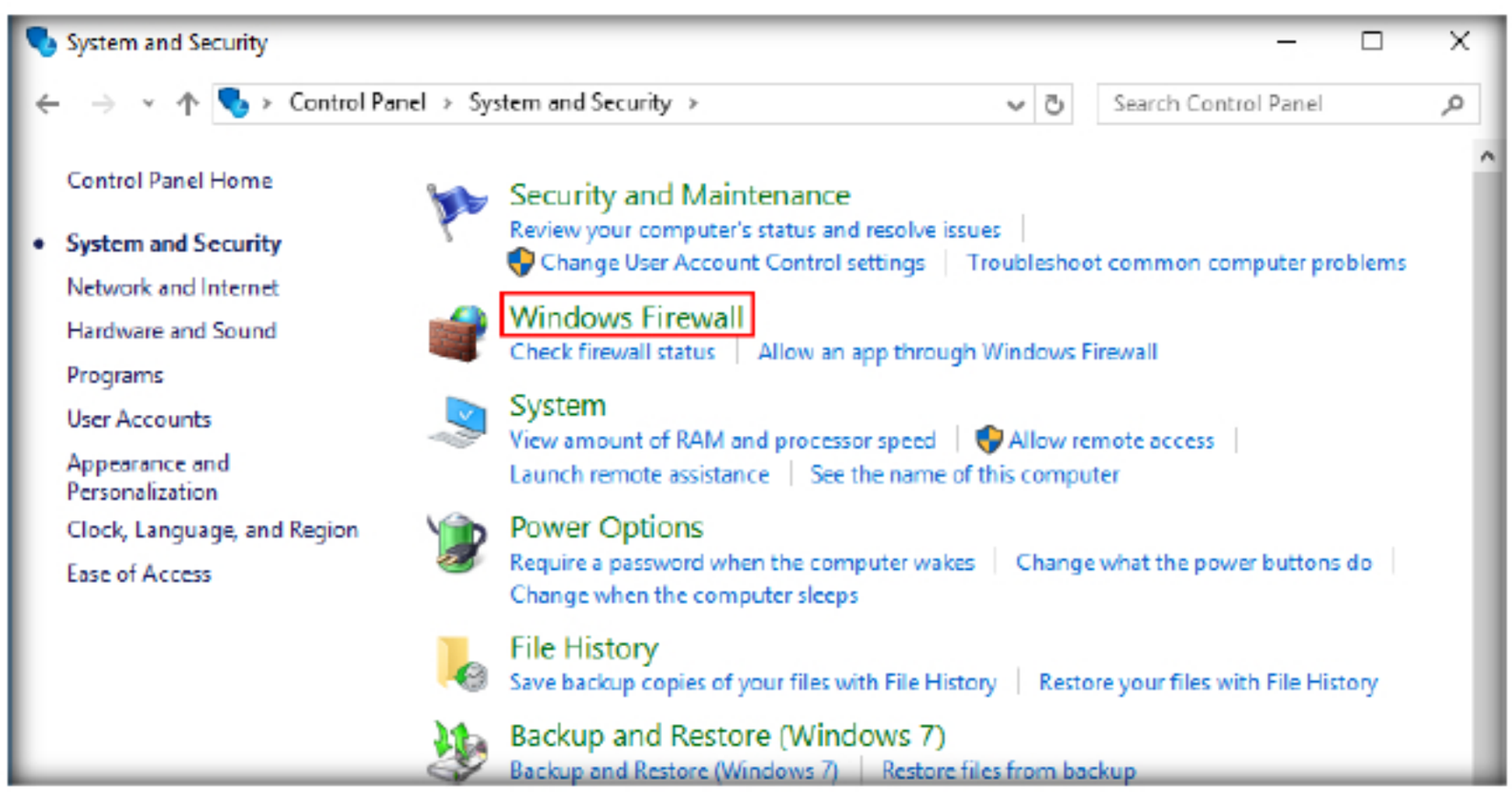


FIGURE 3.5: Navigating to Firewall

10. The **Windows Firewall** appears. Click on **Turn Windows Firewall on or off** on the left side of the page.

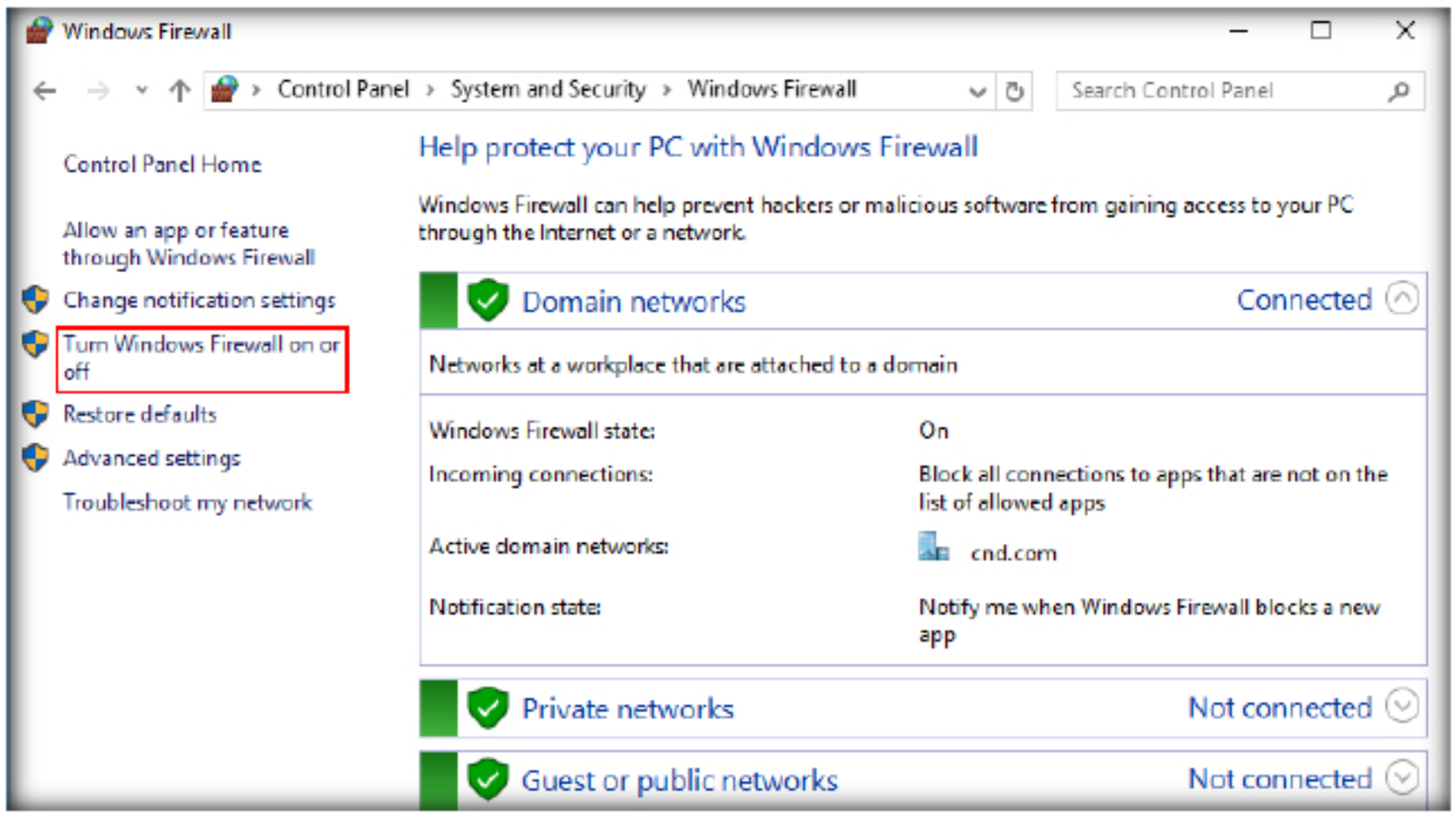


FIGURE 3.6: Windows Firewall

11. The **Customize Settings** window appears. Click on the **Turn Off Windows Firewall** radio buttons for **Domain**, **Private** and **Public** networks then click **OK**.

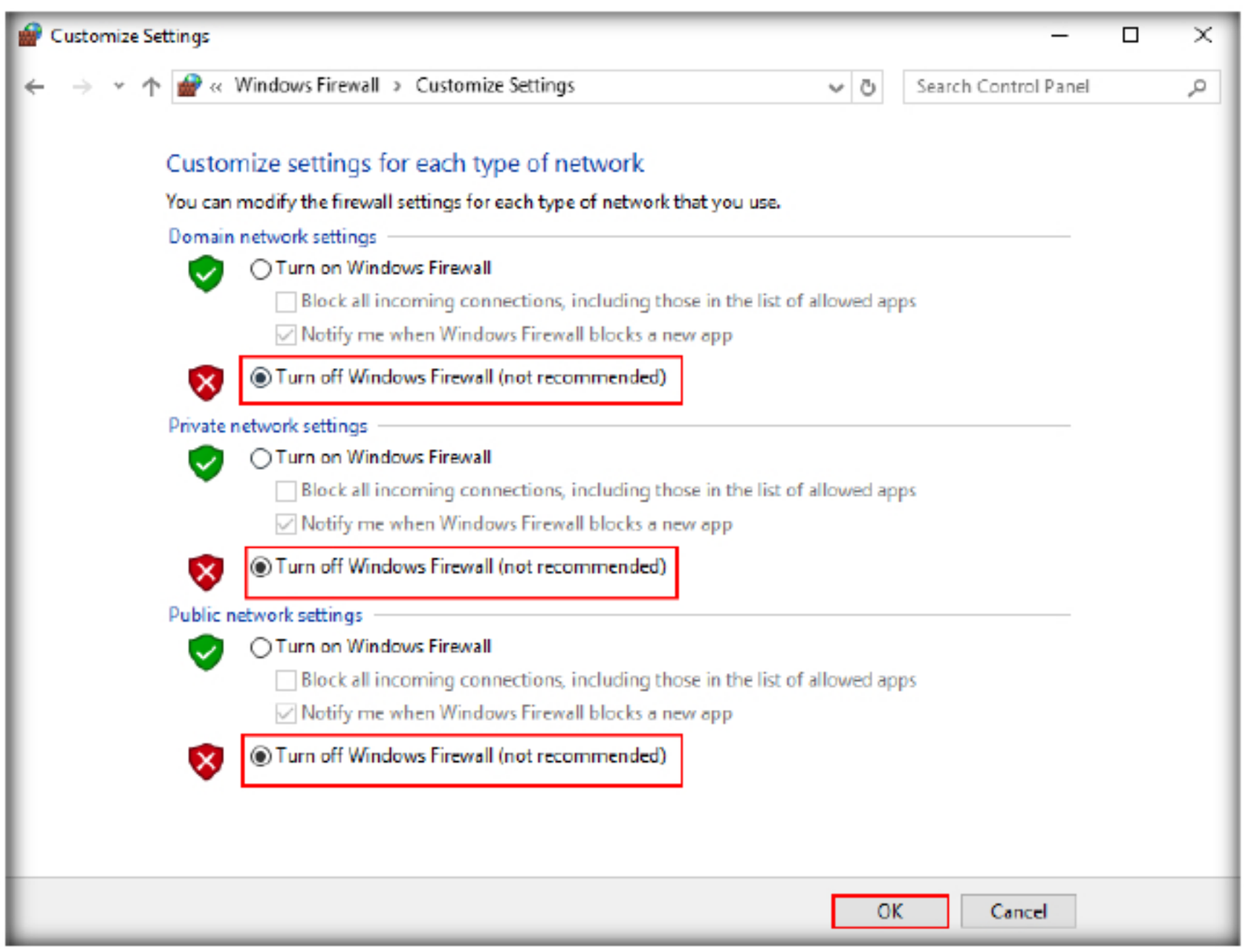


FIGURE 3.7: Windows

TASK 3

Specify the IP address or IP range of user machines and start auditing

12. Switch back to **Windows Server 2012** and go to the **Nsauditor** window. Click **Auditor** in the left pane.

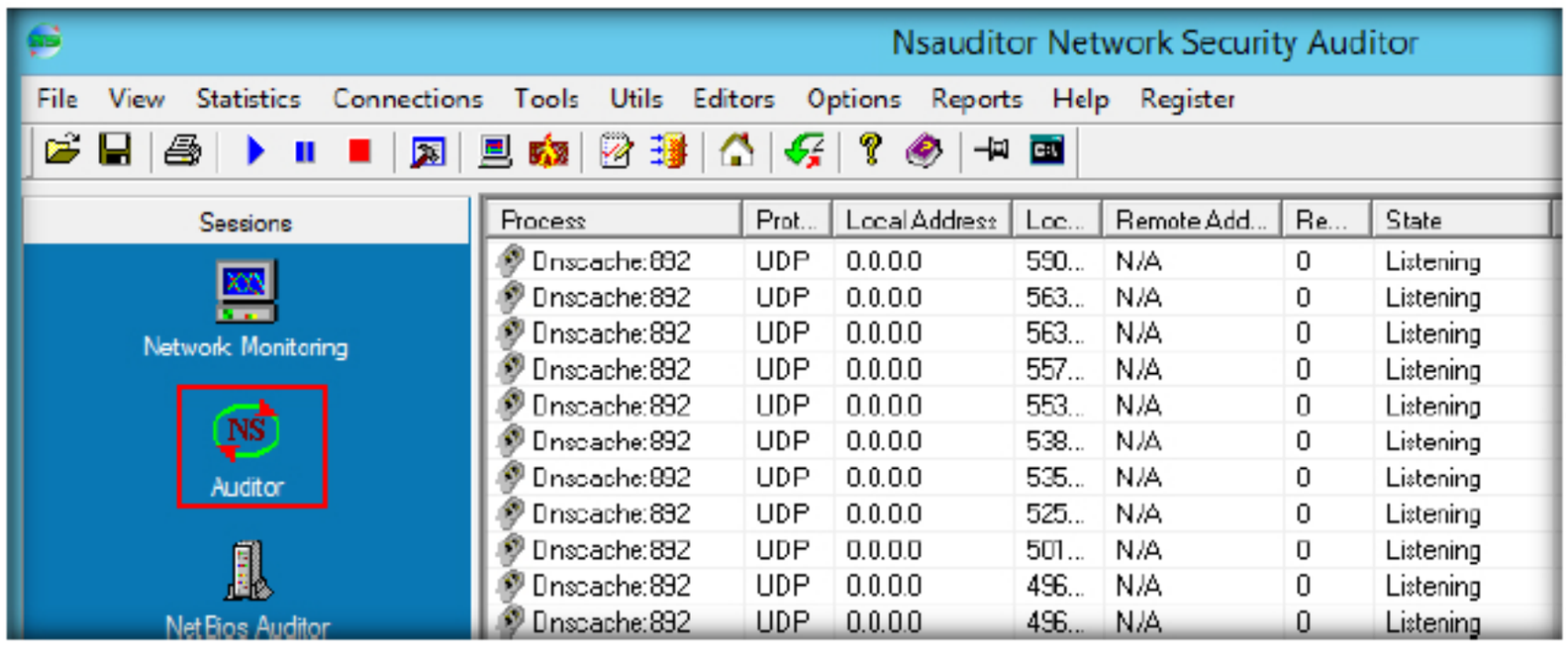


FIGURE 3.8: Starting the auditor

13. The **Host Range and Credentials Selection Dialog** window appears. Enter the IP address of the Windows 10 machine in the **Host Name / Address:** field, click the **Other Credentials** radio button and enter the credentials of the Windows 10 Local Administrator (username: Local-Administrator and password: test@123) then click **OK**.

Note: If you want to audit multiple hosts in the network, enter a range of IP addresses by specifying the Start and End in the IP range option.

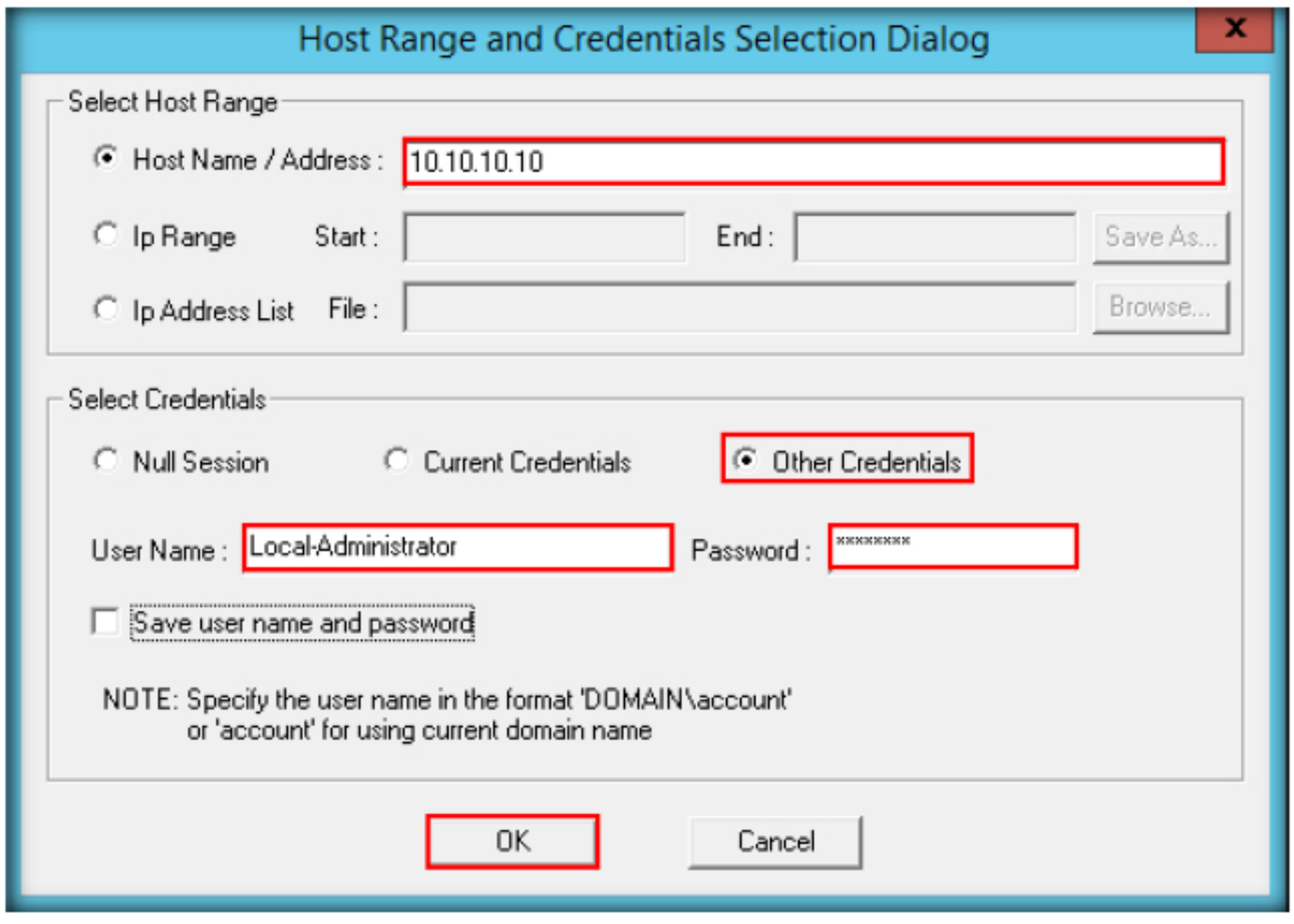


FIGURE 3.9: Target system details

14. The **Network Audit Dialog** window appears. Click **Start Audit**.

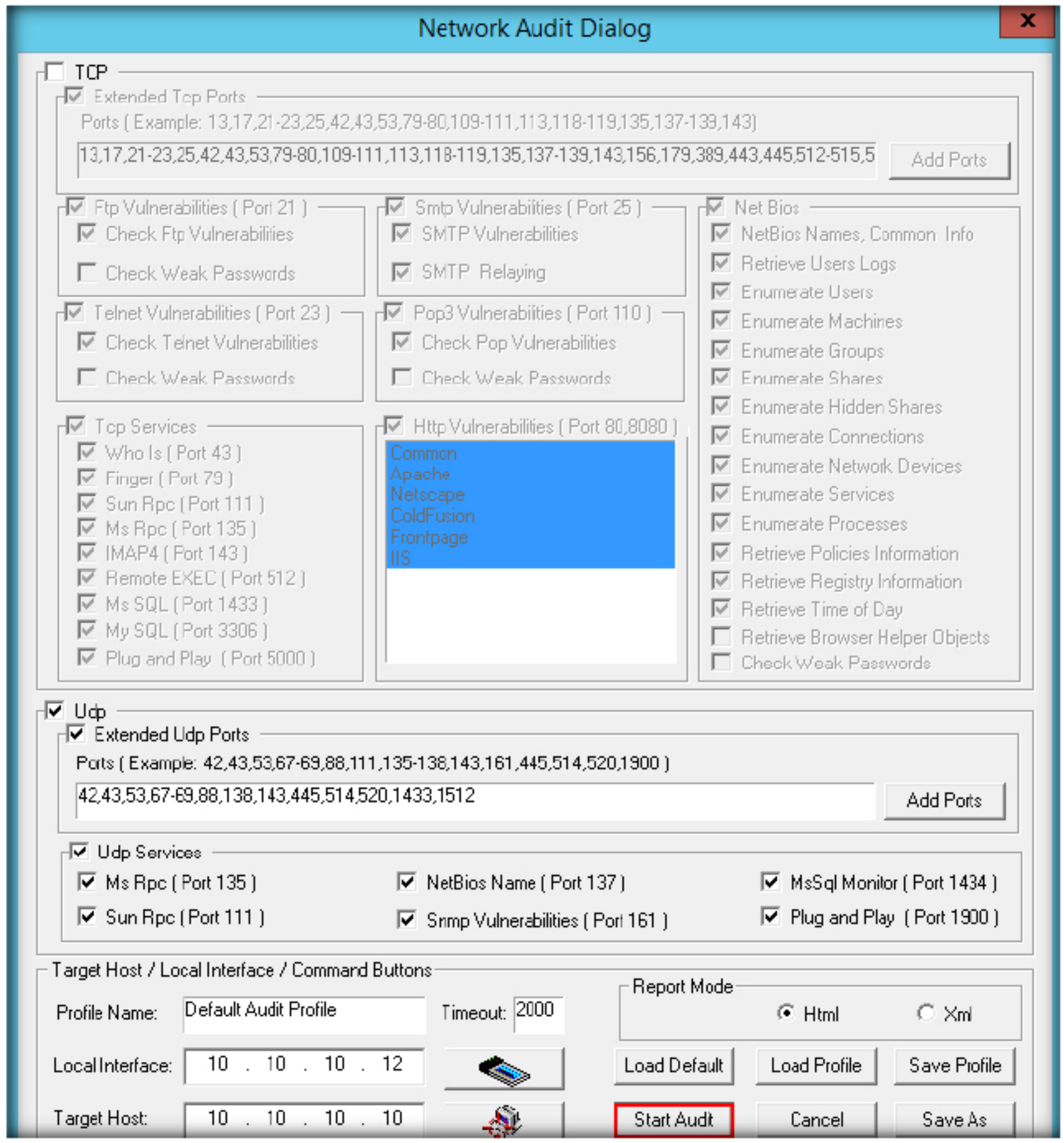


FIGURE 3.10: Starting the Audit

15. The **Nsauditor Network Security Auditor** window appears. Click **OK**.

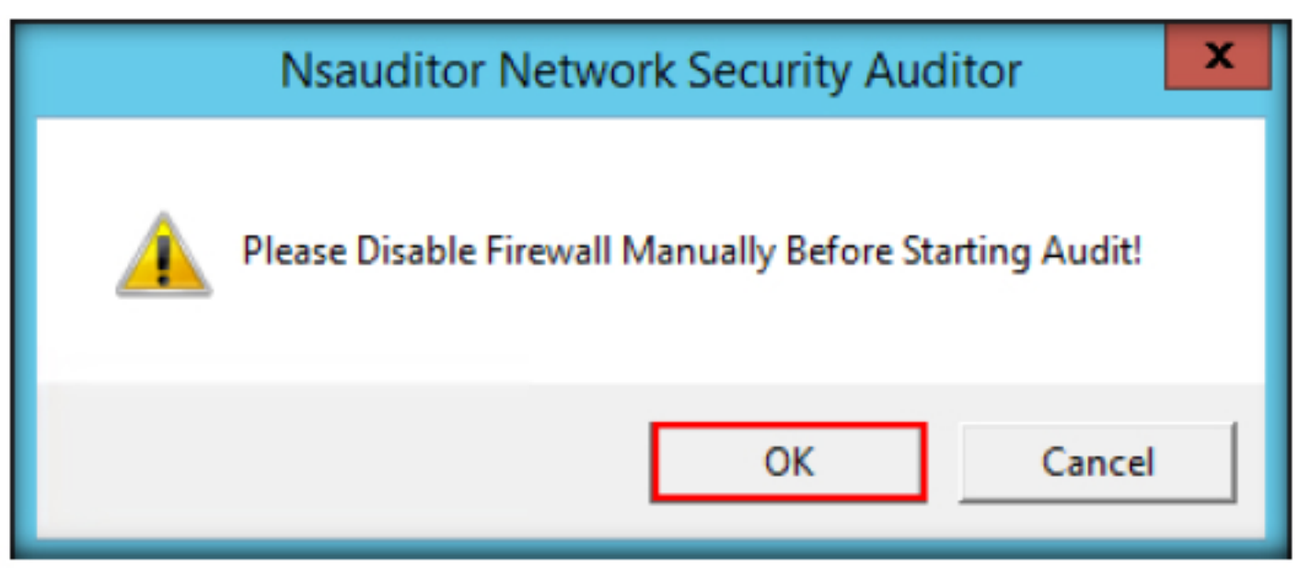
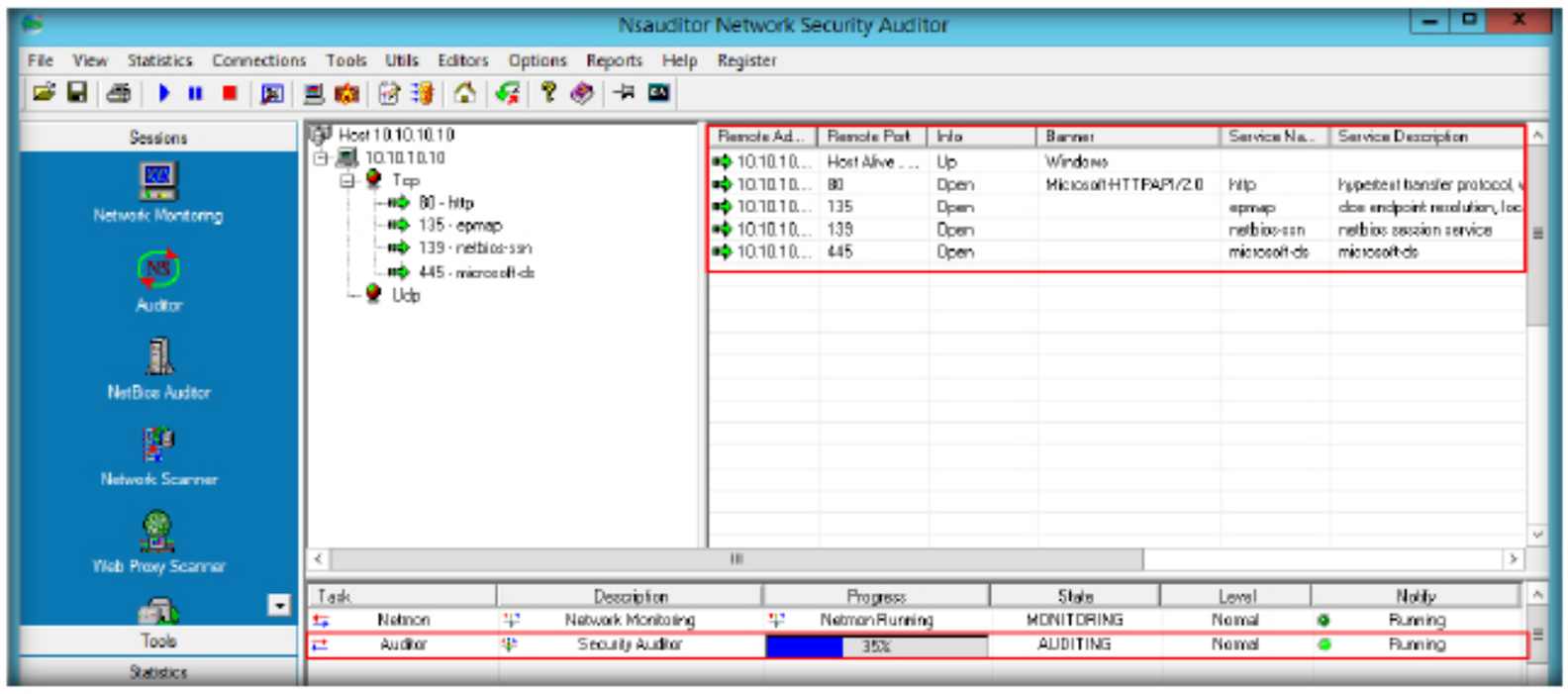


FIGURE 3.11: Firewall disable message

16. System auditing will start. Once the audit is completed, you can see the **Finished** status.



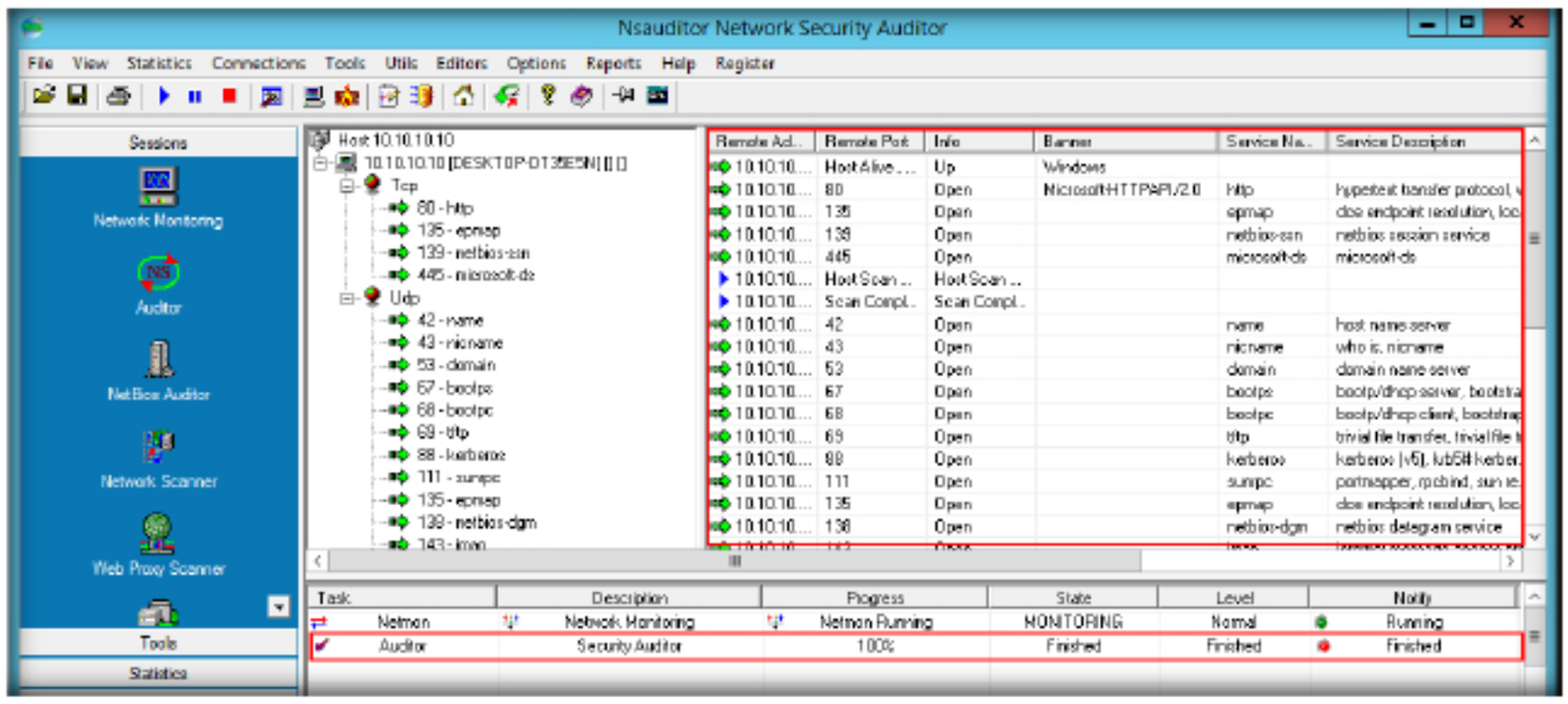


FIGURE 3.12: Auditing coimpleted

17. Click the **Audit Reports list** icon to view the complete audit report.

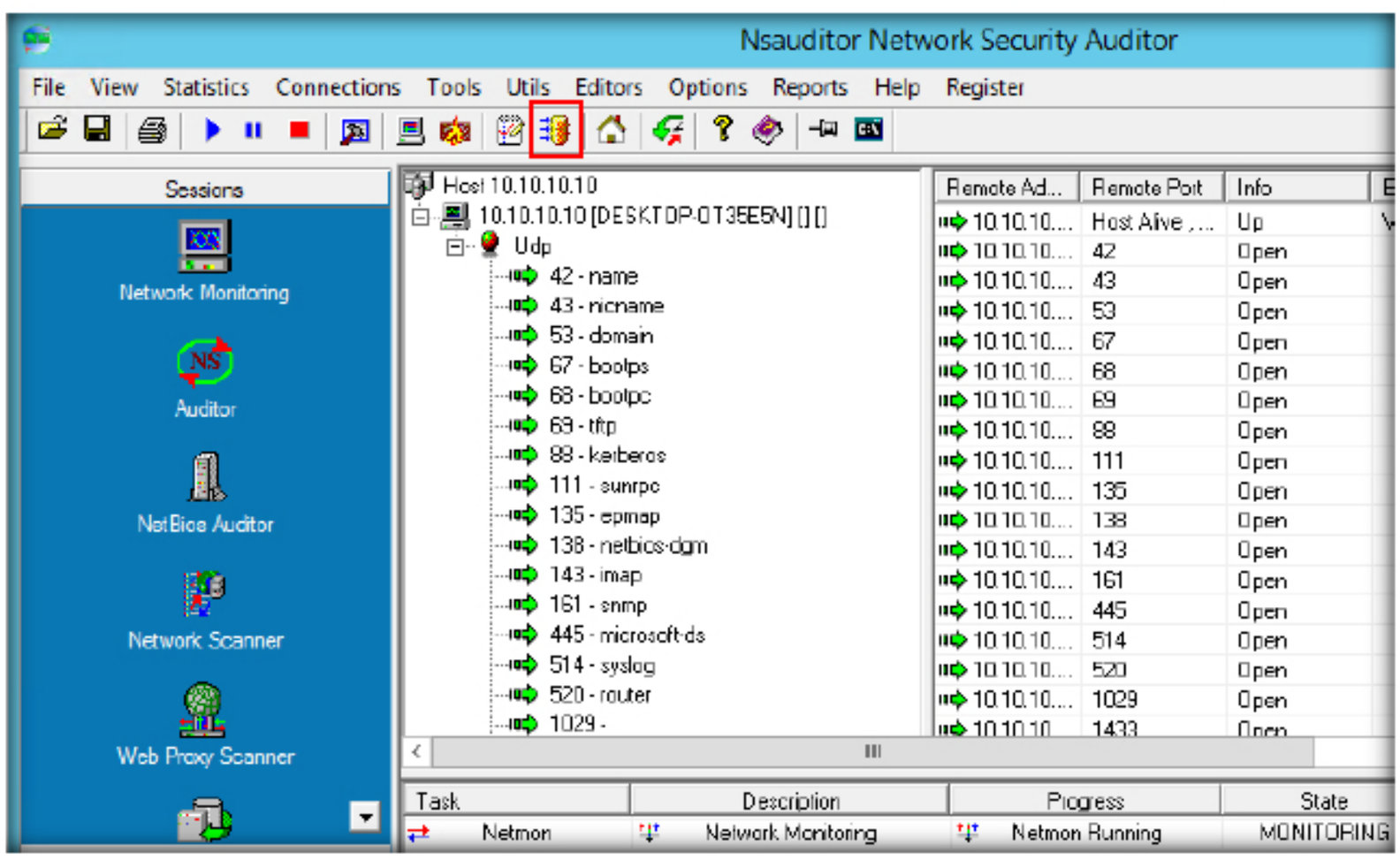


FIGURE 3.13: Navigating to audit reports

TASK 4

Examining Auditing Report

18. Click the report then click **View** (if there are multiple audits, the latest audit report will be at the top of the list).

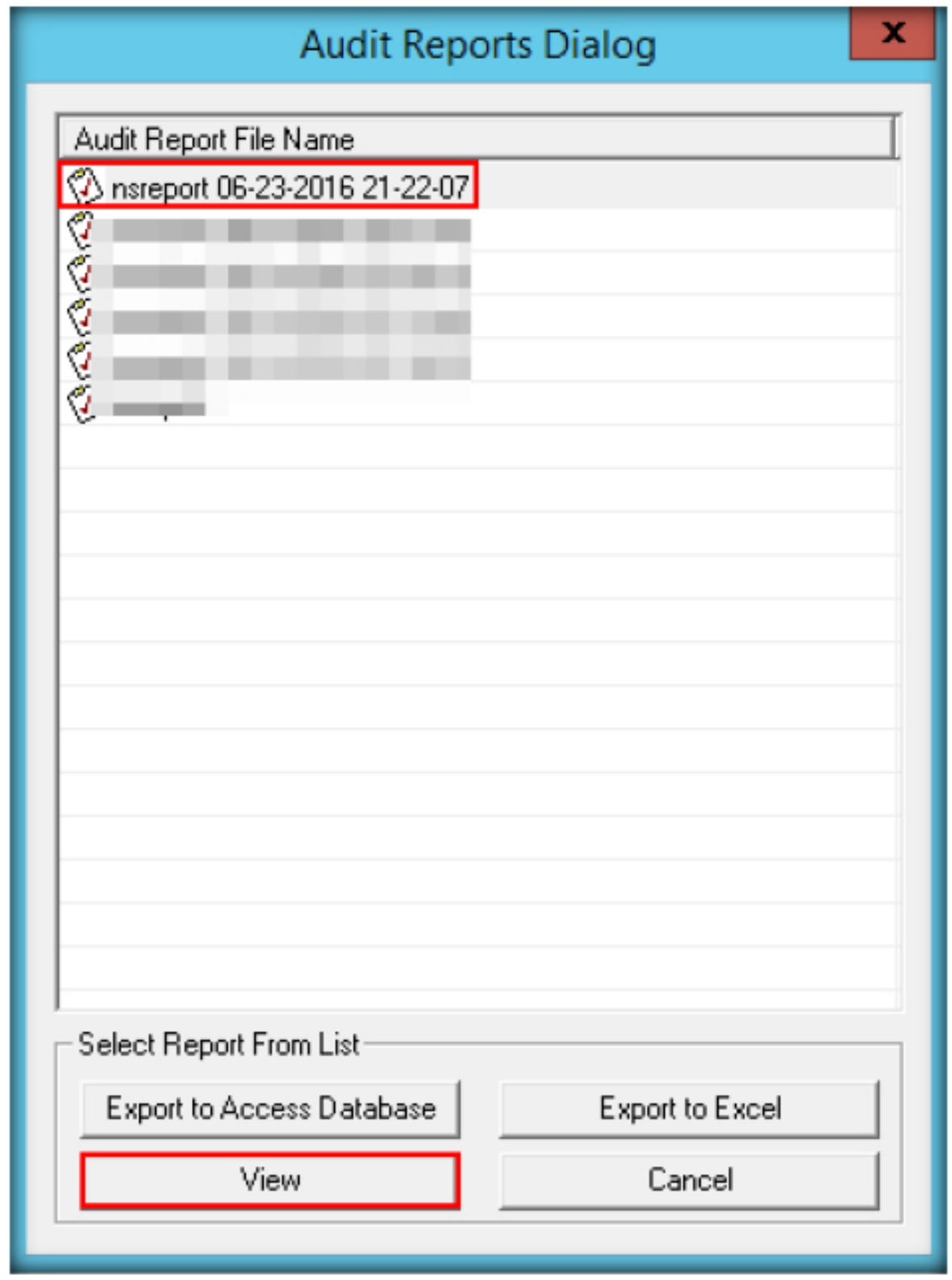


FIGURE 3.14: Viewing audit reports

19. The **Auditor Report** appears. Scroll down to view the contents of the report.

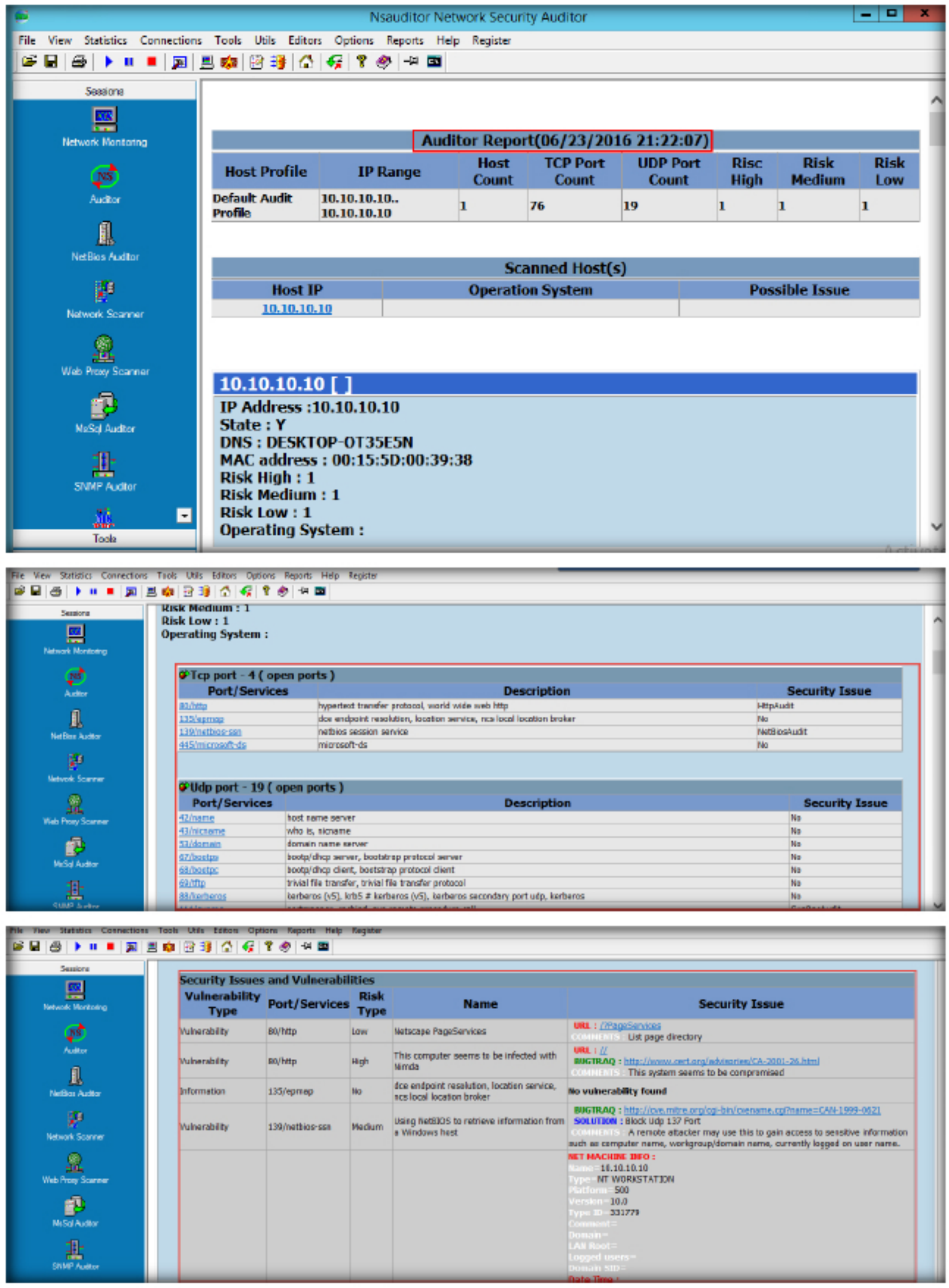


FIGURE 3.15: Audit report

20. In the same manner, you can conduct audits for multiple hosts in your network.

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

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

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

Lab

4

Scanning for Vulnerabilities in a Network using OpenVAS

OpenVAS offers a comprehensive and powerful vulnerability scanning and vulnerability management solution.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

When doing a security test, administrators should use a variety of vulnerability scanners to expose all possible vulnerabilities.

Lab Objectives

The objective of this lab is to help students learn how to:

- Perform a Vulnerability Assessment using the OpenVAS tool.

Lab Environment

To perform this lab, you need:

- A virtual machine running Ubuntu
- A virtual machine running Windows 10

Lab Duration

Time: 25 Minutes

Overview of OpenVAS

The OpenVAS scanner is a comprehensive vulnerability assessment system that can detect security issues in servers and network devices.

Lab Tasks

TASK 1

Turn off Firewall in Launch Windows 10 machine

1. Launch **Windows 10** virtual machine
2. Before starting this lab, turn off the **Windows Firewall** in the **Windows 10** machine. Log in to the machine as an Admin user and go to the **Control Panel**, then click on the **Windows Firewall** and choose the **Turn off** option for the Firewall profiles as shown in the screenshot.

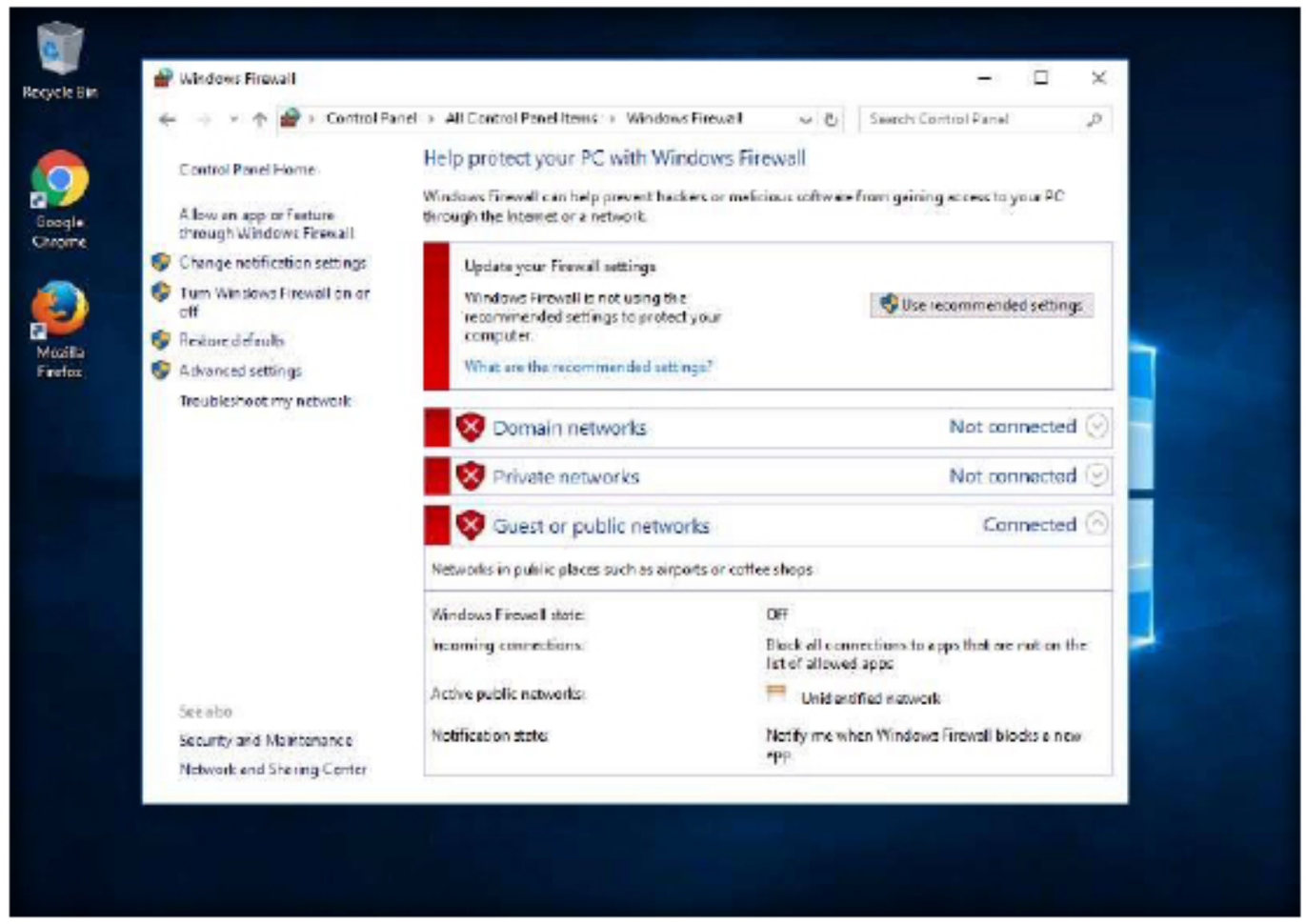


FIGURE 4.1: Turn off firewall

TASK 2

Install OpenVAS

3. Log on to Ubuntu machine. Type **toor** in the **Password** field and click **Next**.

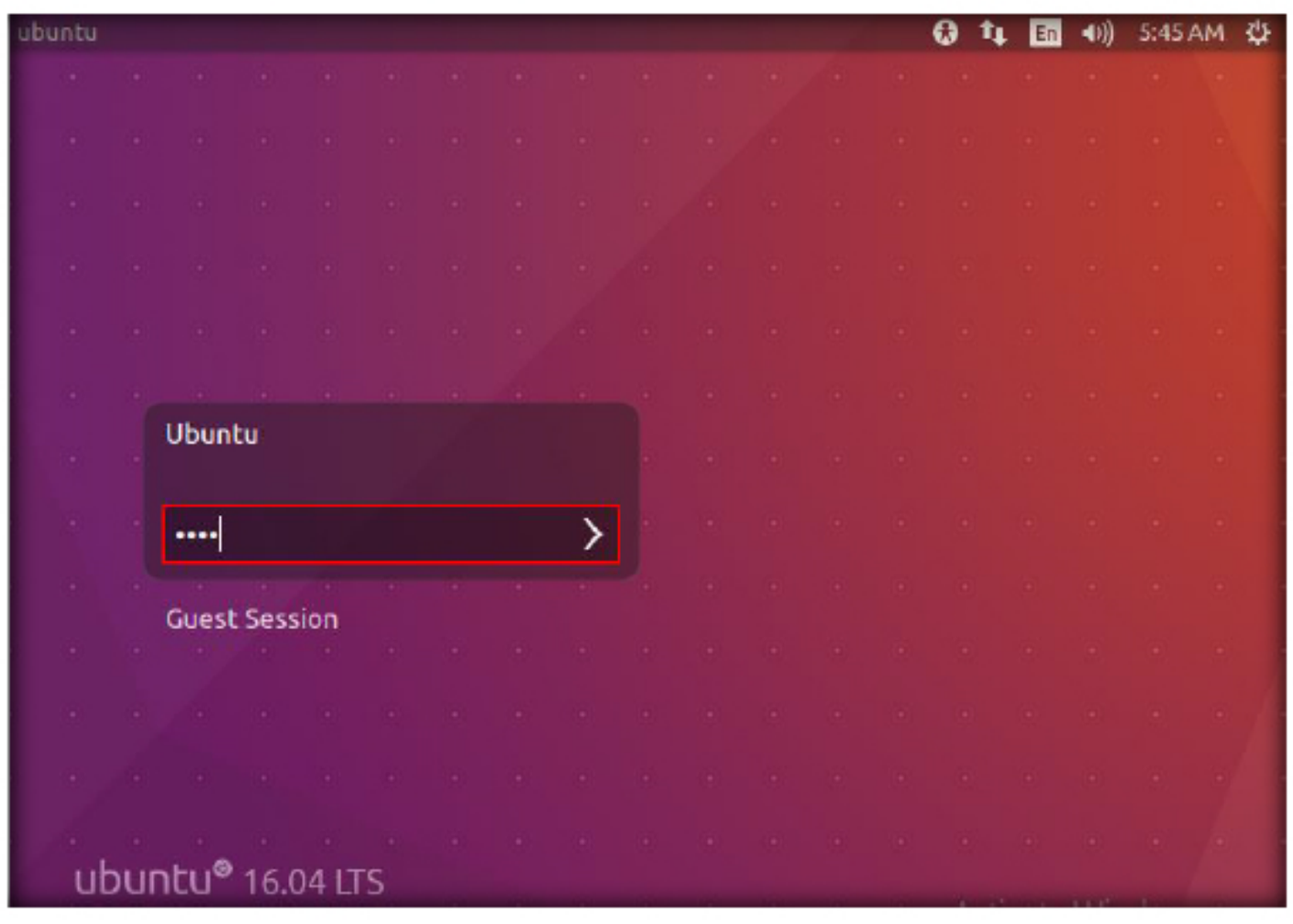


FIGURE 4.2: Entering Username

4. Launch a terminal, type **sudo su** in the terminal and press **Enter**. You will be prompted to enter a password. Type the password as **toor** and press **Enter**.

   Note: The password you enter will not be visible

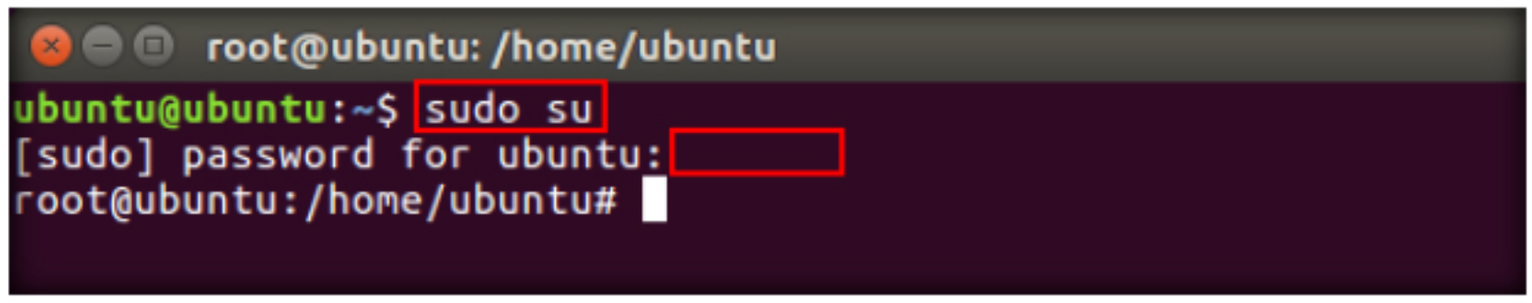


FIGURE 4.3: Getting root Terminal

5. Now, you need to install the **openvas** package from a PPA (personal password archive). For that, you need to add a personal password archive (PPA) to your system's Software Sources. To add, type **add-apt-repository ppa:mrazavi/openvas** in the terminal and press **Enter**.

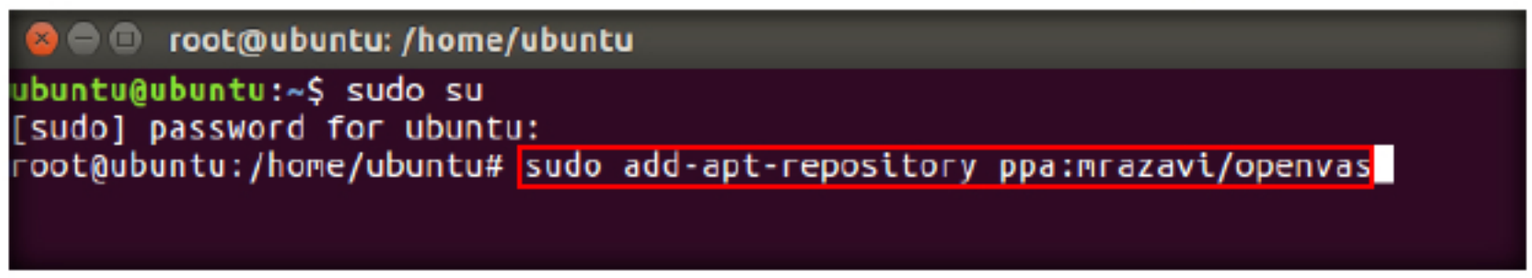


FIGURE 4.4: Adding Repository

6. A prompt appears stating that a set of new packages will be added to the system. Type **y** and press **Enter** to add the packages.

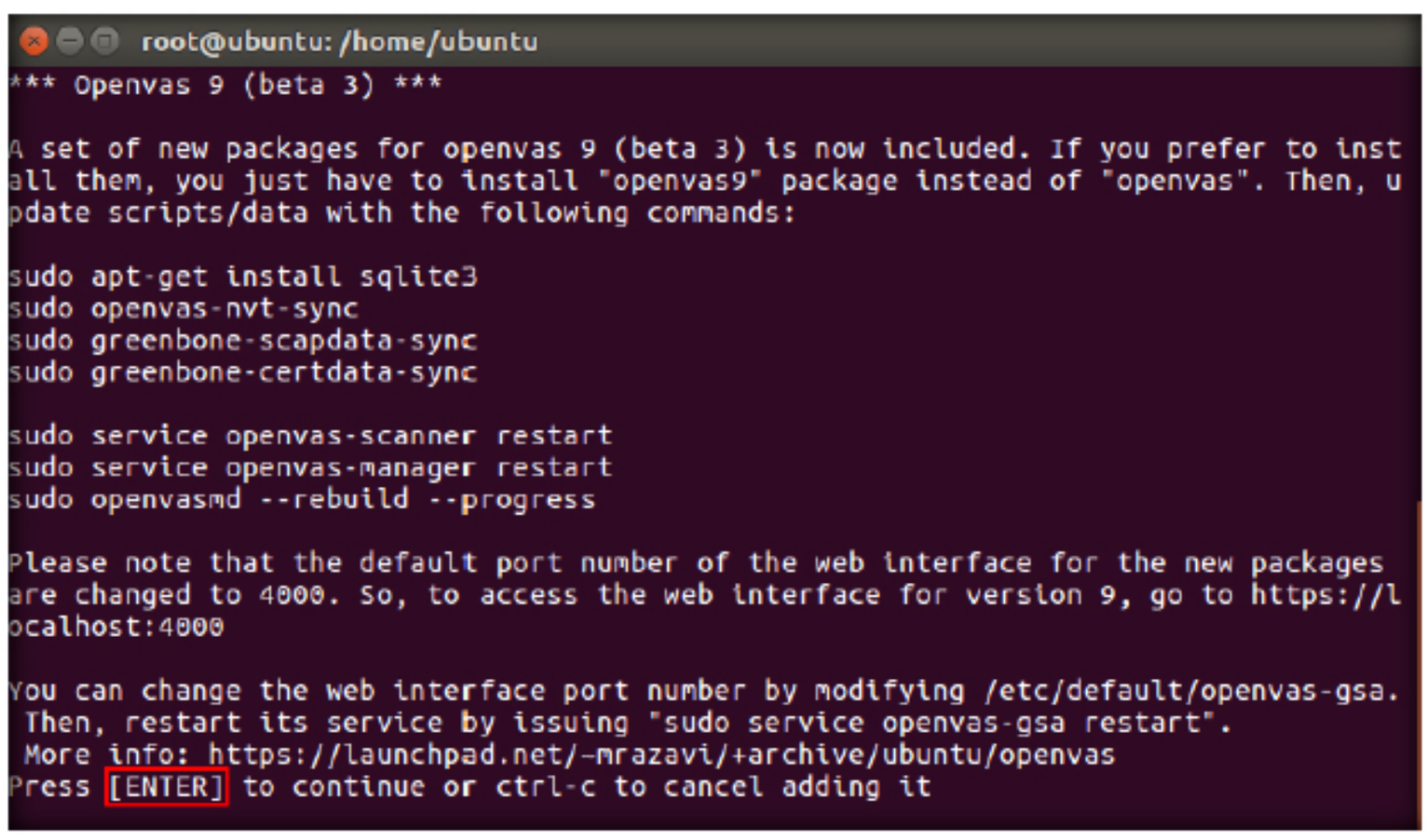


FIGURE 4.5: Adding New Package

7. Once the packages are added, type **apt-get update** and press **Enter** to ensure that all packages are correct and up to date

```
root@ubuntu: /home/ubuntu
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keyring `/tmp/tmpvkq5oax0/secring.gpg' created
gpg: keyring `/tmp/tmpvkq5oax0/pubring.gpg' created
gpg: requesting key 4AA450E0 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpvkq5oax0/trustdb.gpg: trustdb created
gpg: key 4AA450E0: public key "Launchpad PPA for Mohammad Razavi" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
OK
root@ubuntu:/home/ubuntu# apt-get update
Get:1 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial InRelease [17.6 kB]
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:3 http://security.ubuntu.com/ubuntu xenial-security InRelease
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [95.7 kB]
Get:5 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main amd64 Packages [2
,900 B]
Get:6 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main i386 Packages [2,
908 B]
Get:7 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main Translation-en [1
,044 B]
Hit:8 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease
Fetched 120 kB in 2s (57.0 kB/s)
```

FIGURE 4.6: Updating Repositories

8. Once done, type **apt-get install openvas** and press **Enter** to install OpenVAS

```
root@ubuntu: /home/ubuntu
start its service by issuing "sudo service openvas-gsa restart".
 More info: https://launchpad.net/~mrazavi/+archive/ubuntu/openvas
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keyring `/tmp/tmpvkq5oax0/secring.gpg' created
gpg: keyring `/tmp/tmpvkq5oax0/pubring.gpg' created
gpg: requesting key 4AA450E0 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpvkq5oax0/trustdb.gpg: trustdb created
gpg: key 4AA450E0: public key "Launchpad PPA for Mohammad Razavi" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
OK
root@ubuntu:/home/ubuntu# apt-get update
Get:1 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial InRelease [17.6 kB]
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:3 http://security.ubuntu.com/ubuntu xenial-security InRelease
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [95.7 kB]
Get:5 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main amd64 Packages [2,900 B]
Get:6 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main i386 Packages [2,908 B]
Get:7 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main Translation-en [1,044 B]
Hit:8 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease
Fetched 120 kB in 2s (57.0 kB/s)
Reading package lists... Done
root@ubuntu:/home/ubuntu# apt-get install openvas
```

FIGURE 4.7: Installing OpenVAS

9. A prompt appears stating that additional disk space will be used. Type **y** and press **Enter** to continue.

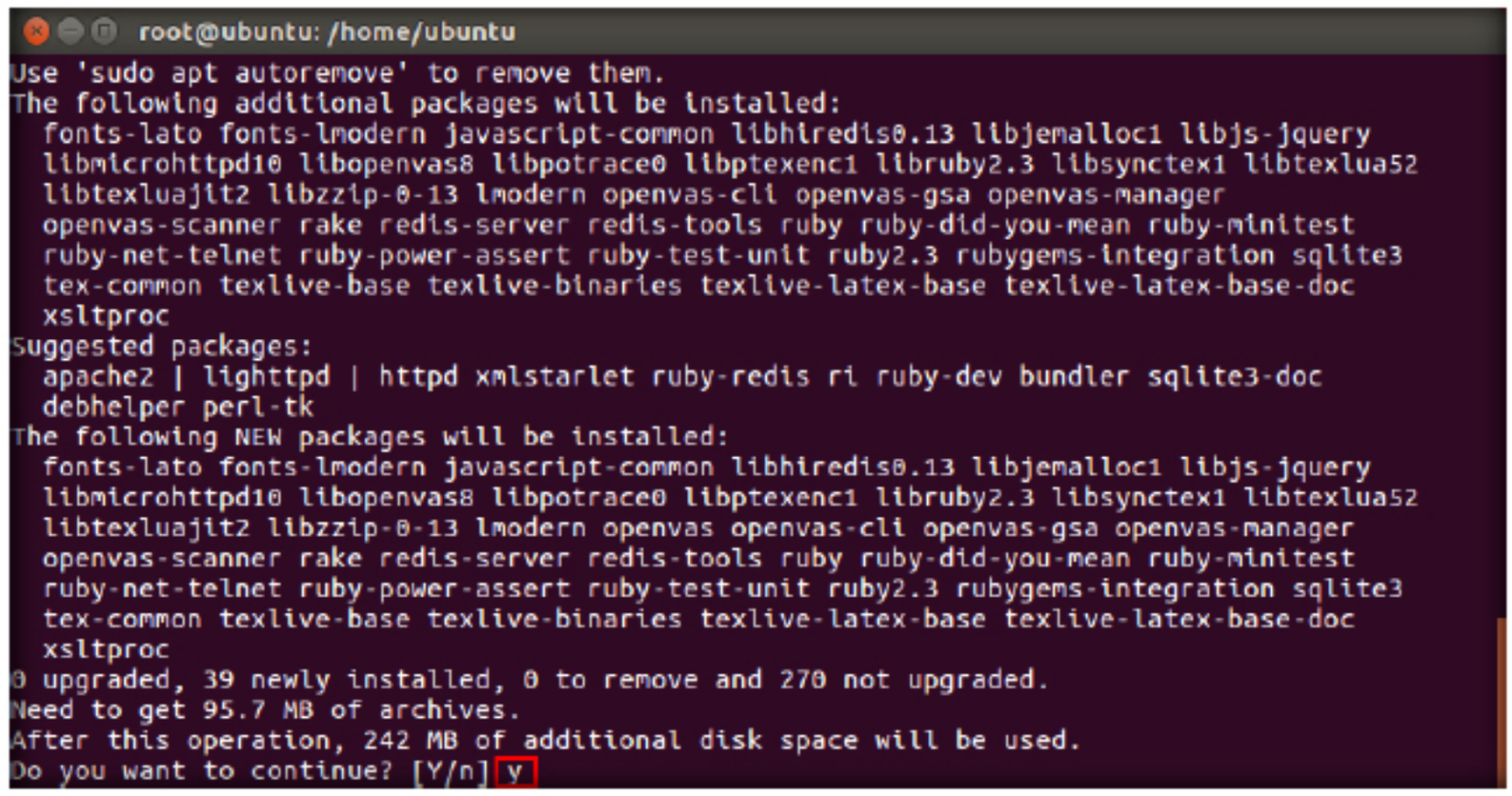


FIGURE 4.8: Installing OpenVAS

10. During installation, a **Configuring openvas-scanner** window appears, type **Yes** and press **Enter** to connect to redis database with a unix socket

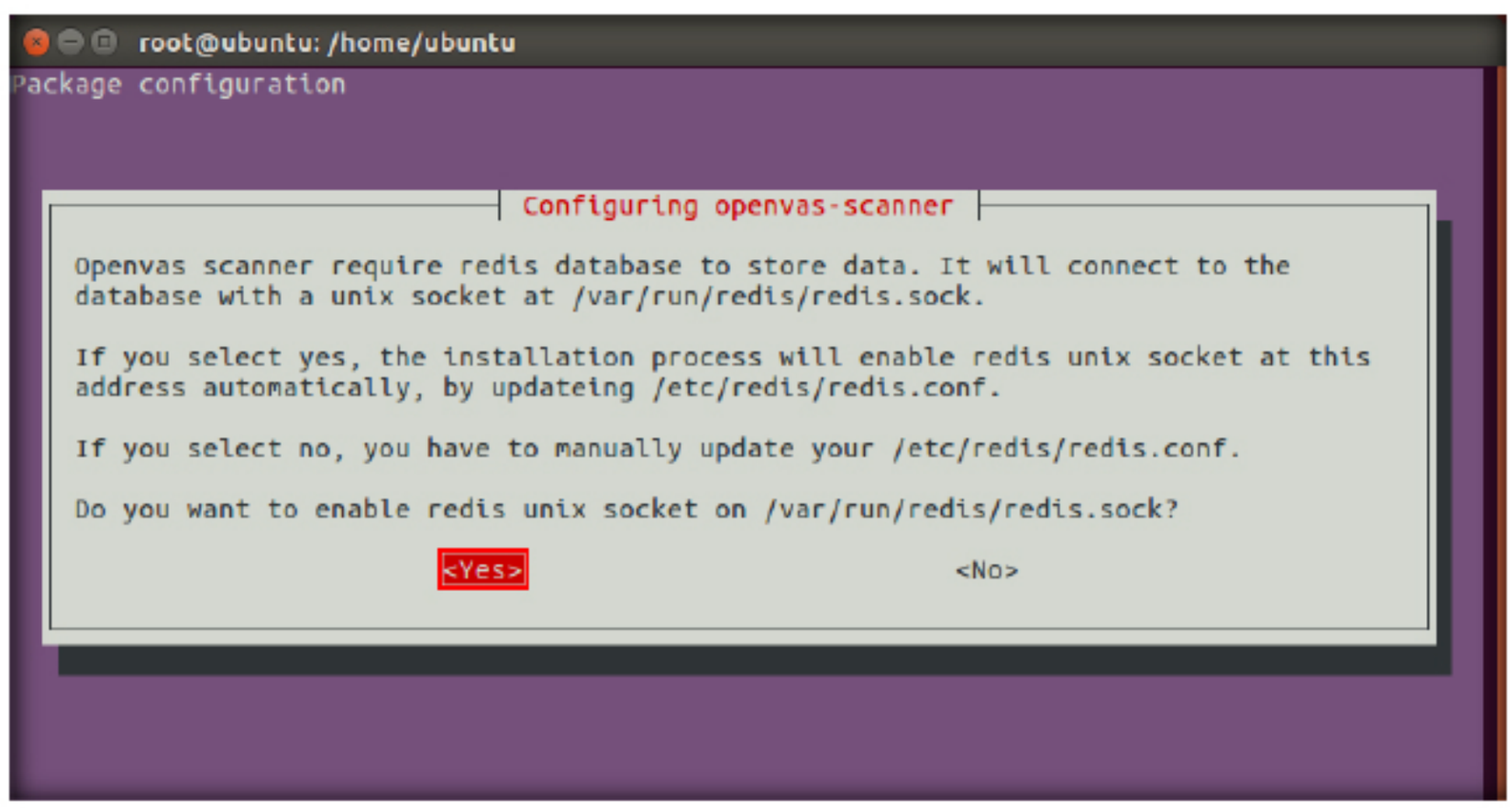


FIGURE 4.9: Configuring OpenVAS

11. Once done with the installation, type **apt-get install sqlite3** and press **Enter** to install sqlite3

```
root@ubuntu: /home/ubuntu
Processing triggers for tex-common (6.04) ...
Running updmap-sys. This may take some time... done.
Running mktexlsr /var/lib/texmf ... done.
Building format(s) --all.
        This may take some time... done.
Setting up ruby2.3 (2.3.1-2~16.04) ...
Setting up ruby (1:2.3.0+1) ...
Setting up rake (10.5.0-2) ...
Setting up libruby2.3:amd64 (2.3.1-2~16.04) ...
Processing triggers for libc-bin (2.23-0ubuntu3) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for systemd (229-4ubuntu4) ...
root@ubuntu:/home/ubuntu# apt-get install sqlite3
Reading package lists... Done
Building dependency tree
Reading state information... Done
sqlite3 is already the newest version (3.11.0-1ubuntu1).
sqlite3 set to manually installed.
The following packages were automatically installed and are no longer required:
  linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic linux-image-4.4.0-21-generic
  linux-image-extra-4.4.0-21-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
root@ubuntu:/home/ubuntu#
```

FIGURE 4.10: Installing sqlite

12. Once the installation is completed, type **openvas-nvt-sync** and press **Enter** to synchronize an NVT collection with the OpenVAS NVT Feed

```
root@ubuntu: /home/ubuntu
The following packages were automatically installed and are no longer required:
  linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic linux-image-4.4.0-21-generic
  linux-image-extra-4.4.0-21-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
root@ubuntu:/home/ubuntu# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[i] NVT dir: /var/lib/openvas/plugins
[w] Could not determine feed version.
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.4xnfAoomzJ/openvas-feed-2016-08-01-21043.tar.bz2
--2016-08-01 00:57:24--  http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org)... 5.9.98.186
Connecting to www.openvas.org (www.openvas.org)|5.9.98.186|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 26369946 (25M) [application/x-bzip2]
Saving to: '/tmp/openvas-nvt-sync.4xnfAoomzJ/openvas-feed-2016-08-01-21043.tar.bz2'

           /tmp/openva   0%[                                    ]       0  --.-KB/s
```

FIGURE 4.11: Synchronizing an NVT

13. Once NVT collection is synchronized with the NVT Feed, type **openvas-scapdata-sync** and press **Enter** to synchronize SCAP data directory with the one present in OpenVAS

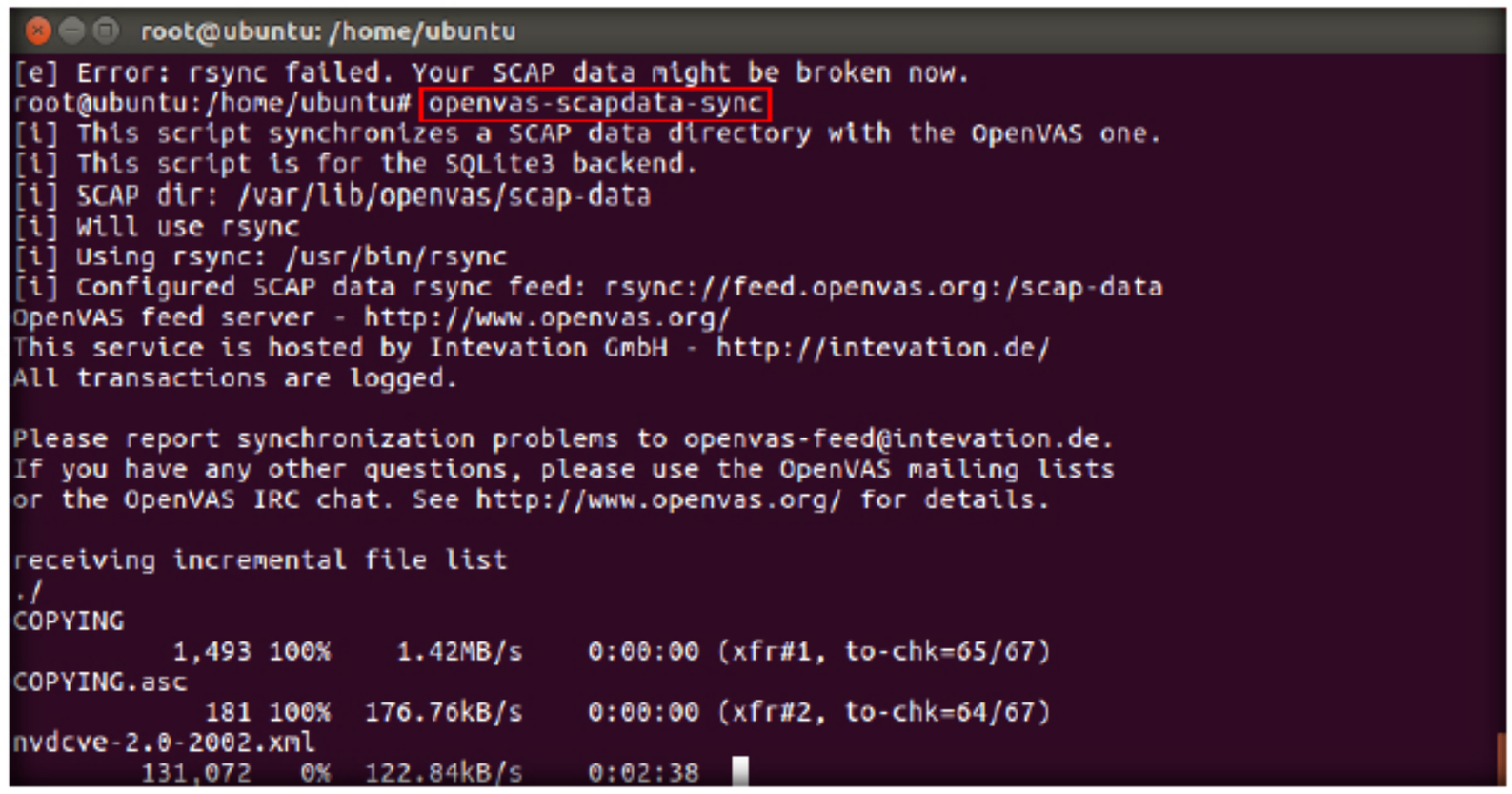


FIGURE 4.12: Synchronizing scapdata

14. Once done, type **openvas-certdata-sync** and press **Enter** to synchronize a CERT advisory directory with the once present in OpenVAS

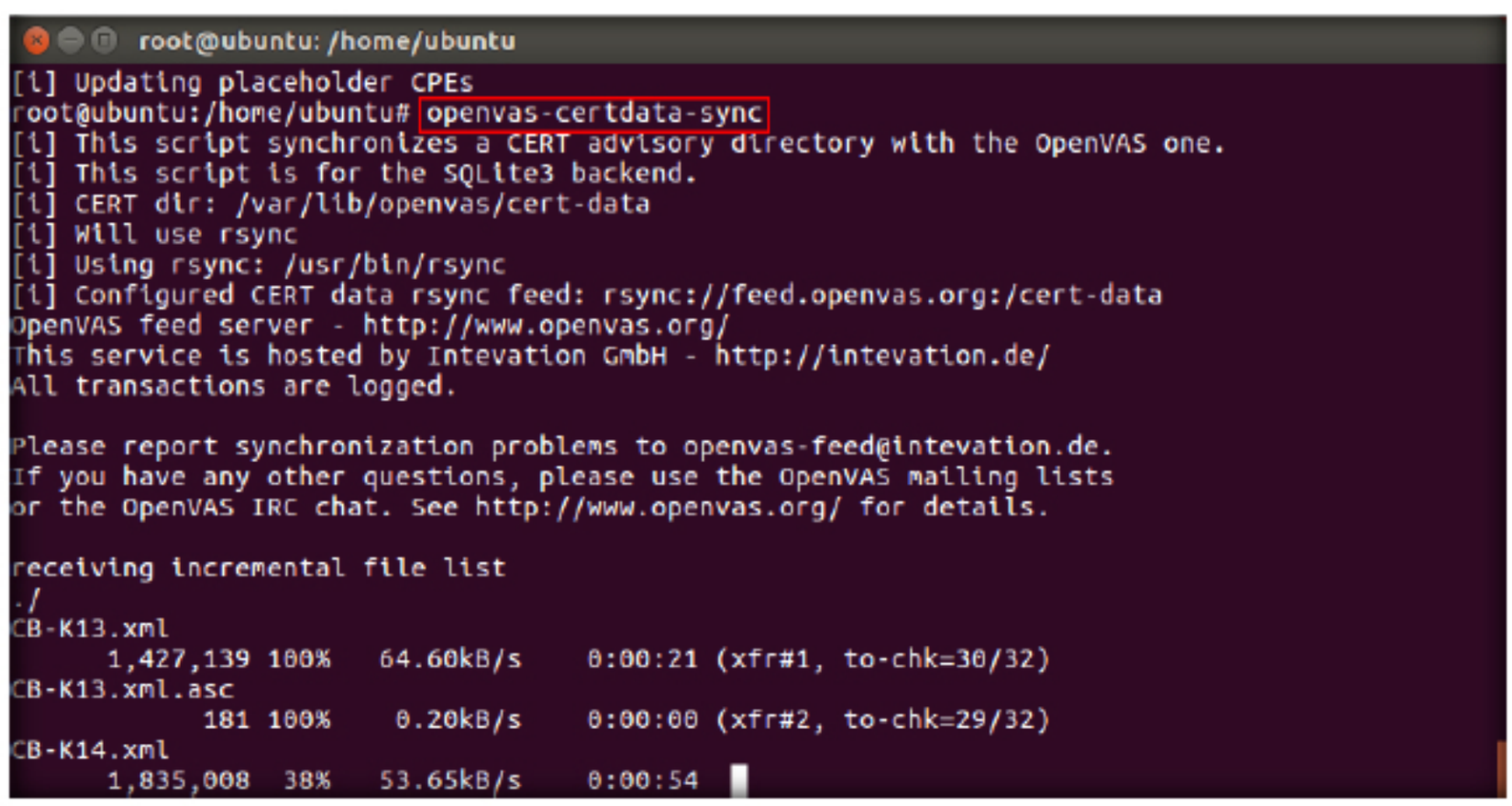


FIGURE 4.13: Synchronizing certdata

15. Once the synchronization is successful, you need to restart the openvas scanner. To restart, type **service openvas-scanner restart** and press **Enter**.

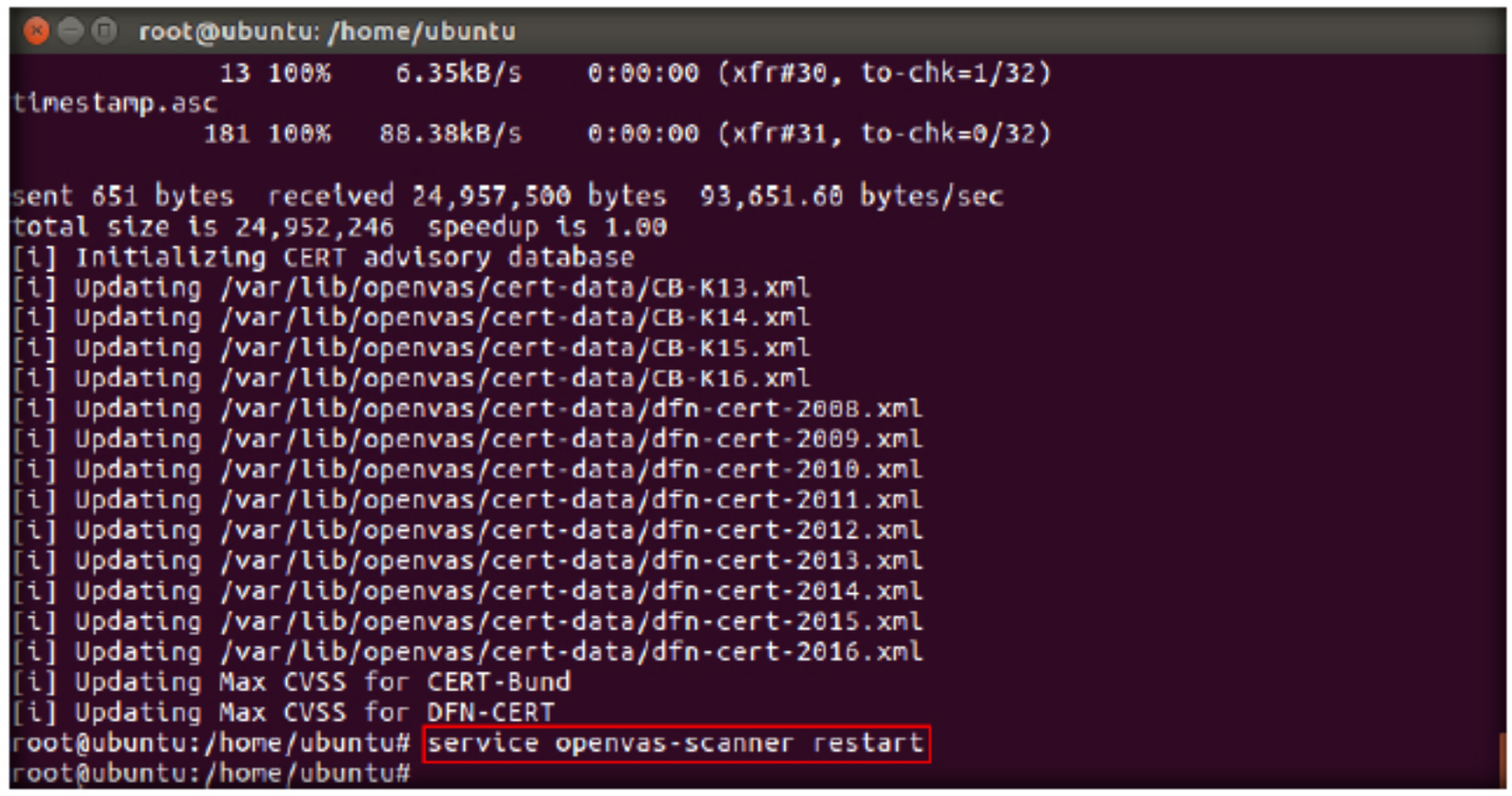


FIGURE 4.14: Restart OpenVAS Scanner

16. Now, restart OpenVAS manager by issuing the command **service openvas-manager restart**

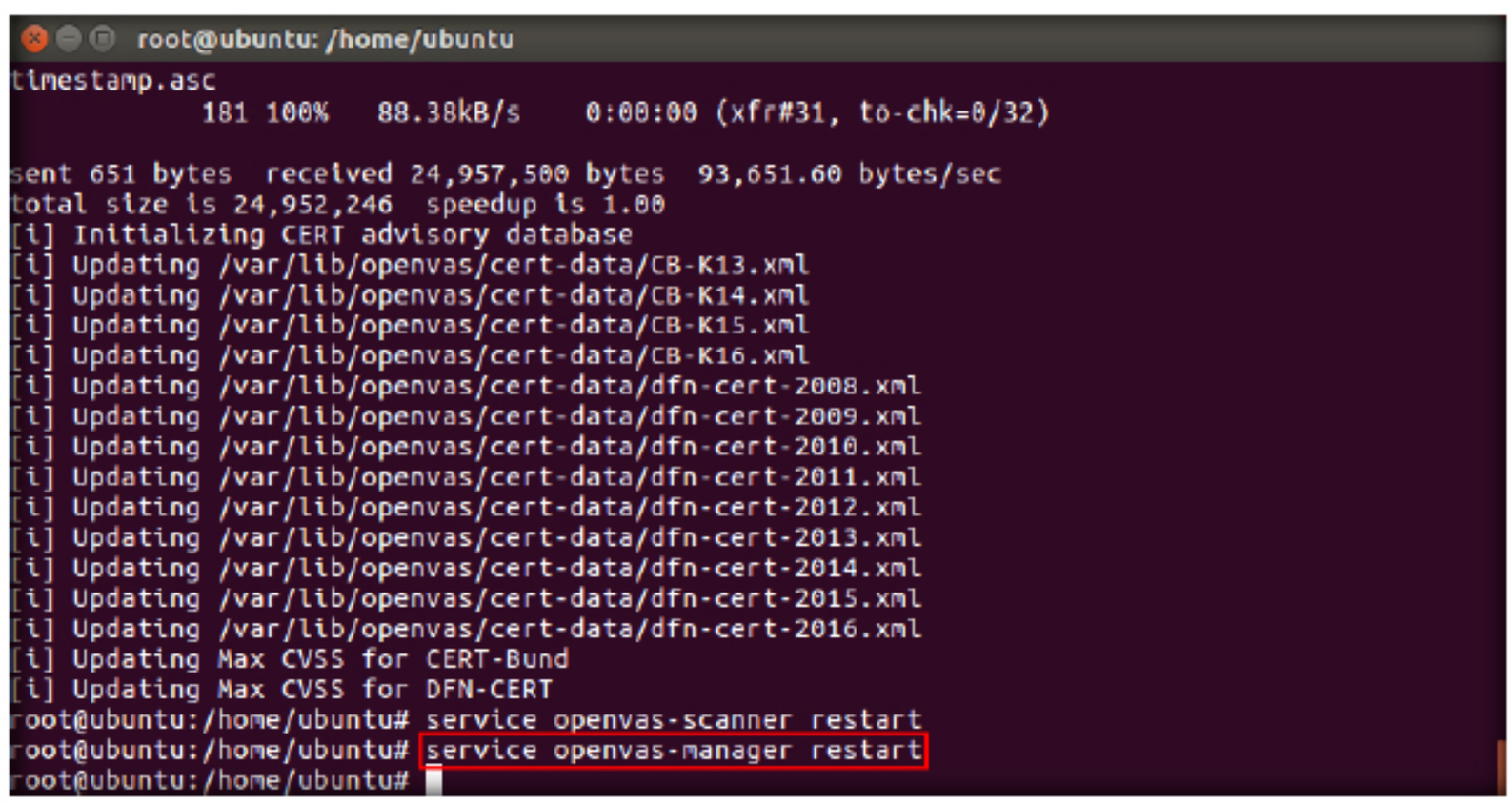


FIGURE 4.15: Restart OpenVAS Manager

17. Once the manager is restarted, type **openvasmd --rebuild --progress** and press **Enter** to rebuild the NVT cache. It takes 10-15 minutes to rebuild the NVT cache.

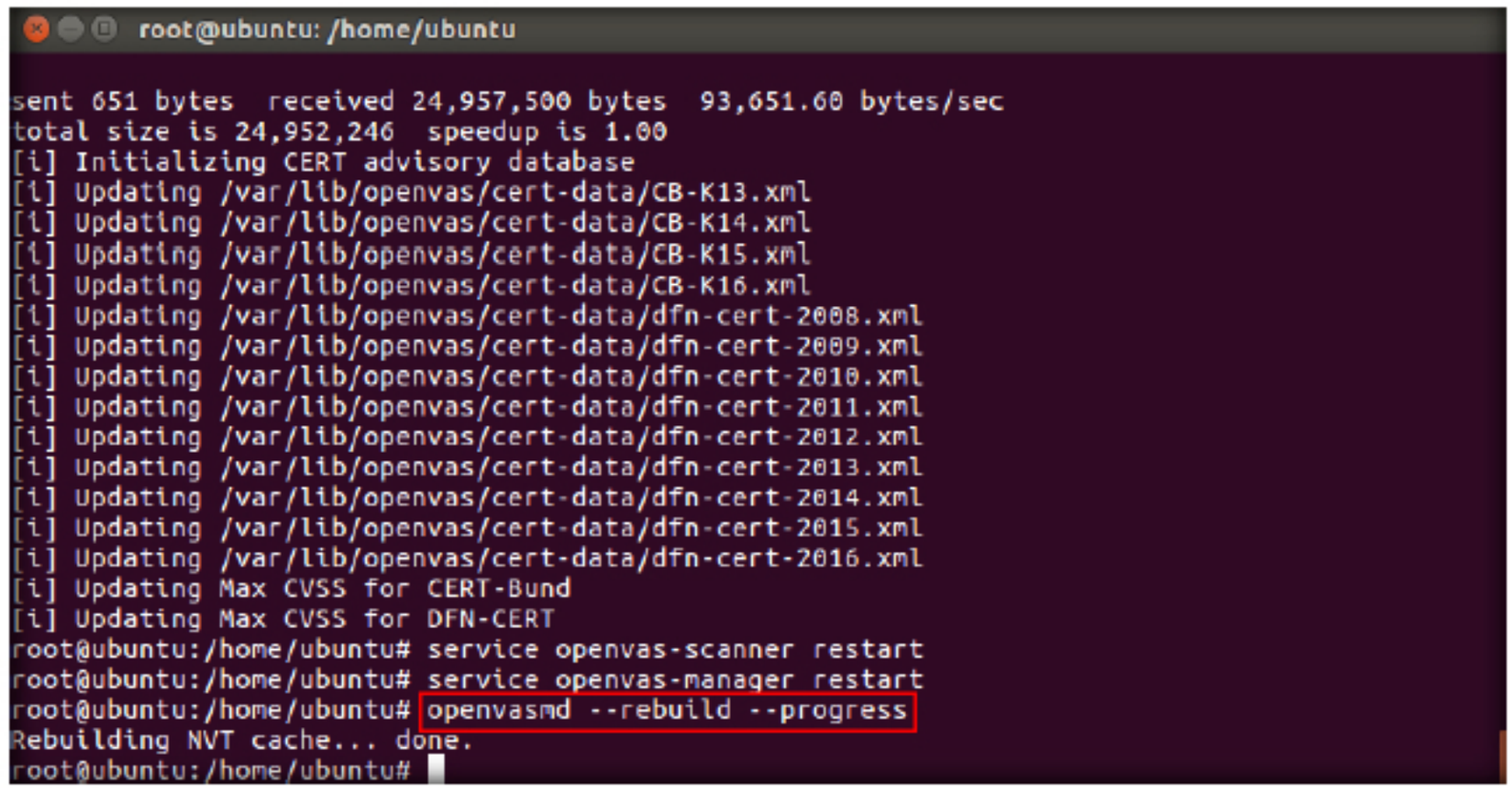


FIGURE 4.16: Rebuilding NVT Cacnhe

18. Once the cache is rebuilt, launch **Mozilla Firefox** web browser, type **https://127.0.0.1** in the address bar and press **Enter**. A webpage appears stating that the connection is insecure. Click **Advanced**.

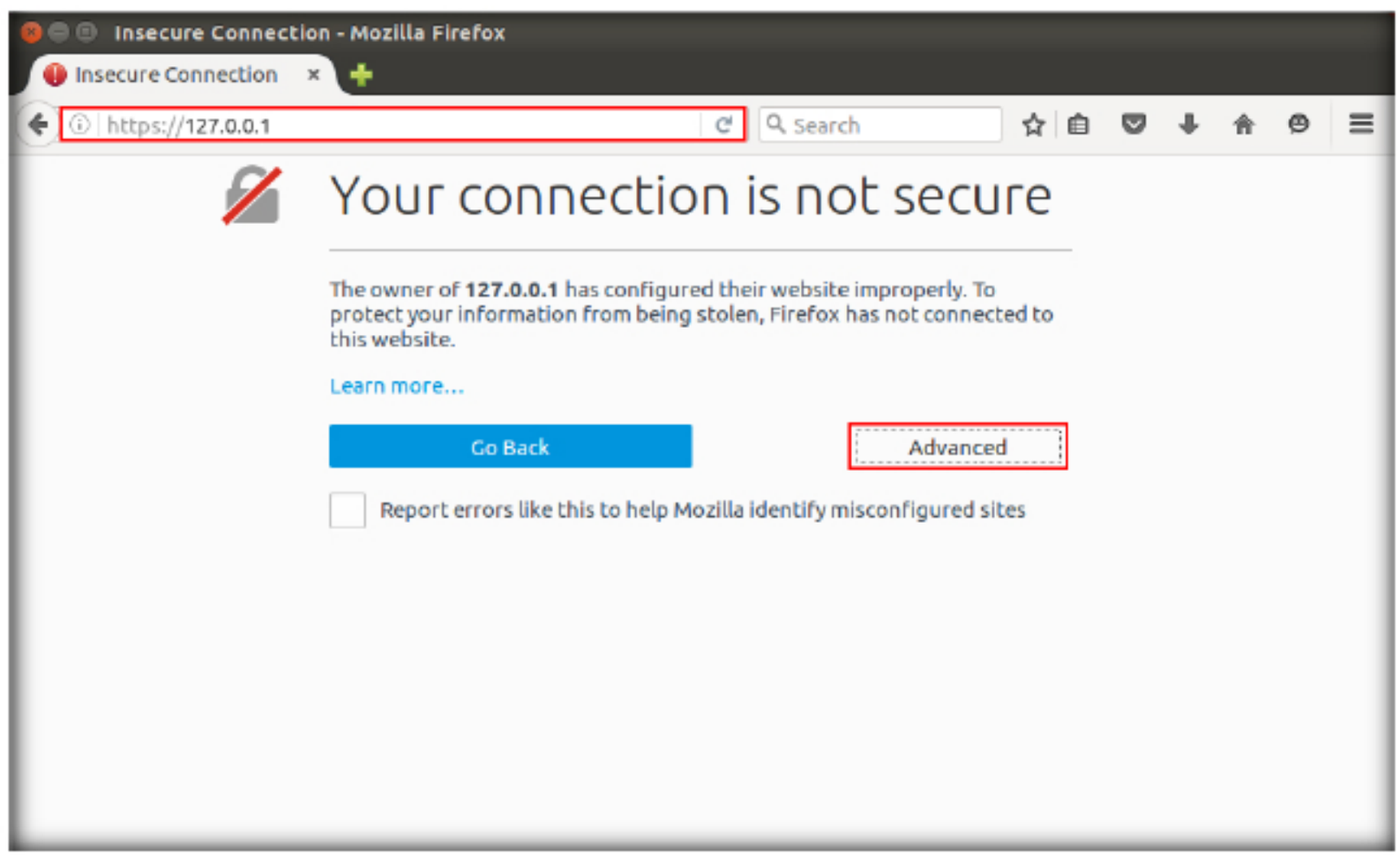


FIGURE 4.17: Connection Insecure

19. Now, click **Add Exception...** button to add certificate exception

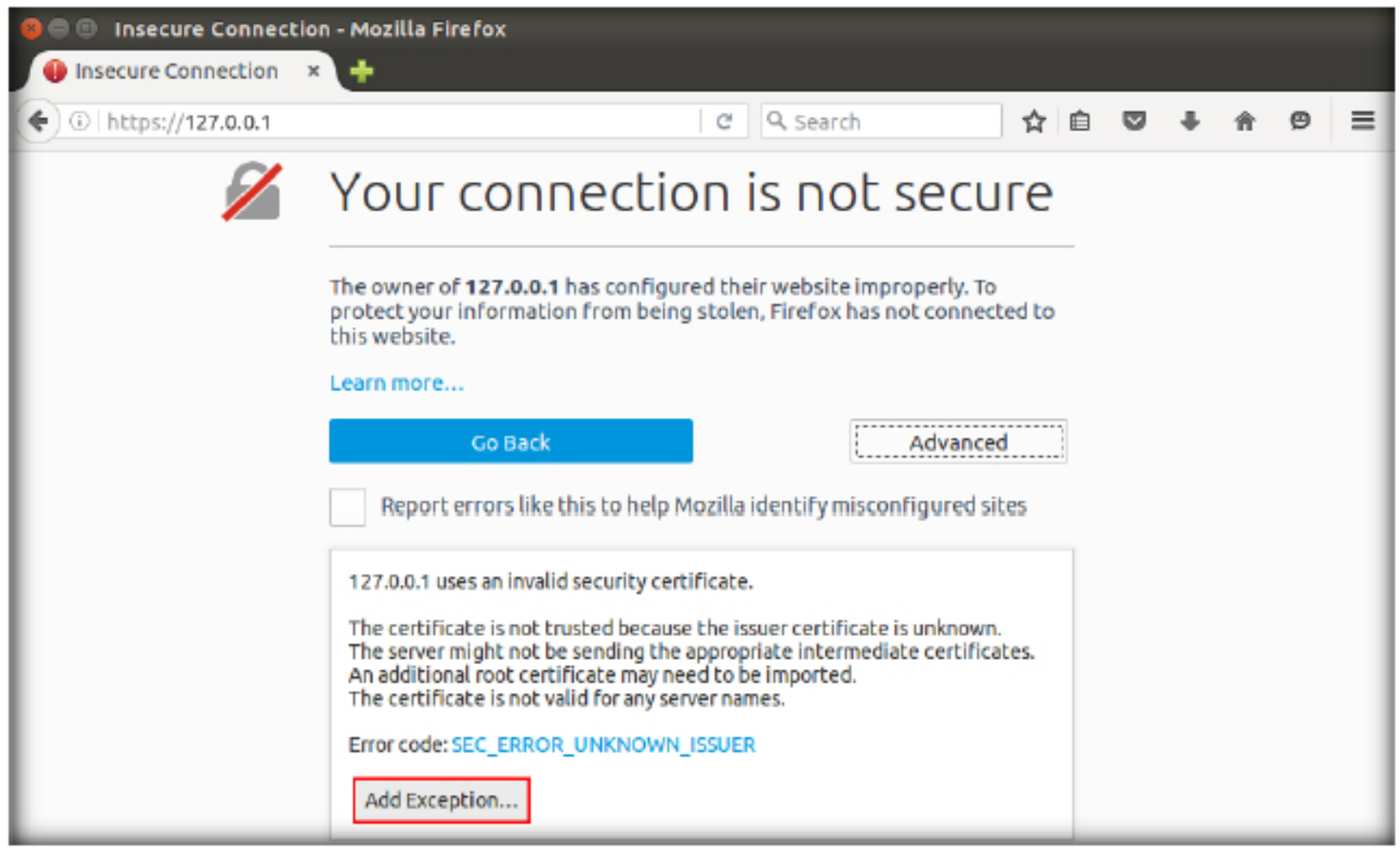


FIGURE 4.18: Adding Exception

20. **Add Security Exception** window appears, click **Confirm Security Exception** button

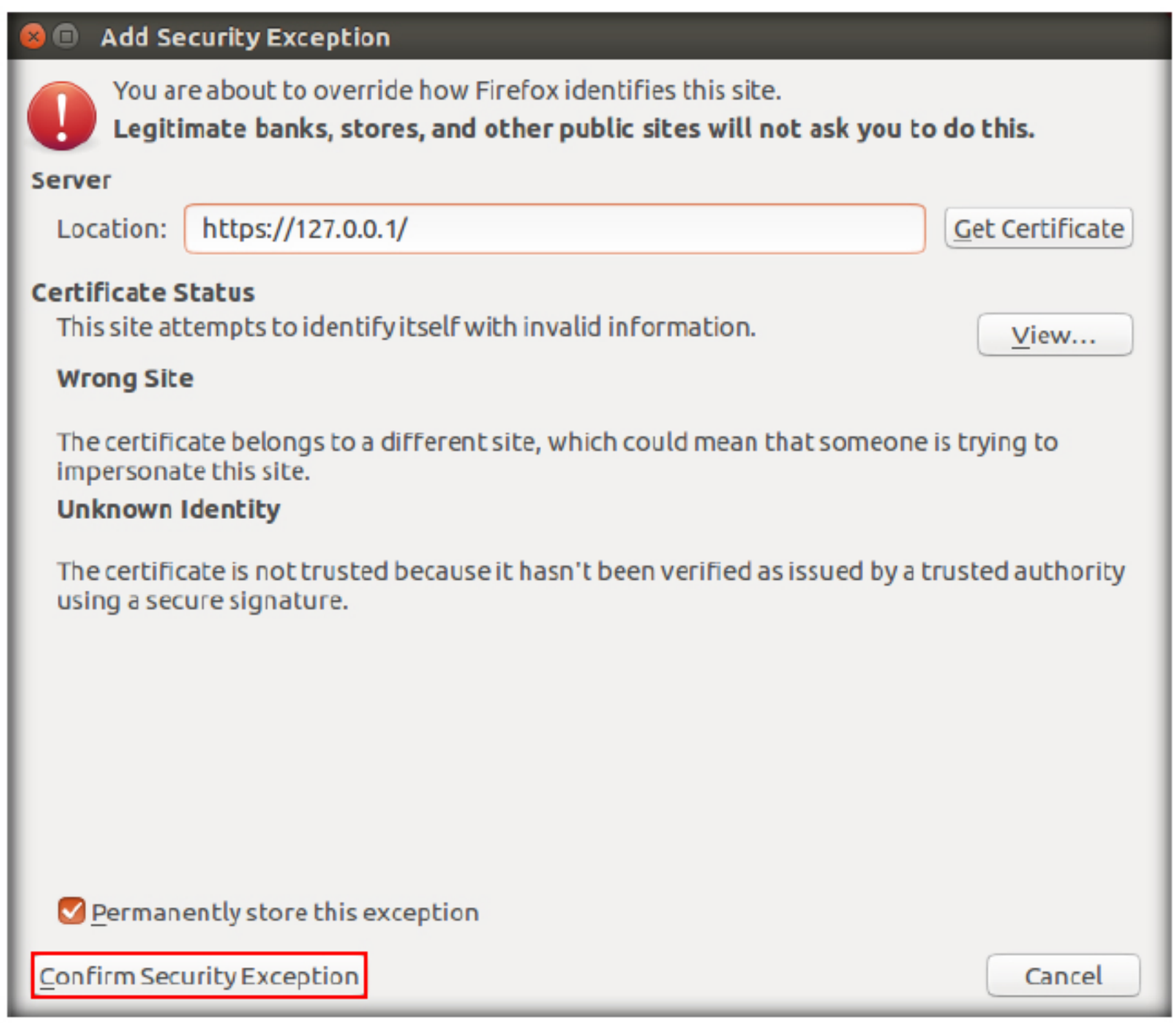


FIGURE 4.19: Adding Exception

21. Greenbone Security Assistant login page appears, type **Username** and **Password** as **admin**, and click **Login**

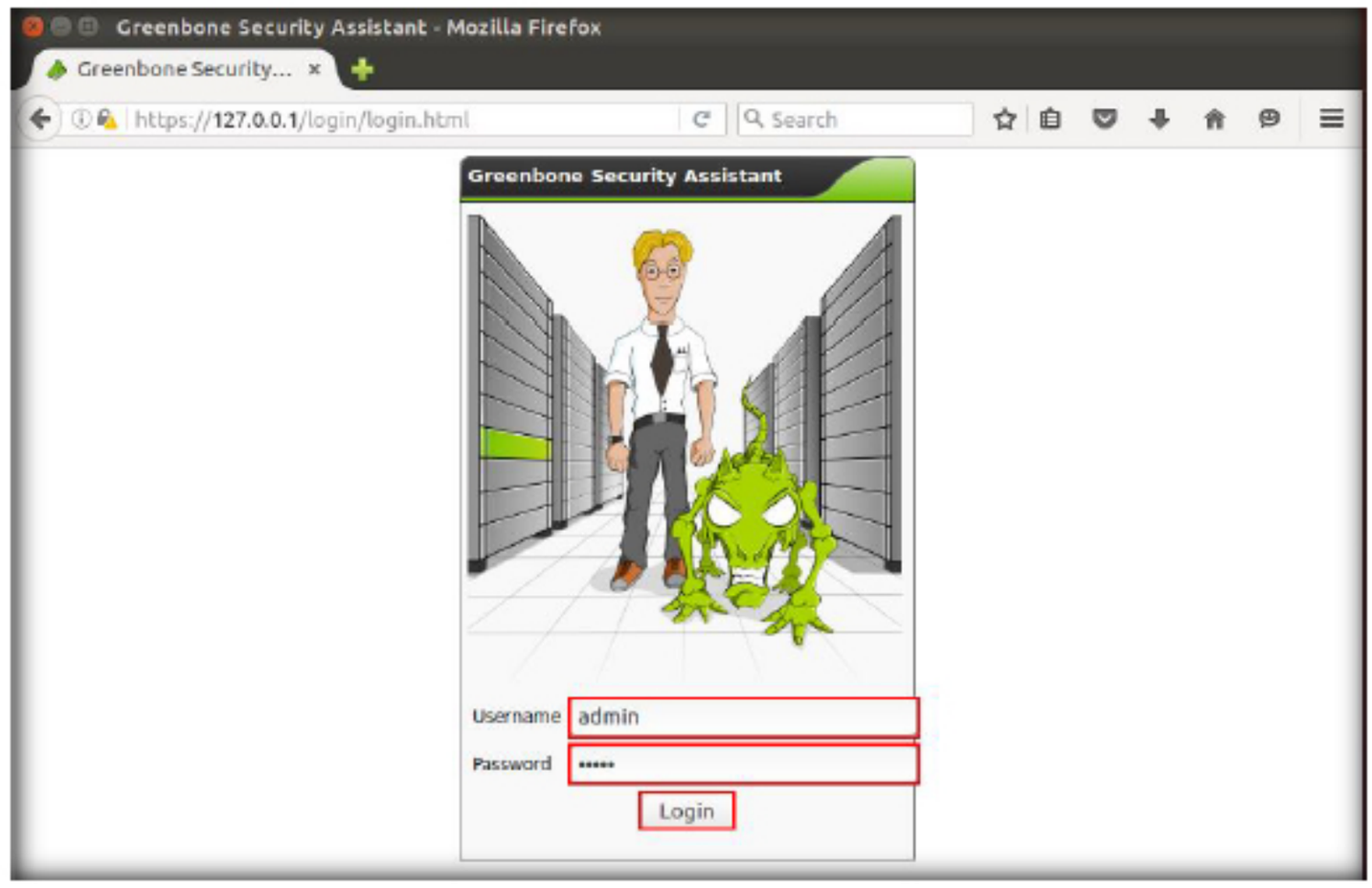


FIGURE 4.20: Logging into OpenVAS

TASK 3

Configure the Target

22. The OpenVAS Homepage appears, as shown in the screenshot. Hover the mouse cursor on **Configuration** and select **Targets**.

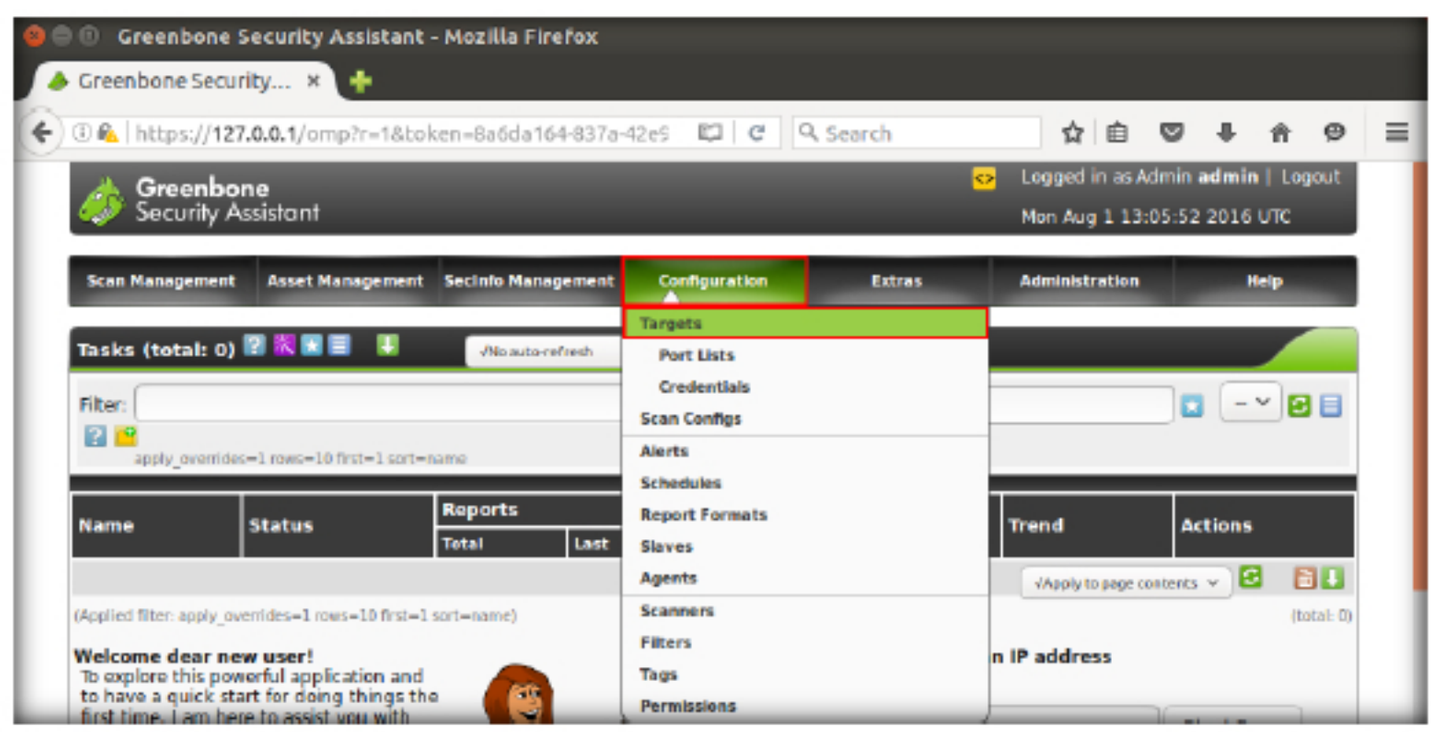


FIGURE 4.21: Choosing Target

23. Click the **star** icon in order to add a new target.

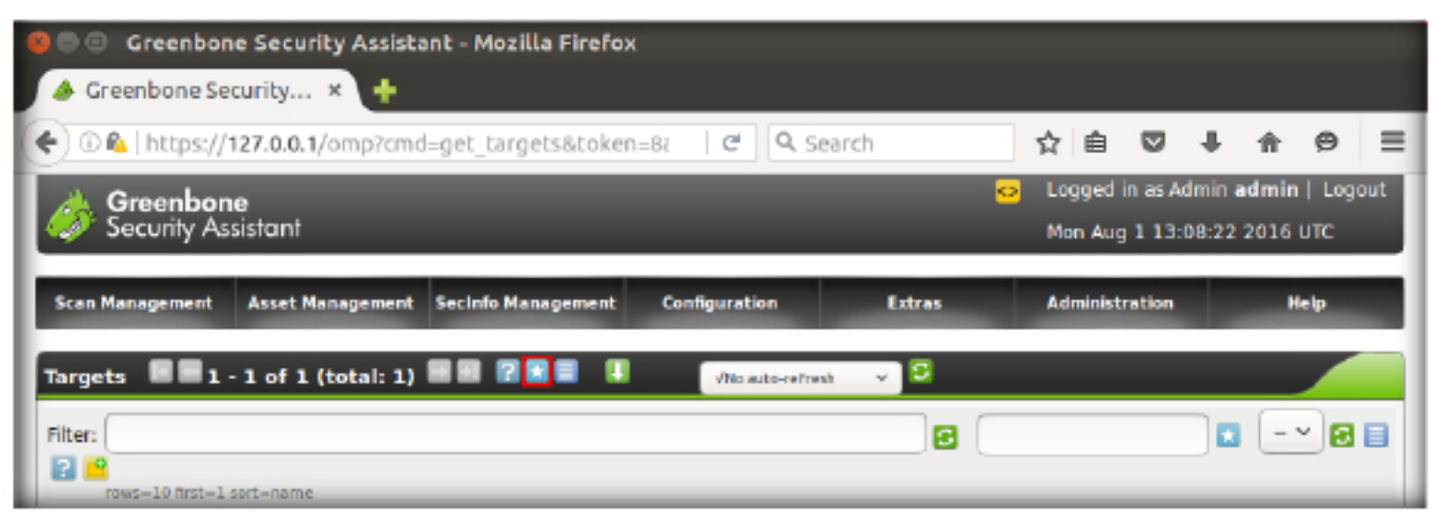


FIGURE 4.22: Clicking Start Icon

The admin password is generated during the setup phase

24. The **New Target** window appears, enter the target name (Windows 10 in this lab) in the Name text field. Next, select the **Manual** radio button under the hosts section and enter the IP address of the target machine. The IP address of Windows 10 is **10.10.10.10**. Select the All **IANA assigned TCP 2012-02-10** option from the Port List drop-down. Leave the other options set to the defaults then click **Create Target**.

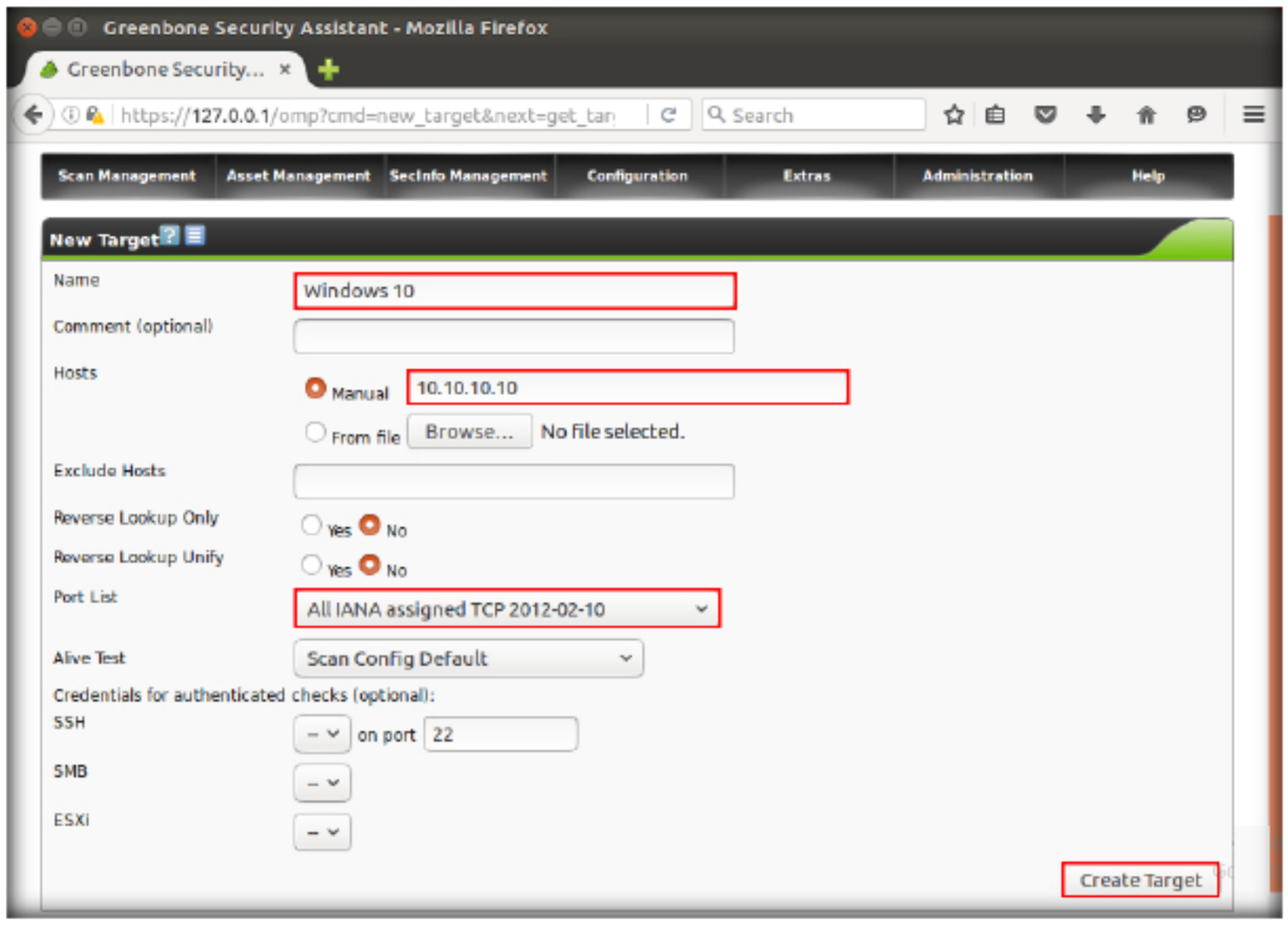


FIGURE 4.23: Entering target for scan

25. Once you click the **Create Target** button, OpenVAS will add the target and show you the **Target Details** as shown in the screenshot.

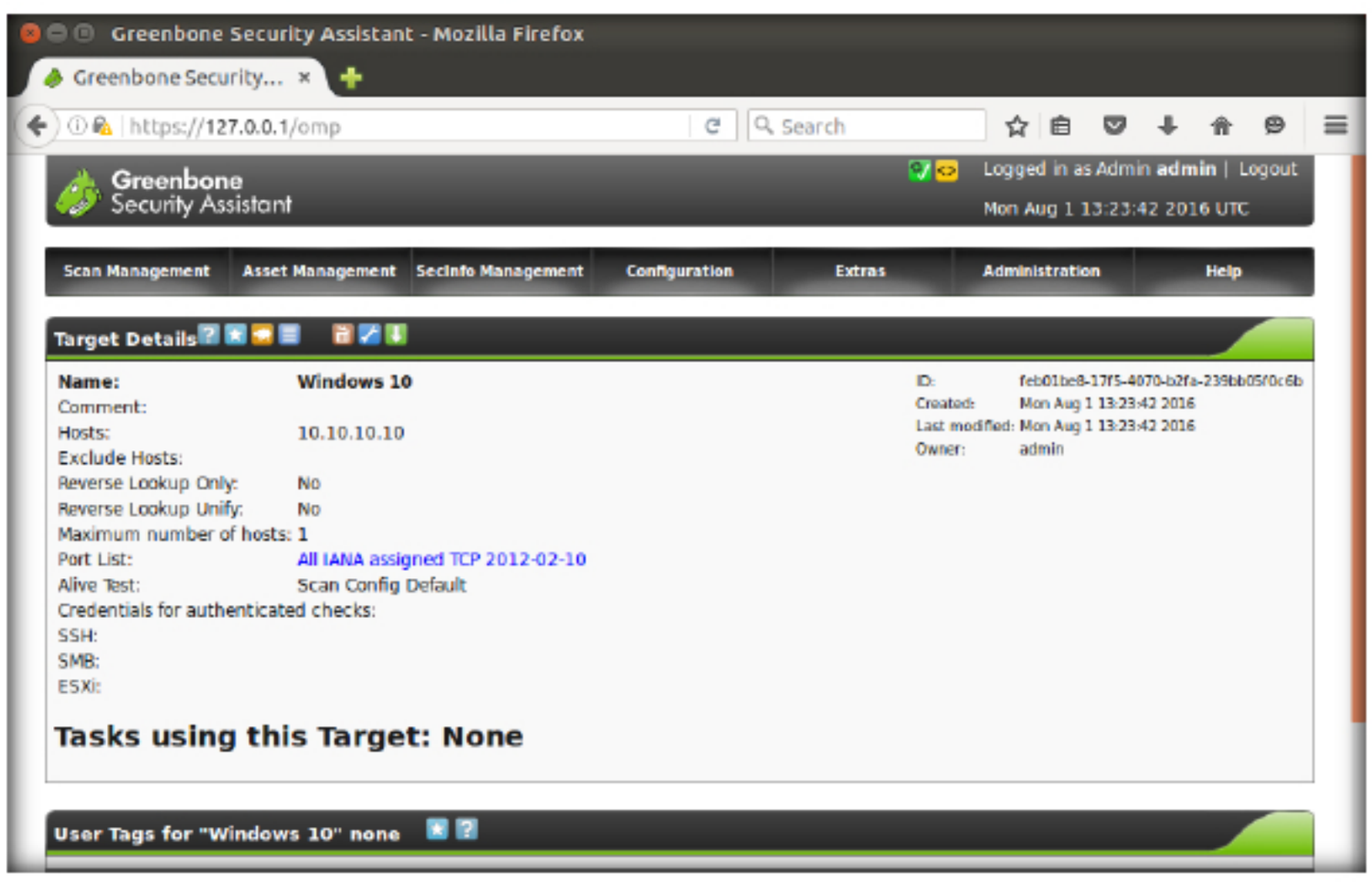


FIGURE 4.24: Target Details

26. To view list of the Targets added to OpenVAS, go to **Configurations** and click the **Targets** option.

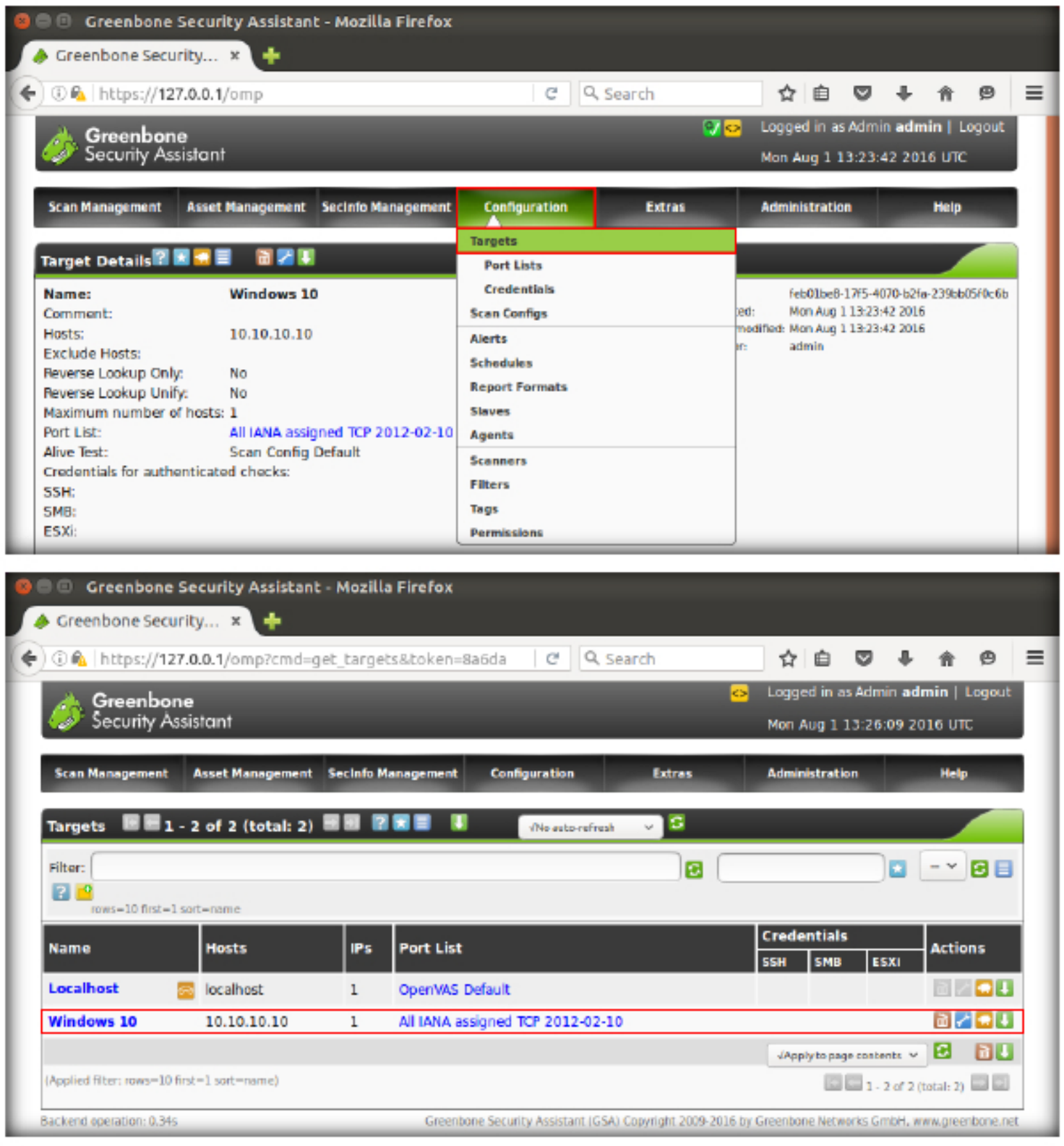


FIGURE 4.25: List of Targets

27. To add a new task to OpenVAS hover the mouse cursor on **Scan Management** then click **Tasks**.

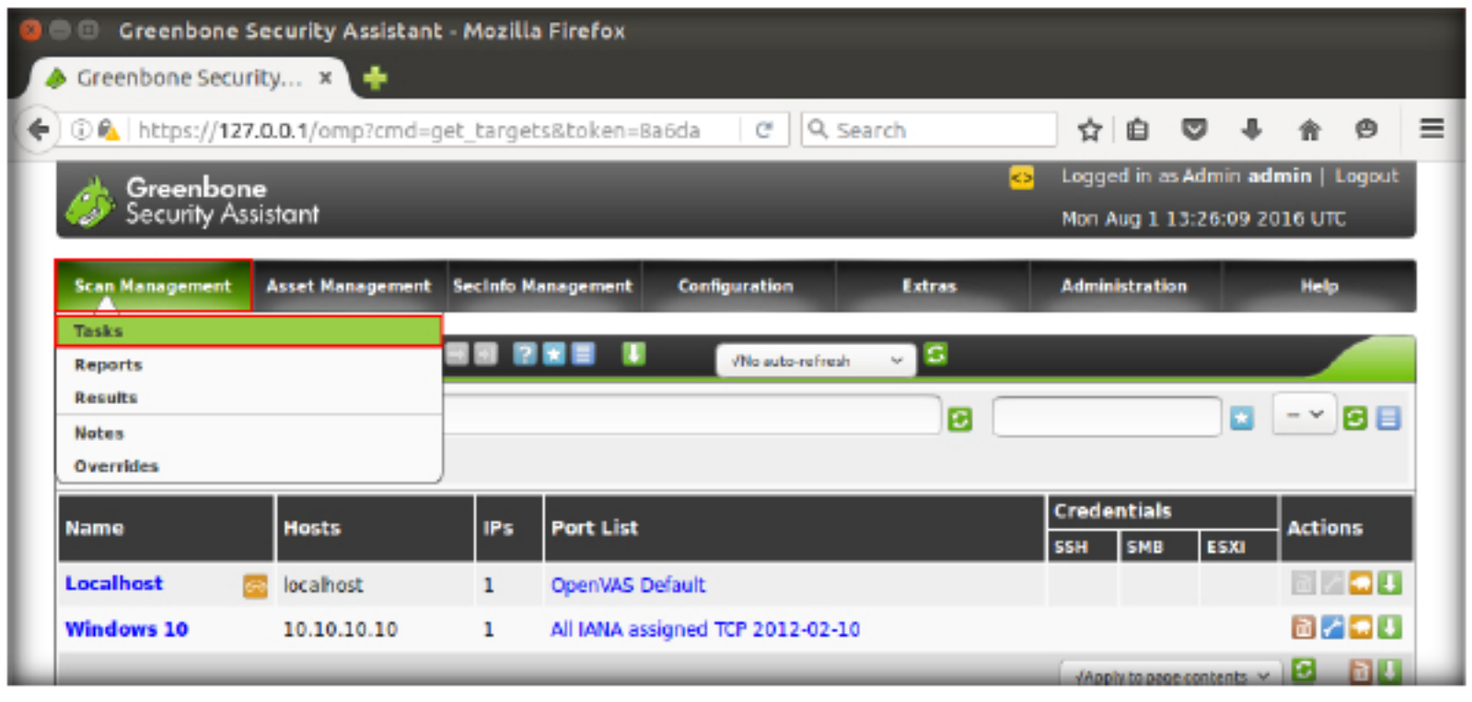


FIGURE 4.26: Adding new task

28. The **Tasks** wizard appears, as we haven't added any tasks to OpenVAS it will be empty. Now we need to create a new task. To do this click on the **Star** icon near Tasks (total: 0).

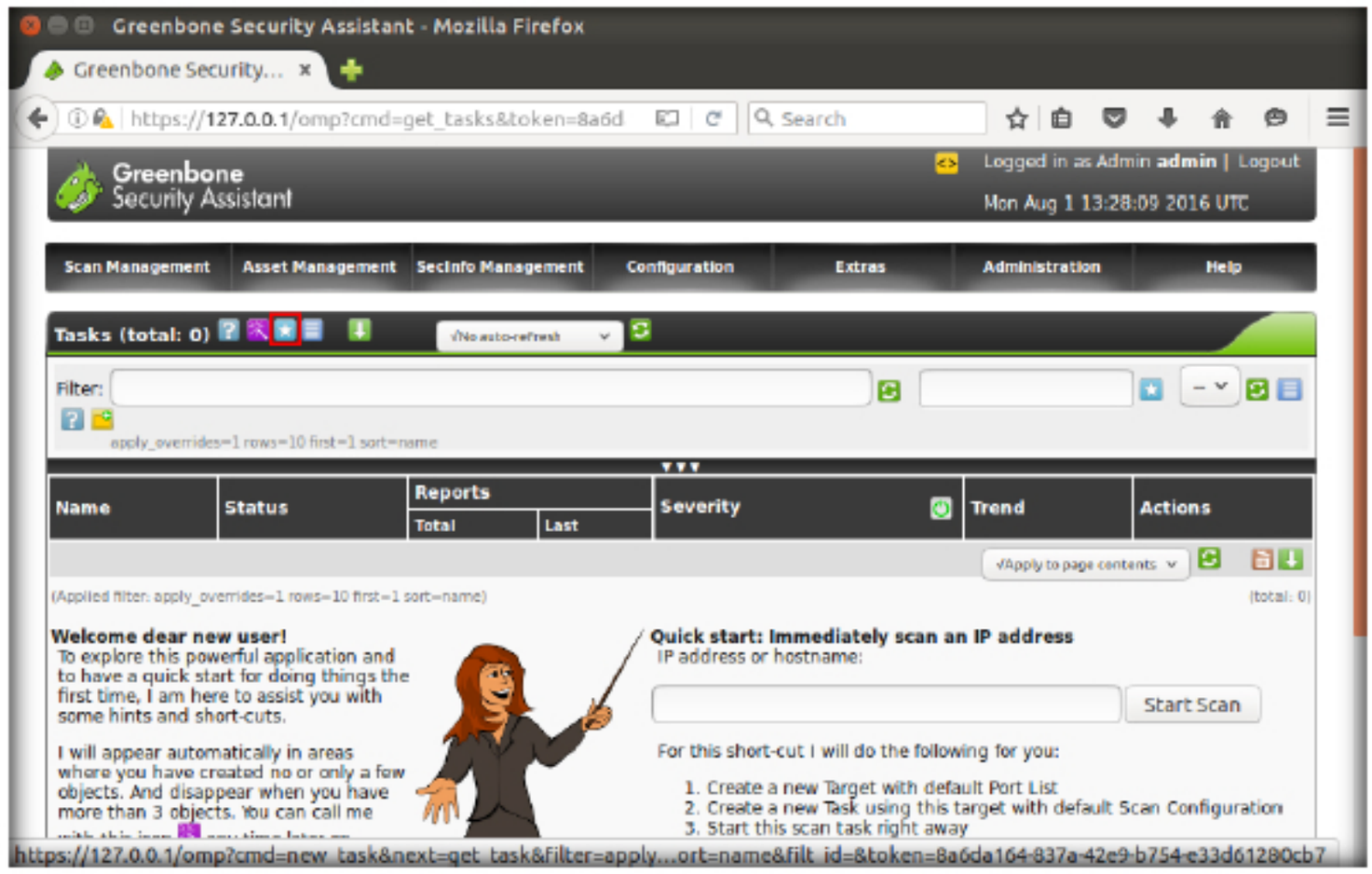


FIGURE 4.27: Creating new task

29. The New Task page appears, enter the name of the task (Windows 10 Scan), choose **Full and very deep scan** from the **Scan Config** drop-down and select Windows 10 from the **Scan Targets** drop-down. Leave the other options set to default, and scroll down and click **Create Task**. This creates a task which will be performed in the forthcoming steps.

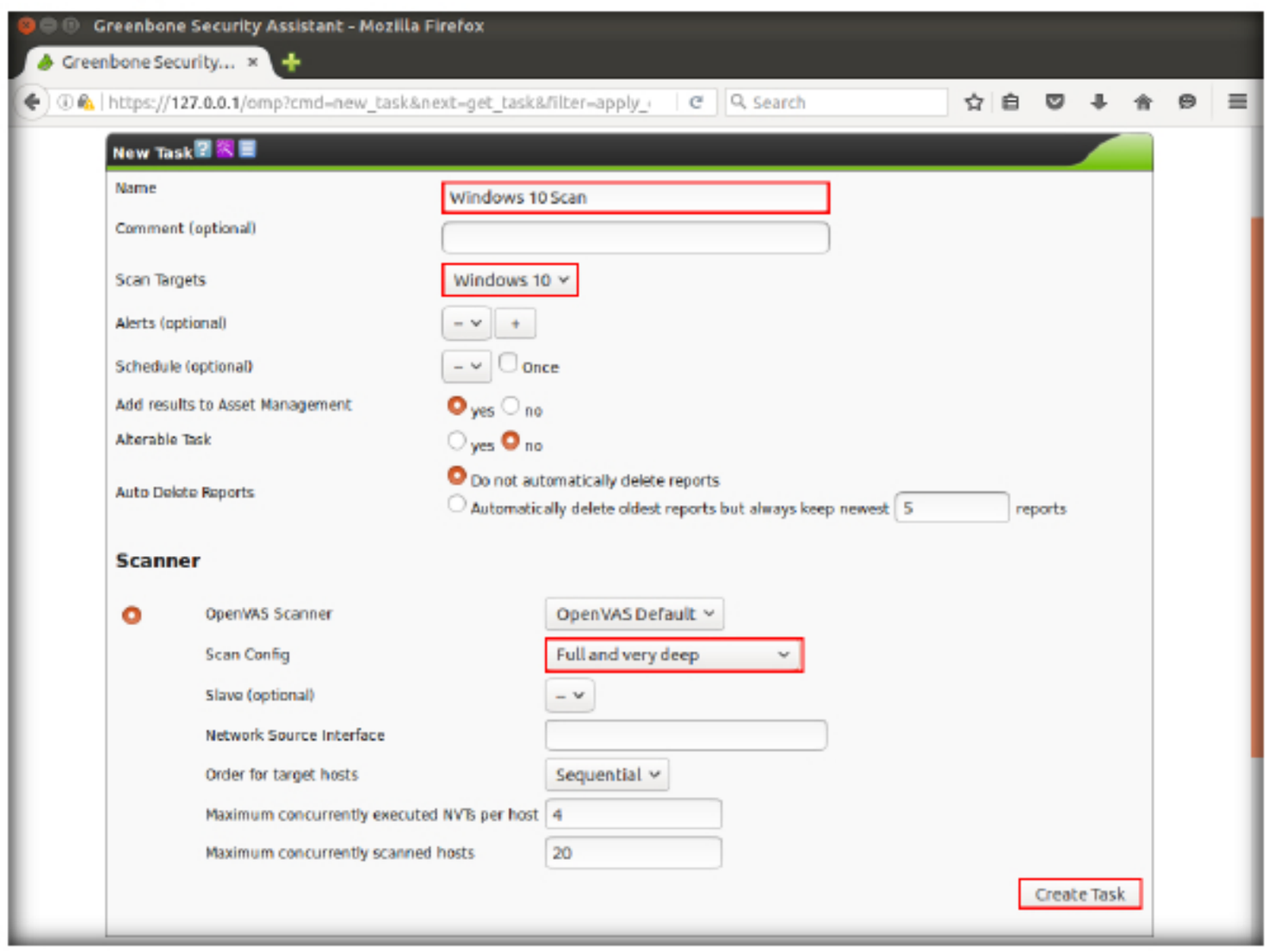


FIGURE 4.28: Entering name of the task

TASK 4

Starting Vulnerability Scan

30. The task named **Windows 10 Scan** has been successfully added to OpenVAS as shown in the screenshot. Begin a vulnerability scan by clicking the **Start** (Seventh (play symbol) icon in green color), in **Task Details**.

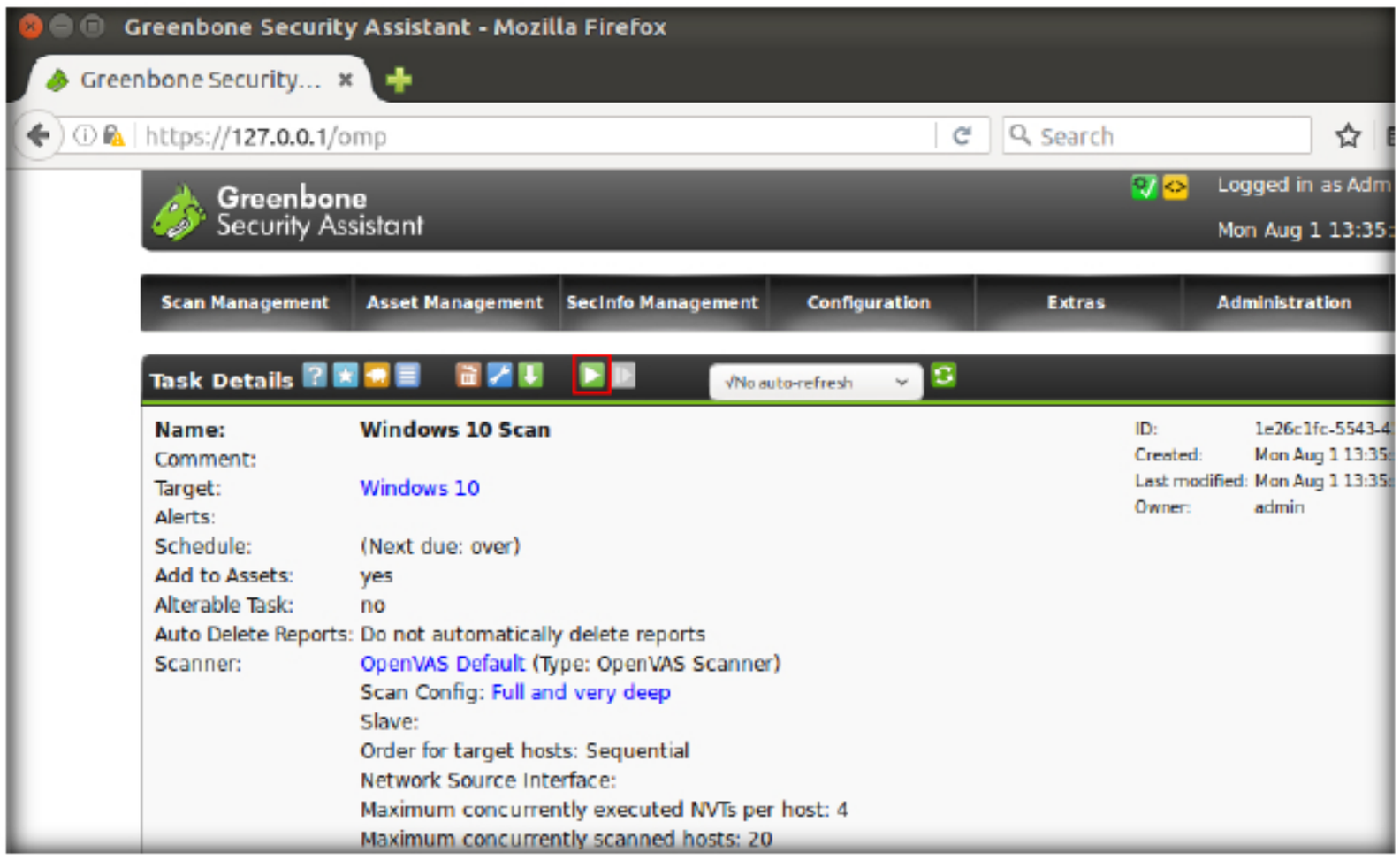


FIGURE 4.29: Task name is successfully added

31. The vulnerability scan has been initiated successfully. Now, select the **Refresh** every **30 Sec**. option from the drop down in the **Tasks** section and click the **Refresh** button. By doing this, the scan status will be updated every 30 seconds.

    Wait until the scan is completed, it will take approximately **5** to **10** Minutes to complete the scan.

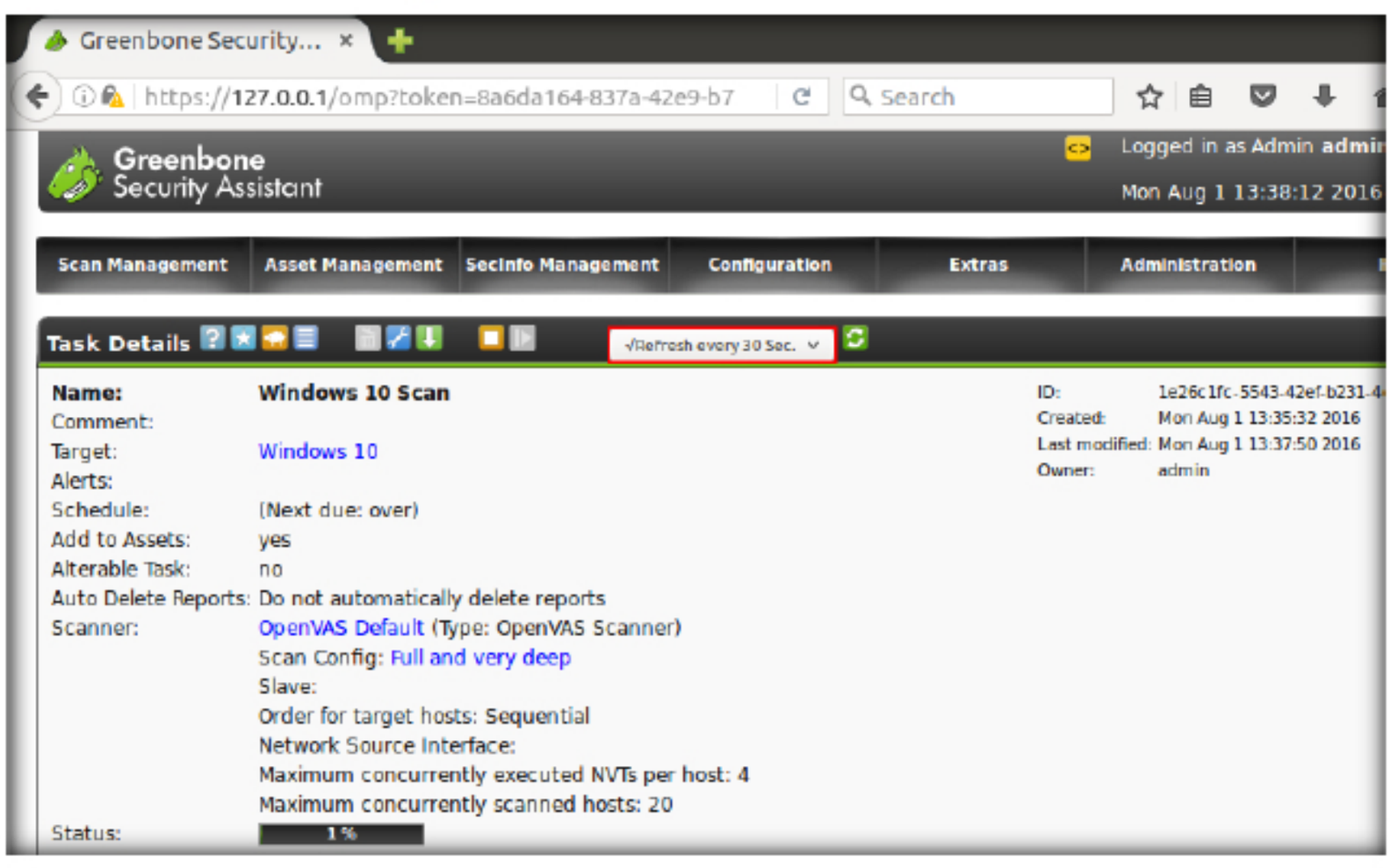


FIGURE 4.30: Scanning in progress

32. On completion of the scan, the status of the scan changes to Done as shown in the screenshot. Once this happens, change the Refresh every **30** Sec to **No auto refresh**.

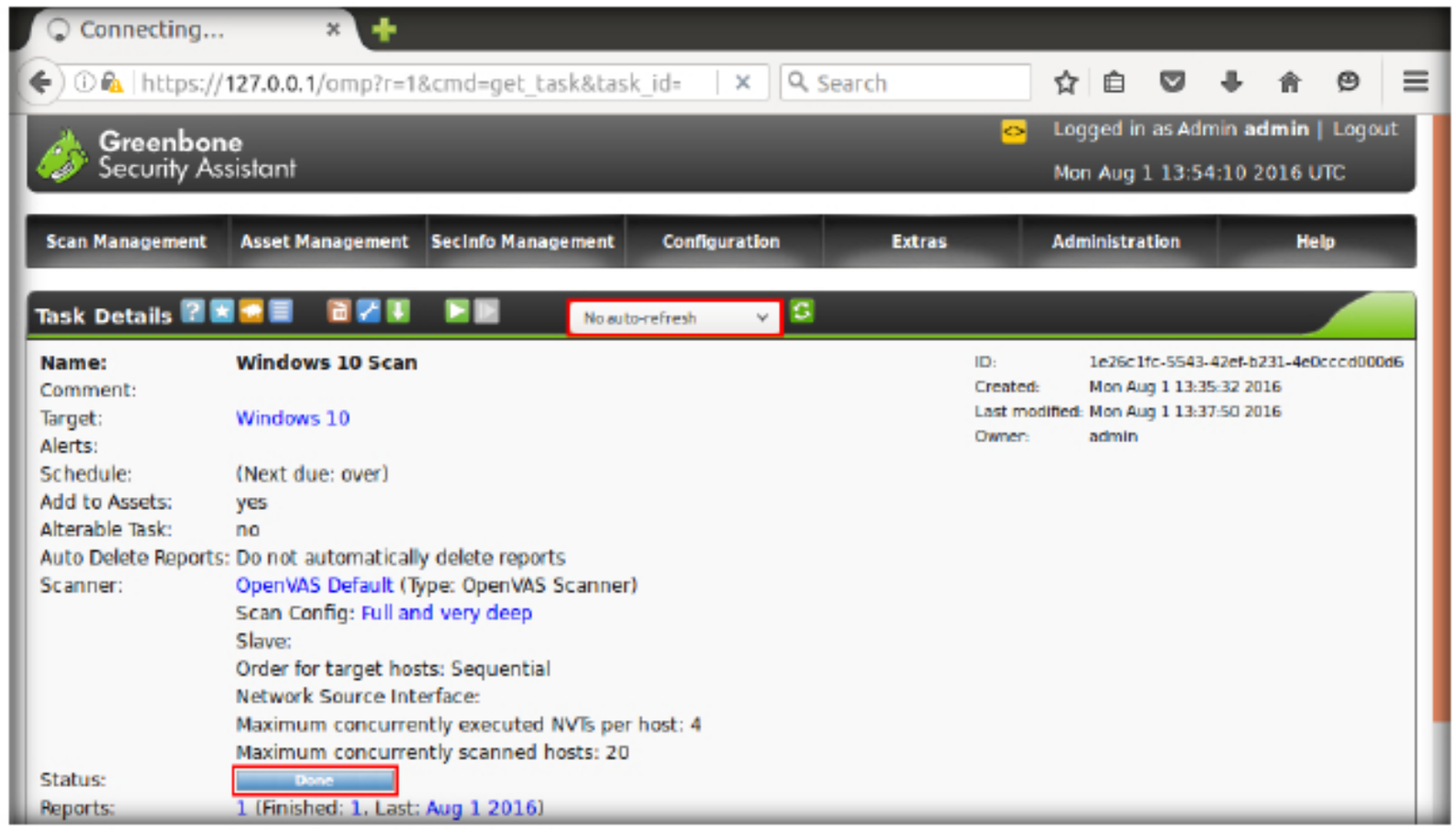


FIGURE 4.31: Scan completed

33. Click on the date link in the **Reports** section of the **Task Details**. The date displayed in this lab varies from your lab environment.

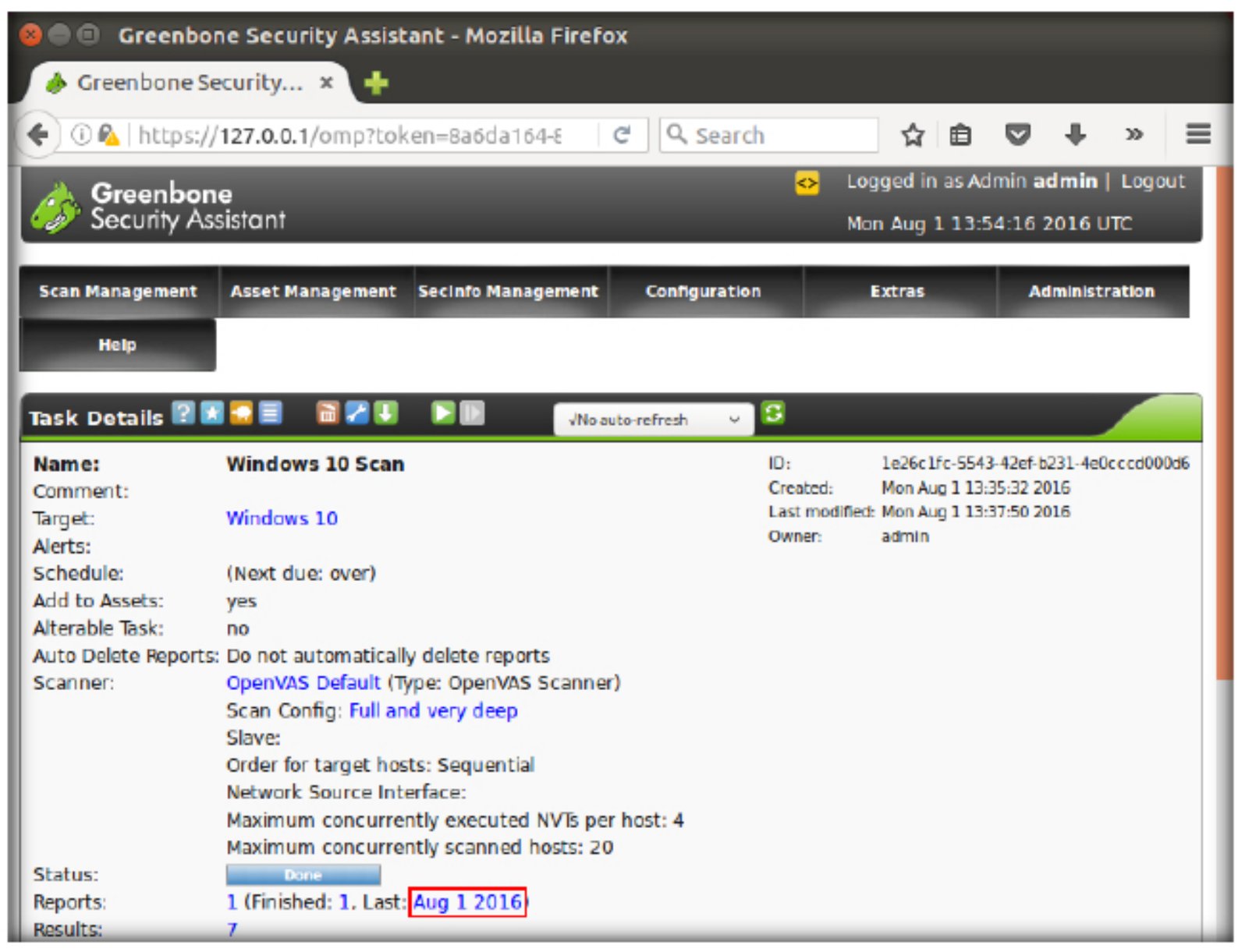


FIGURE 4.32: Date displayed

34. The results window appears as shown in the screenshot. This is where OpenVAS will display all the Vulnerabilities and their Severity levels.

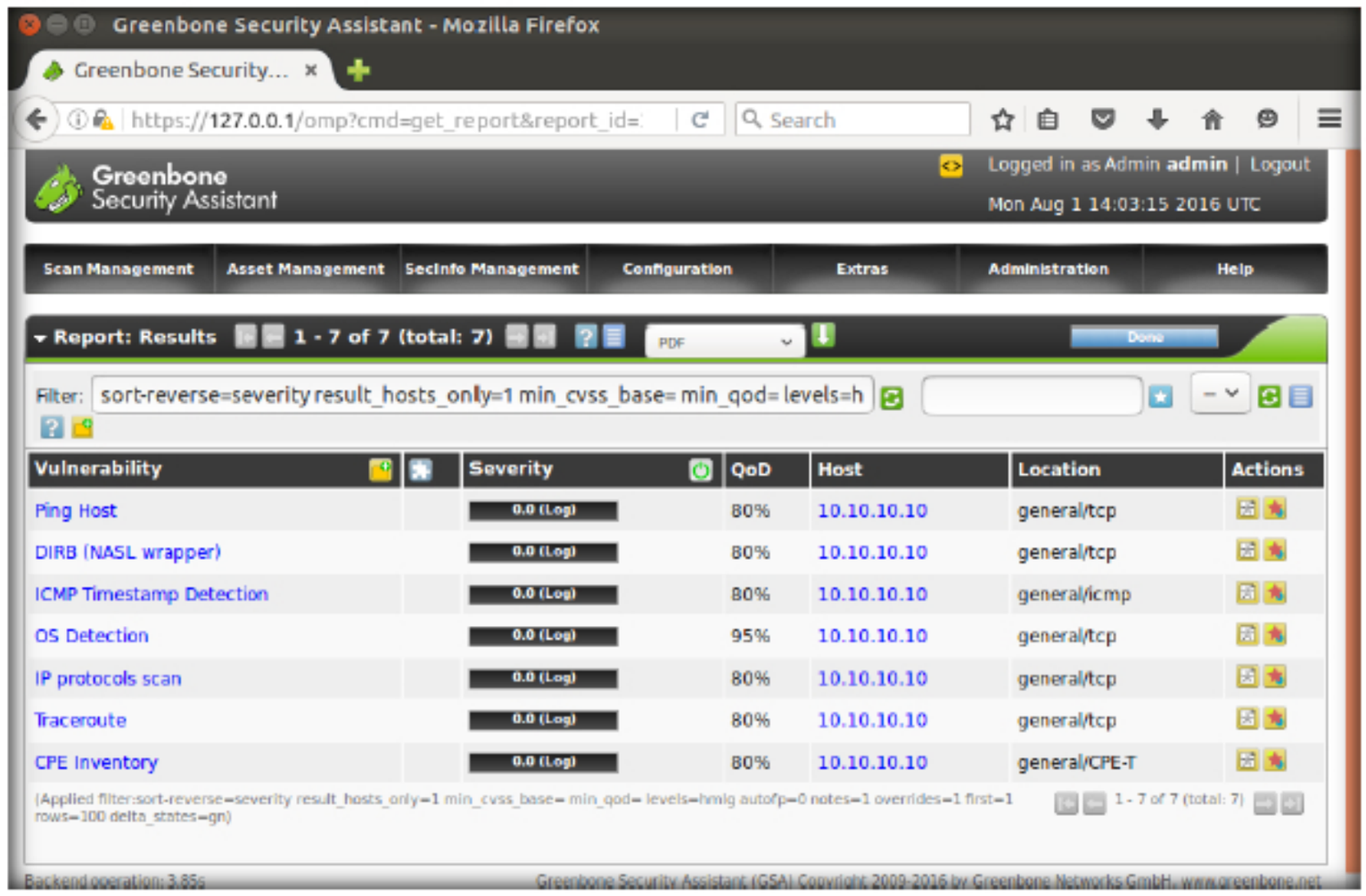


FIGURE 4.33: Vulnerability Report

35. Click on any of the vulnerabilities found. OpenVAS will show you a complete summary of the vulnerability and also provide a solution for it. As a network administrator, you have the ability to scan all the machines in your network. If any vulnerabilities are found, you will need to patch them.

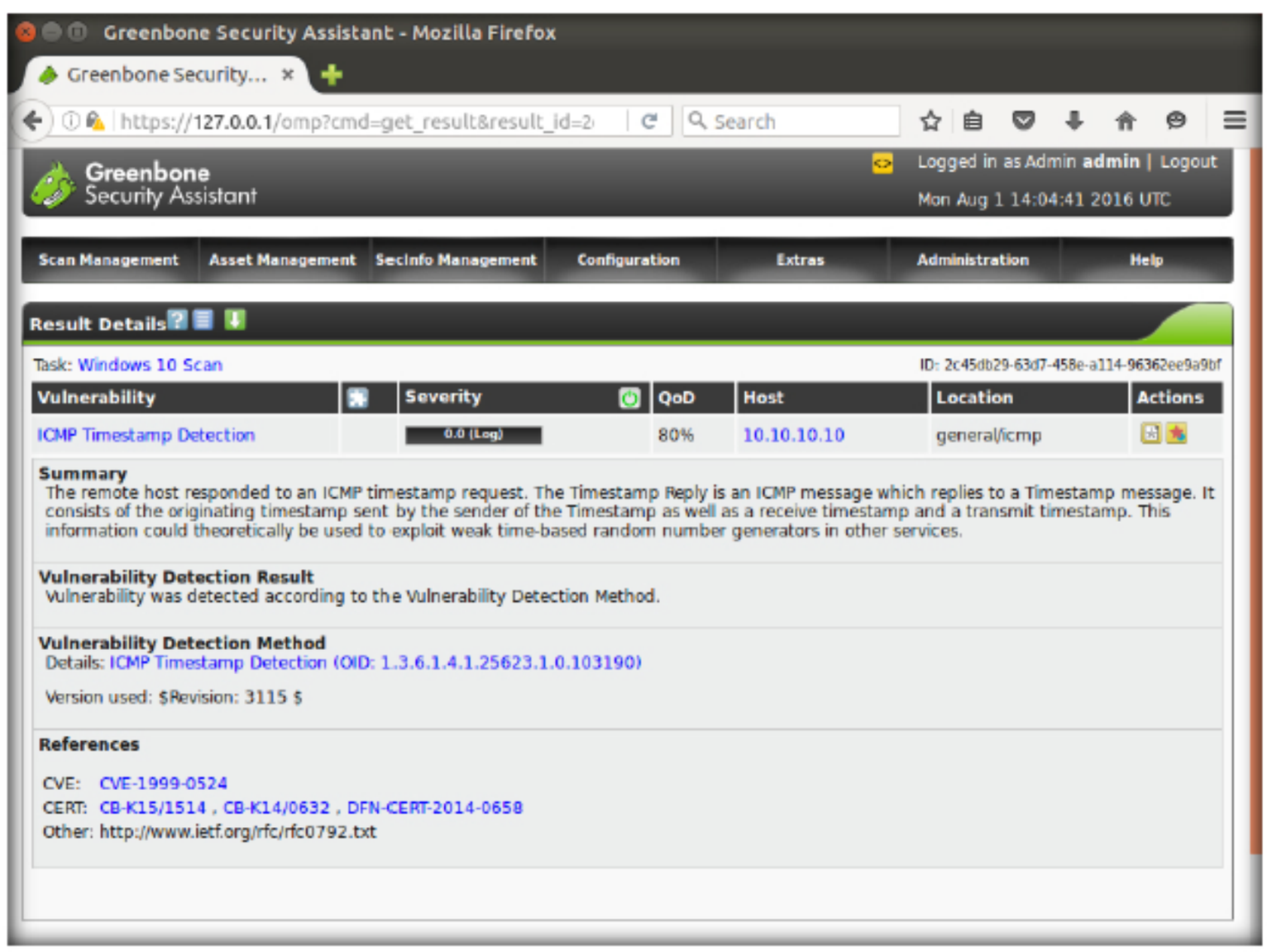


FIGURE 4.34: Summary of the vulnerability

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

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

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

Lab

5

Conducting a Vulnerability Assessment using OSSIM

OSSIM (Open Source Security Information Management) is an open source security information and event management system

Lab Scenario

An organization's infrastructure may contain a large number of hosts deployed on its network. As the number of hosts increase, threats to the organization's data also increase since there are additional chances hosts are running deprecated versions of operating systems. Other issues include one or more hosts affected by malware such as Trojans, virus, worms, etc. As a network defense architect, it is essential to perform vulnerability scanning on the target network, find the vulnerabilities and resolve them.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Objectives

The objective of this lab is to help students understand how to perform vulnerability scanning on a system/network using OSSIM.

Lab Environment

To carry out the lab, you need:

- OSSIM virtual machine
- A virtual machine running Windows Server 2008
- A Web browser with an Internet connection
- **Administrative** privileges to run tools

Lab Duration

Time: 35 Minutes

Overview of Vulnerability Scanning

The vulnerability scanning is a process of scanning a single or several hosts on a network and identifying their flaws.

Lab Tasks

TASK 1

Logon to OSSIM

1. Before starting this lab, make sure both the Windows 10 and the Windows Server 2008 machines are turned on.
2. Power on the OSSIM virtual machine from the VMware workstation and wait until the log in screen appears.
3. Once the log in screen appears, type **root** in the alienvault login field and press **Enter**. In the password field type **toor** as the password and press **Enter**.

   Note: The password is not visible.

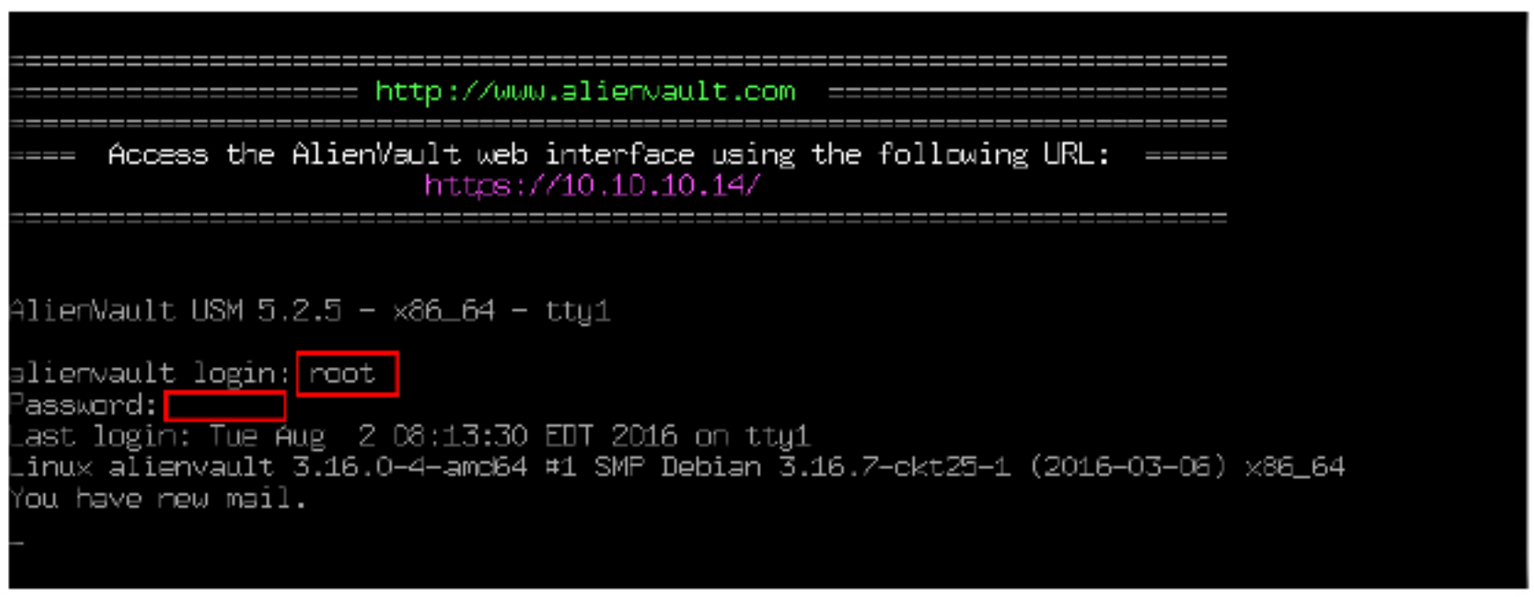


FIGURE 5.1: OSSIM Login Window

4. Launch the Windows Server 2012 machine and log in. Now close the Server Manager window and open a web browser. In this lab we are using the Chrome browser.

   Note: If you are using a different browser the screenshots may differ in your lab environment.

5. Type https://10.10.10.14 and press Enter in the address bar of the browser.

6. The OSSIM Login page appears. Enter **admin** in the USERNAME field, **qwerty@123** in the PASSWORD field then click LOGIN.

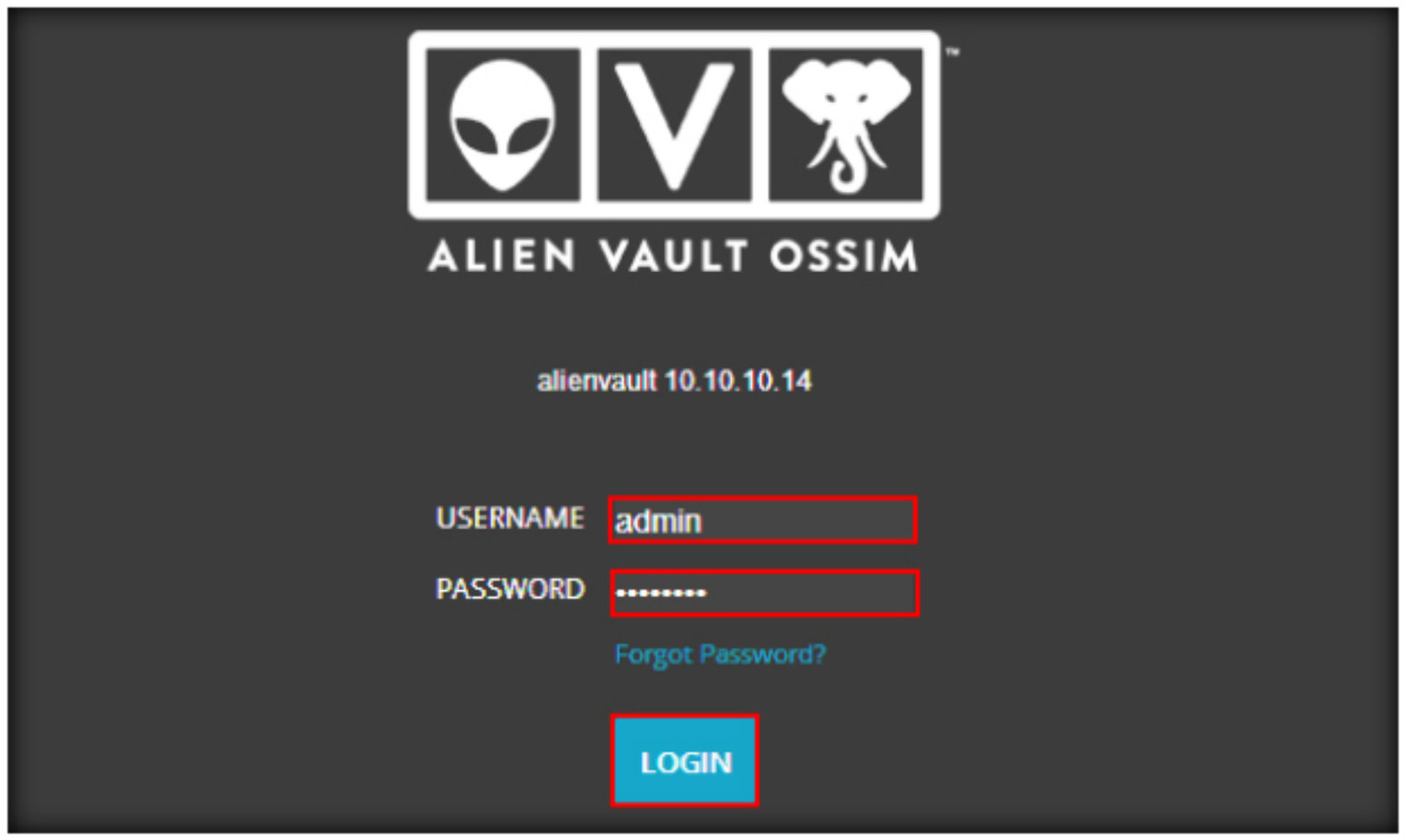


FIGURE 5.2: Logging in to Alien Vault

TASK 2

Perform a Vulnerability Scan

7. To check the vulnerabilities present (if any), hover the mouse on **ENVIRONMENT** and select **VULNERABILITIES**.

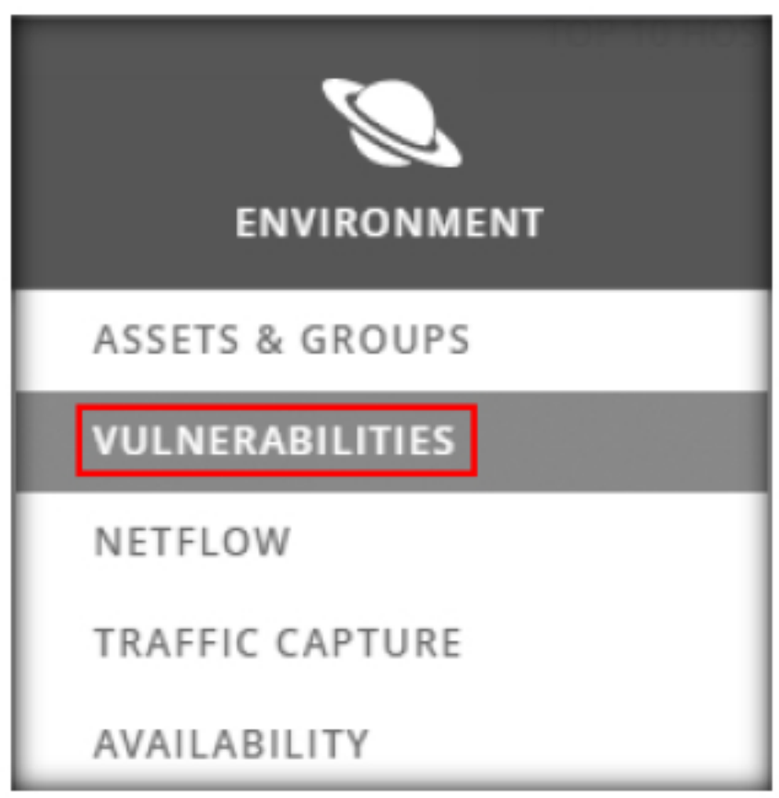


FIGURE 5.3: Navigating to Vulnerability

8. Scroll down and expand CURRENT VULNERABILITIES. Click NEW SCAN JOB.

FIGURE 5.4: Navigating to New Scan

9. The **CREATE SCAN JOB** appears. Provide a **Job Name**:

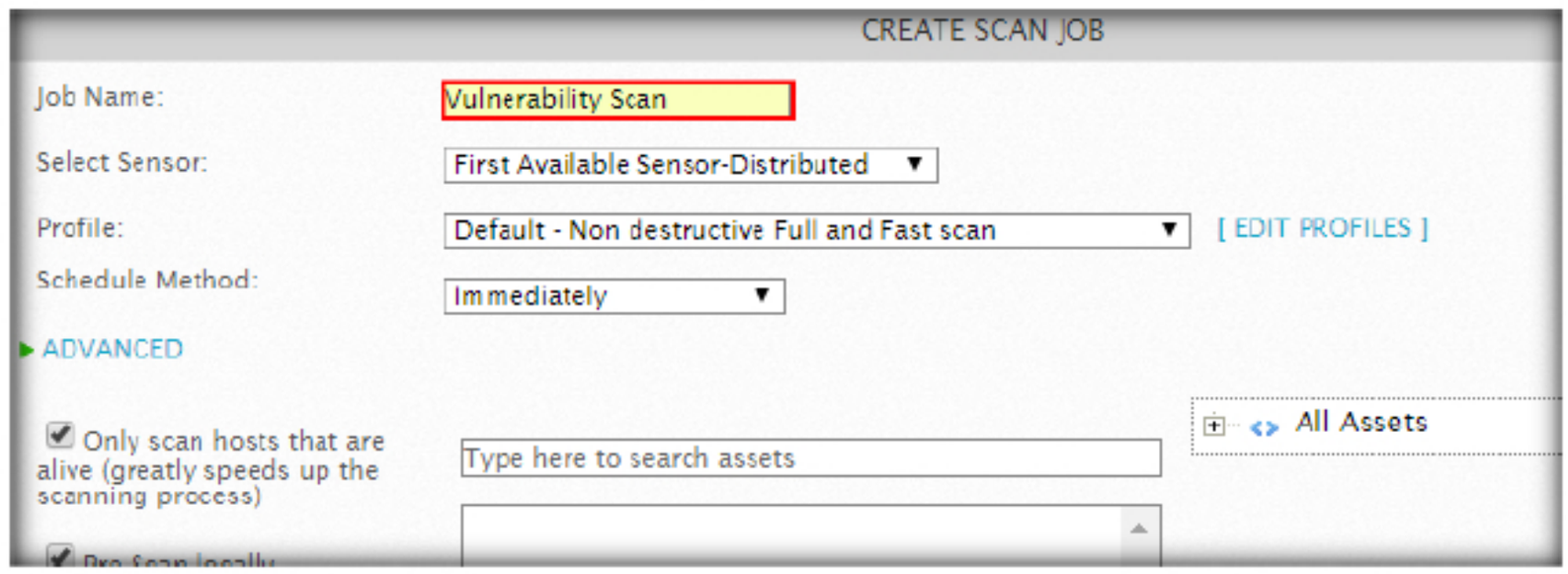


FIGURE 5.5: Providing the Scan a Name

10. Expand **All Assets**, **Assets**, **10.10.10** and select **10.10.10.8** and Click **Save**.

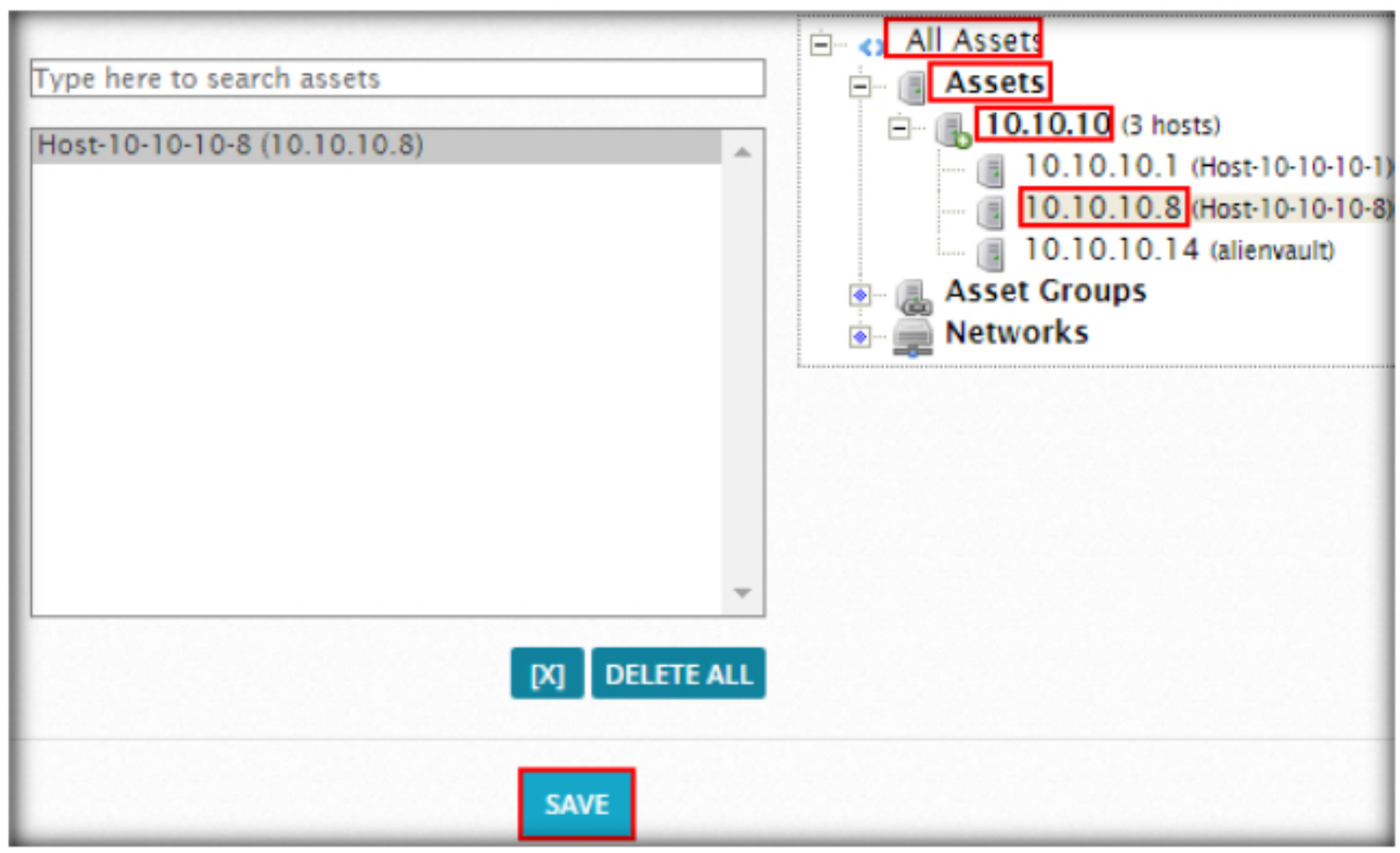


FIGURE 5.6: Saving the Scan

11. You can see the new scan job created and the time at which it will be launched. Wait until the vulnerability scan completes.

FIGURE 5.7: New Scan Created

12. Once the scan is completed you will see the Completed status as shown in the screenshot.
13. You may see a few options in the ACTION section, where you can change the owner and pull out the vulnerability scan report in different formats.
14. Now, we are going to view the scan report by clicking on the pdf icon in the ACTION section.

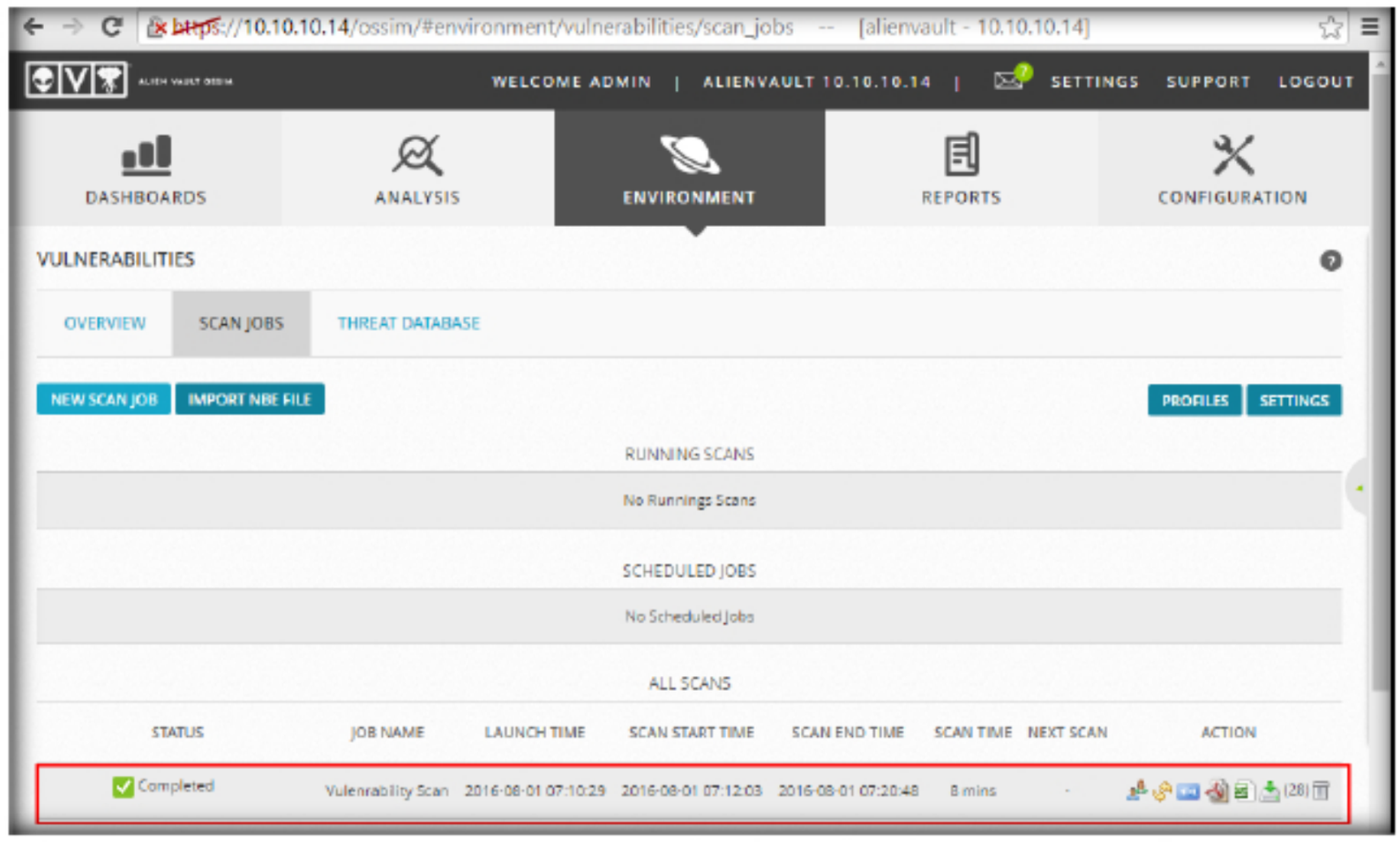


FIGURE 5.8: New Scan Created

15. Once you click on the pdf icon under the ACTION section, a new tab opens in the browser window with a detailed report. Scroll down to view the entire report.

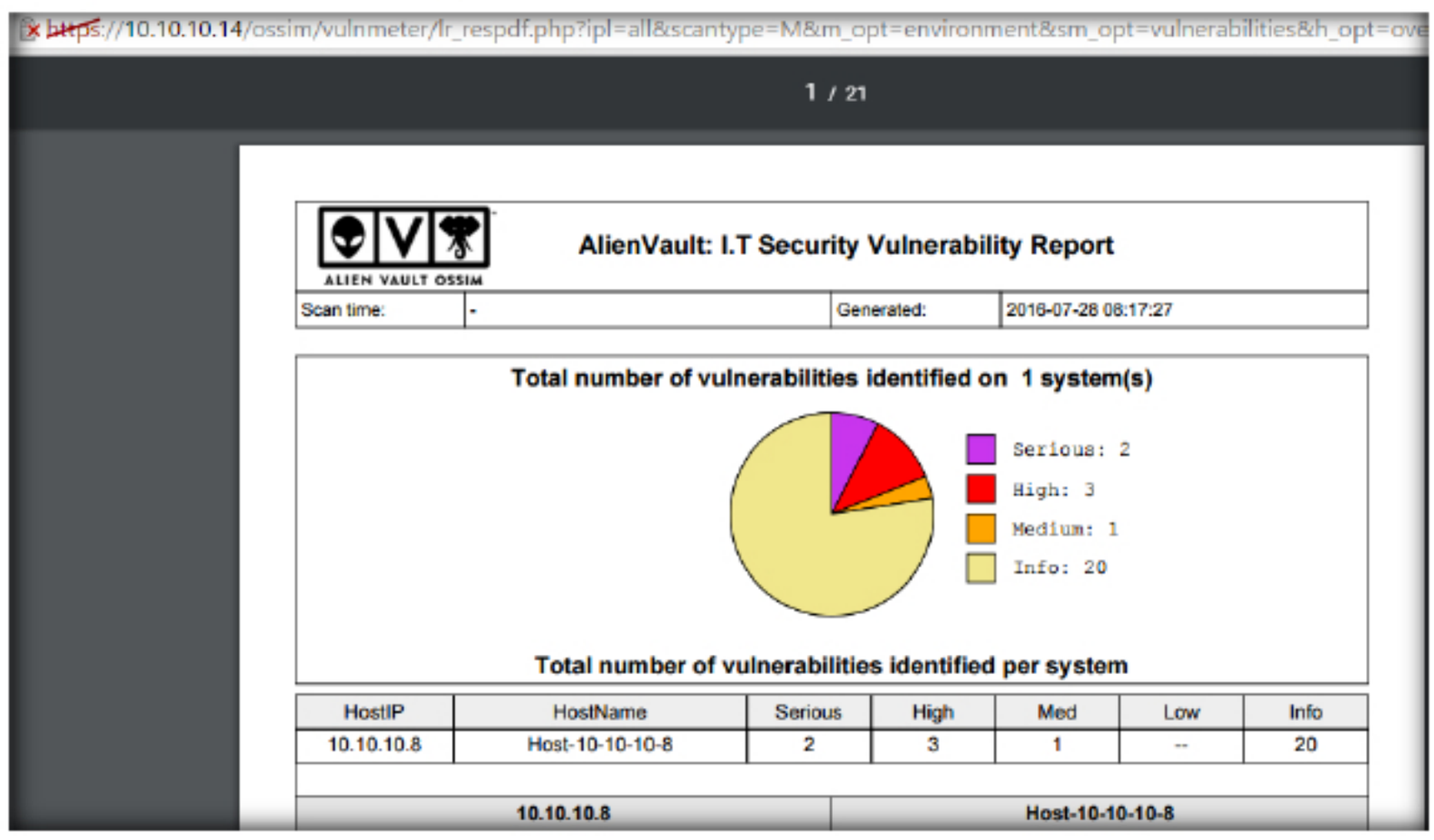


FIGURE 5.9: Detailed vulnerability Report

16. Double-click on the scan to view the scan report. You will see the Vulnerability pie chart with the different types of vulnerabilities found.

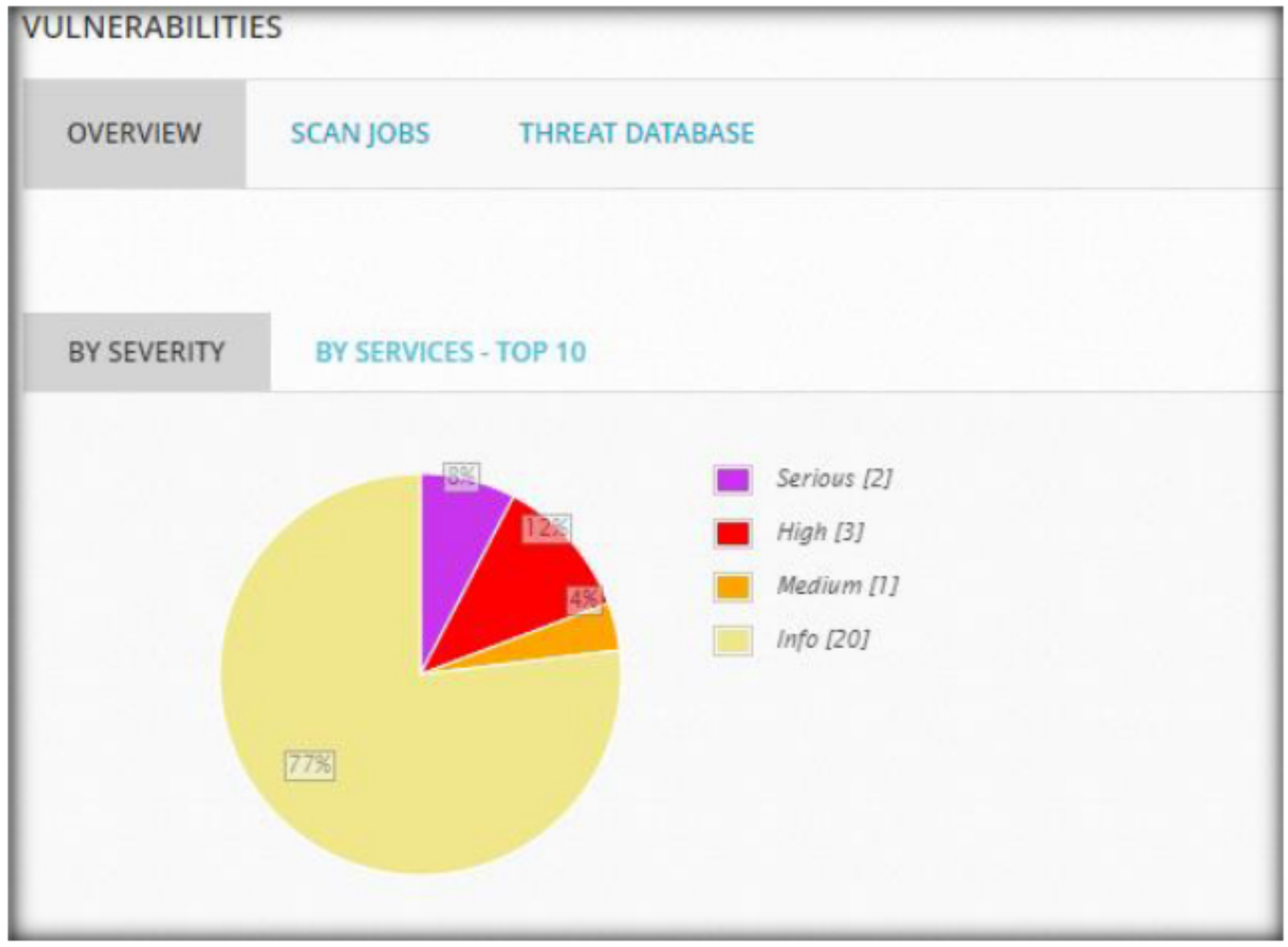


FIGURE 5.10: Vulnerabilities in 10.10.10.8

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

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

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