Vulnerability Analysis

Module 05

Vulnerability Assessment

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand an assault. Vulnerability research is the process of discovering vulnerabilities and design flaws that leave an OS and its applications open to attack or misuse.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Earlier, all possible information about a target system such as system name, OS details, shared network resources, policies and passwords details, and users and user groups were gathered.

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Additionally, it assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

The information gleaned from a vulnerability assessment helps you to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

The labs in this module will give you real-time experience in collecting information regarding underlying vulnerabilities in the target system using various online sources and vulnerability assessment tools.

Lab Objectives

The objective of this lab is to extract information about the target system that includes, but not limited to:

- Network vulnerabilities
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and services that are listening
- Application and services configuration errors/vulnerabilities
- The OS version running on computers or devices
- Applications installed on computers
- Accounts with weak passwords

- Files and folders with weak permissions
- Default services and applications that may have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Vulnerability Assessment

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute vulnerability assessment.

Network vulnerability scanning can be categorized into active scanning and passive scanning:

- **Active Scanning**: Interacts directly with the target network to find vulnerabilities by sending probes and specially crafted requests to the target host in the network
- **Passive Scanning**: Finds vulnerabilities without directly interacting with the target network and identifying vulnerabilities via information exposed by systems in their normal communications

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the underlying vulnerability in a target system or network. Recommended labs that will assist you in learning various vulnerability assessment techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Vulnerability Research with Vulnerability Scoring Systems and Databases	√	√	√
	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)	√		√
	1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)		√	√
	1.3 Perform Vulnerability Research in National Vulnerability Database (NVD)		√	√
2	Perform Vulnerability Assessment using Various Vulnerability Assessment Tools	√	√	√
	2.1 Perform Vulnerability Analysis using OpenVAS	√		√
	2.2 Perform Vulnerability Scanning using Nessus		√	√
	2.3 Perform Vulnerability Scanning using GFI LanGuard		√	√
	2.4 Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

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

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

Lab 1

Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Vulnerability scoring systems and databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and risk associated with identified vulnerabilities.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)
- Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
- Perform vulnerability research in National Vulnerability Database (NVD)

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerability scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)

Lab Tasks

TASK 1

Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Here, we will use CWE to view the latest underlying system vulnerabilities.

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

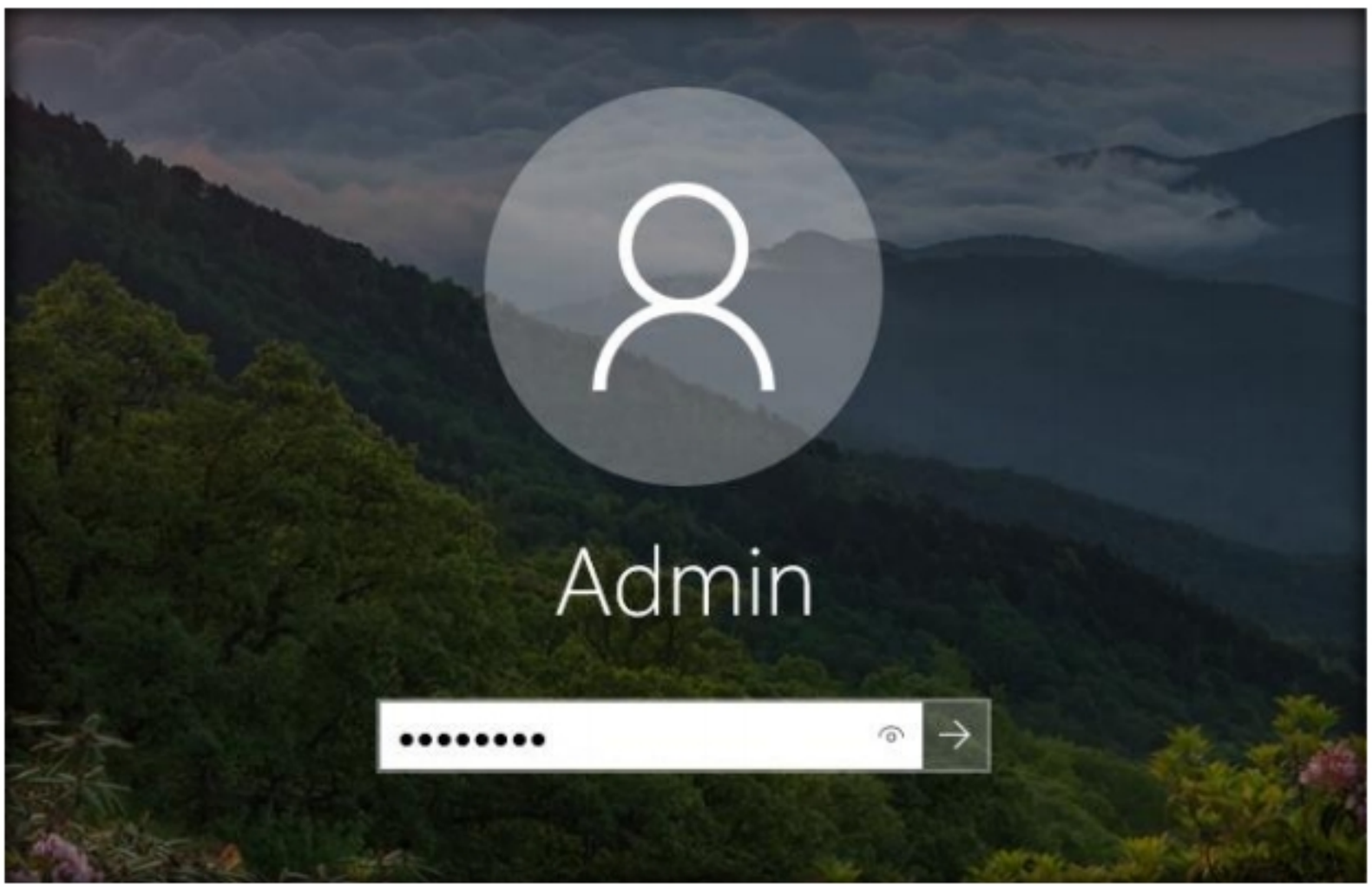


Figure 1.1.1: Login window

Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts

2. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://cwe.mitre.org/**.

Note:

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
- If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.

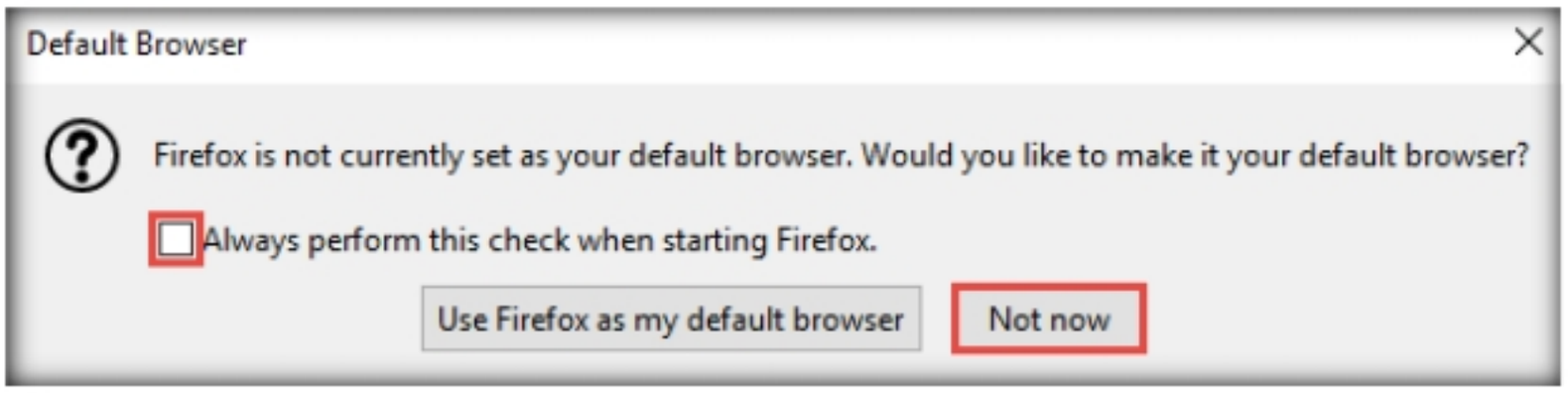


Figure 1.1.2: Default browser pop-up window

3. **CWE** website appears. In the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search ( ) icon.

Note: Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

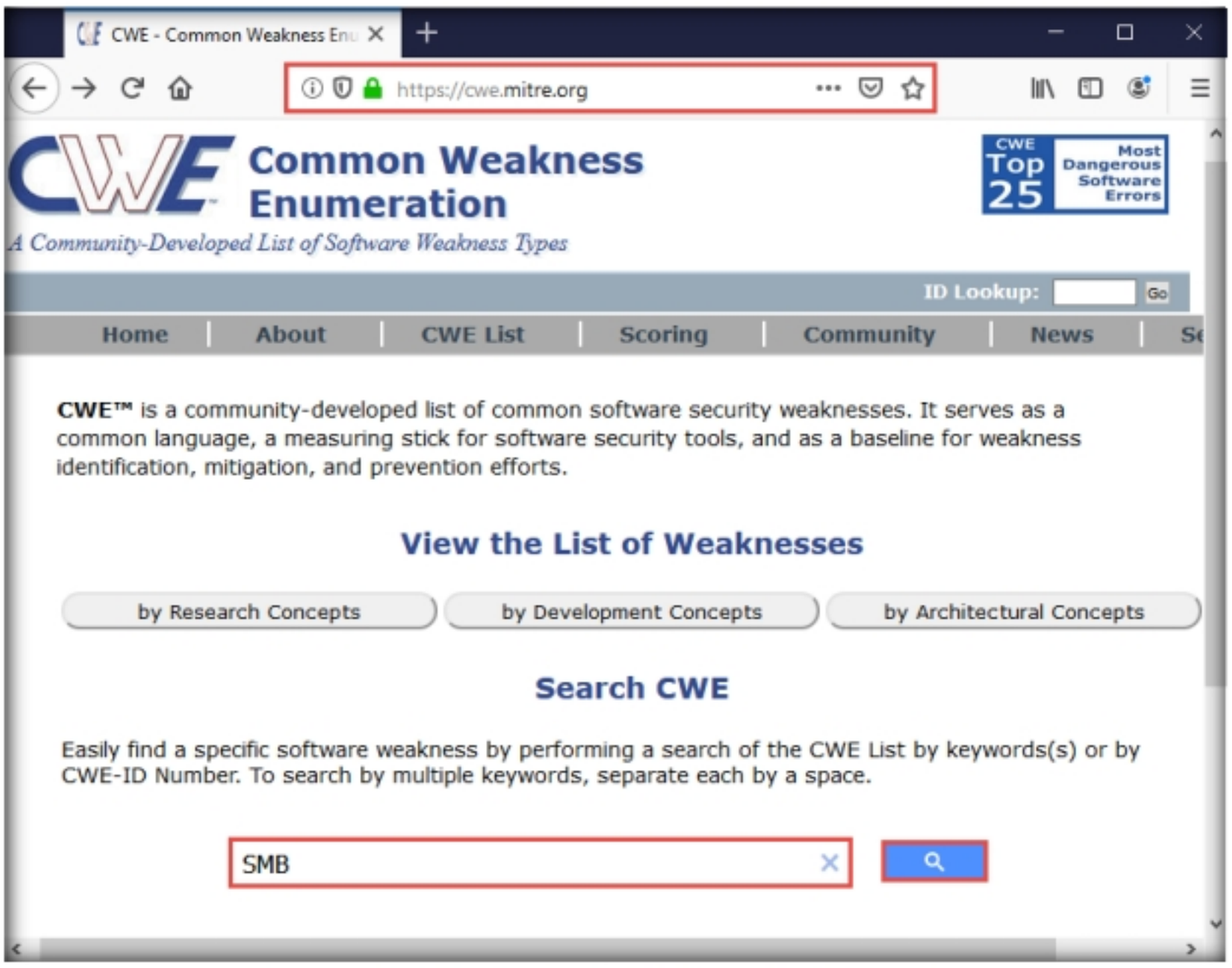


Figure 1.1.3: CWE website: searching for vulnerabilities in the service

4. The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

Note: The search results might differ in your lab environment.

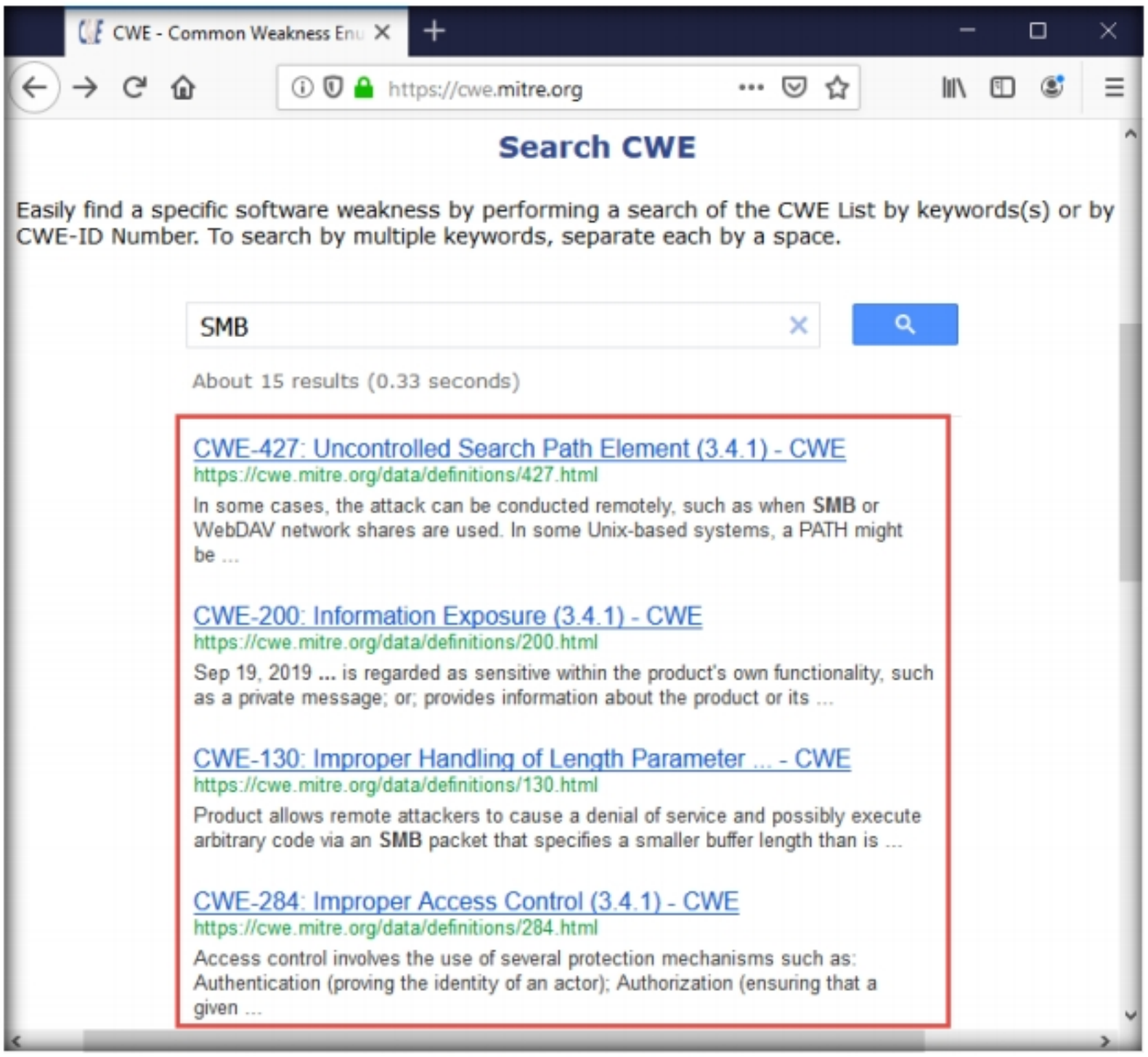


Figure 1.1.4: CWE search result

5. Now, click any link (here, **CWE-427**) to view detailed information about the vulnerability.
6. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.

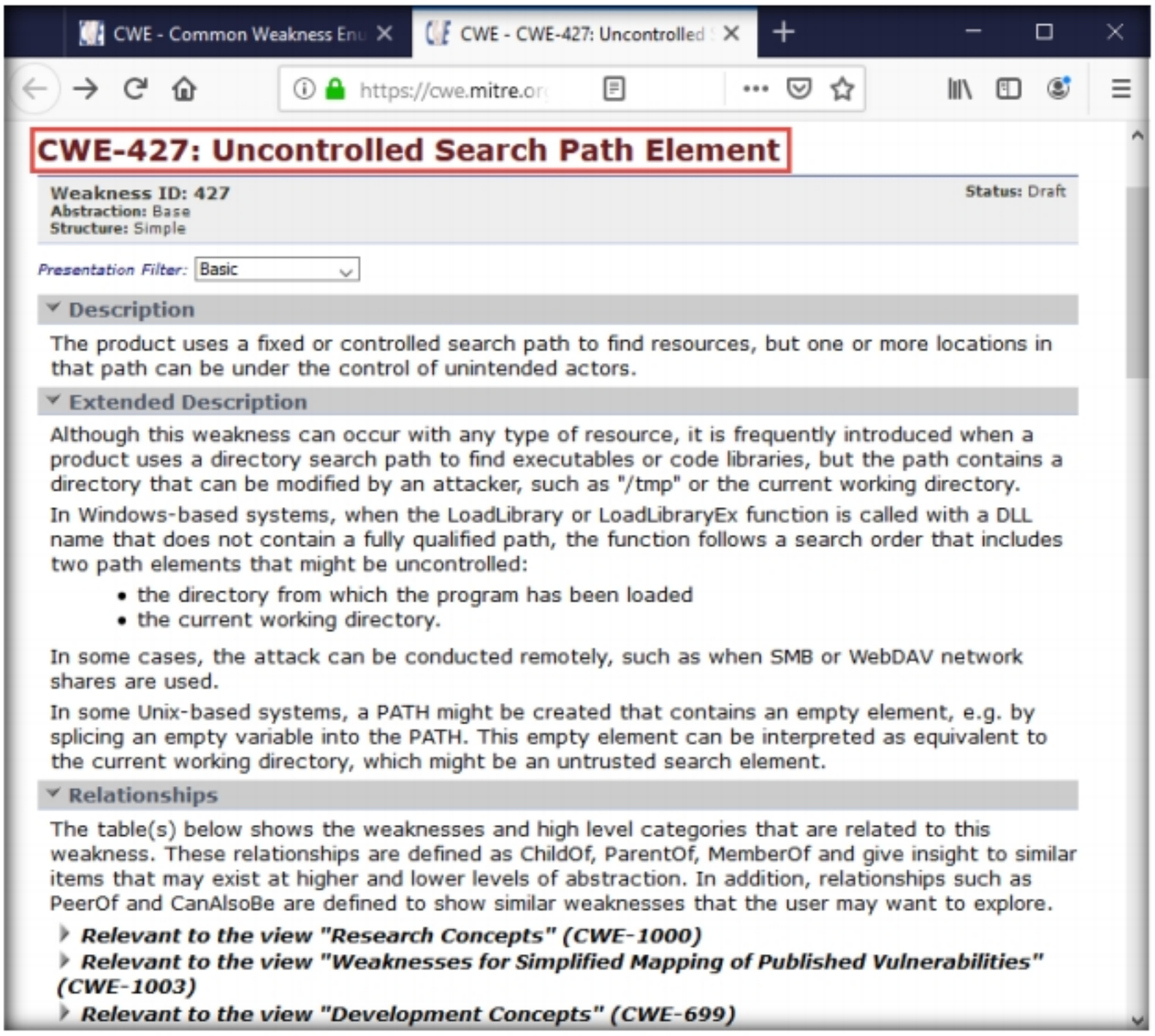


Figure 1.1.5: CWE: vulnerability information

7. Similarly, you can click on other vulnerabilities and view detailed information.

8. Now, navigate back to the **CWE** website, scroll down, and click the **CWE List** link present below the searched results.

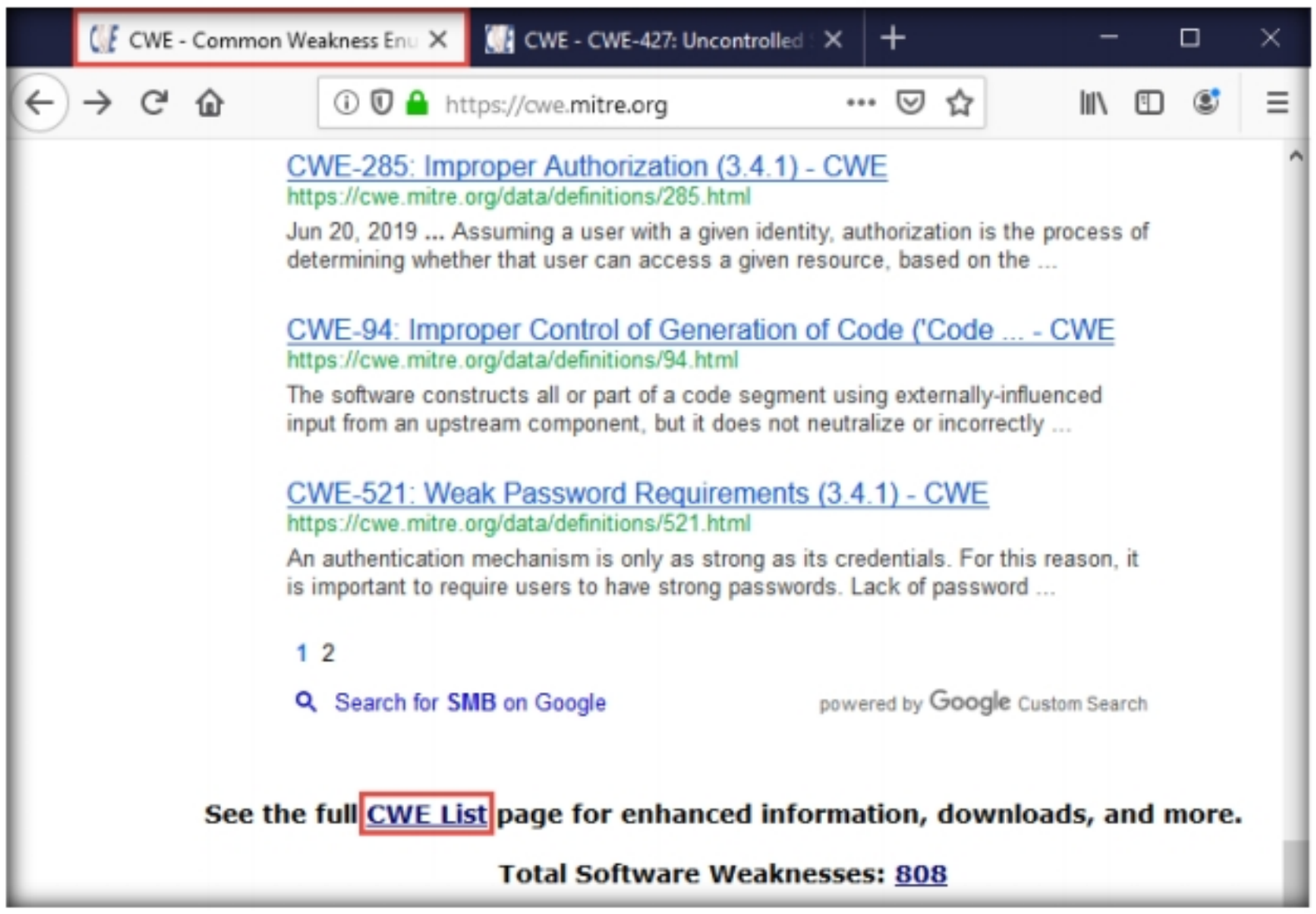


Figure 1.1.6: CWE click on CWE List

9. A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2019)**.

Note: Result might differ.

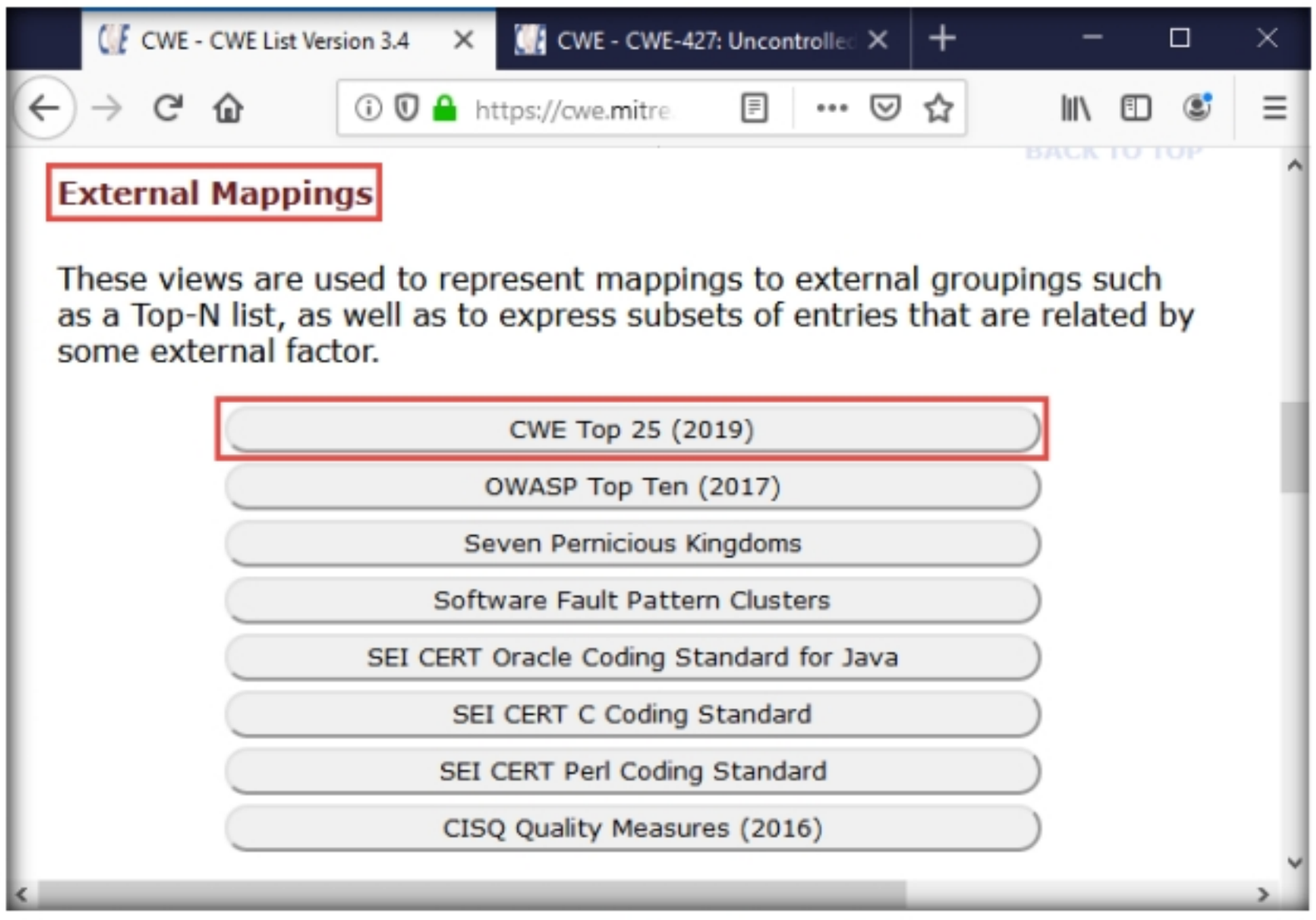


Figure 1.1.7: CWE: click on CWE Top 25 (2019)

10. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors**. Scroll down and view a list of **Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors** under the **Relationships** section. You can click on each weakness to view detailed information on it.

Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

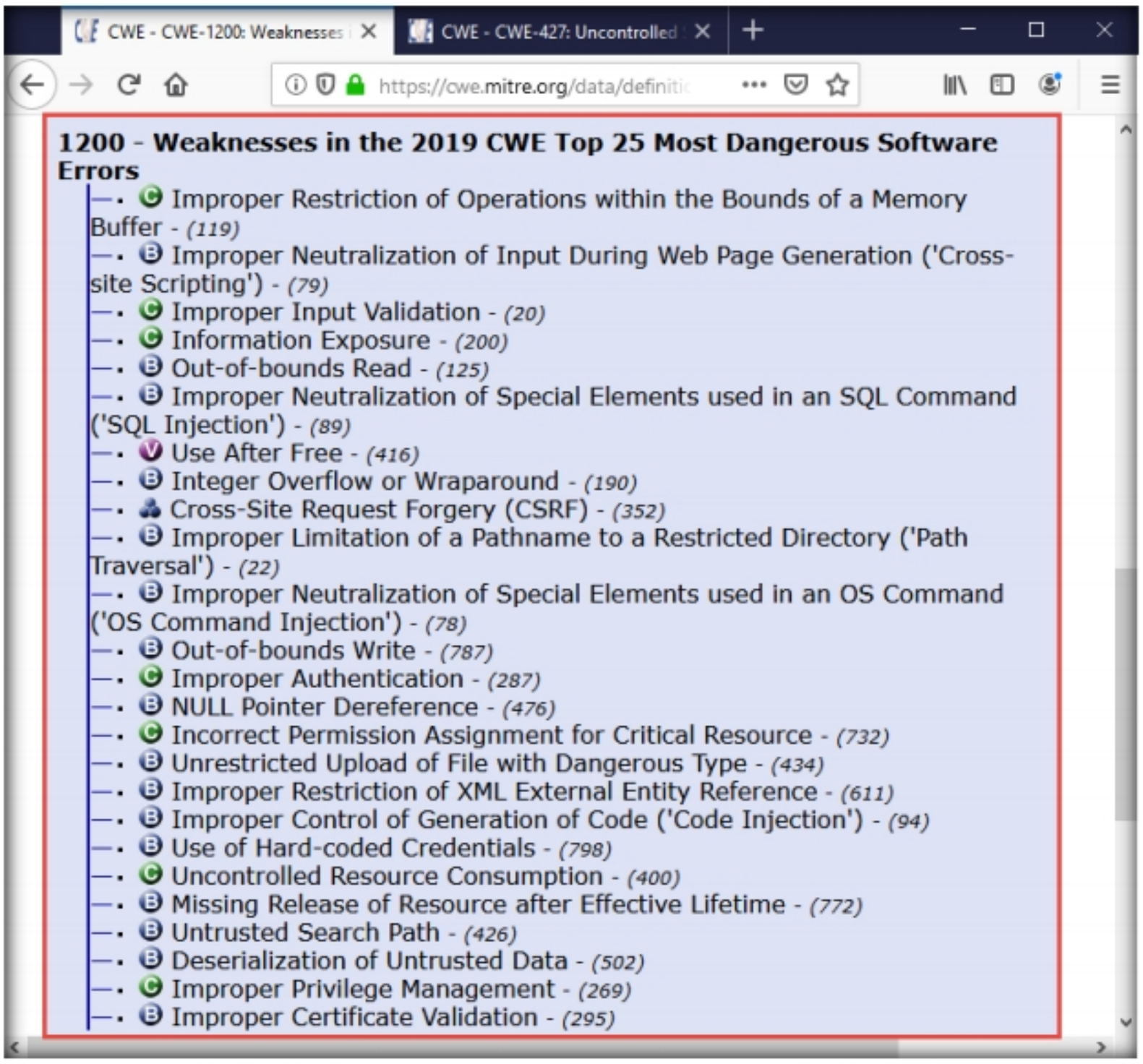


Figure 1.1.8: CWE: CWE Top 25 result

11. Similarly, you can go back to the CWE website and explore other options, as well.
12. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
13. Close all open windows and document all the acquired information.

TASK 2

Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

Here, we will use CVE to view the latest underlying system and software vulnerabilities.

Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://cve.mitre.org/**.
2. **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

Note: The results might differ in your lab environment.

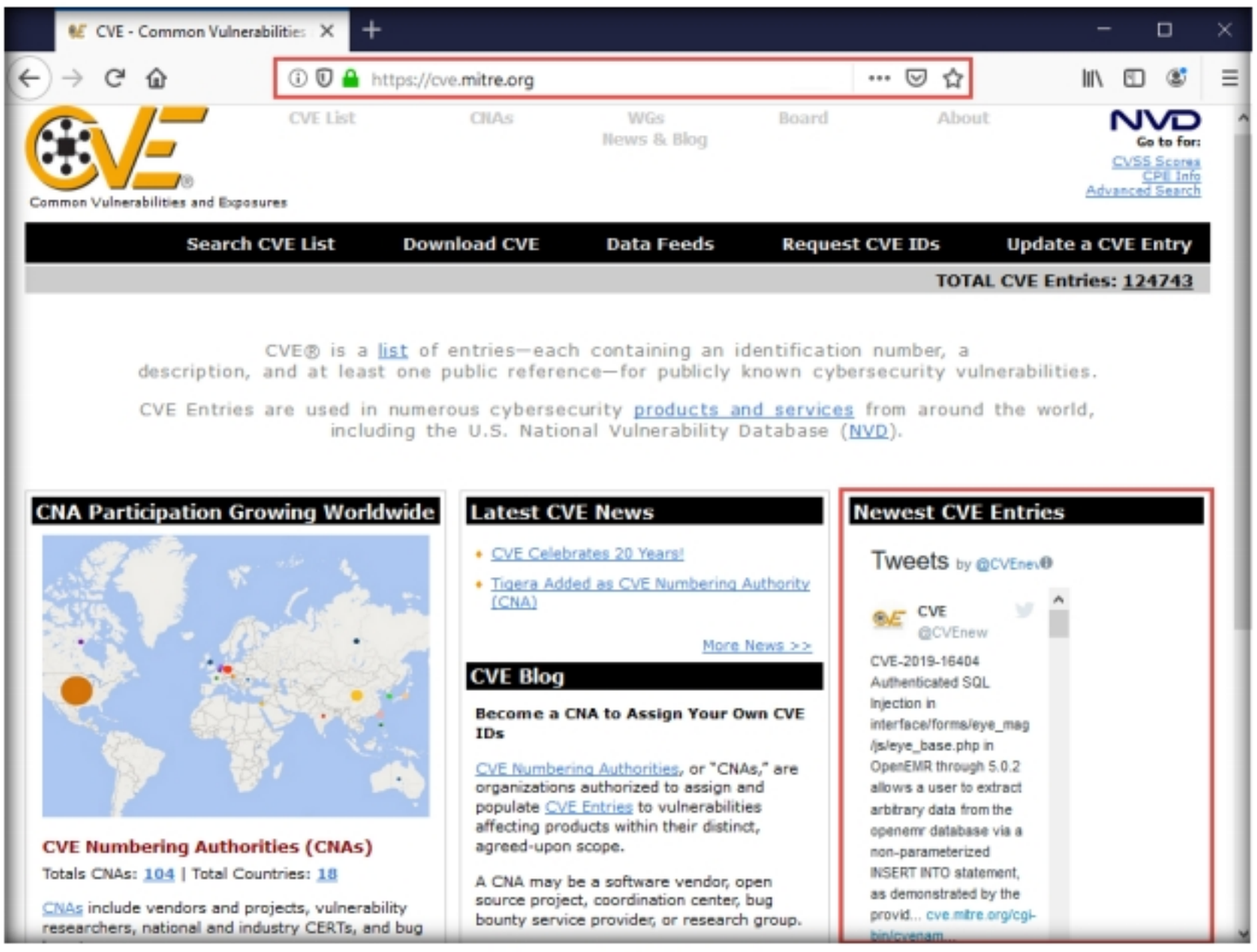


Figure 1.2.1: CVE website

3. You can copy the name of any vulnerability under the **Newest CVE Entries** section and search on CVE to view detailed information on it. (here, we are selecting the vulnerability **CVE-2019-16404**)
4. Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2019-16404**) in the search bar, and click **Submit**.

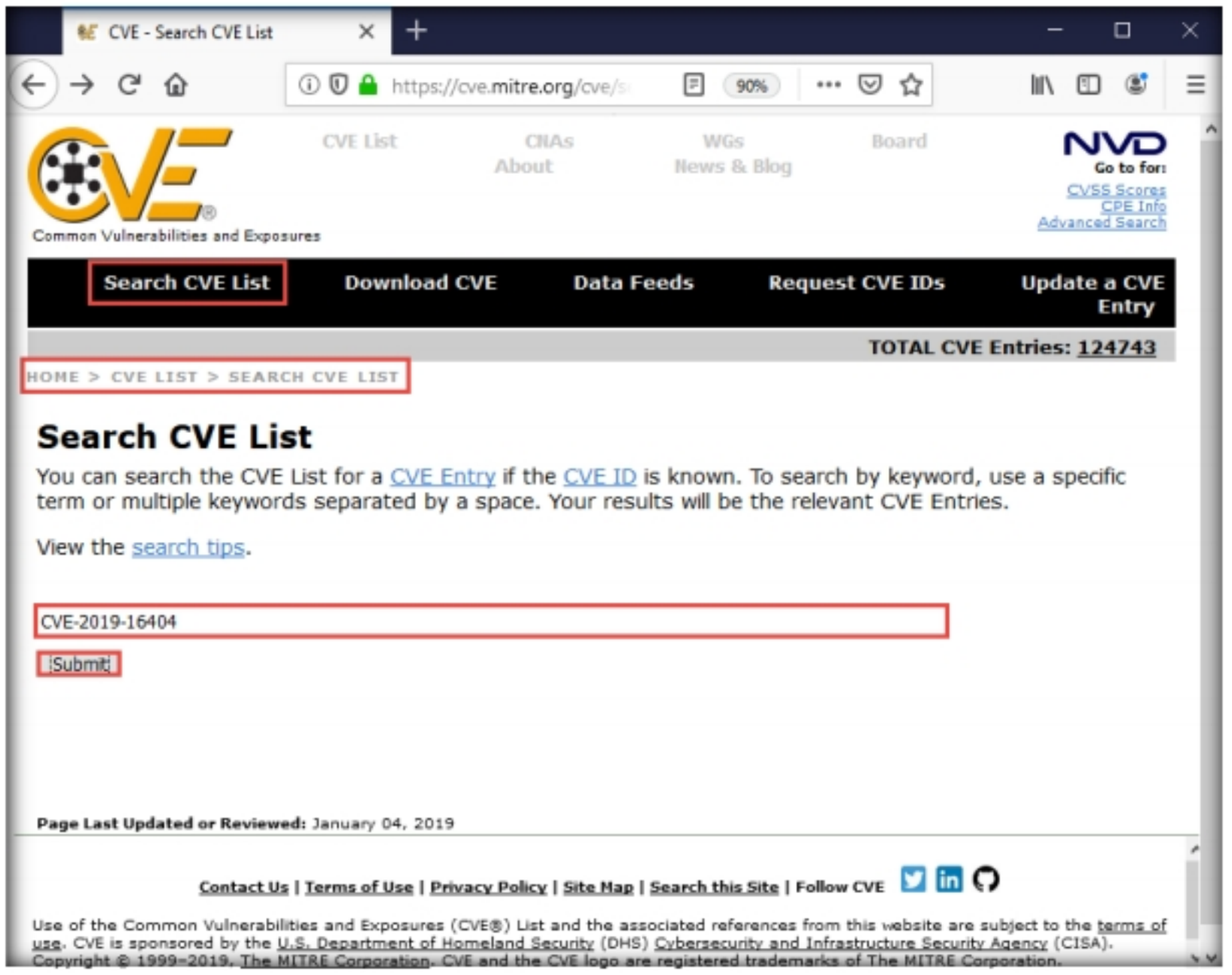


Figure 1.2.2: CVE - Search CVE List

5. **Search Results** page appears, displaying the information regarding the searched vulnerability. You can click the vulnerability link to view further detailed information regarding the vulnerability.

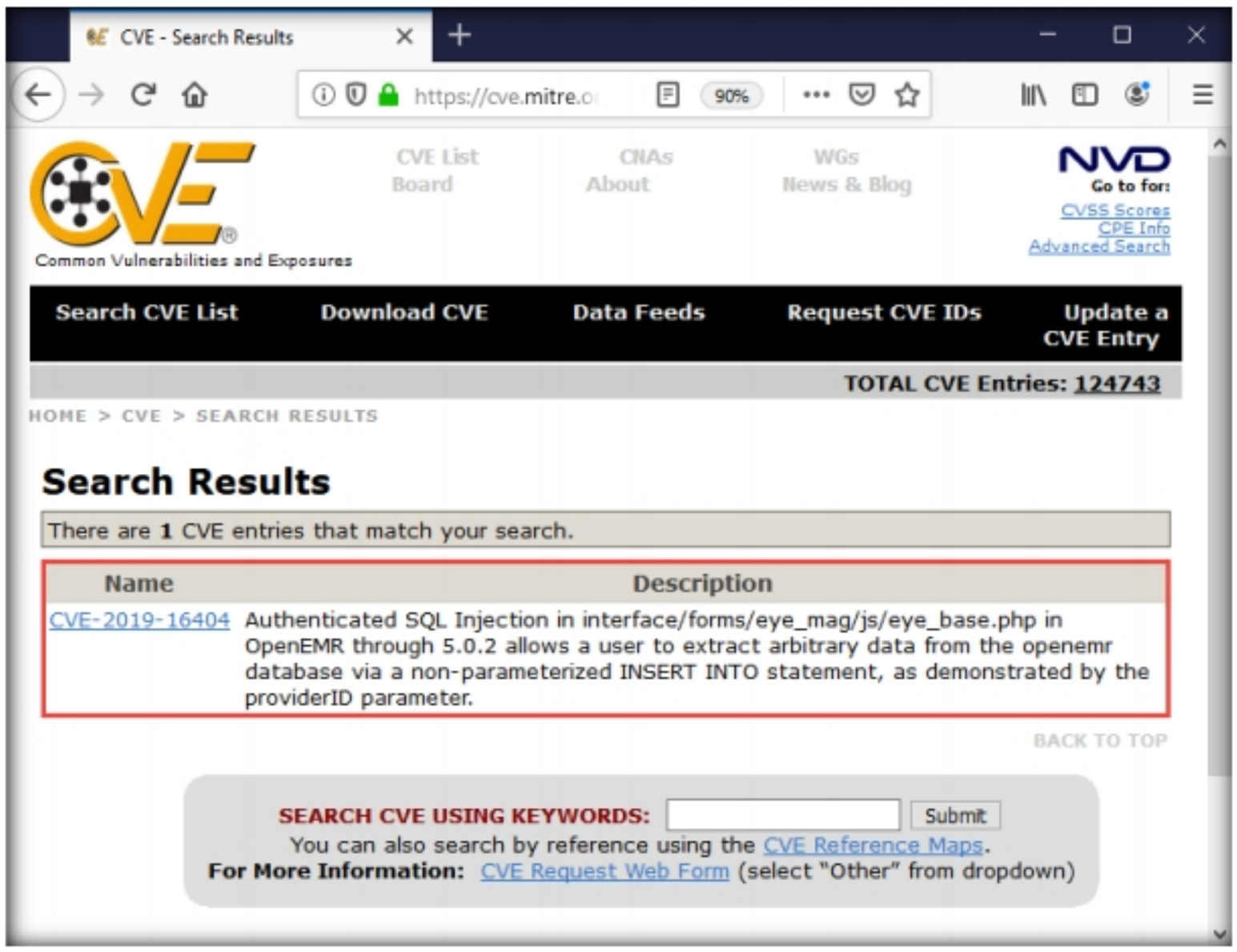


Figure 1.2.3: CVE - Search Results

6. Similarly, in the **Search CVE List** section, you can search for a service-related vulnerability by typing the service name (here, **SMB**) and click **Submit**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

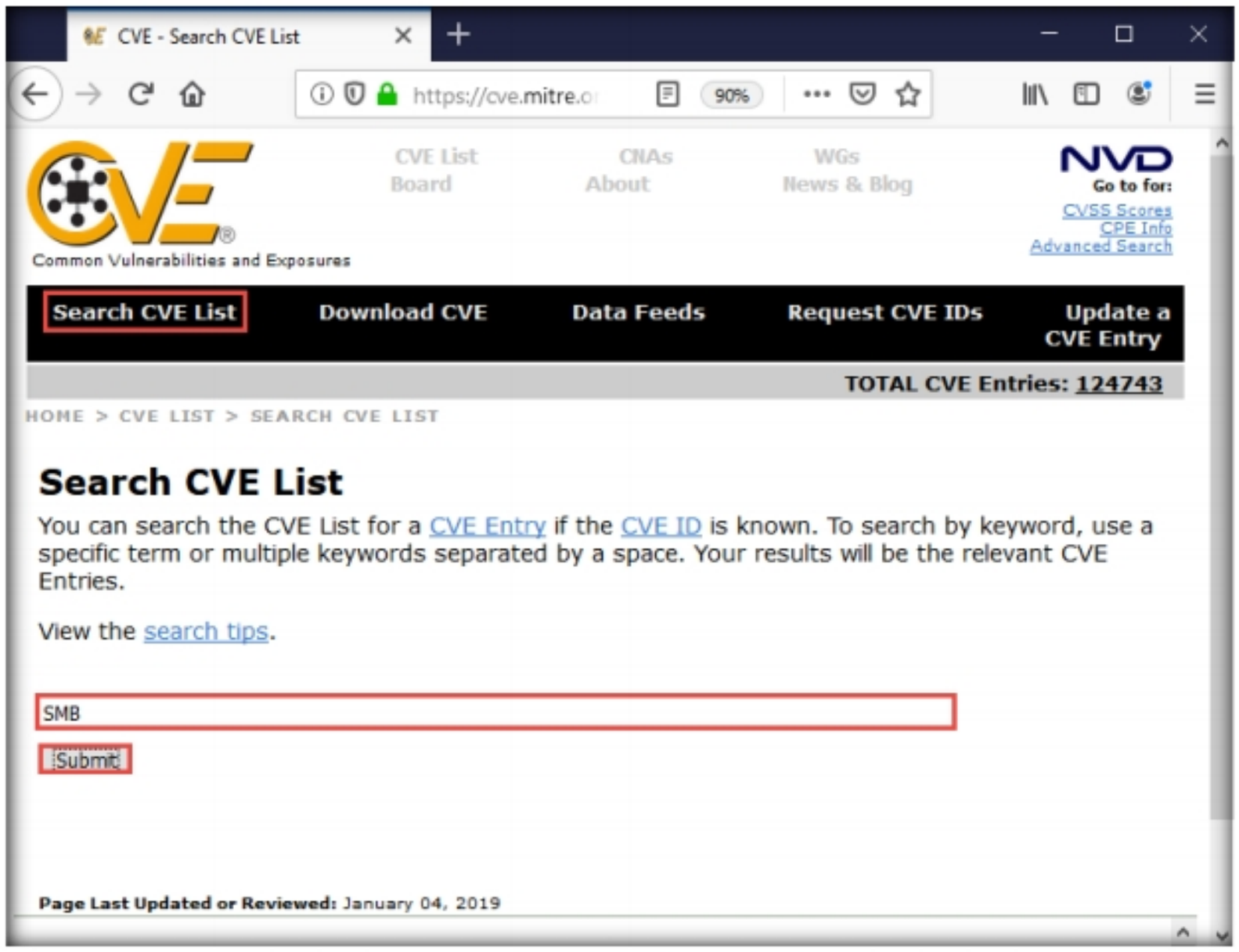


Figure 1.2.4: CVE - Search CVE List

7. **Search Results** page appears, displaying a list of vulnerabilities in the target service (**SMB**) along with their description, as shown in the screenshot.

Note: The results might vary in your lab environment.

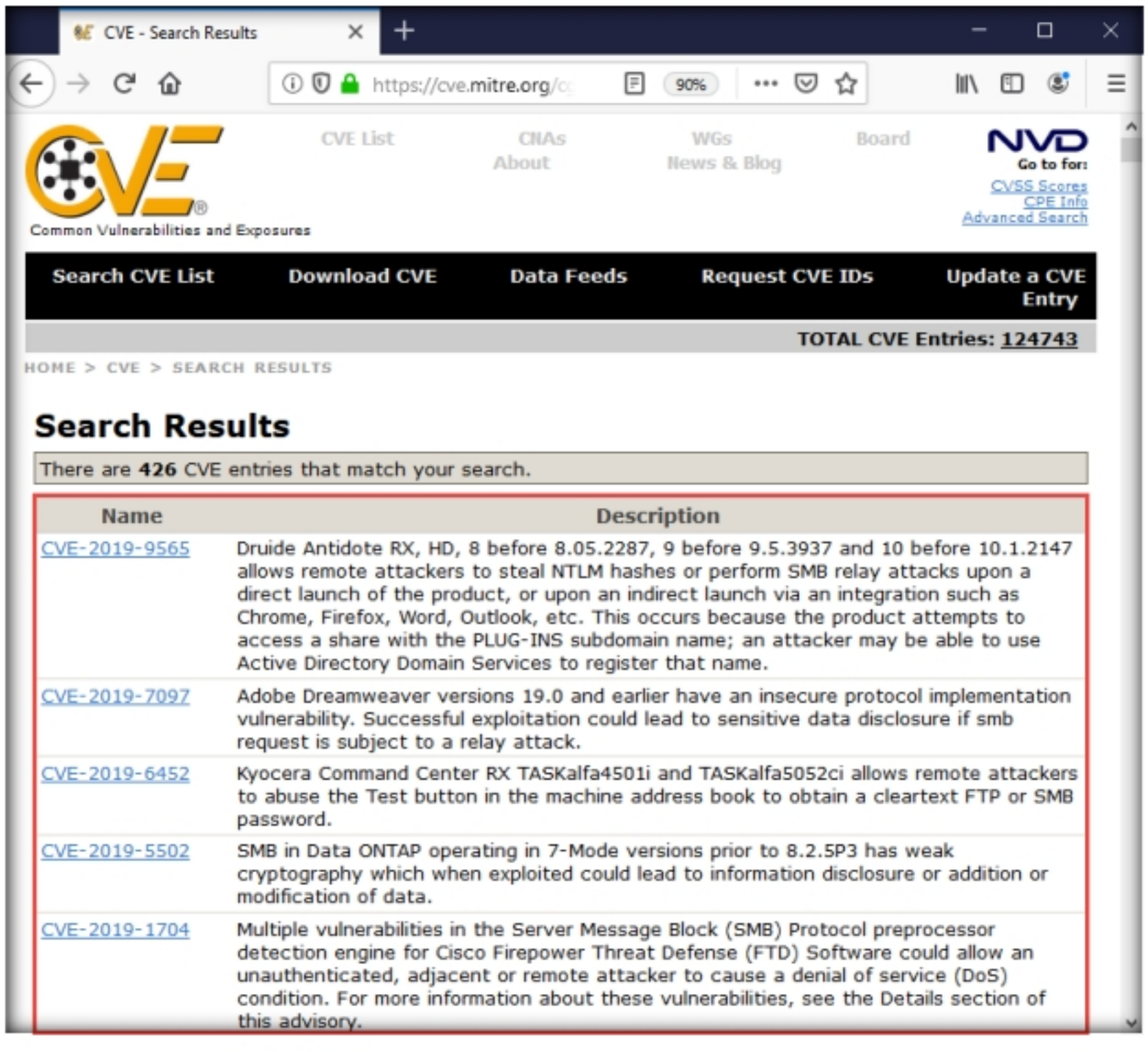


Figure 1.2.5: CVE - Search Results

8. Further, you can click on **CVE-ID** of any vulnerability to view its detailed information. Here, we will click on the first CVE-ID link.
9. Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Entry Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.

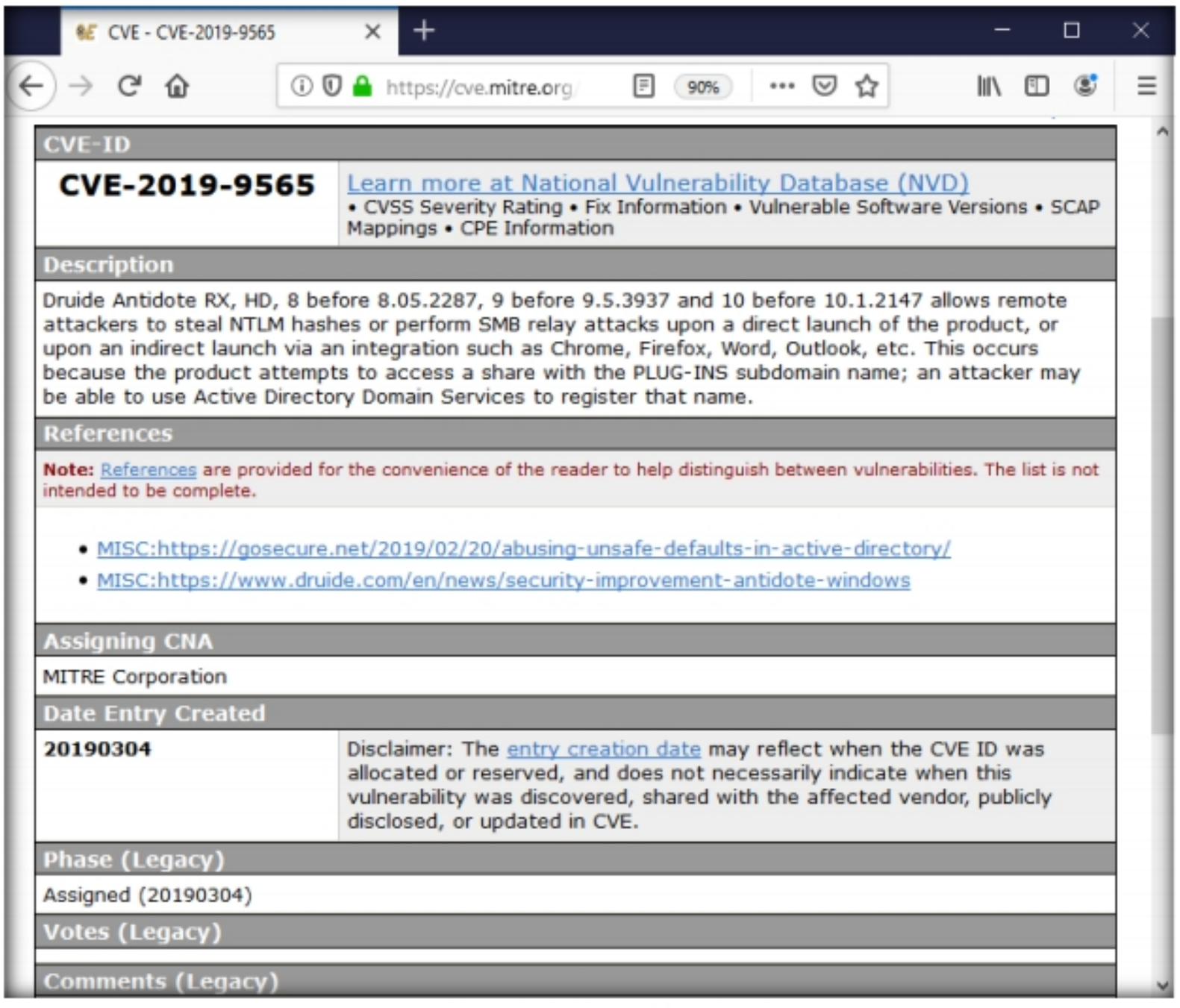


Figure 1.2.6: CVE: vulnerability information

10. Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
11. This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
12. Close all open windows and document all the acquired information.

TASK 3

Perform Vulnerability Research in National Vulnerability Database (NVD)

Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://nvd.nist.gov/**.
2. **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.
3. You can click on the CVE-ID link (here, **CVE-2019-2981**) to view detailed information about the vulnerability.

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Note: The results might differ in your lab environment.

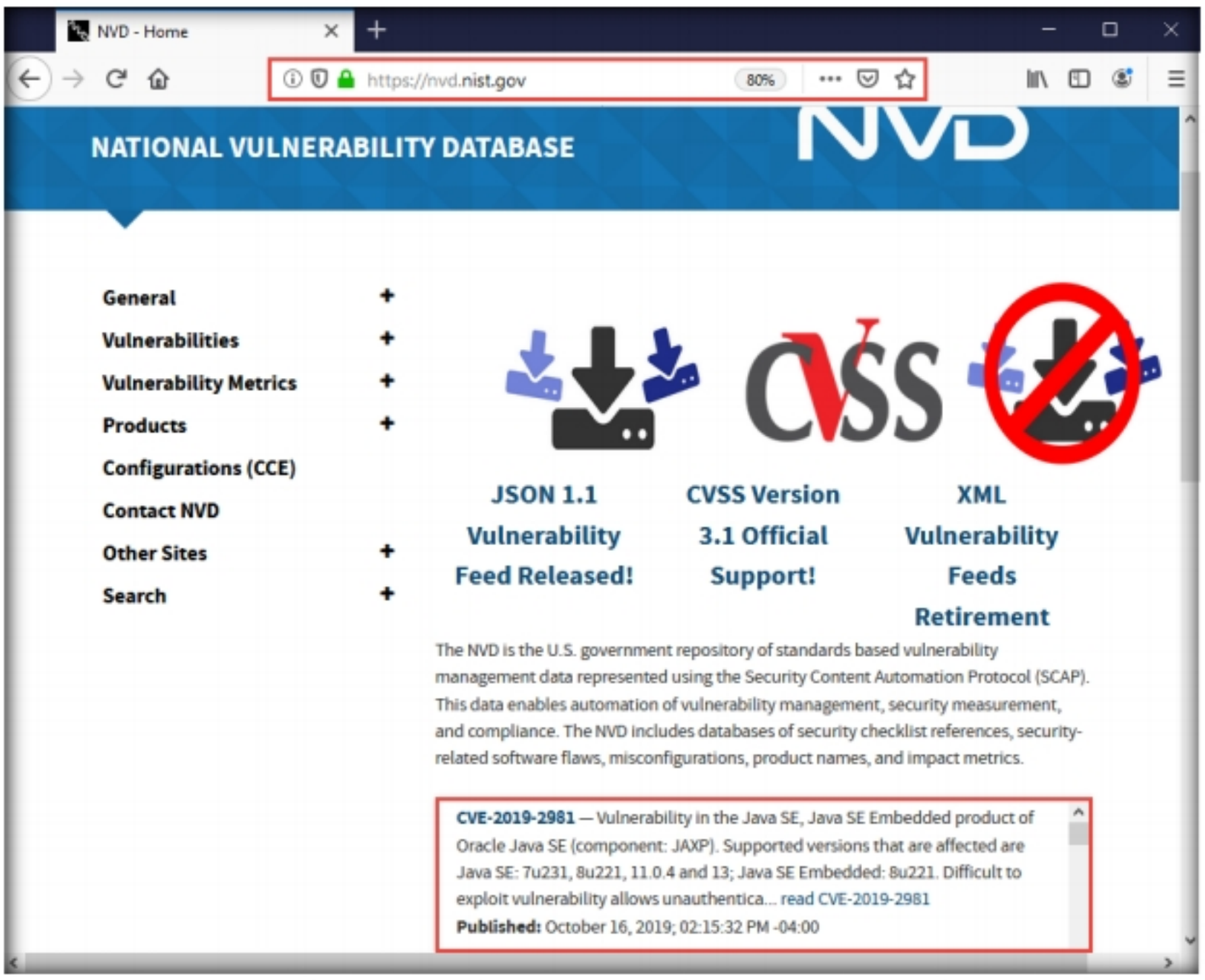


Figure 1.3.1: NVD website

4. A new webpage appears, displaying **CVE-2019-2981 Detail**. You can view detailed information such as **Current Description**, **Severity**, **References**, and **Weakness Enumeration**.

5. Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.

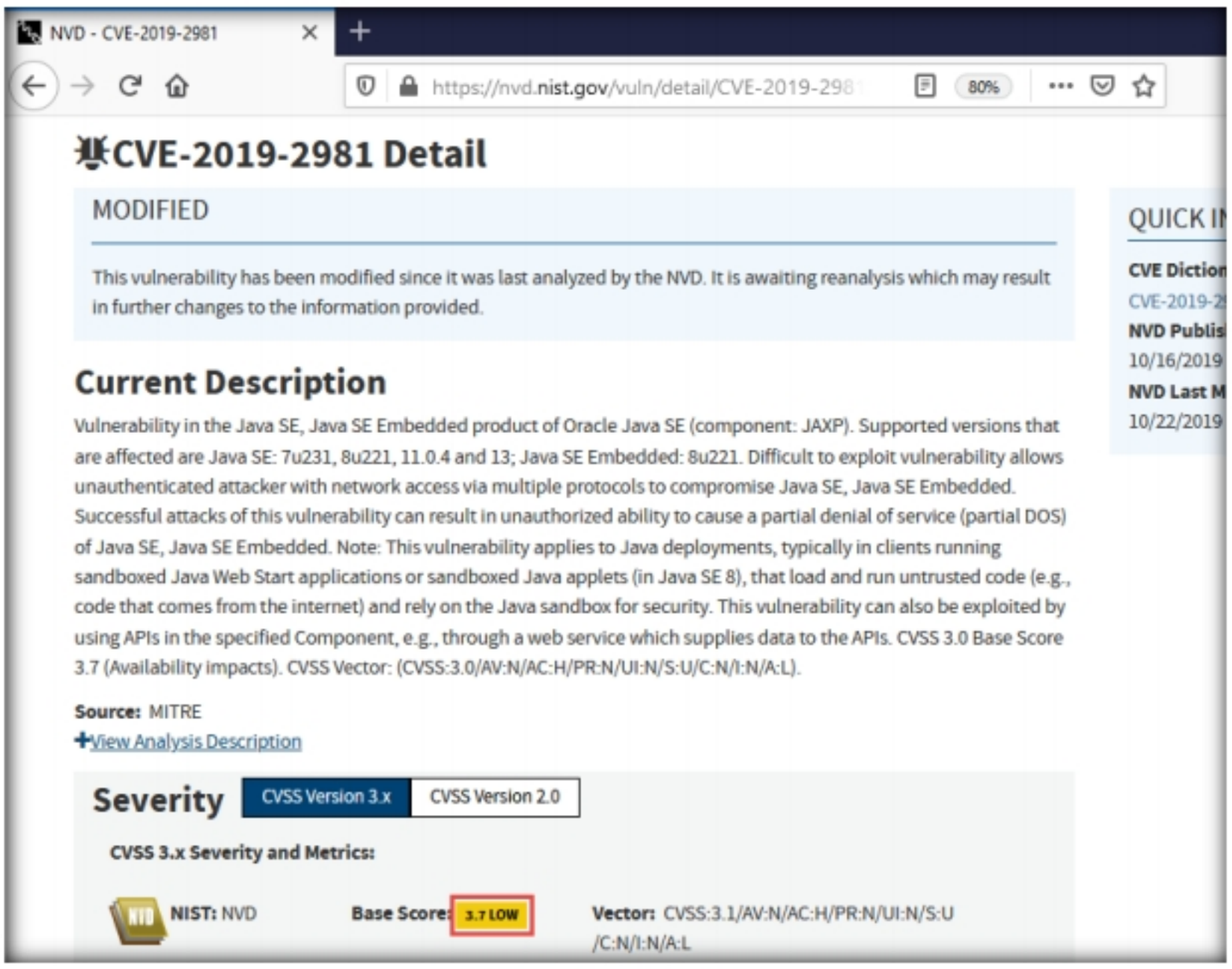


Figure 1.3.2: NVD: results

6. A new webpage appears, displaying information such as **Base Scores**, **Temporal Score**, and **Environmental Score Overall Score** related to a vulnerability in graphical form, under **Common Vulnerability Scoring System Calculator CVE-2019-2981**.

Note:

- **Base Score**: The metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The table below describes the severity of a vulnerability depending upon the Base Score range:

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

- **Temporal Score**: Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.
- **Overall Score**: Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).

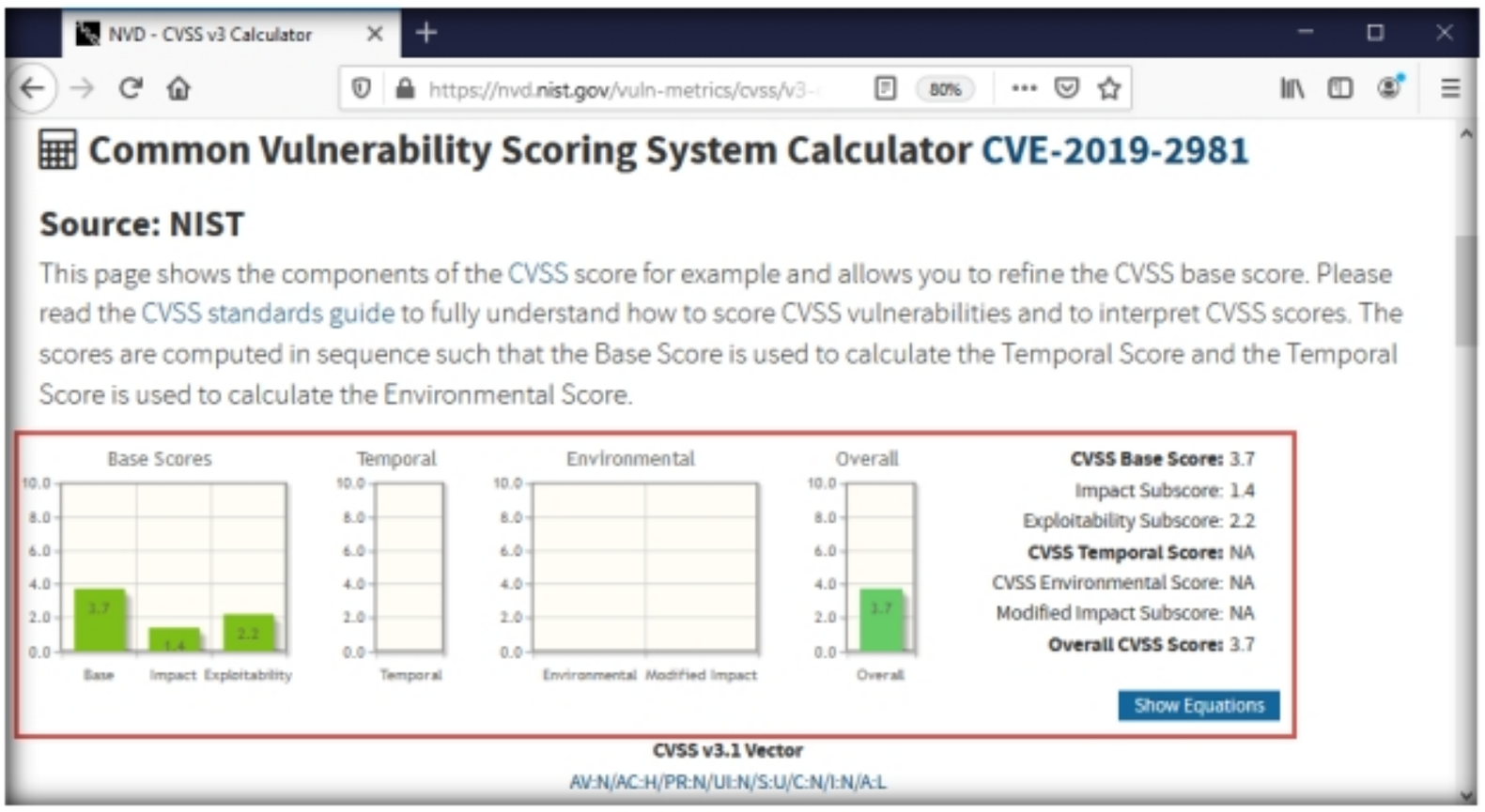


Figure 1.3.3: NVD: CVSS details

7. Scroll down to view more detailed information on different score metrics such as **Base Score Metrics**, **Temporal Score Metrics**, and **Environmental Score Metrics**.

Note: The results might differ depending upon the selected vulnerability.

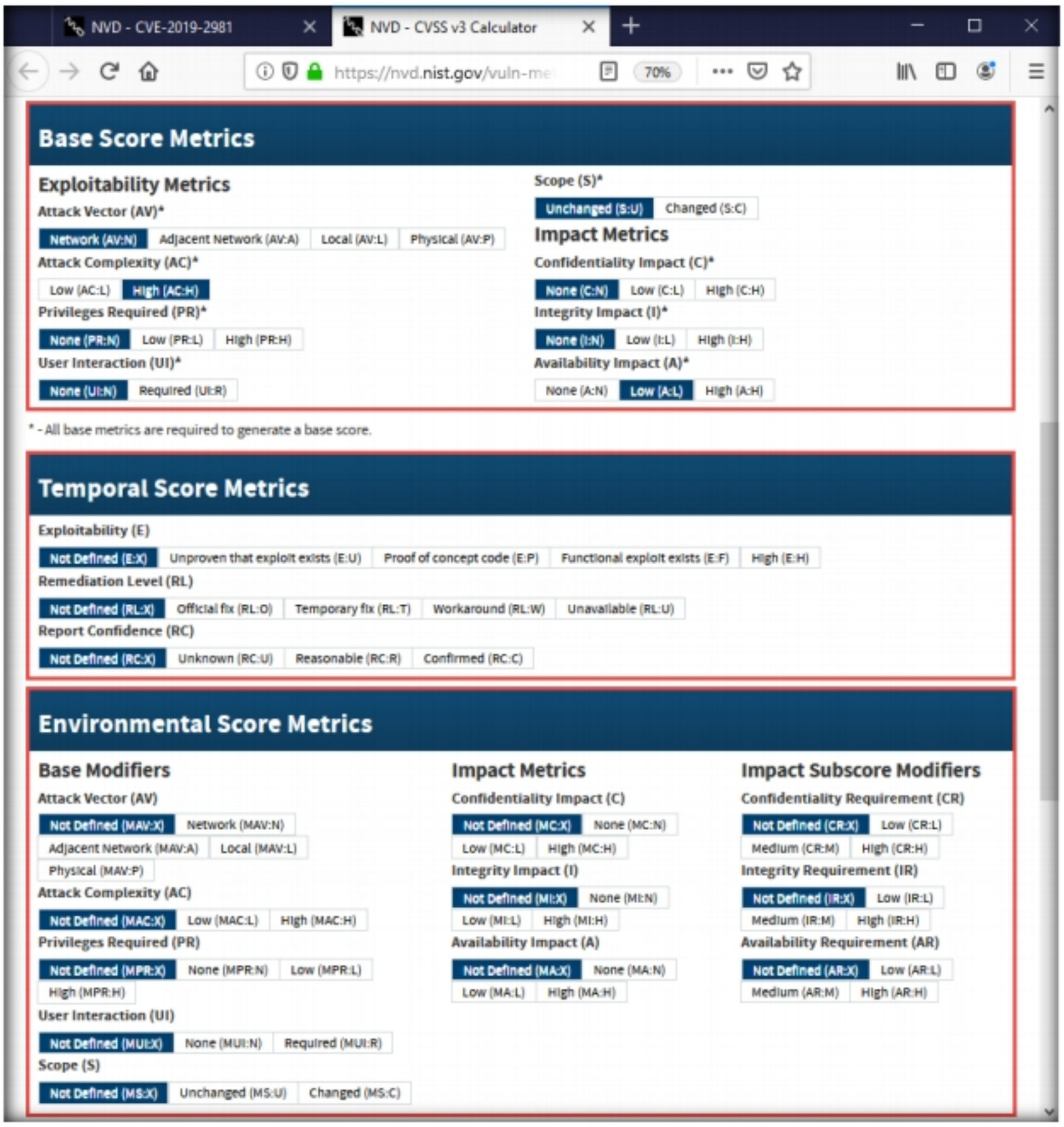


Figure 1.3.4: NVD: CVSS details

8. Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.

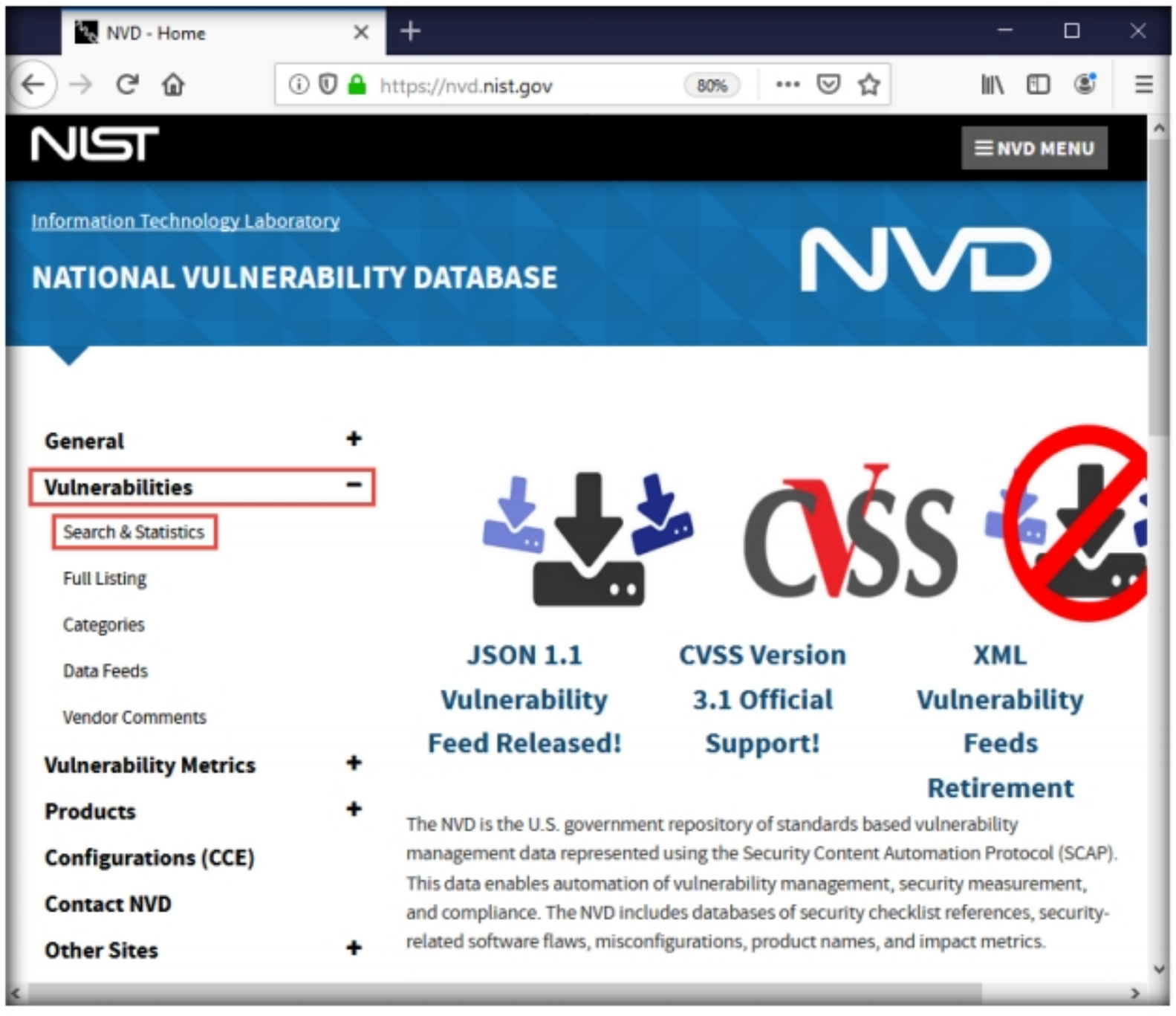


Figure 1.3.5: NVD: Select Search & Statistics option

9. **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

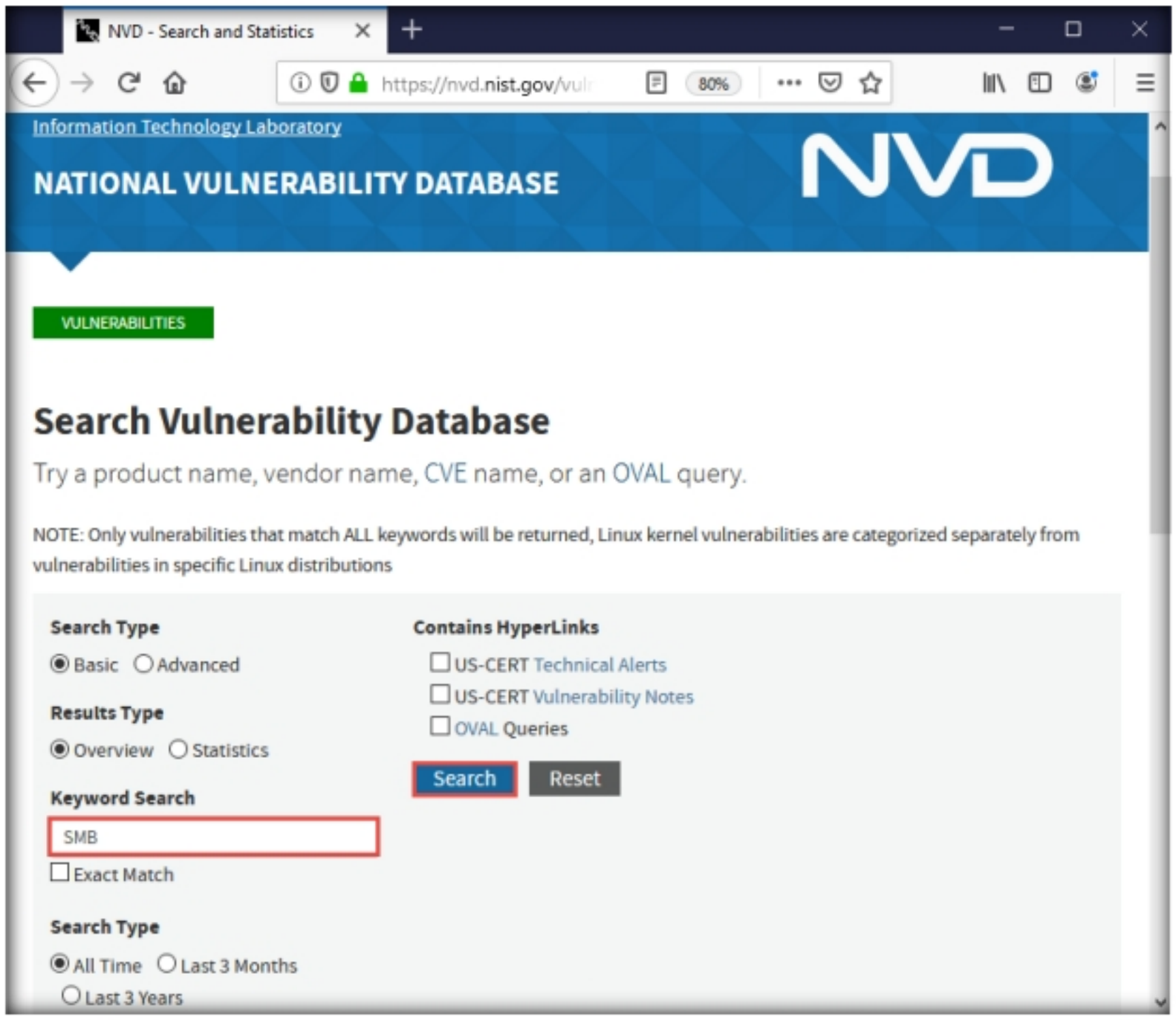


Figure 1.3.6: NVD - Search target service

10. The **Search Results** page appears, displaying detailed information on the underlying vulnerabilities in the target service.
11. You can further view detailed information on each vulnerability by clicking on the **Vuln ID** link.

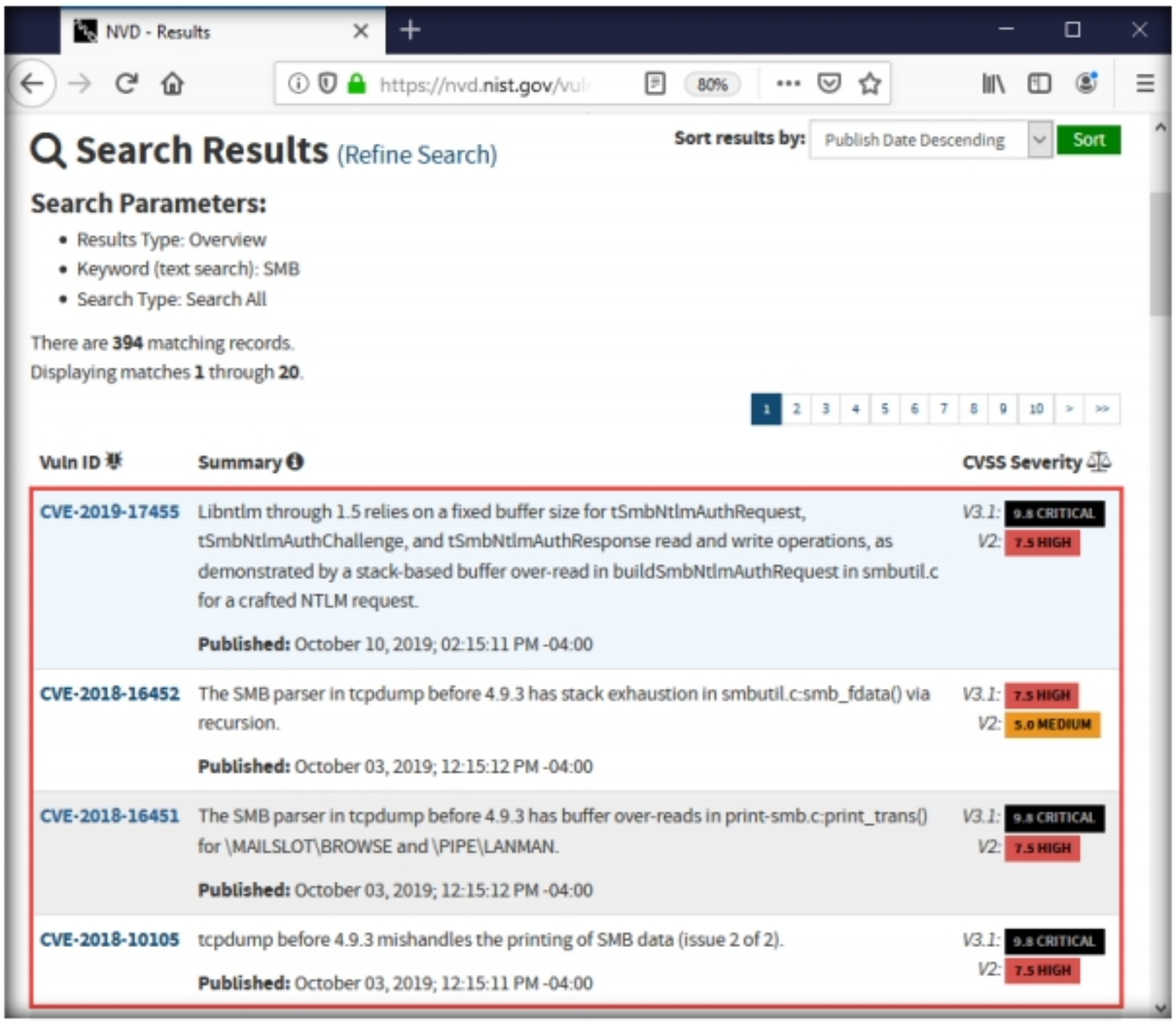


Figure 1.3.7: NVD: Search Results

12. Likewise, you can search for other target services for the underlying vulnerability in the **Search Vulnerability Database** section.
13. This concludes the demonstration of checking vulnerabilities in the National Vulnerability Database (NVD).
14. Close all open windows and document all the acquired information.
15. Turn off **Windows 10** virtual machine.

Lab Analysis

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

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

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

Lab 2

Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Ethical hackers and pen testers are aided in vulnerability assessments with the help of various tools that make vulnerability assessment an easy task.

ICON KEY

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

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

Lab Objectives

- Perform vulnerability analysis using OpenVAS
- Perform vulnerability scanning using Nessus
- Perform vulnerability scanning using GFI LanGuard
- Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Nessus located at **E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus**
- You can also download the latest version of **Nessus** from the official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 55 Minutes

Overview of Vulnerability Assessment Tools

Vulnerability assessment tools are used to secure and protect the organization's system or network: security analysts can use these tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them. Network vulnerability scanners analyze and identify vulnerabilities in the target network or network resources using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

Lab Tasks

TASK 1

Perform Vulnerability Analysis using OpenVAS

Here, we will perform a vulnerability analysis using OpenVAS.

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as a host machine and the **Windows Server 2016** (**10.10.10.16**) virtual machine as a target machine.

1. Turn on the **Parrot Security** and **Windows Server 2016** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

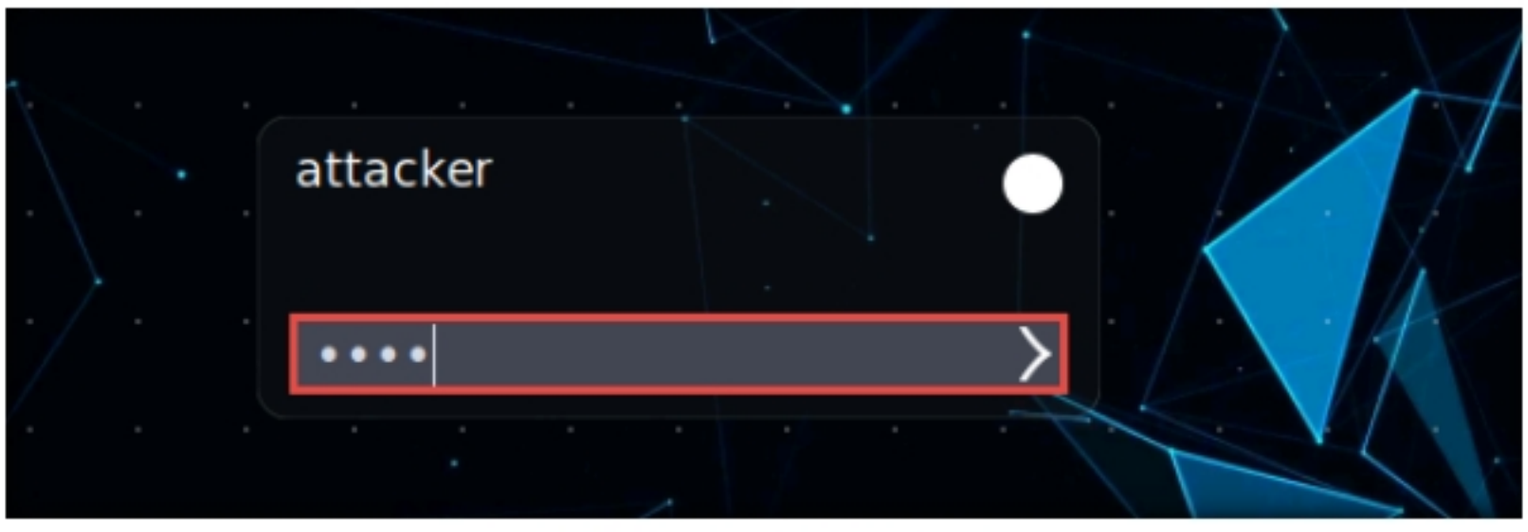


Figure 2.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Launch OpenVAS Tool

3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → OpenVAS - Greenbone→ Start** to launch OpenVAS tool.
4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.
5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.

The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

6. The **Firefox** browser appears, in the address bar, type **https://127.0.0.1:9392** and press **Enter**.
7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

Note: The version of OpenVAS might differ in your lab environment.

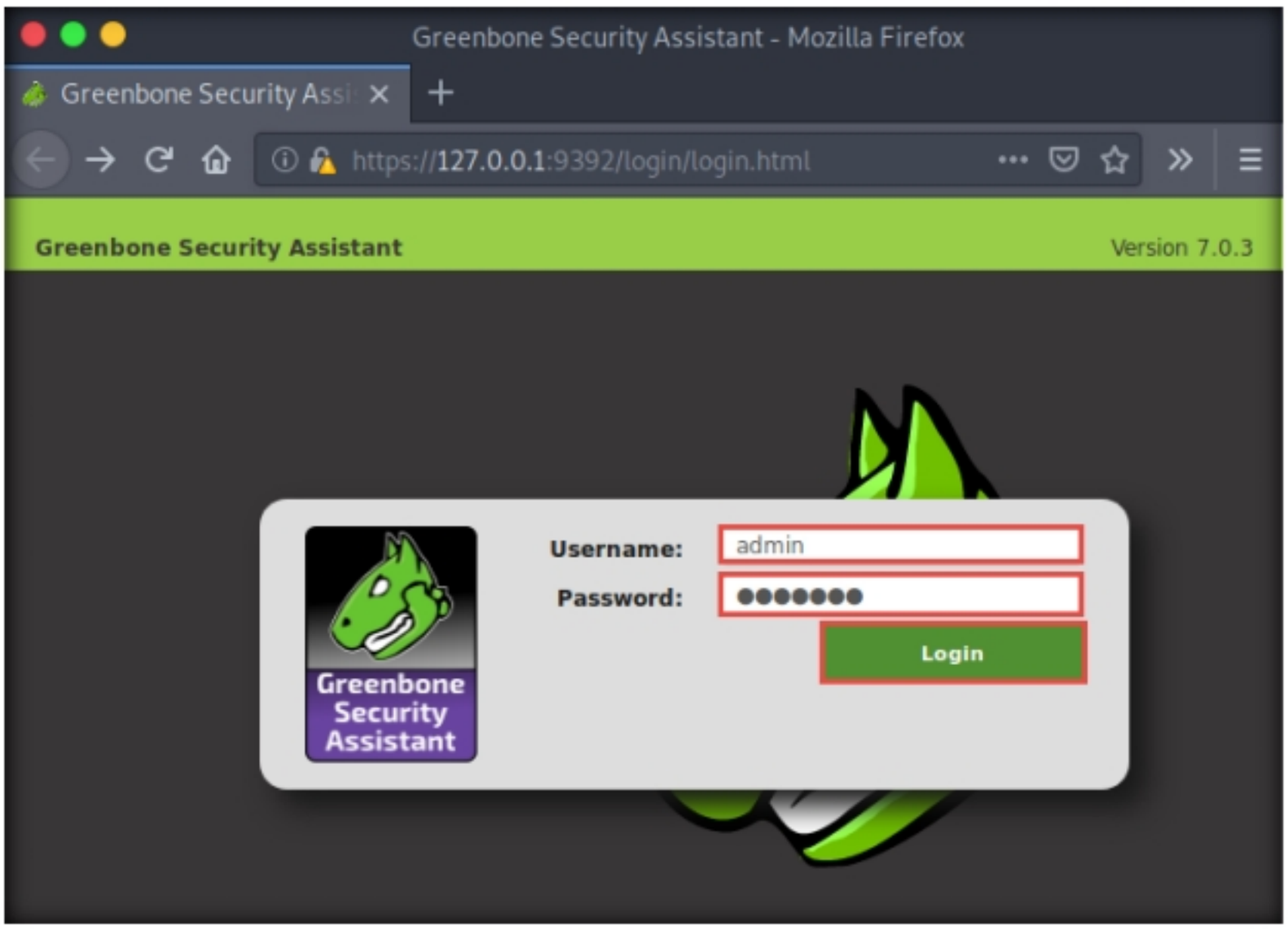


Figure 2.1.2: OpenVAS Login page

8. **OpenVAS Dashboard** appears, as shown in the screenshot.

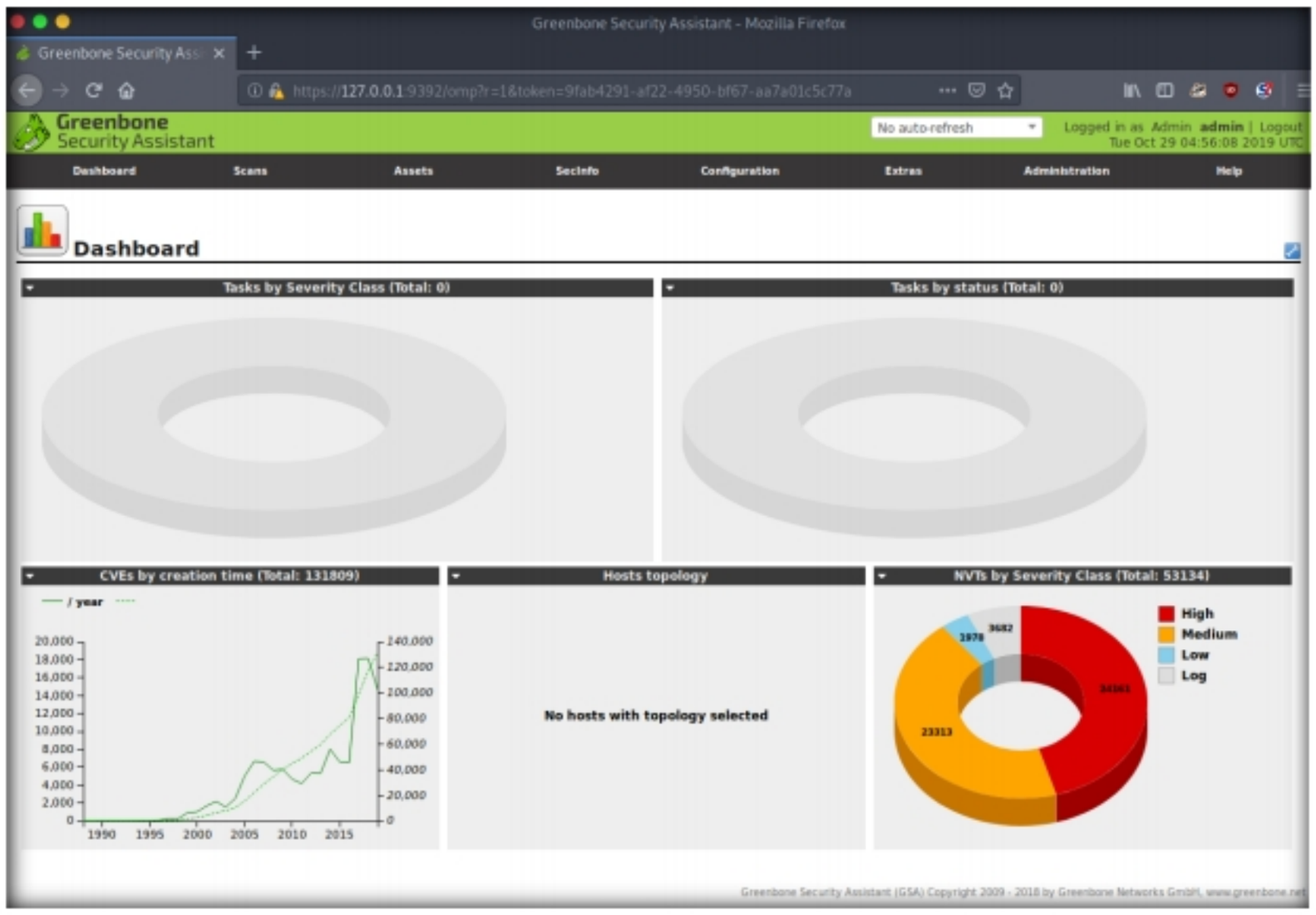


Figure 2.1.3: OpenVAS dashboard

9. Navigate to **Scans → Tasks** from the **Menu** bar.

Note: If a **Welcome to the scan management!** pop-up appears, close it.

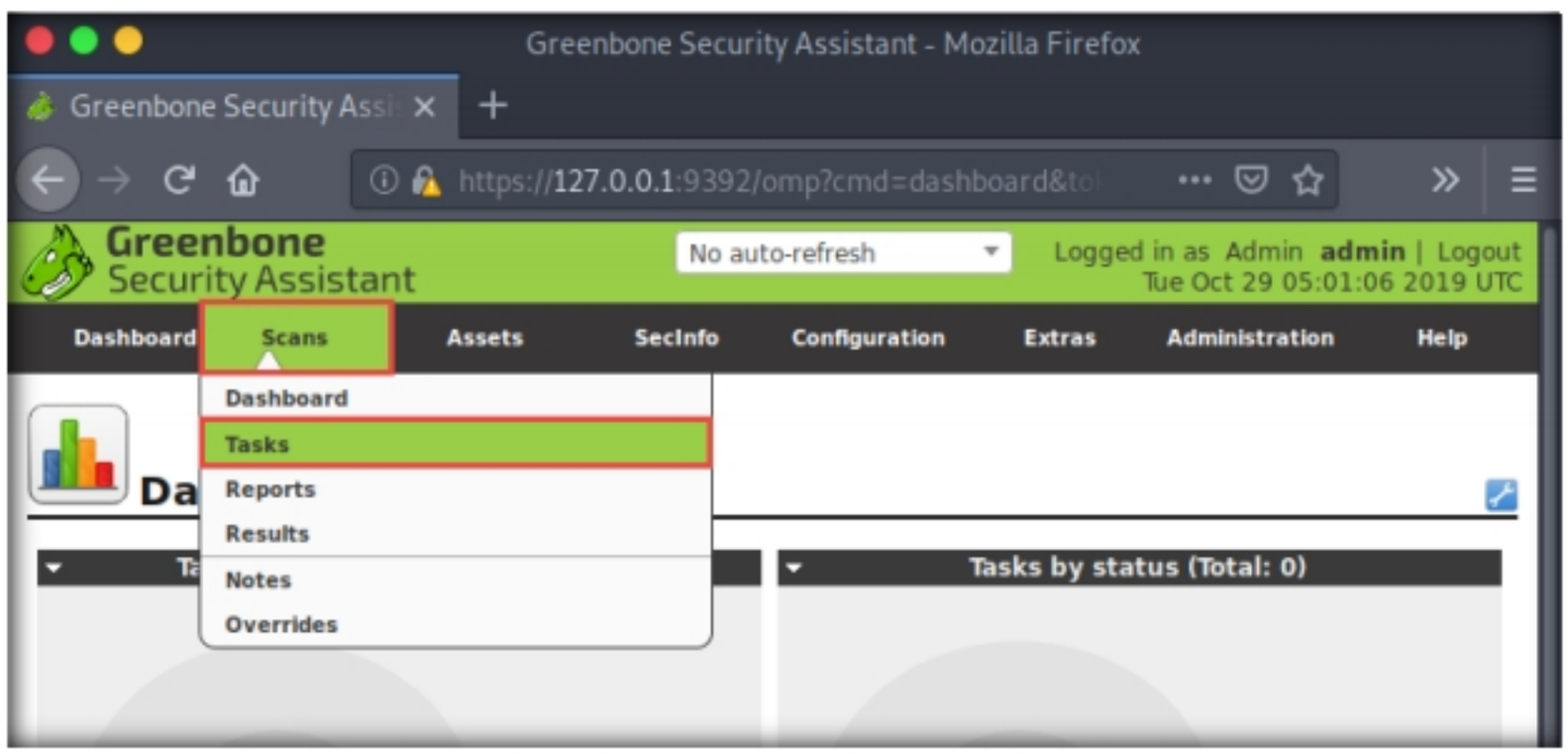


Figure 2.1.4: OpenVAS: select Scans option

TASK 1.2

Scan the Target

10. Hover over ( ) icon and click the **Task Wizard** option.

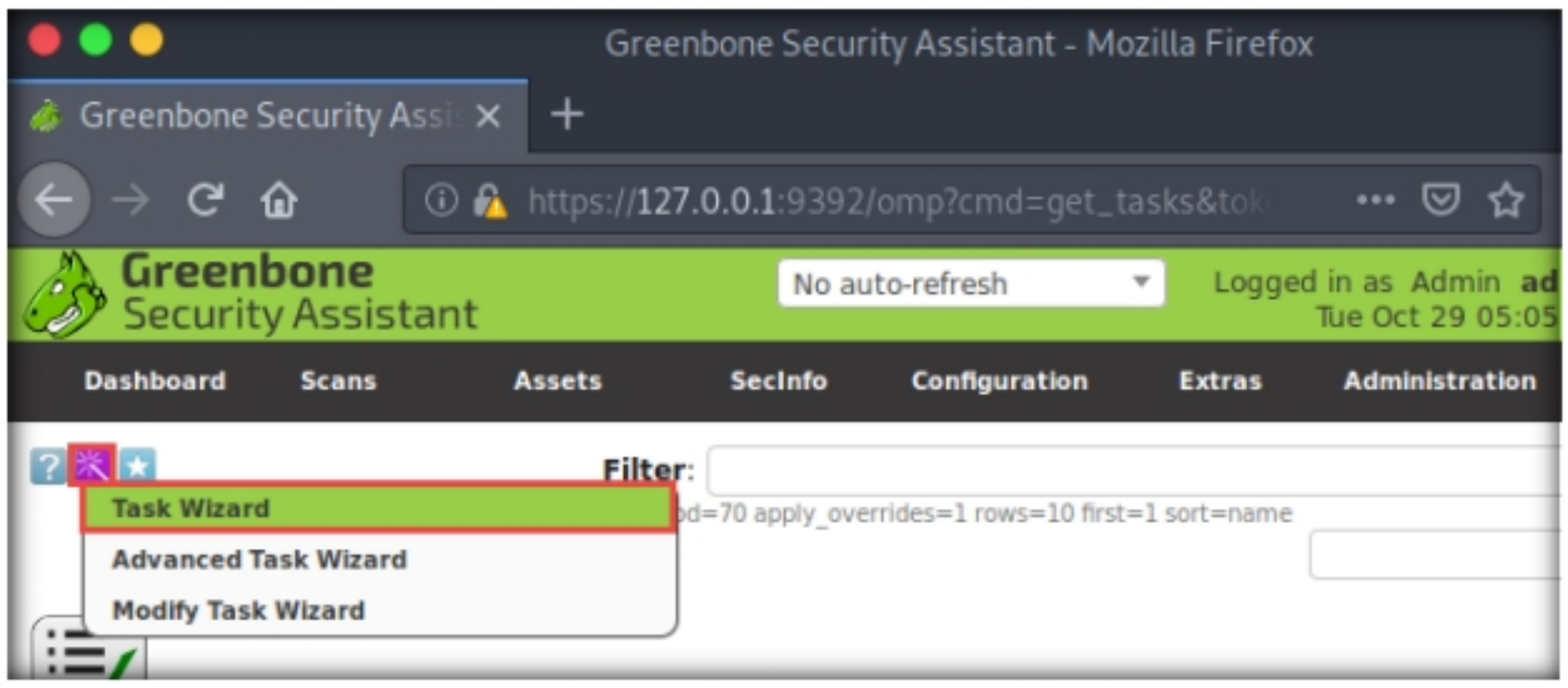


Figure 2.1.5: OpenVAS: select Task Wizard option

11. The **Task Wizard** window appears; enter the target IP address in the **IP address or hostname** field (here, the target system is **Windows Server 2016** [**10.10.10.16**]) and click the **Start Scan** button.

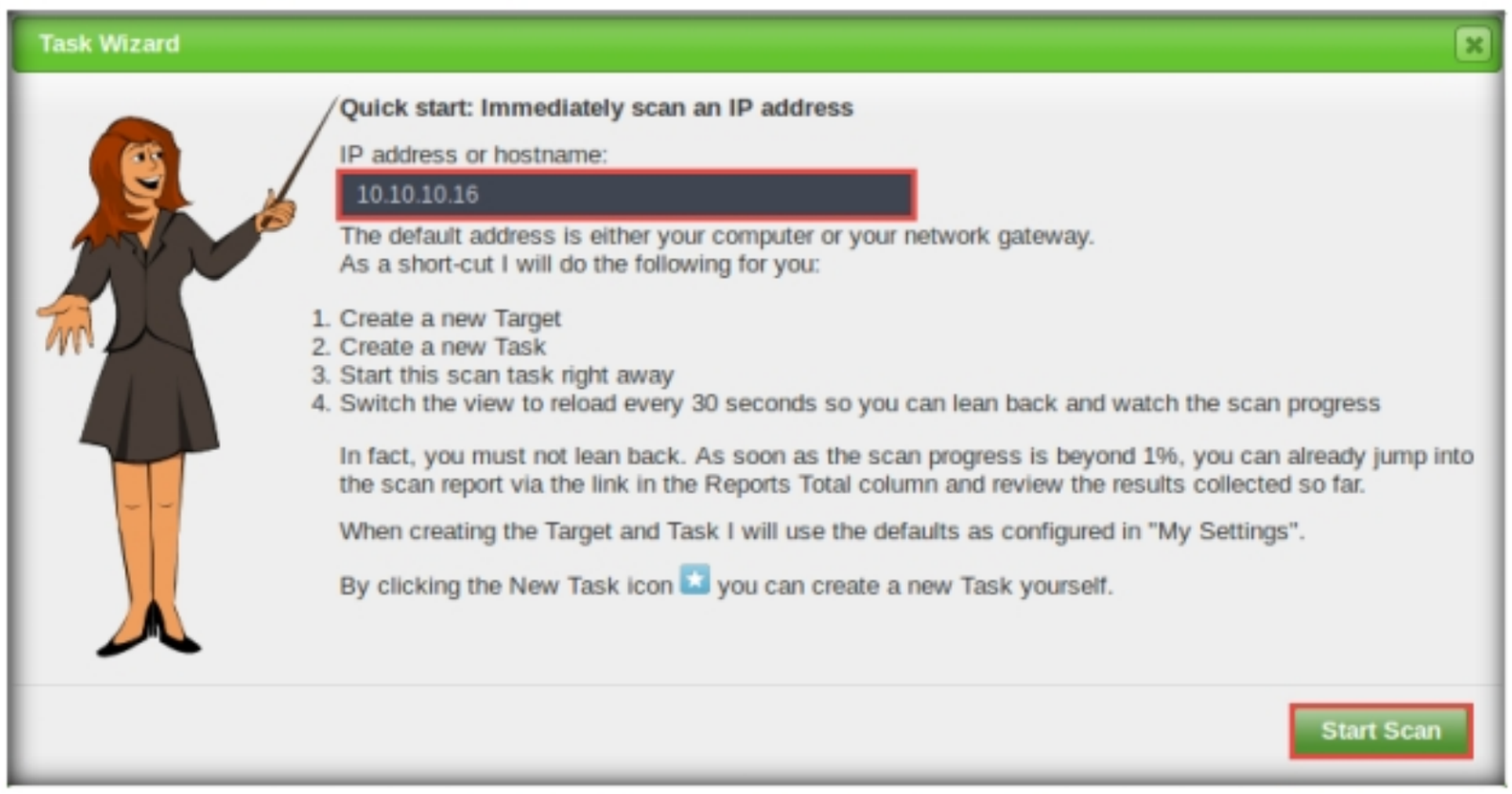


Figure 2.1.6: OpenVAS: enter the target IP address

12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.

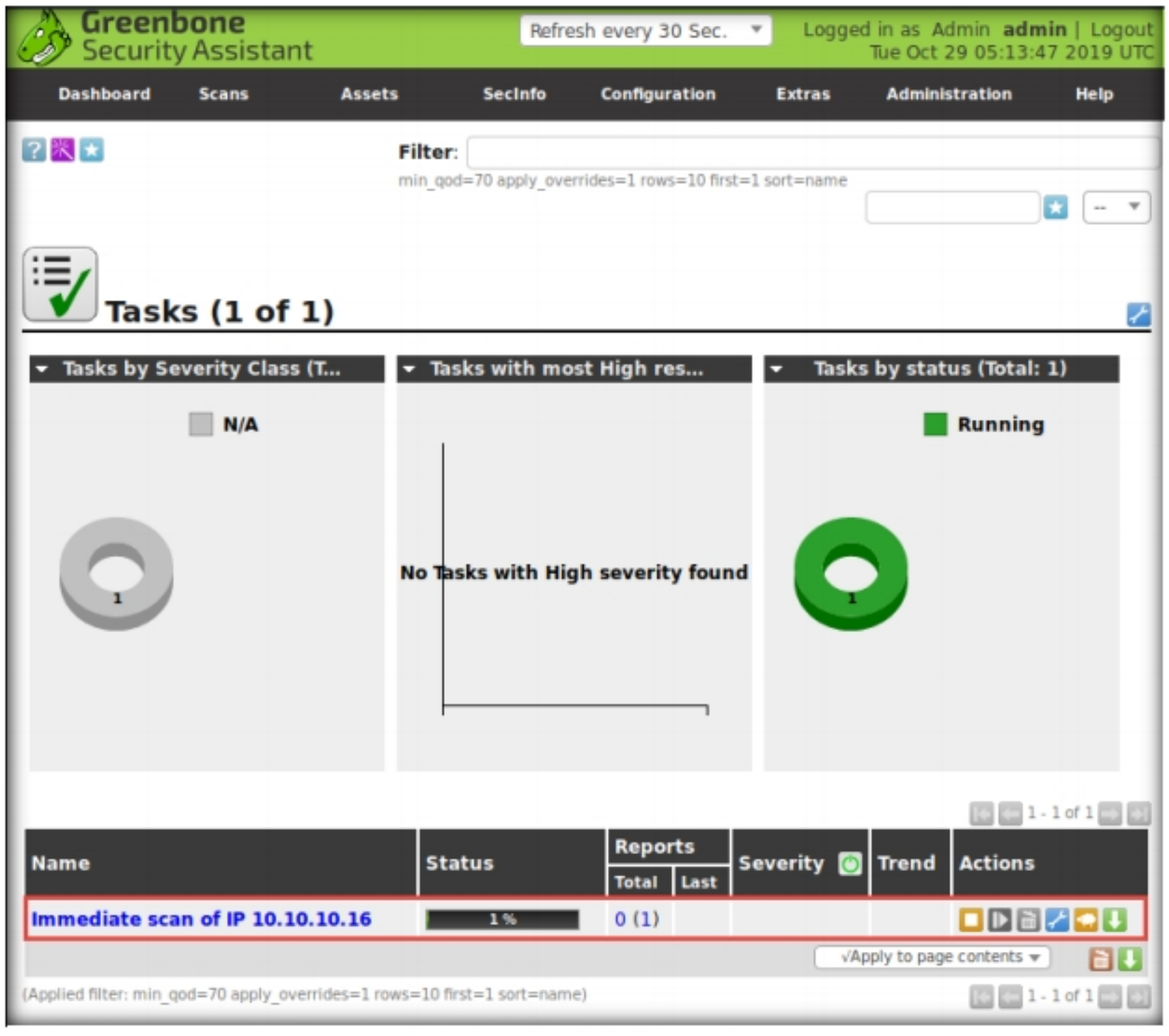


Figure 2.1.7: OpenVAS: Scan initiates

13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

Note: The scan will take approximately 10 minutes to complete.

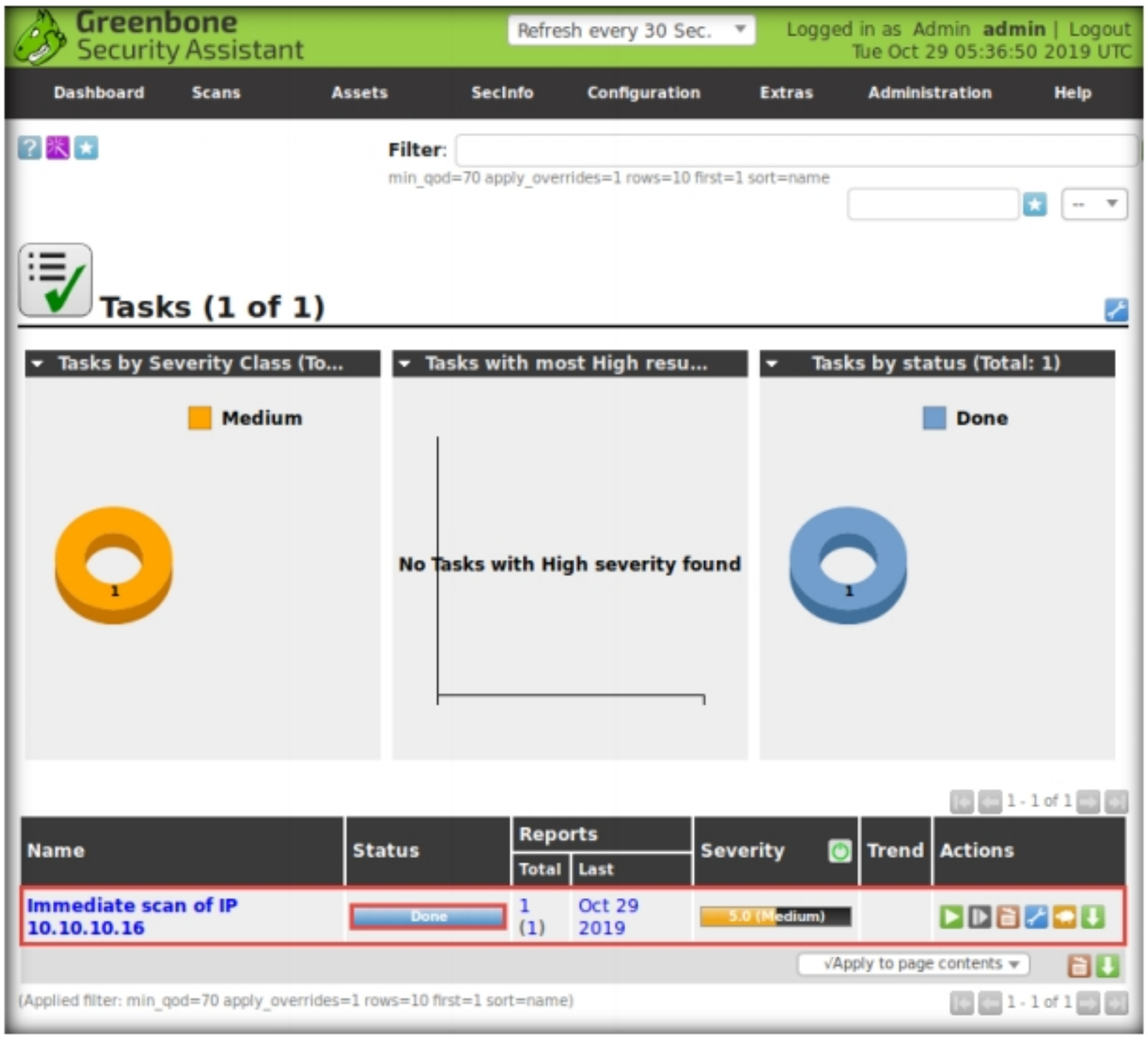


Figure 2.1.8: OpenVAS: Scan Completes

14. **Report: Results** appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might vary in your lab environment.

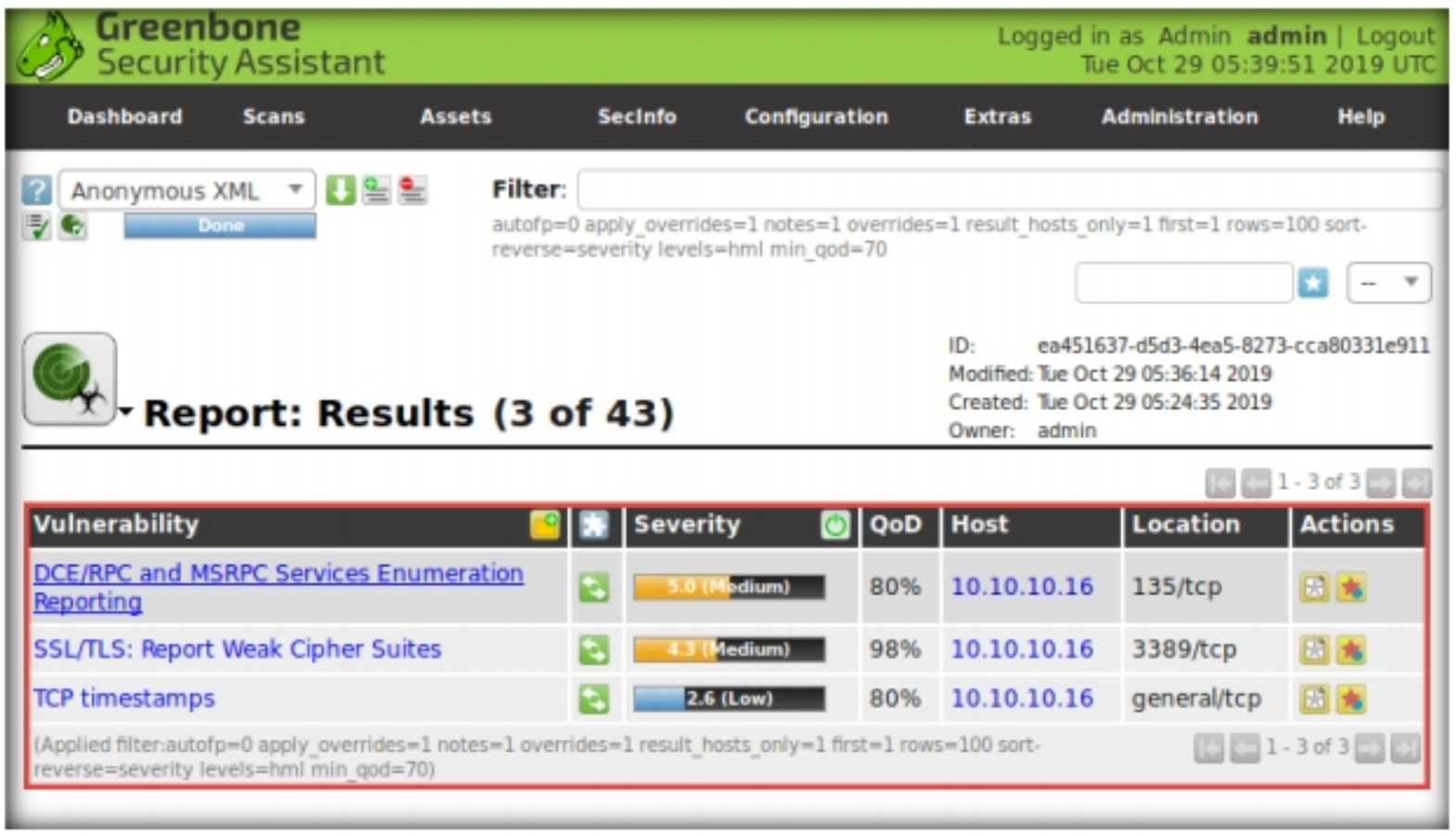


Figure 2.1.9: OpenVAS: Report: Results

15. Click on any vulnerability under the **Vulnerability** column (here, **DCE/RPC and MSRPC Services Enumeration Reporting**) to view its detailed information.
16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.

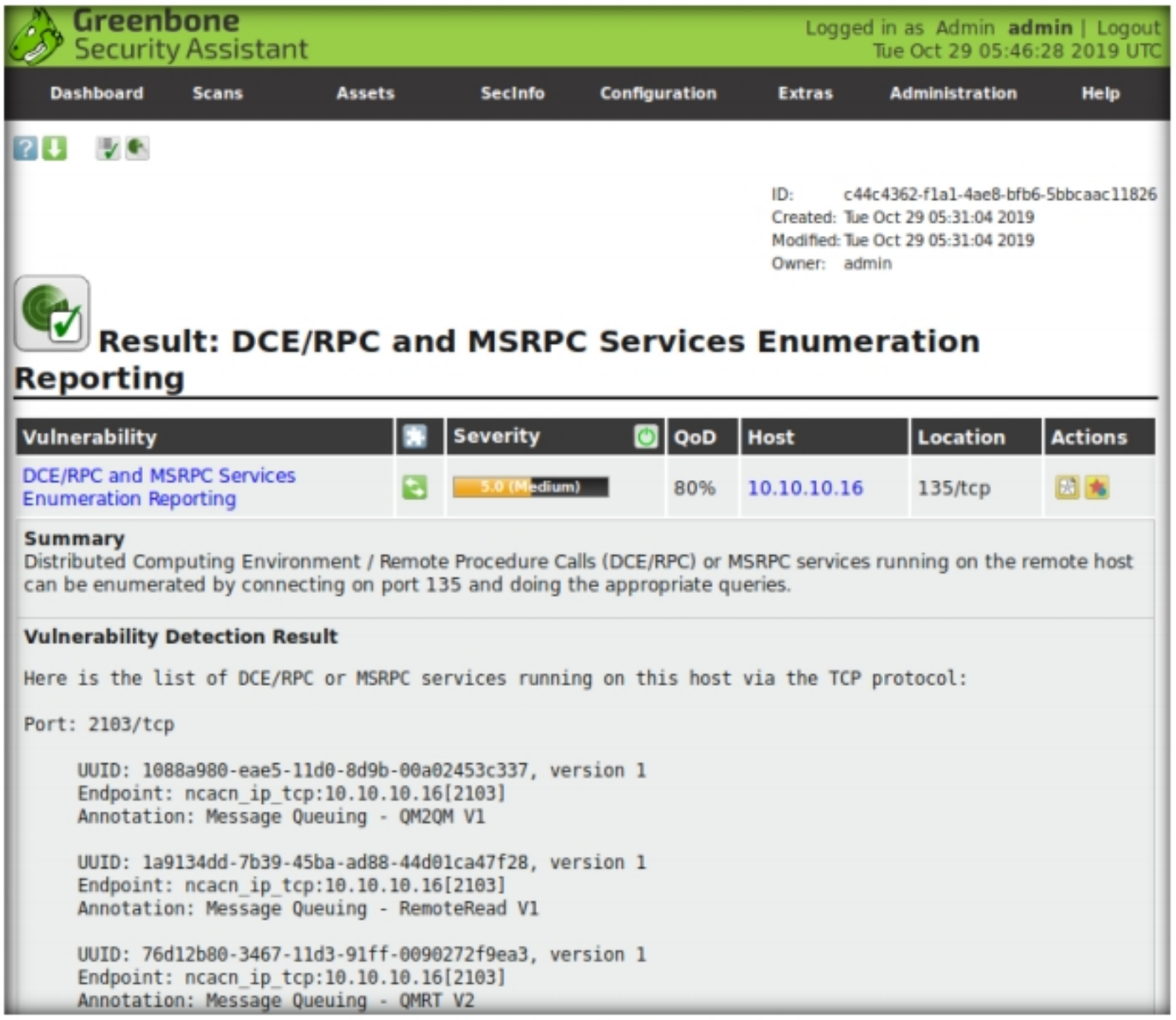


Figure 2.1.10: OpenVAS: Vulnerability Results

17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.
18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your **firewall ON** in the **Windows Server 2016** virtual machine.

TASK 1.3

Scan the Target with Firewall Enabled

19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.
20. Switch to the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

21. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, enable Windows Firewall, and click **OK**.

Note: By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.

22. Perform **Steps# 9-11** to create another task for scanning the target system.

23. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.

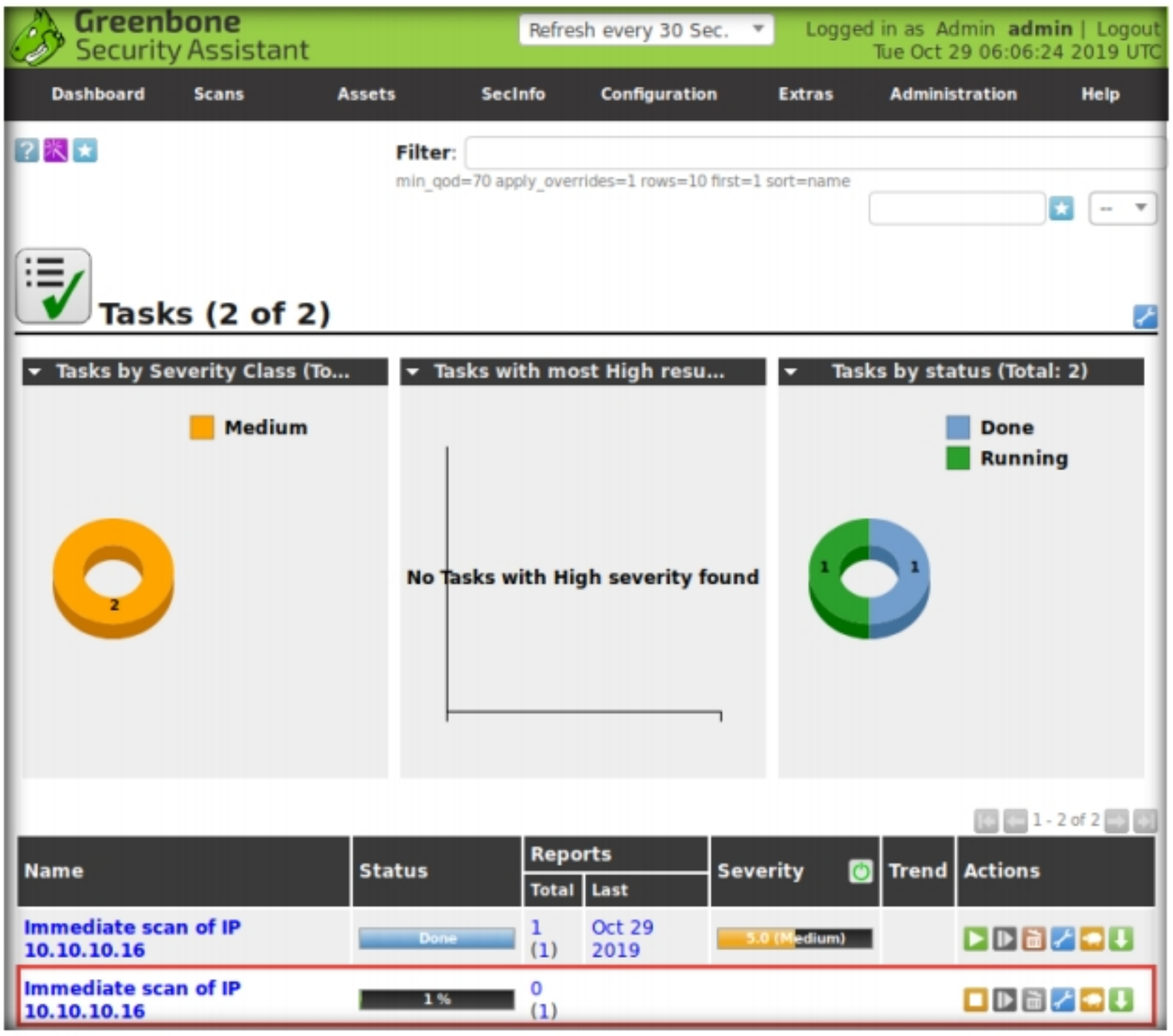


Figure 2.1.11: OpenVAS: Scanning the target IP address

24. After the completion of the scan, click the **Done** button under the **Status** column.

25. **Report: Results** appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might vary in your lab environment.

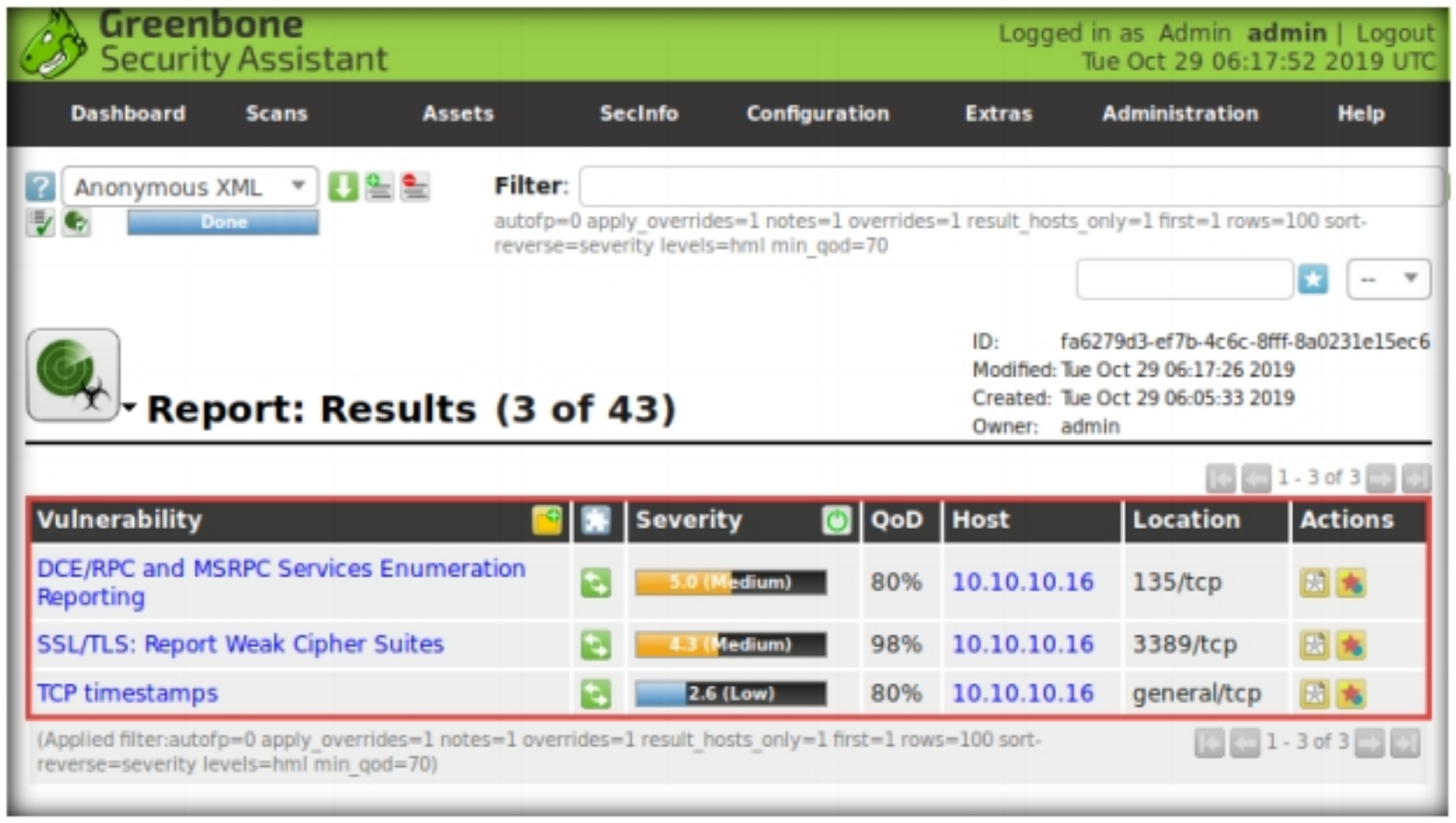


Figure 2.1.12: OpenVAS: Report: Results

26. The scan results for the target machine before and after the Windows Firewall was enabled are the same, thereby indicating that the target system is vulnerable to attack even if the Firewall is enabled.
27. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.
28. Close all open windows and document all the acquired information.
29. Switch to **Windows Server 2016** virtual machine. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, disable Windows Firewall, and click **OK**.
30. Turn off **Parrot Security** virtual machine.

TASK 2 Perform Vulnerability Scanning using Nessus

Here, we will use Nessus to perform vulnerability scanning on the target system.

TASK 2.1 Install Nessus

1. Turn on **Windows 10** virtual machines.

Note: Ensure that the **Windows Server 2016** virtual machine is turned on.

2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus** and double-click **Nessus-8.7.2-x64.msi**.
4. **Tenable Nessus InstallShield Wizard** appears. Follow the installation steps to install Nessus with all default settings.

Note: If **User Account Control** pop-up appears, click **Yes**.

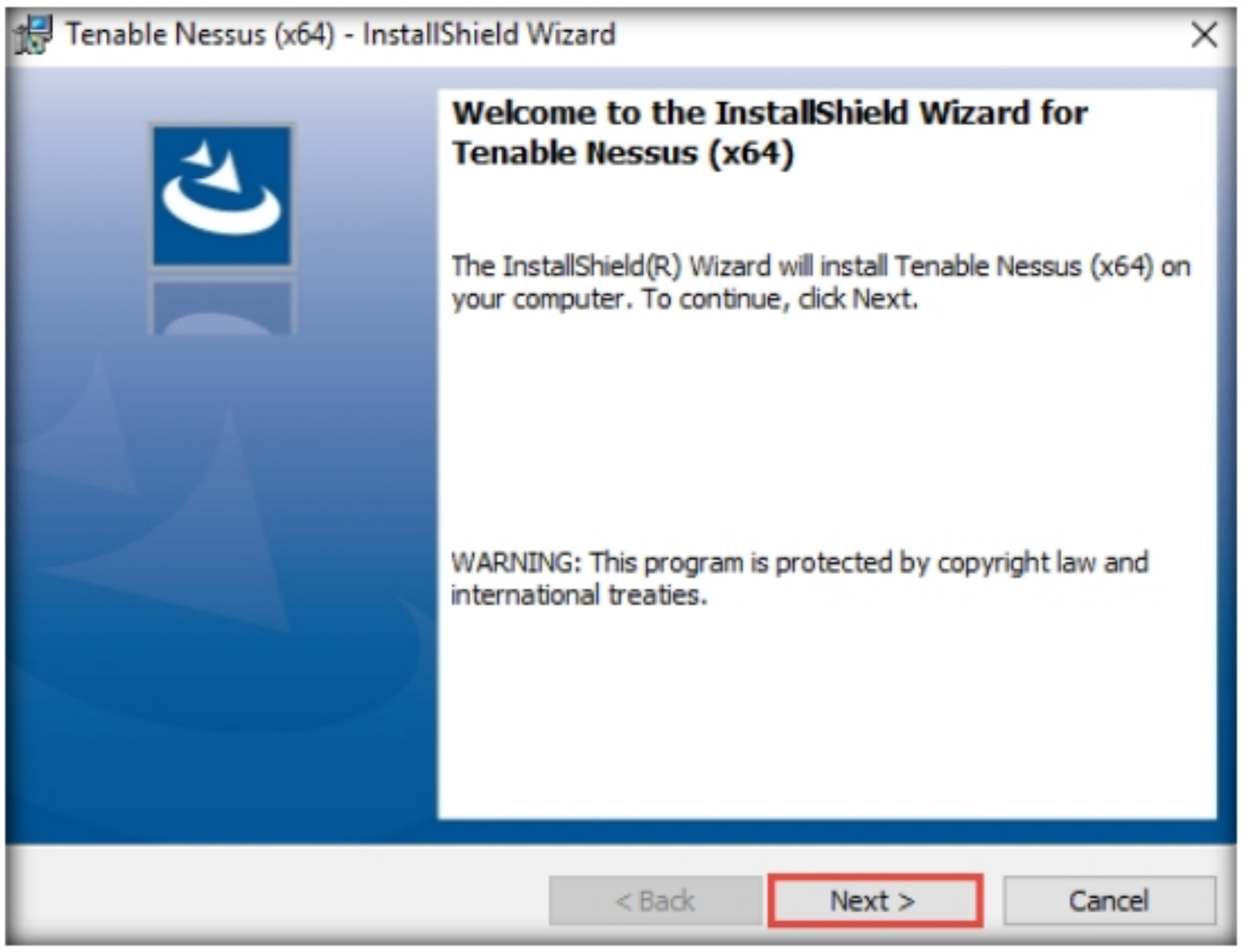


Figure 2.2.1: Nessus Install Shield Wizard

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment.

Note: During installation, if a **Windows Security** pop-up appears, click **Install** or skip to the next step.

Note: During installation, if a **WinPcap Setup** window appears, click **Install** and follow the installation wizard to install WinPcap with default settings. Once the installation finishes, click **Finish**.

5. After the completion of the installation, in the **Tenable Nessus InstallShield Wizard** window, click **Finish**.

It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

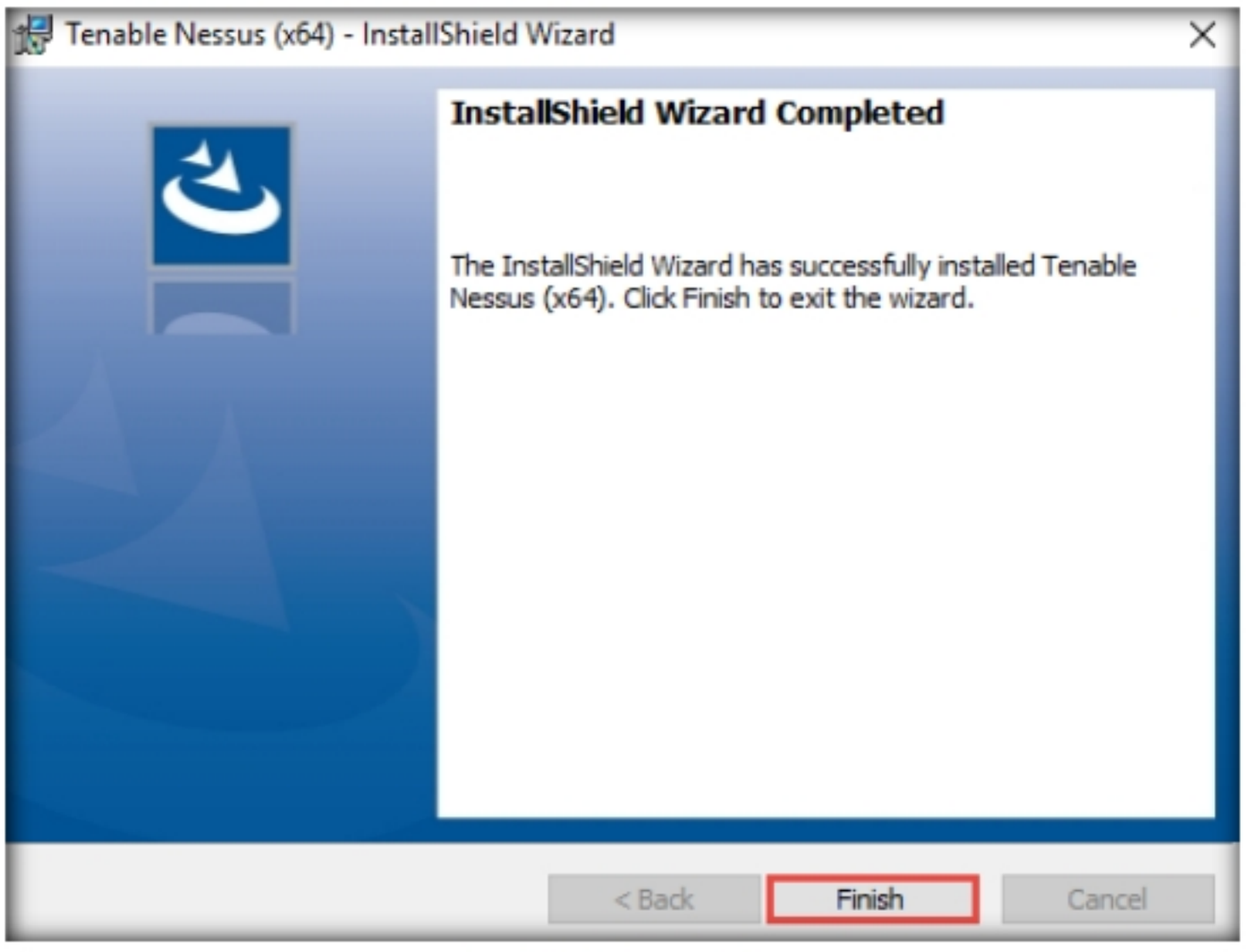


Figure 2.2.2: Nessus window

6. The **Nessus** opens-up in the default browser. Click **Connect via SSL** button to proceed.

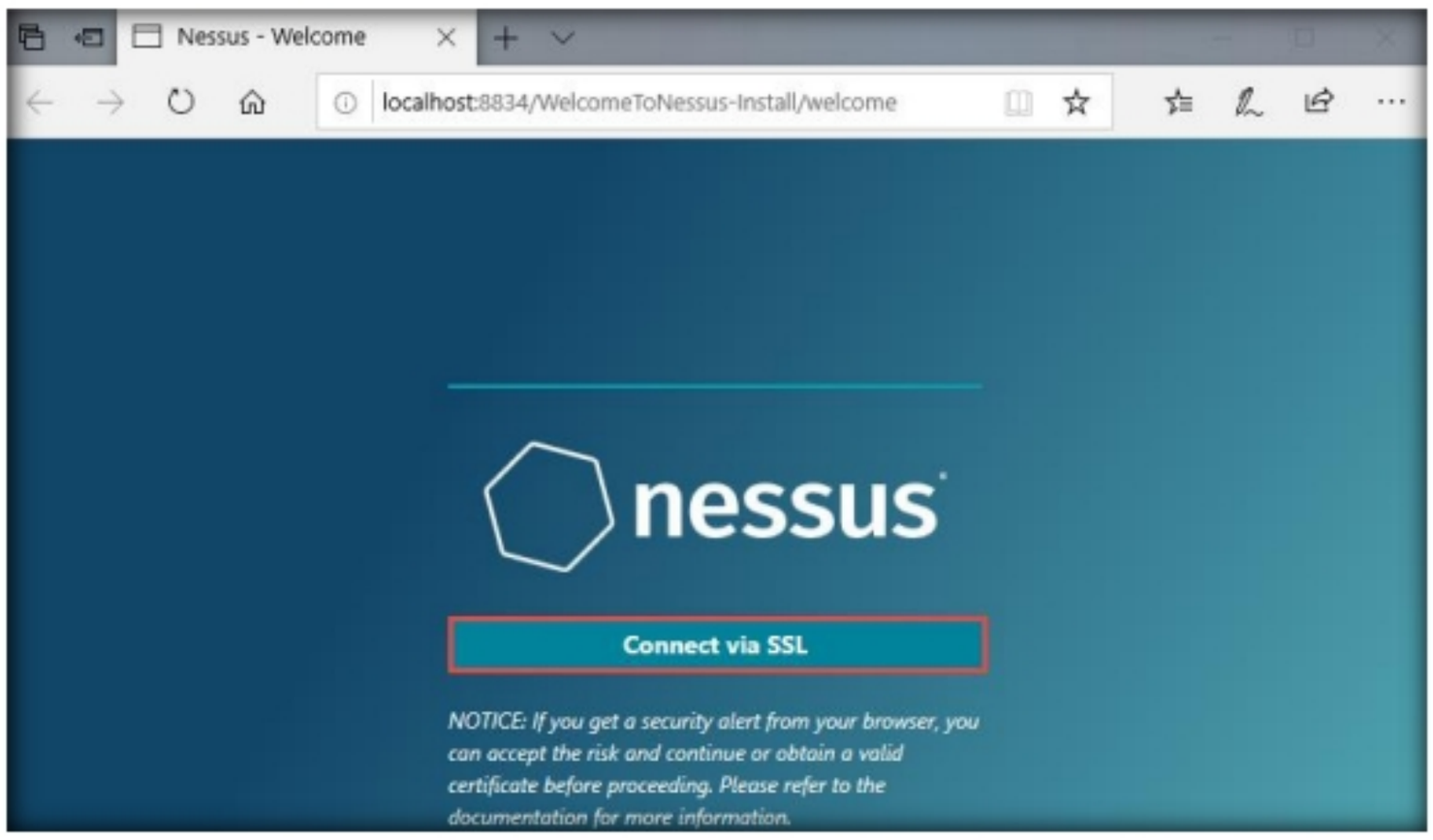


Figure 2.2.3: Nessus window: click Connect via SSL

7. **Tenable Nessus (x64) Installer Information** pop-up appears asking to restart the system for the configuration changes; click **No**.
8. **This site is not secure** page appears, expand the **Details** section and click **Go on to the webpage**.

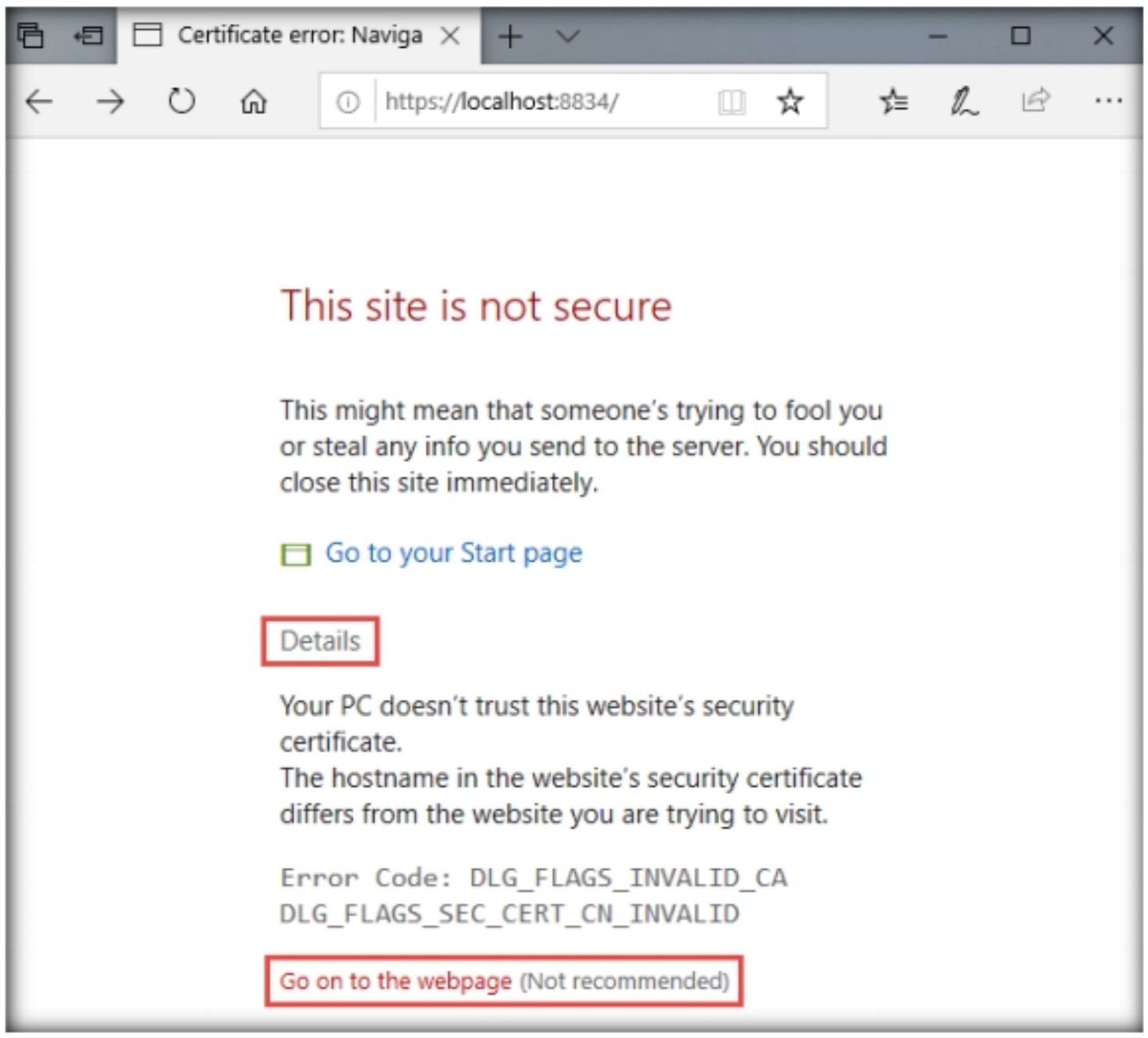


Figure 2.2.4: This site is not a secure webpage

9. **Welcome to Nessus** page appears, ensure that **Nessus Essentials** radio button is selected and click **Continue**.

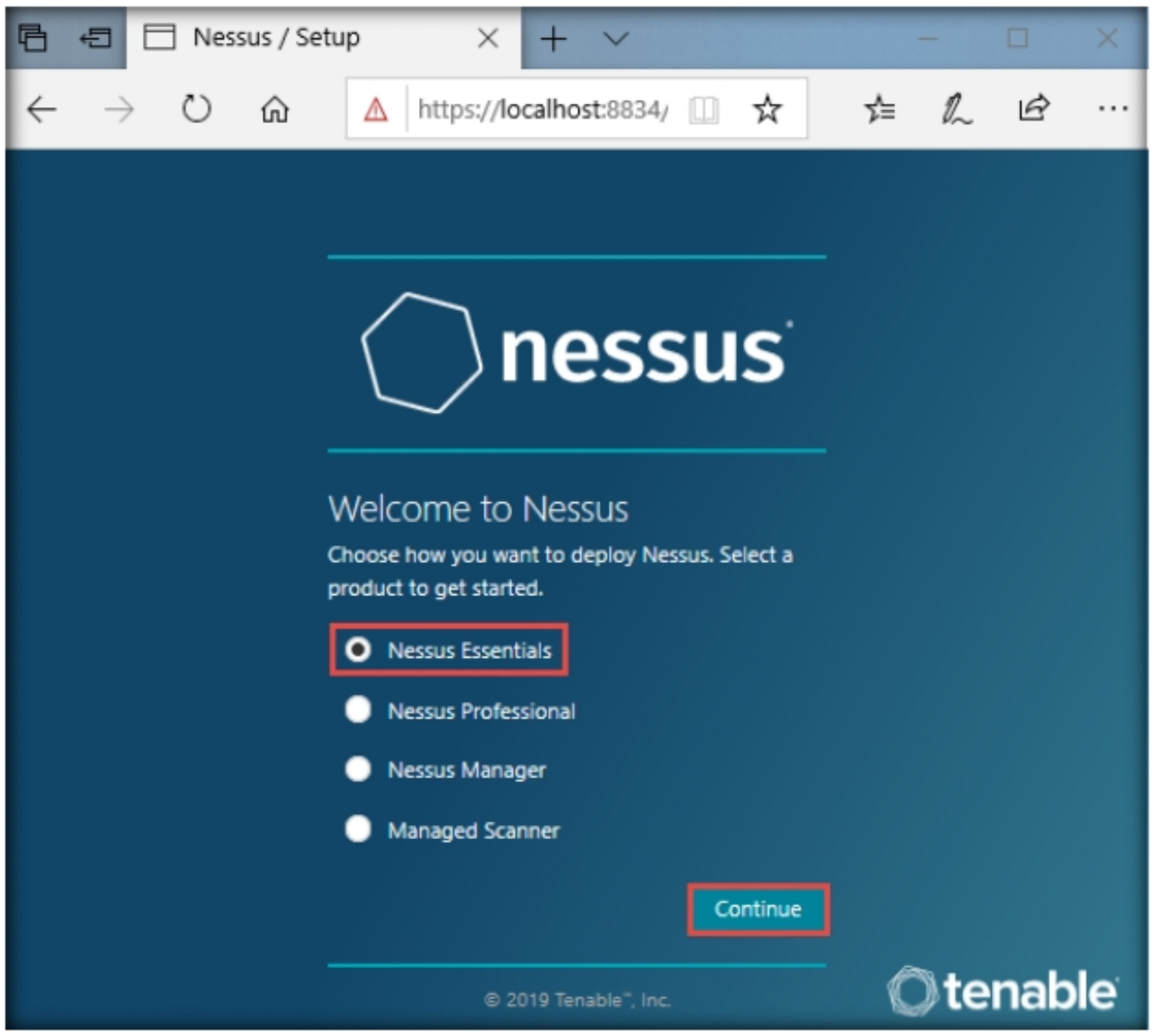


Figure 2.2.5: Welcome to Nessus

TASK 2.2

Register in Nessus to Obtain the Activation Code

10. The **Get an activation code** page appears. Enter your personal details and click the **Email** button.

Note: You can use an alias, however, you will need a valid e-mail to retrieve the activation code. Consider creating an alias e-mail account if you do not have one.

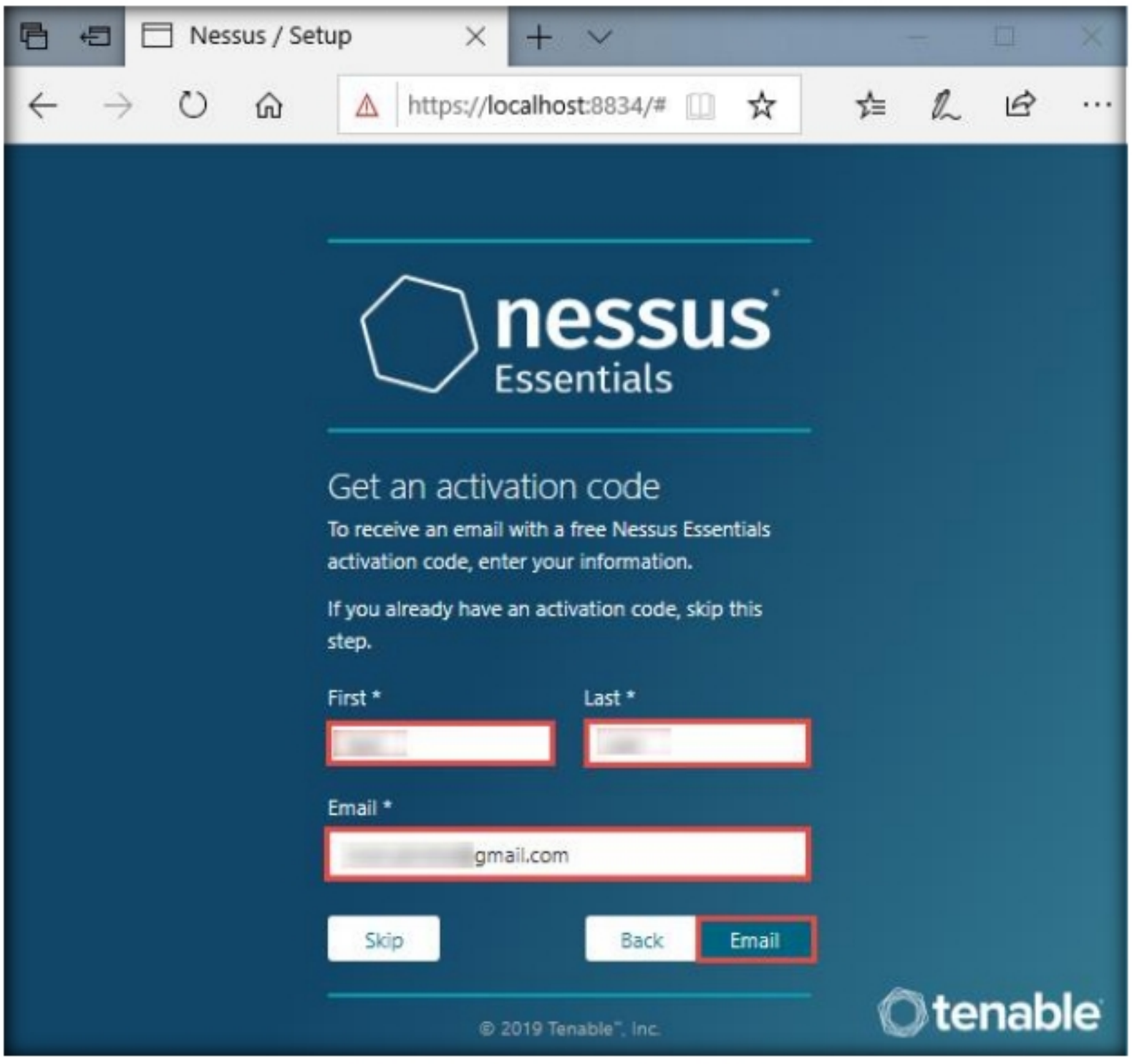


Figure 2.2.6: Get an activation code wizard

11. Once the above is completed, open a new tab and log in to your email account provided in the previous step, open the mail from **Tenable Nessus Essentials**, and copy the activation code. Close the web browser.

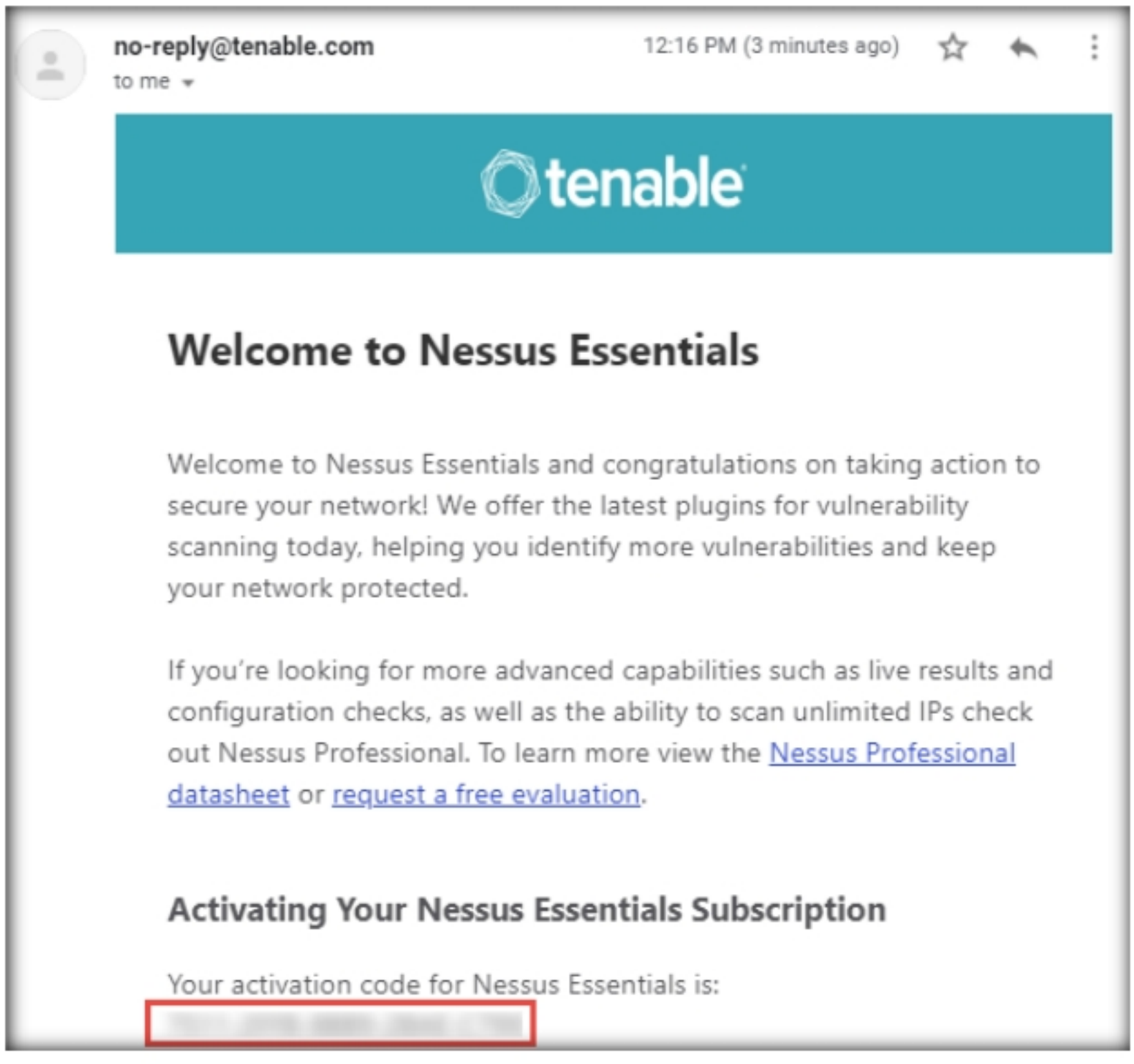


Figure 2.2.7: Activation code sent to your personal mail

12. Switch back to the **Microsoft Edge** web browser; in the **Register Nessus** page, paste the copied activation code in the **Activation Code** field; then, click **Continue**.

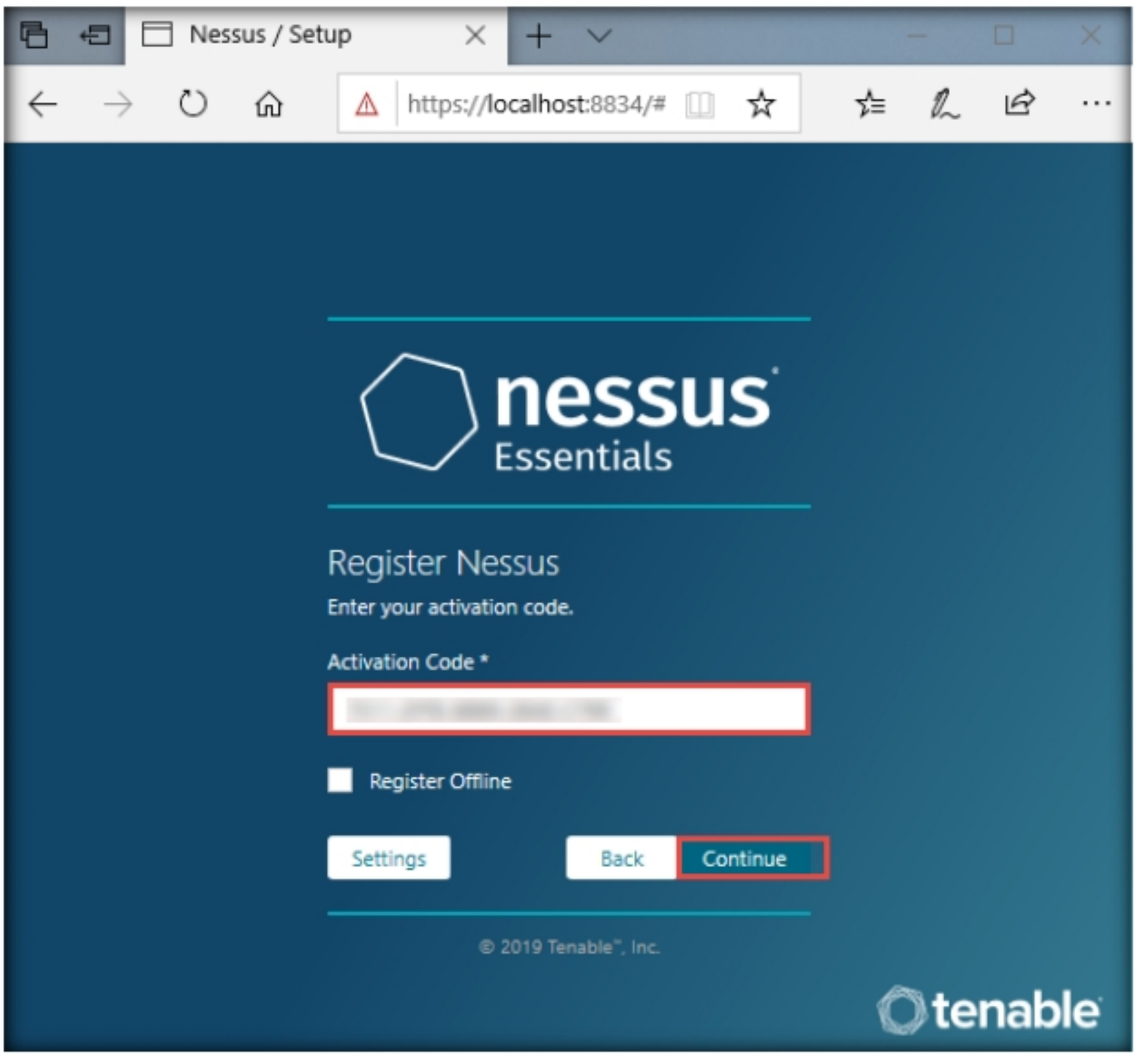


Figure 2.2.8: Register Nessus: Enter Activation Code

TASK 2.3

Create a User Account

13. **Create a user account** page appears. Create credentials for administrative control of the scanner. (here, Username: **Admin** and Password: **password**); then, click **Submit**.

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

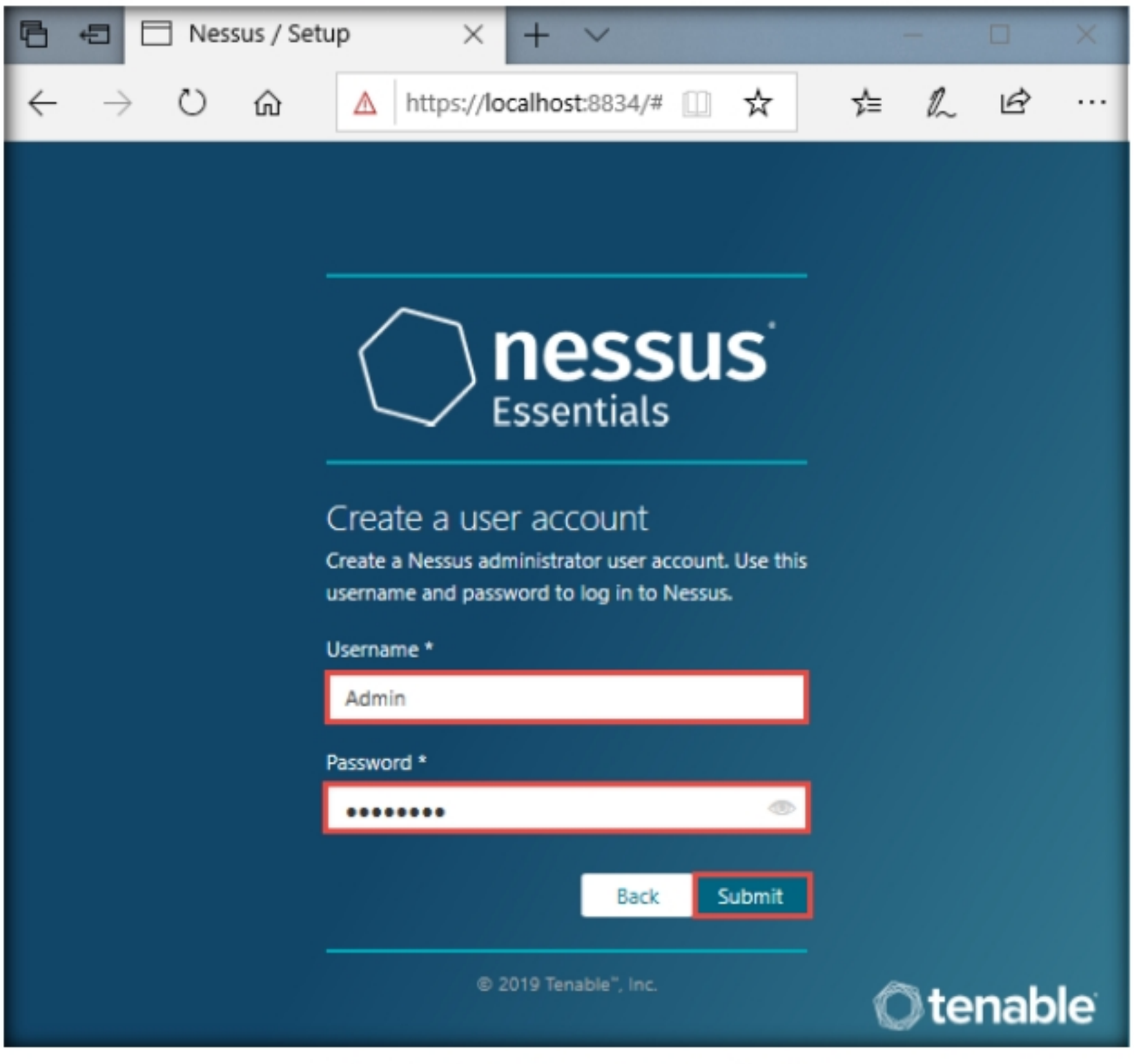


Figure 2.2.9: Create a user account: enter credentials

14. The **Downloading plugins...** wizard appears. Nessus will start fetching the plugins and will install them.

Note: It will take approximately 10 minutes to download plugins and perform the initialization.

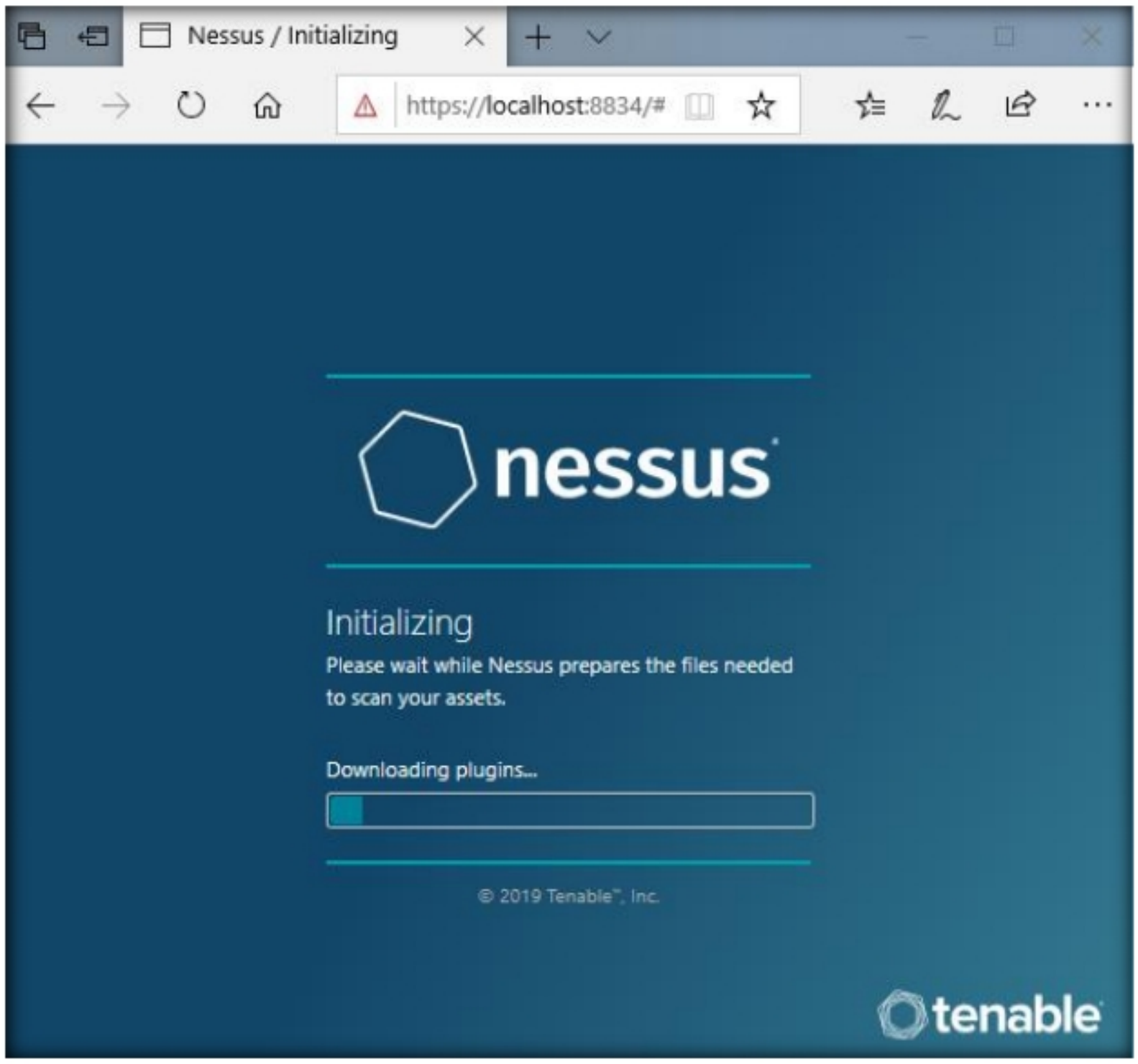


Figure 2.2.10: Nessus: Downloading plugins…

15. Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard appears along with the **Welcome to Nessus Essentials** pop-up. Close the pop-up.

Note: In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.

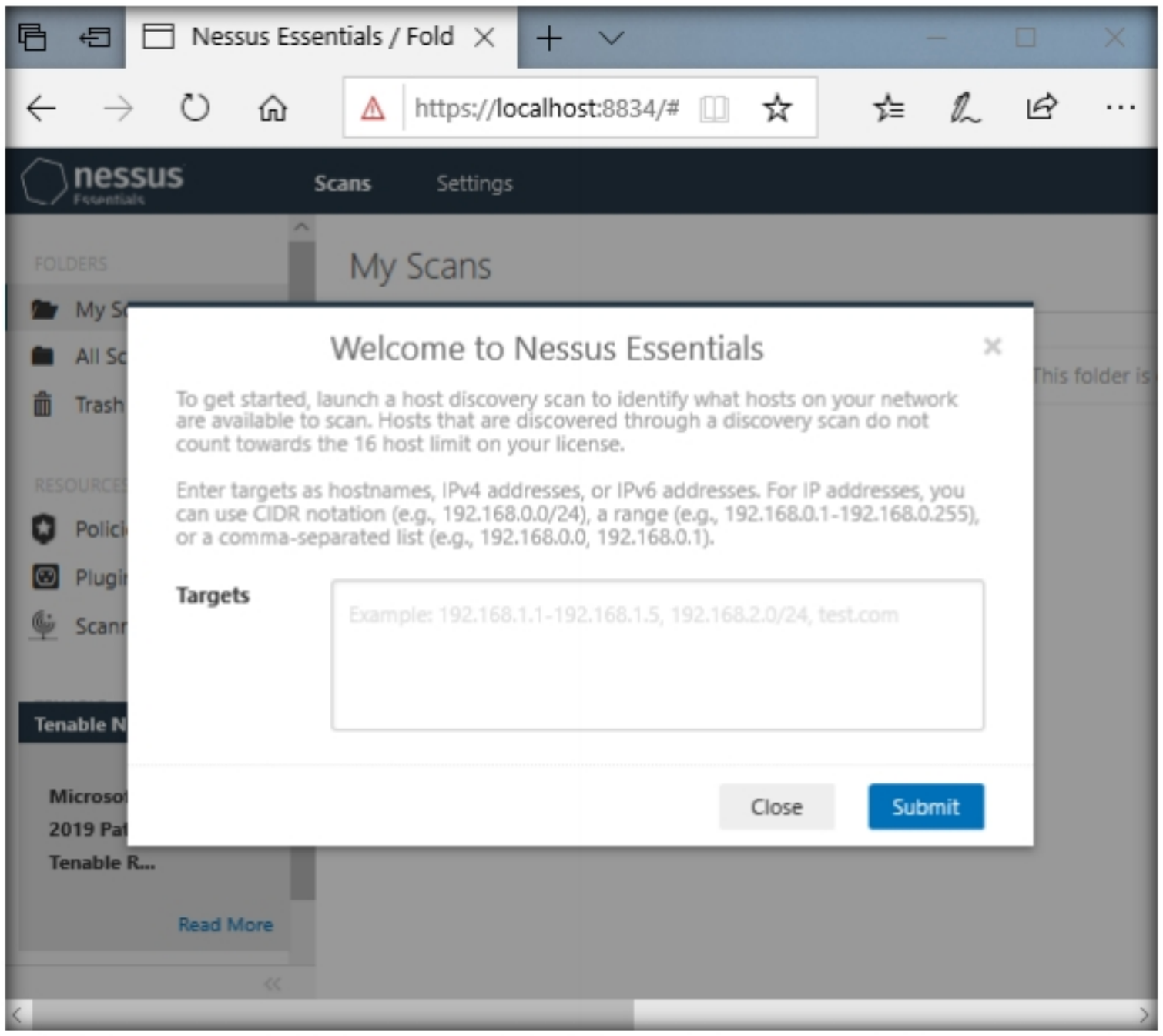


Figure 2.2.11: Welcome to Nessus Essentials page

TASK 2.4

Add a Network Policy

16. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.

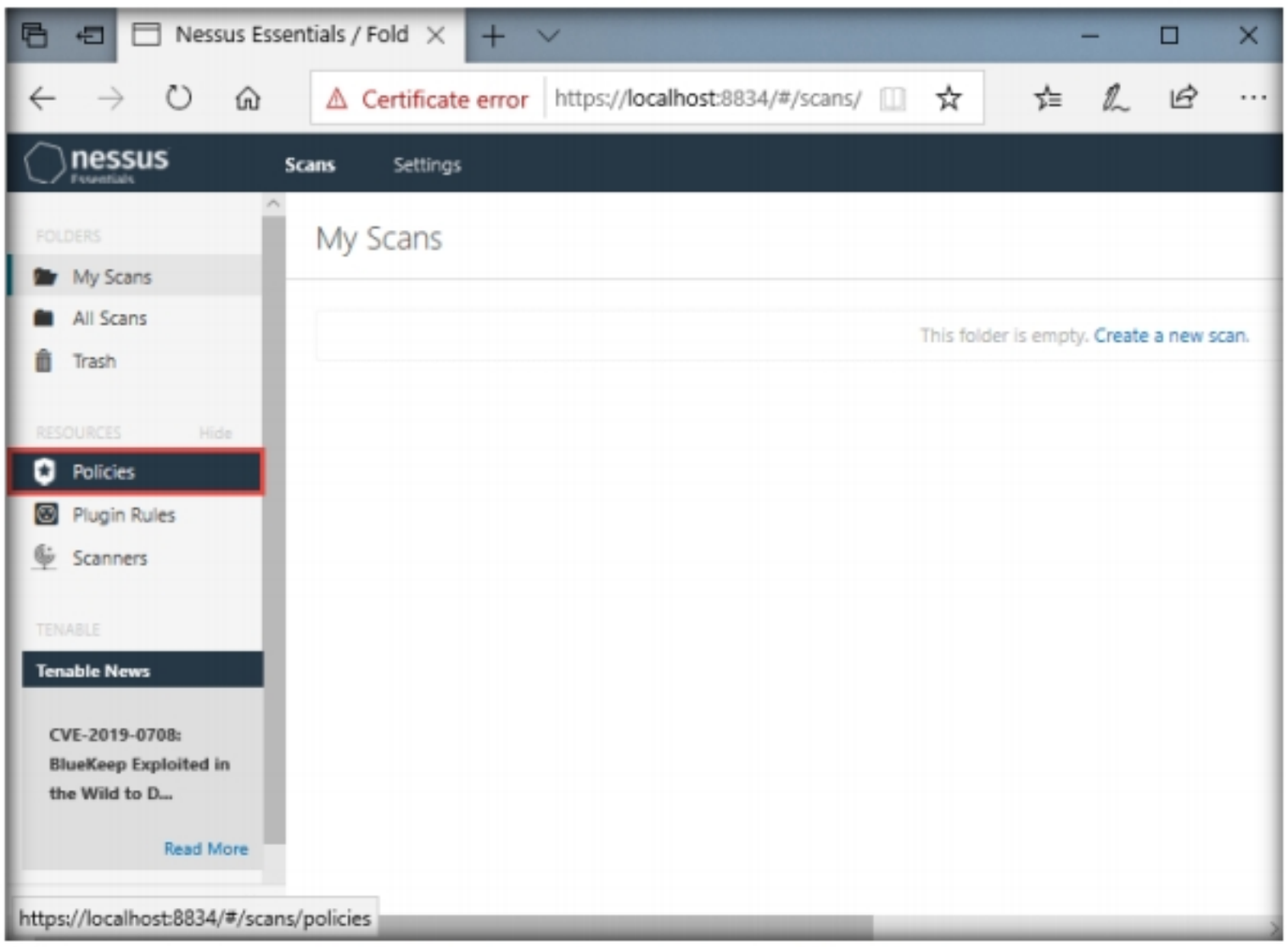


Figure 2.2.12: Nessus Essentials dashboard: Click Policies

17. The **Policies** window appears; click **Create a new policy**.

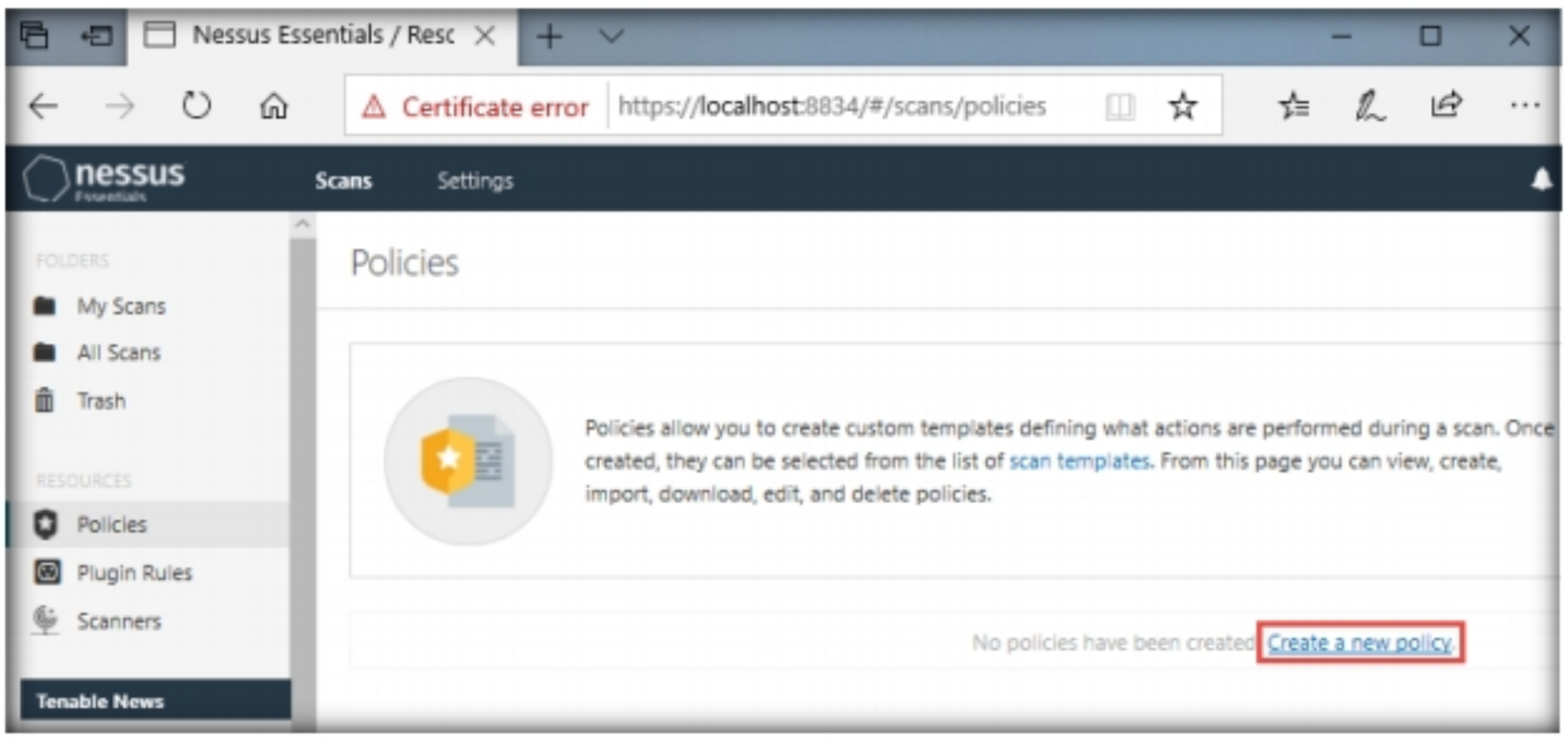


Figure 2.2.13: Adding a new policy in Nessus

18. The **Policy Templates** window appears; click **Advanced Scan**.

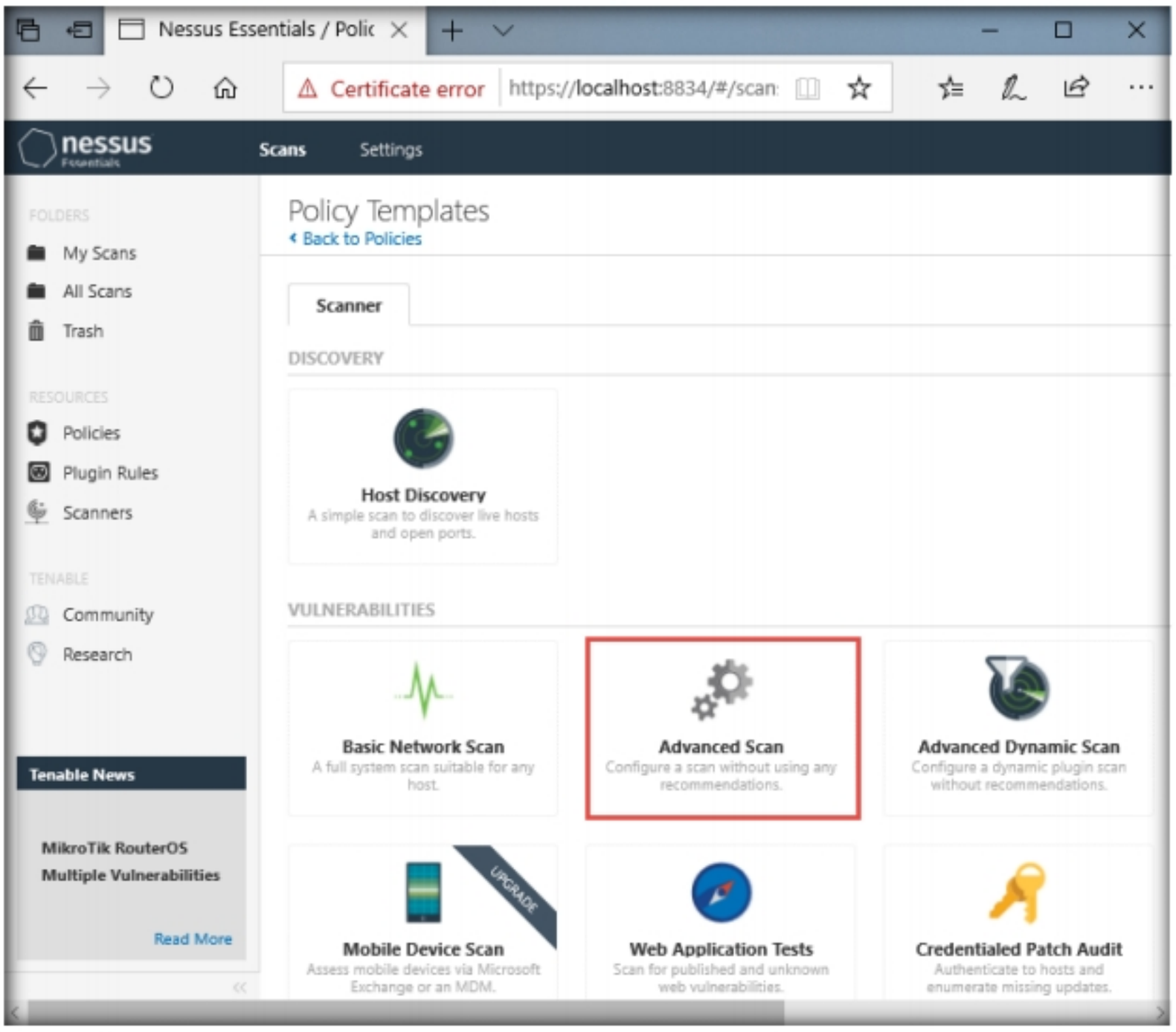


Figure 2.2.14: Choosing Advance Policy from the policy templates

TASK 2.5

Configure a Network Policy

19. The **New Policy / Advanced Scan** section appears. In the **Settings** tab under the **BASIC** setting type, specify a policy name in the **Name** field (here, **NetworkScan_Policy**), and give a **Description** about the policy (here, **Scanning a Network**).

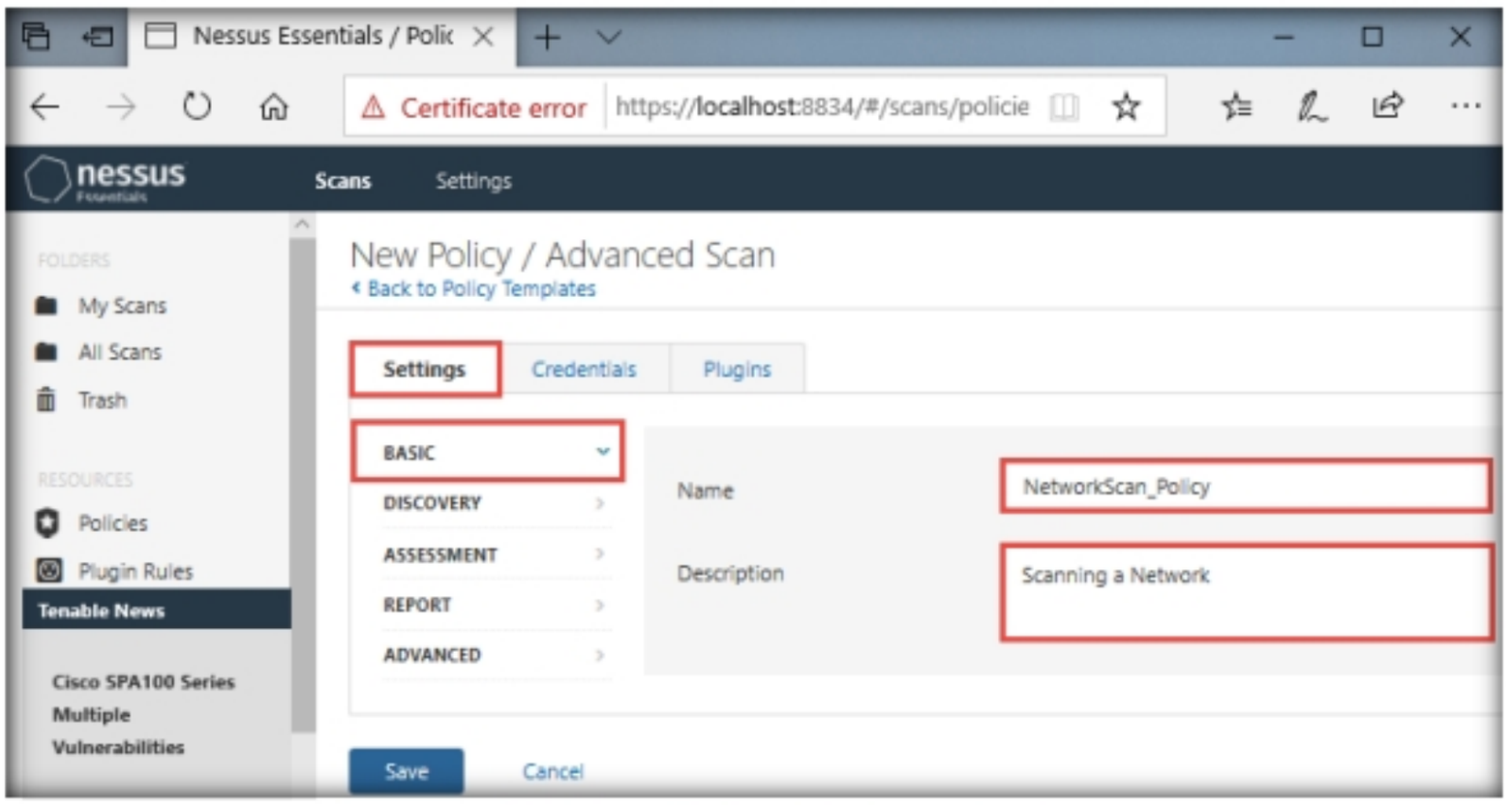


Figure 2.2.15: Customizing the general settings

20. In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.

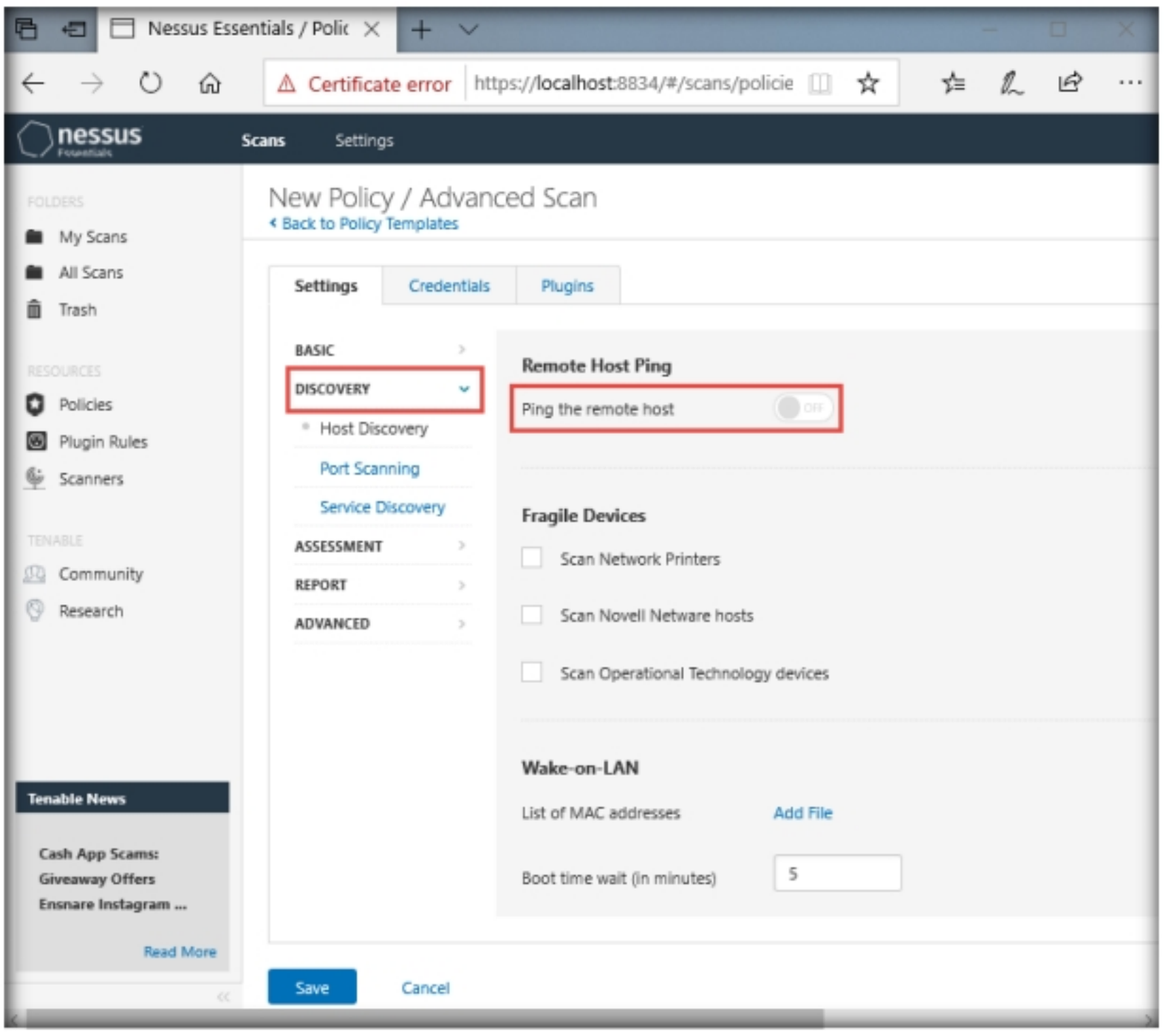


Figure 2.2.16: Policy General Settings window with Port Scanning Setting Type

21. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox. Leave the other fields with default options, as shown in the screenshot.

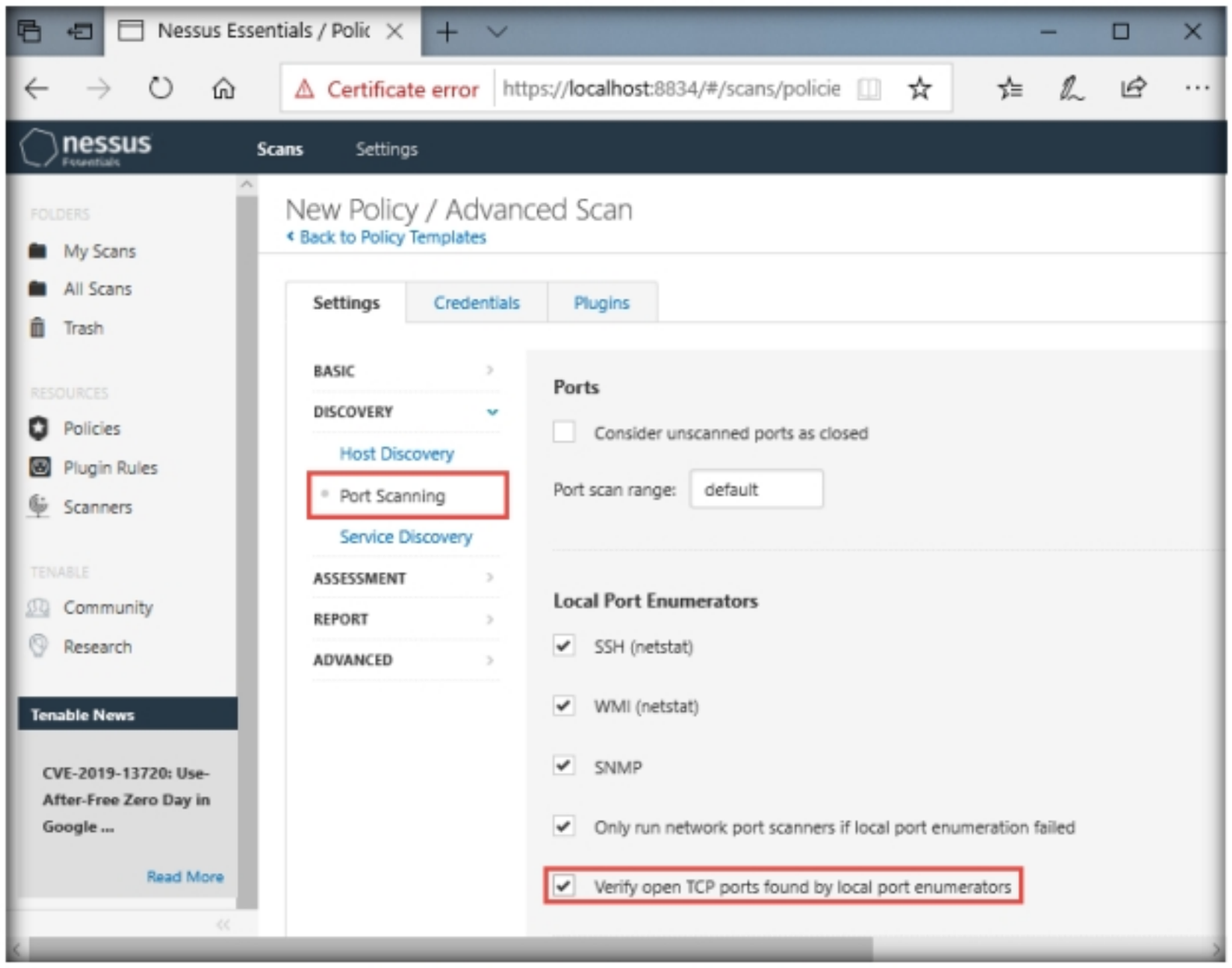


Figure 2.2.17: Customizing the Port Scanning Setting Type

22. Select the **ADVANCED** setting type. In the right pane, under the **Performance Options** settings, set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **Unlimited**.

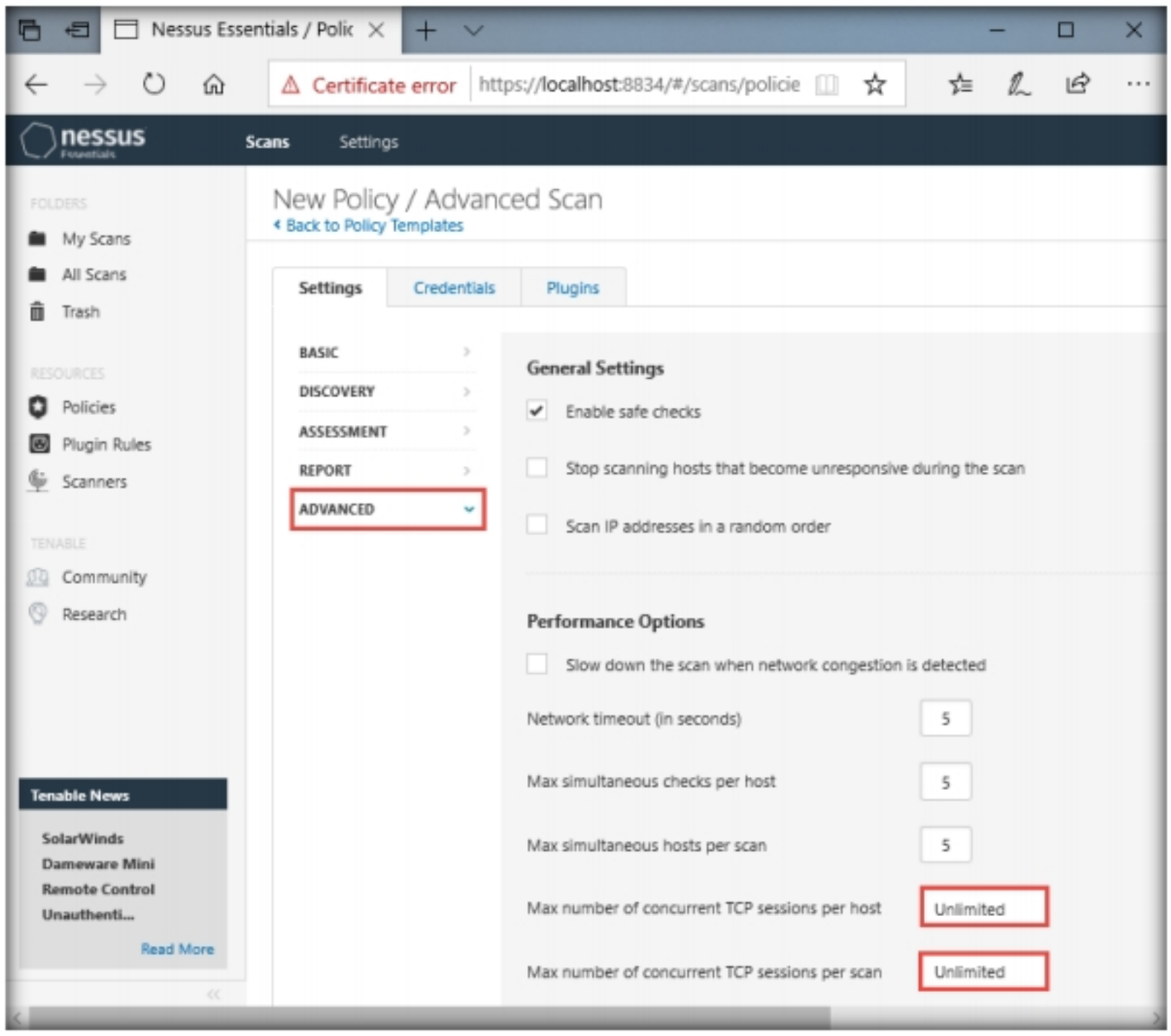


Figure 2.2.18: Advanced Setting Type window

23. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.

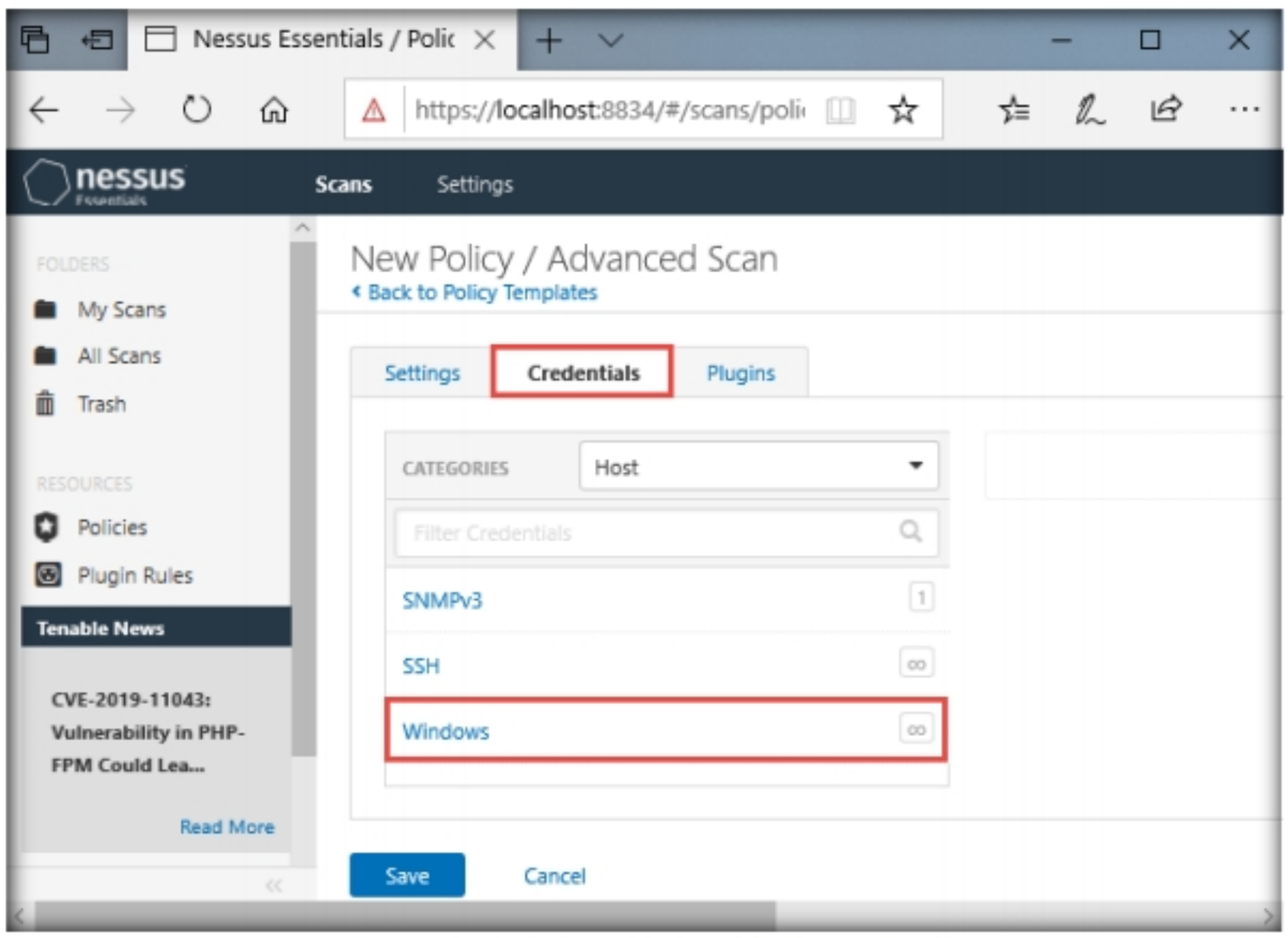


Figure 2.2.19: Adding Policies and setting Credentials

24. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123**/**qwerty@123**.

Note: Re-enter the created user account credentials, **Admin**/**password**, if session timeout notification pop-up appears.

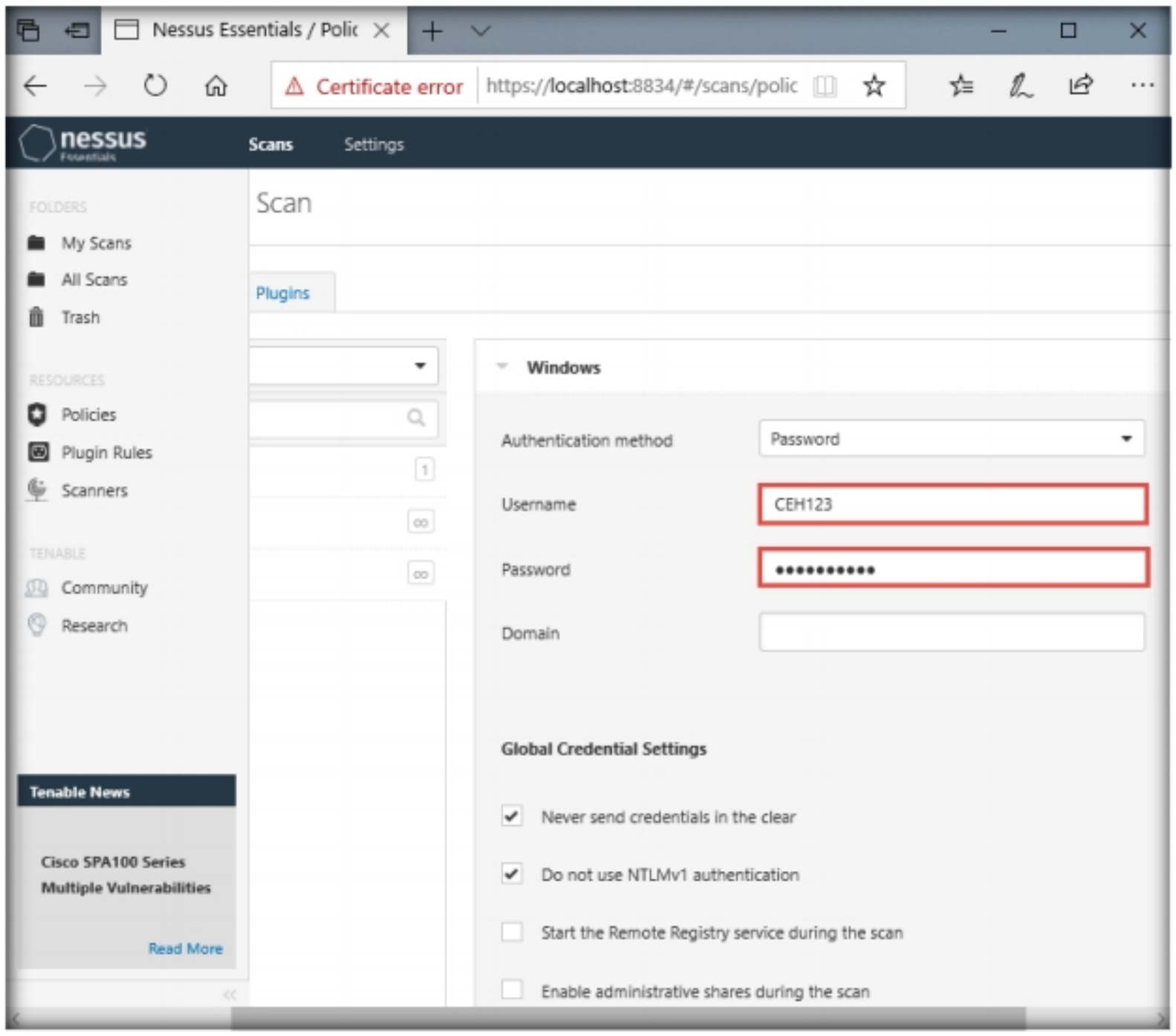


Figure 2.2.20: Customizing the windows credentials

25. Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.

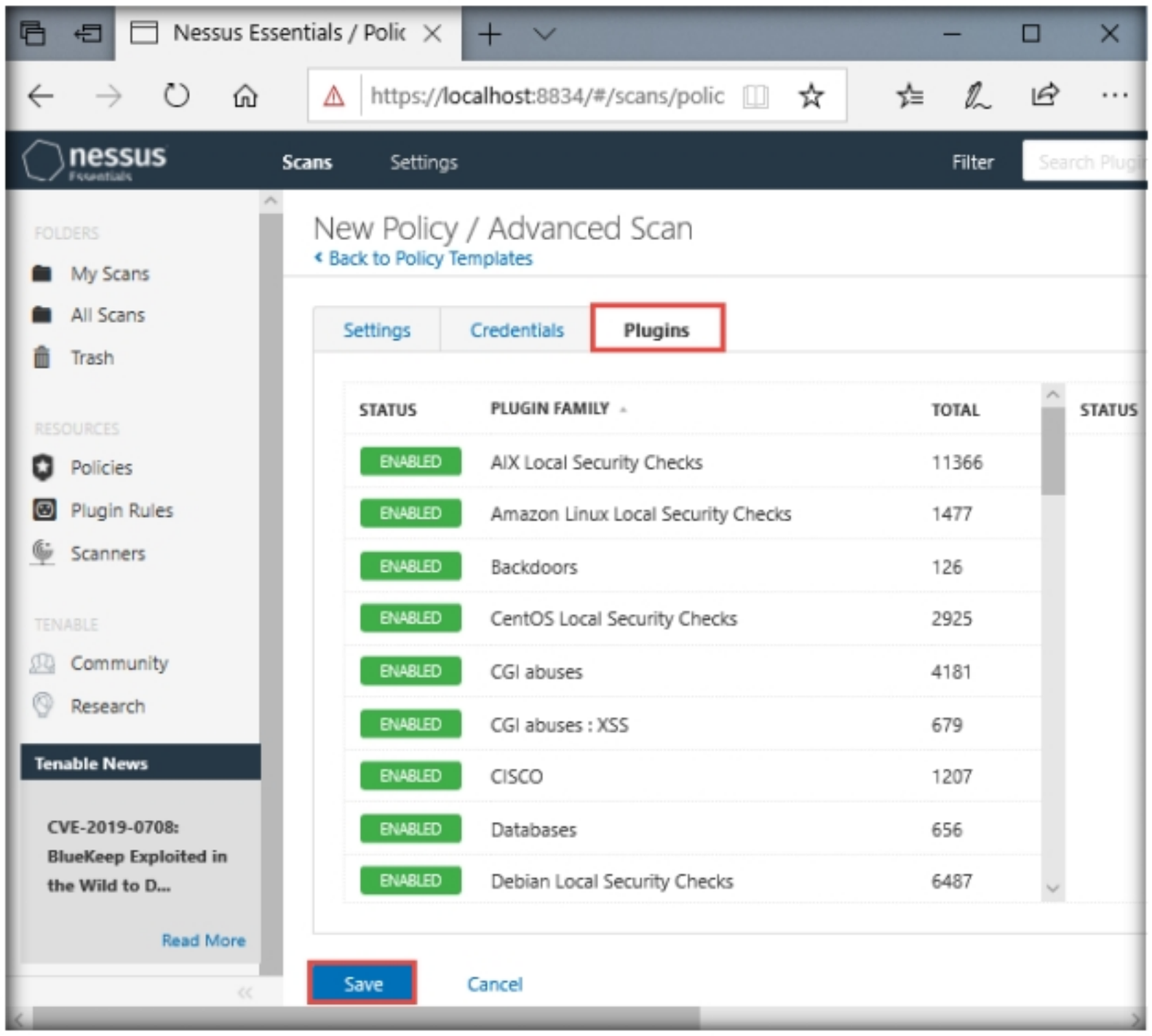


Figure 2.2.21: The Nessus: Policy Plugin Configurations window

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

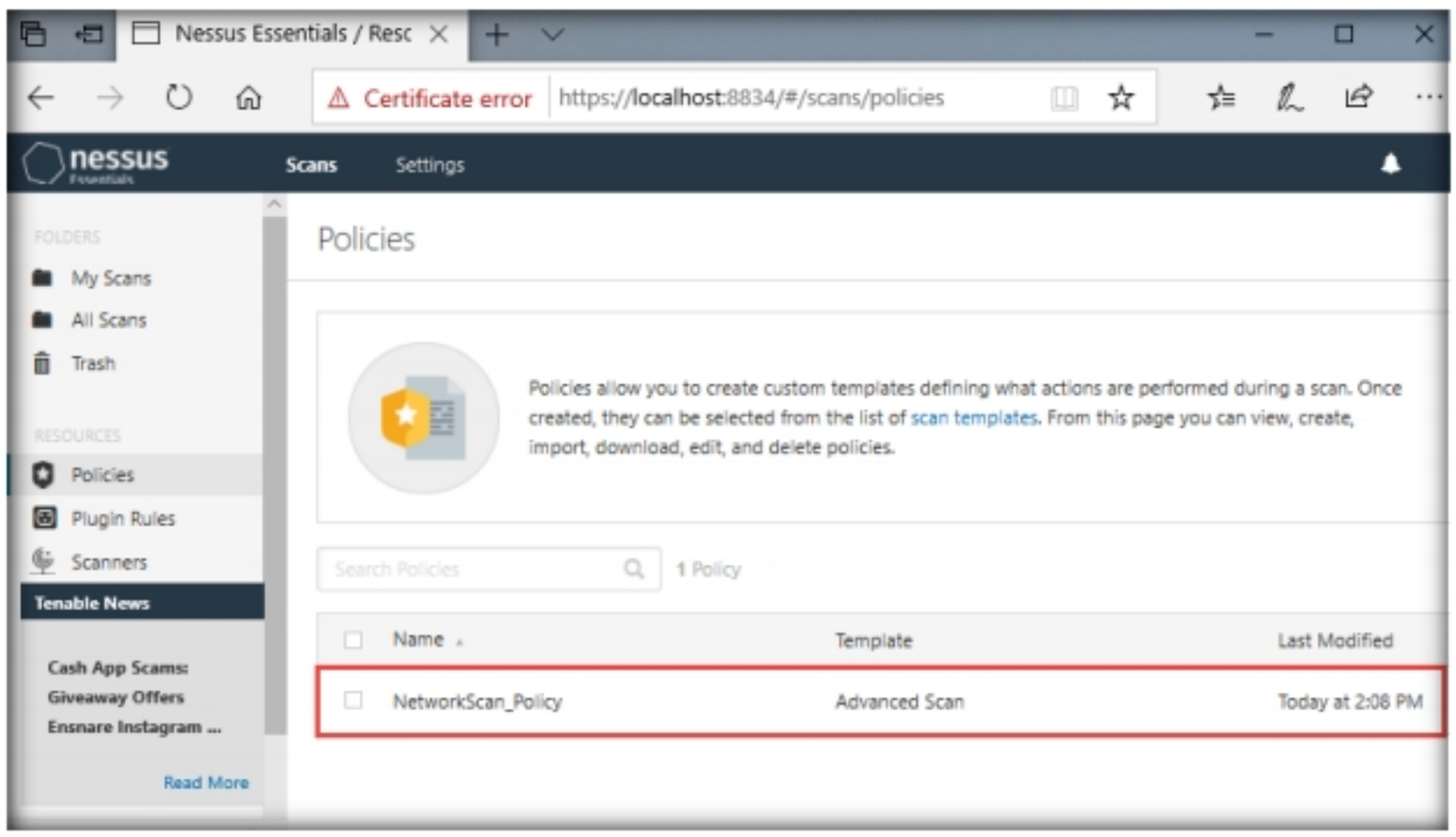


Figure 2.2.22: The Nessus: Policies window with the newly added policy

27. Now, click **Scans** from the menu bar to open **My Scans** window; click **Create a new scan**.

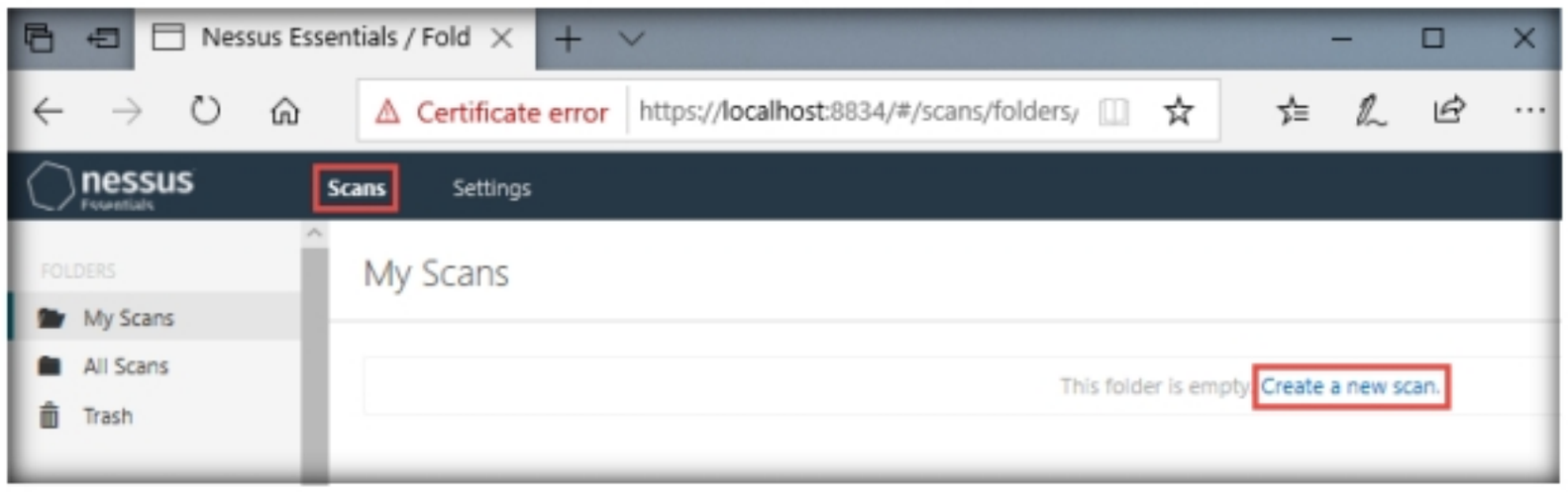


Figure 2.2.23: Setting a new scan in Nessus

28. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan Policy**.

Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin**/**password**).

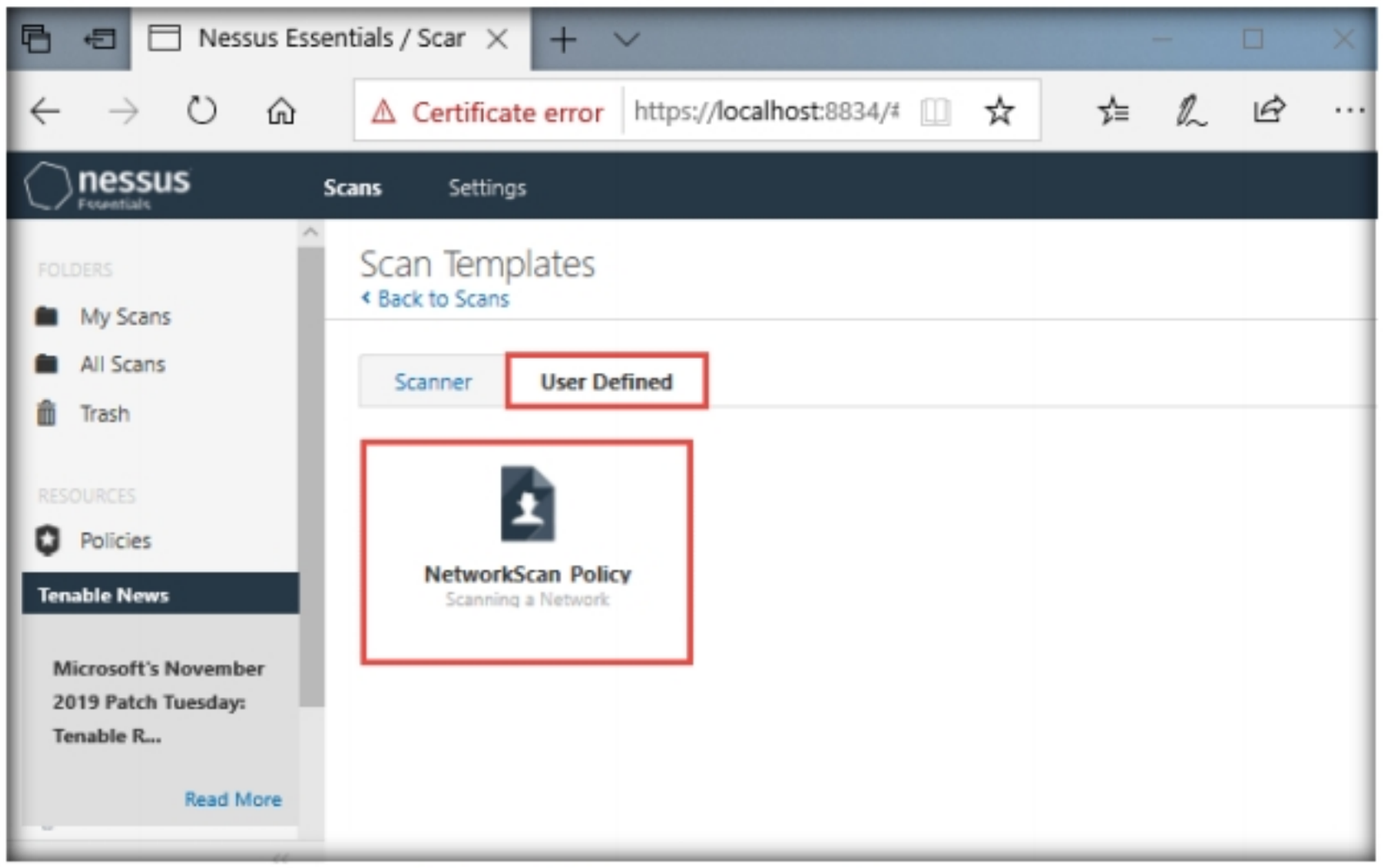


Figure 2.2.24: Setting a new scan in Nessus

29. The **New Scan / NetworkScan_Policy** window appears. Under **General Settings** in the right pane, input the **Name** of the scan (here, **Local Network**) and enter the **Description** for the scan (here, **Scanning a local network**); in the **Targets** field, enter the IP address of the target on which you want to perform the vulnerability analysis. In this lab, the target IP address is **10.10.10.16** (**Windows Server 2016**).

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

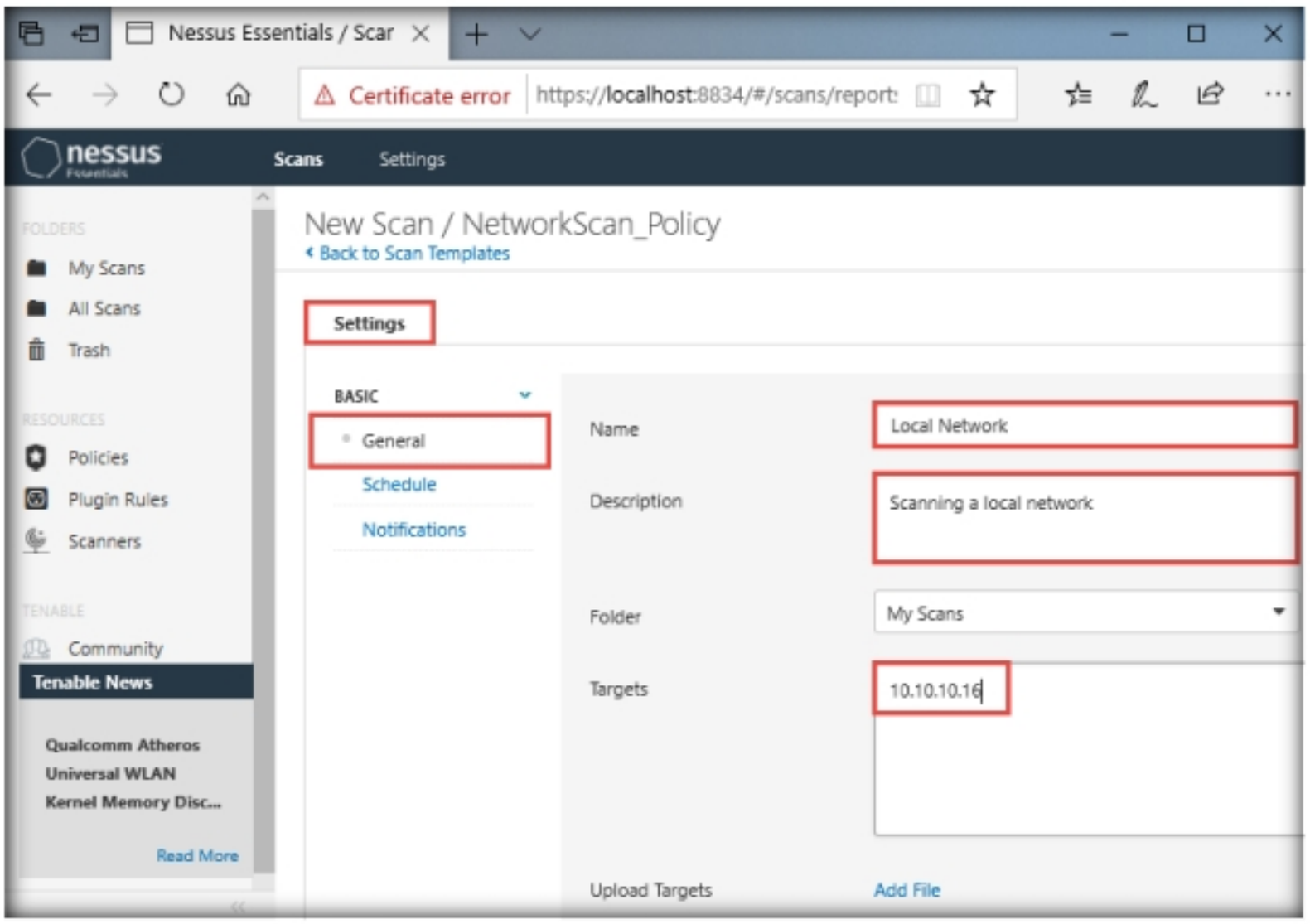


Figure 2.2.25: Configuring the basic settings in the scans window

TASK 2.6

Launch a Network Scan

30. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.

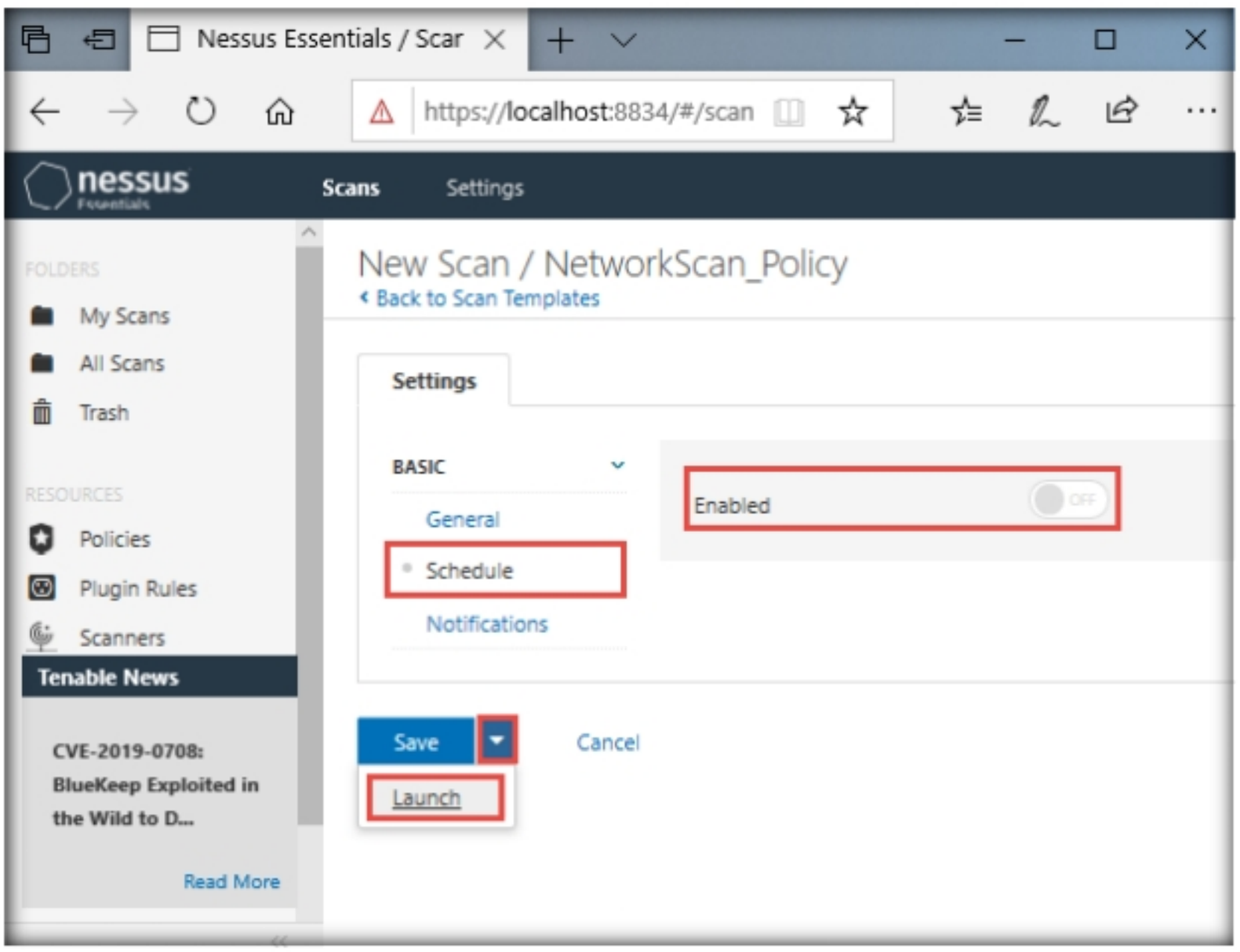


Figure 2.2.26: Setting a scan schedule

31. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.

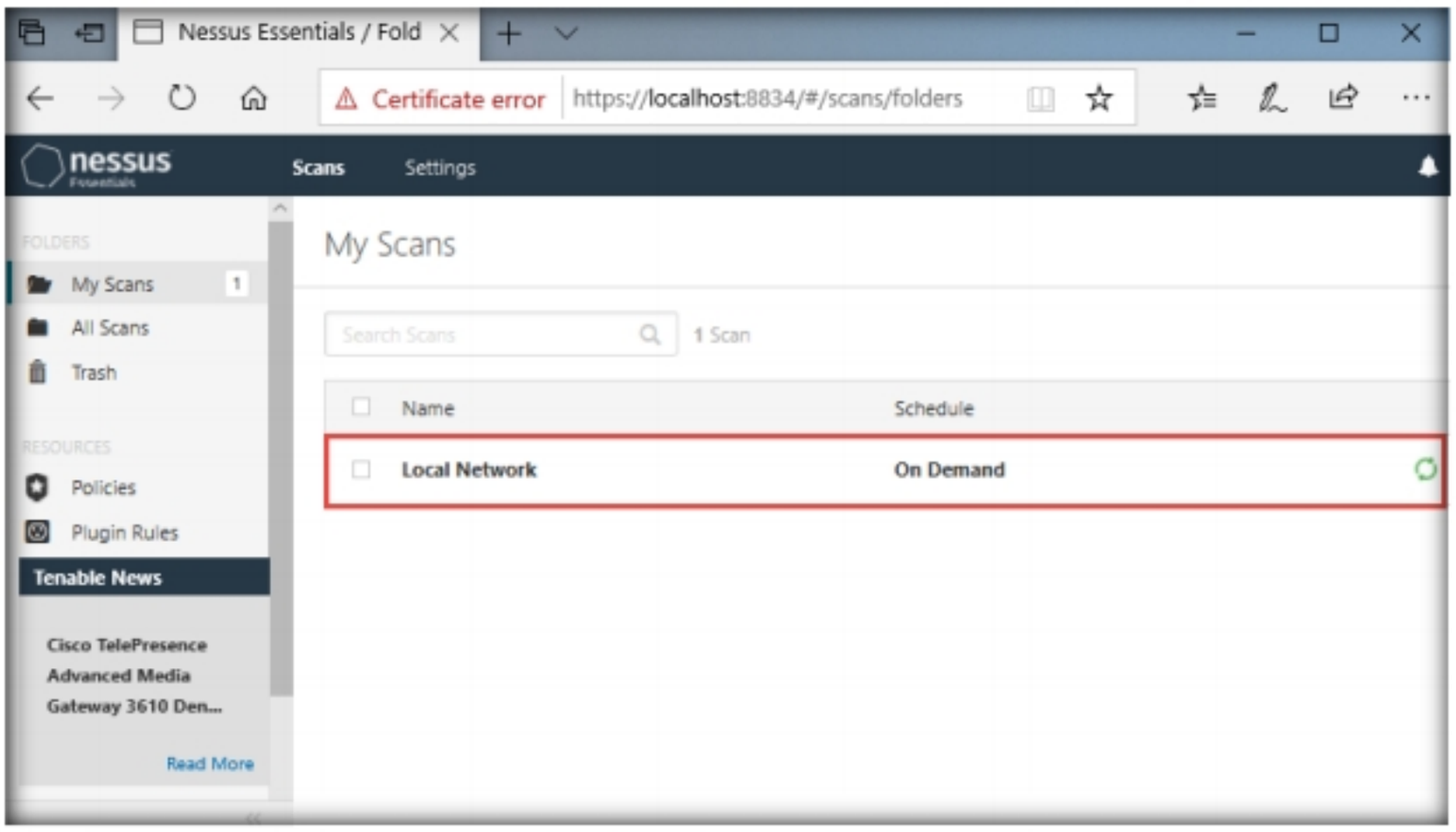


Figure 2.2.27: Local Network scanning

32. After the completion of the scan: click **Local Network** to view the detailed results.

TASK 2.7

Examine the Vulnerabilities

33. The **Local Network** window appears, displaying the summary of target hosts, as well as the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab, as shown in the screenshot.

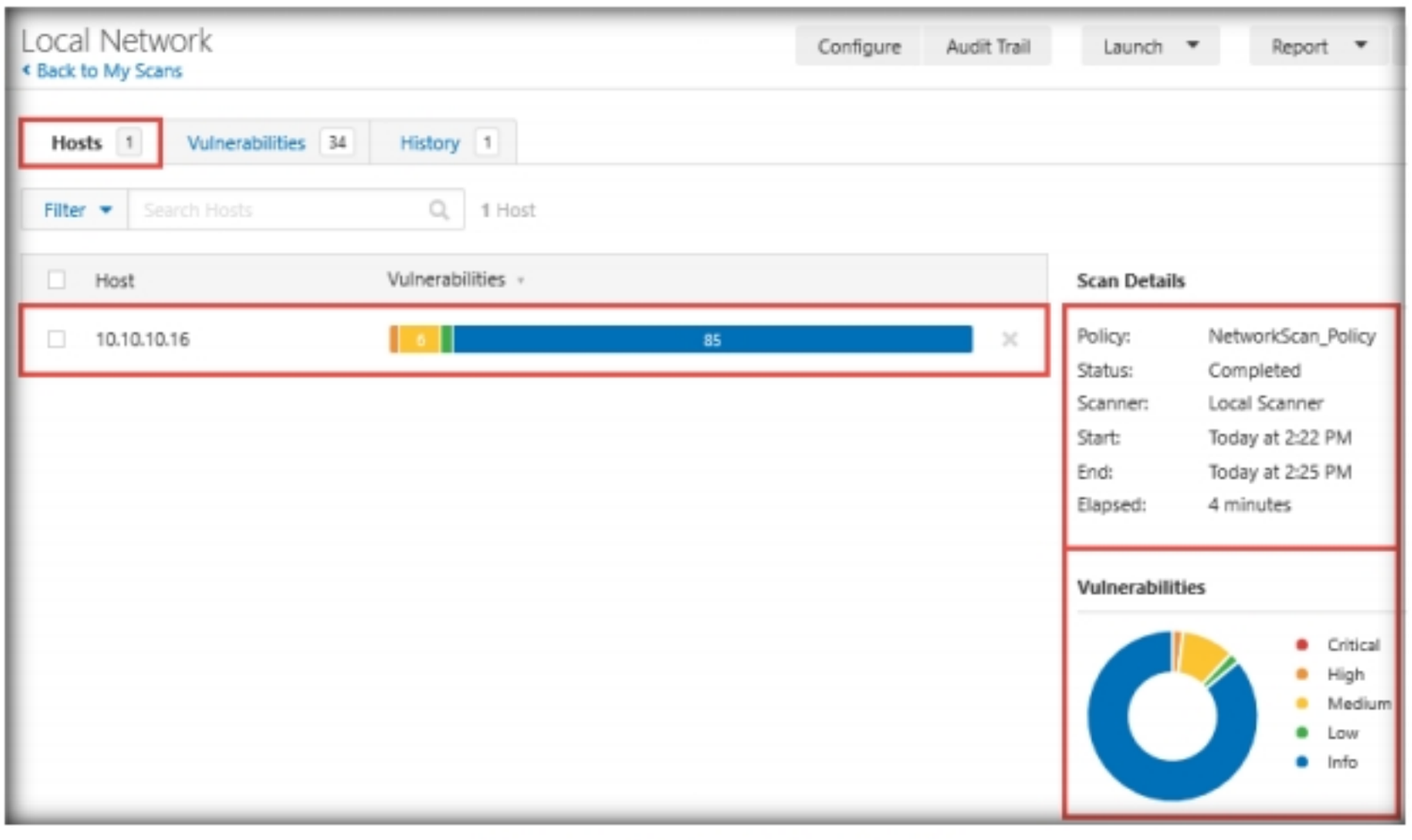


Figure 2.2.28: Hosts Summary window

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

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

35. Click these vulnerabilities to view detailed reports about each. For instance, in this lab, we are selecting the first vulnerability in the list, that is, **SNMP (Multiple Issues)**.

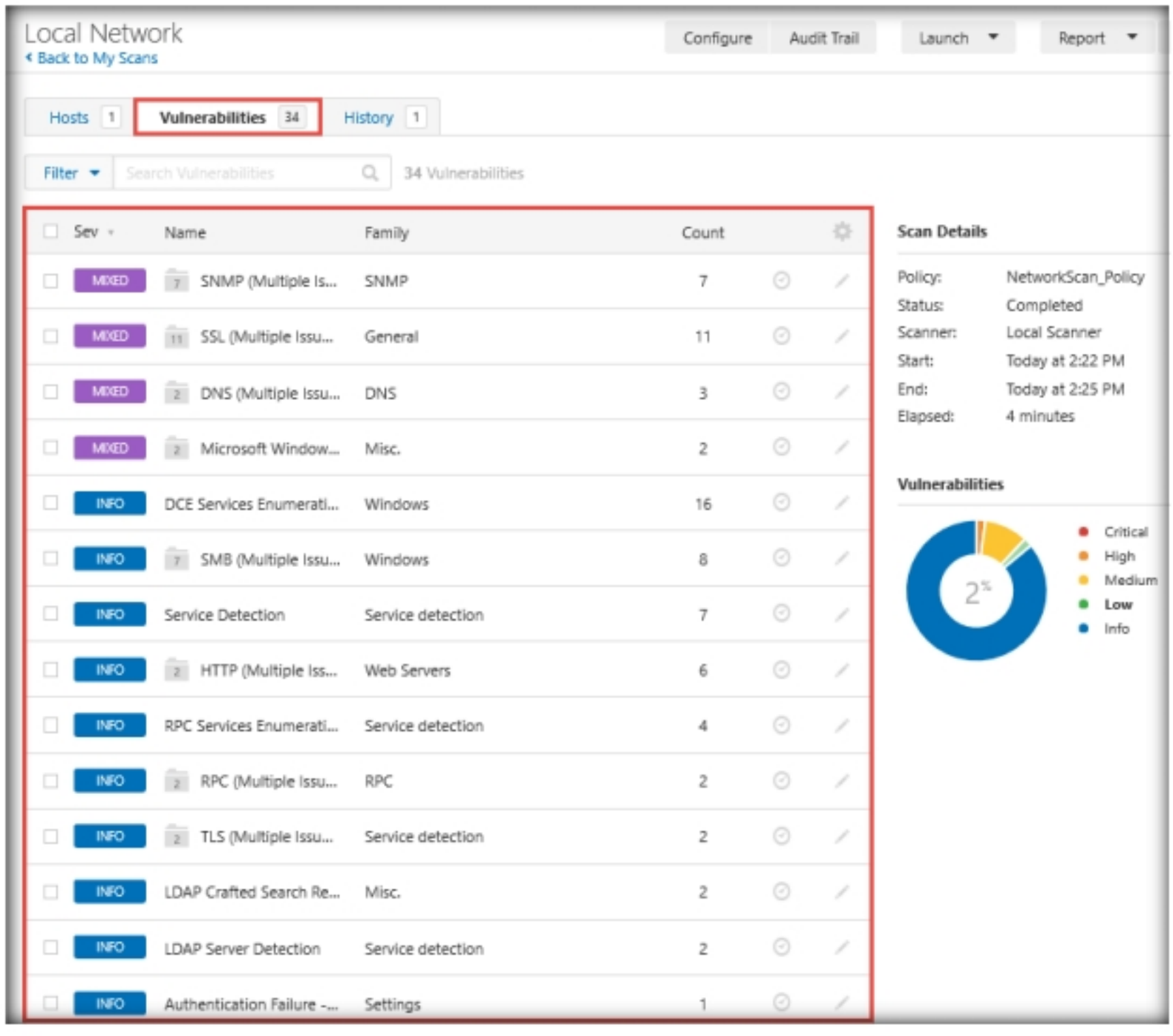


Figure 2.2.29: Vulnerability Summary window

36. The **Local Network / SNMP (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SNMP Agent Default**) to view its detailed information.

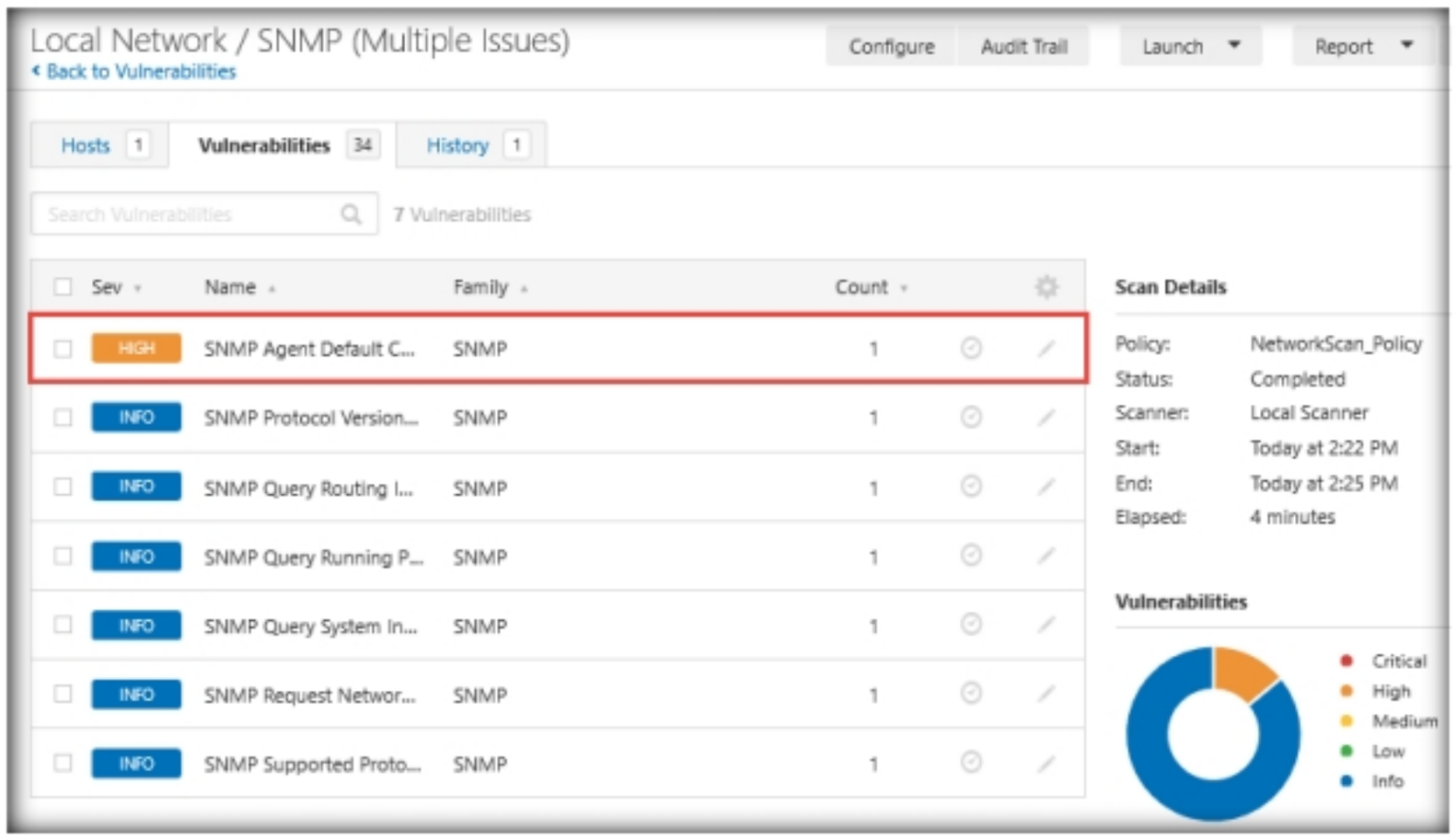


Figure 2.2.30: List of issues in SNMP

37. The report regarding selected vulnerability **SNMP Agent Default Community Name (public)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

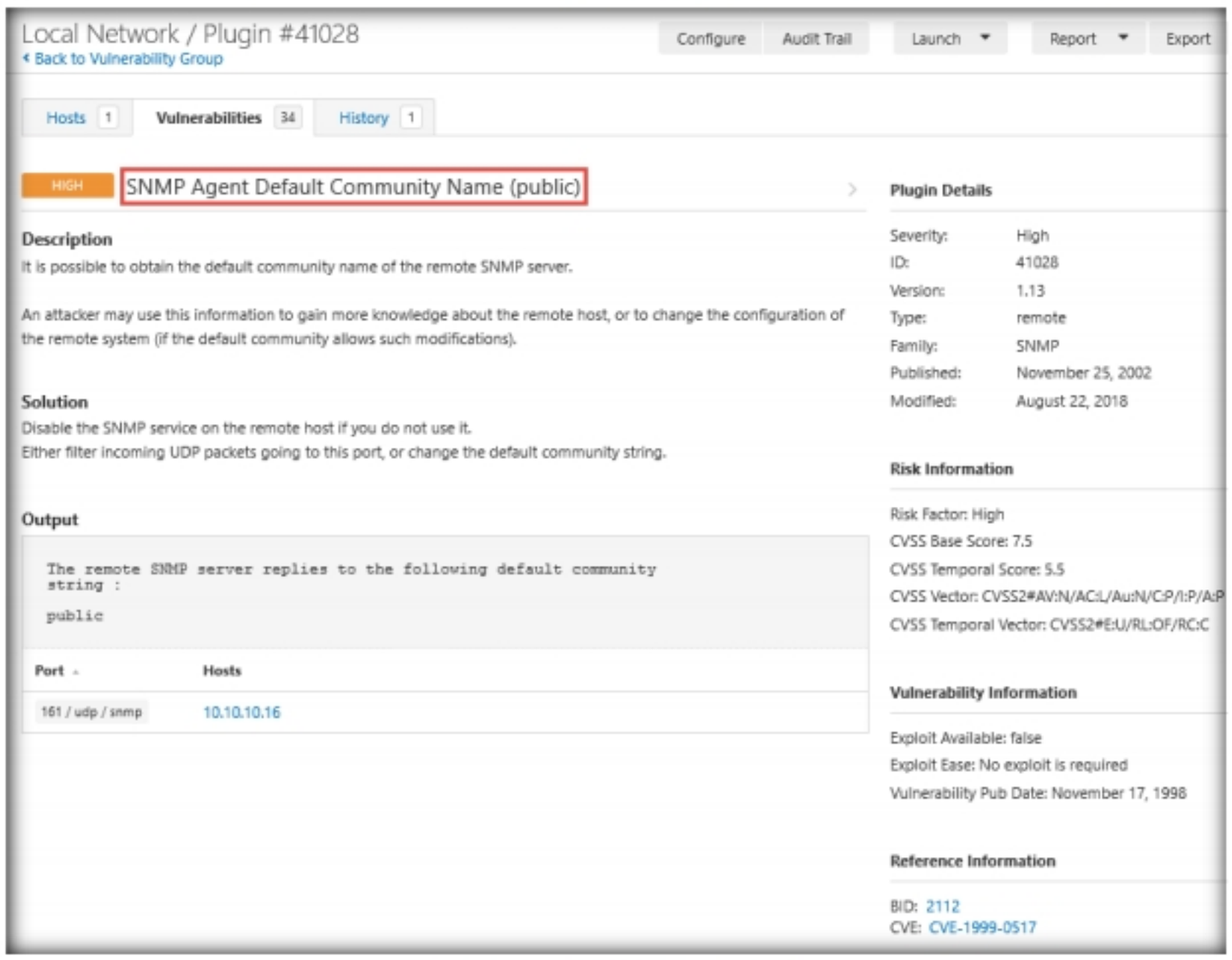


Figure 2.2.31: Vulnerability report

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

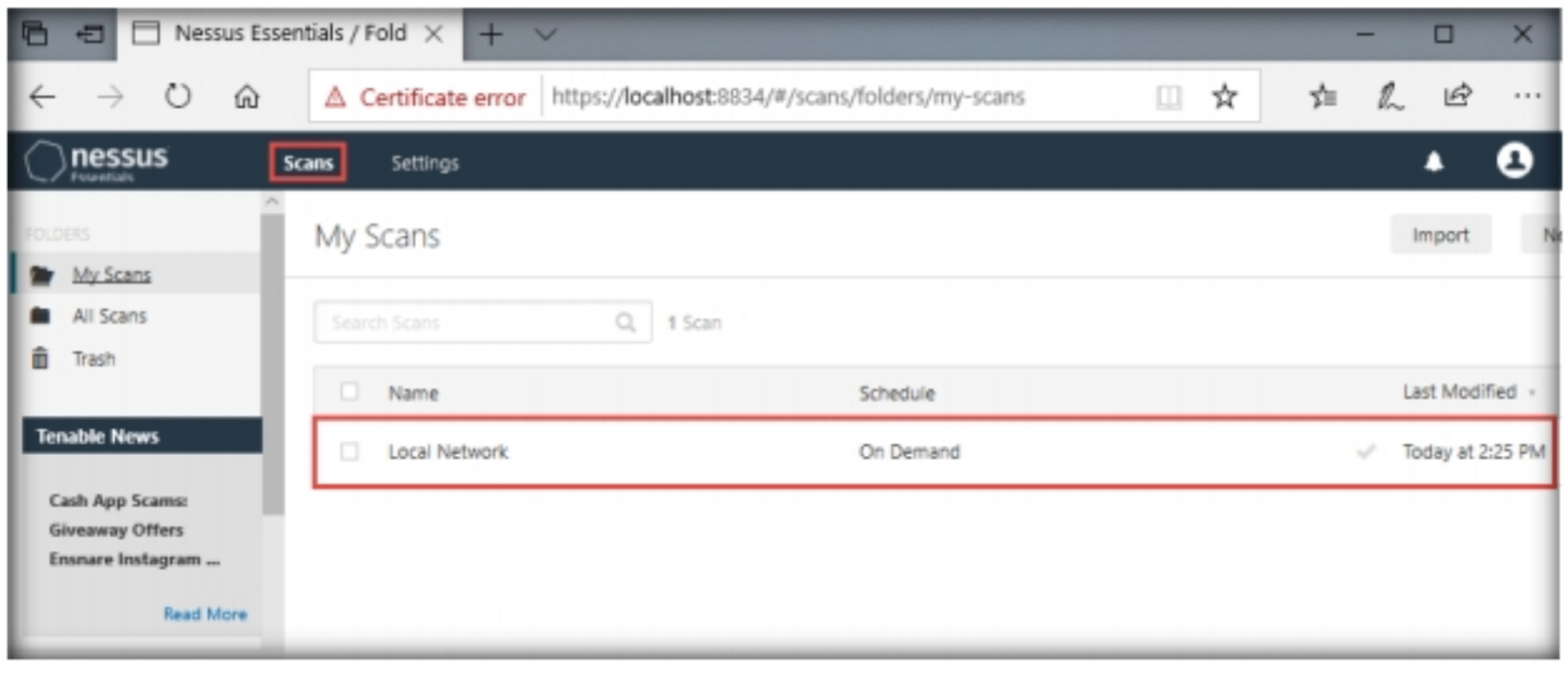


Figure 2.2.32: Selecting a Local Network Scan

TASK 2.8

Generate a Vulnerability Report

39. In the **Local Network** window, click the **Report** tab from the top-right corner, and choose a file format (here, **HTML**) from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.

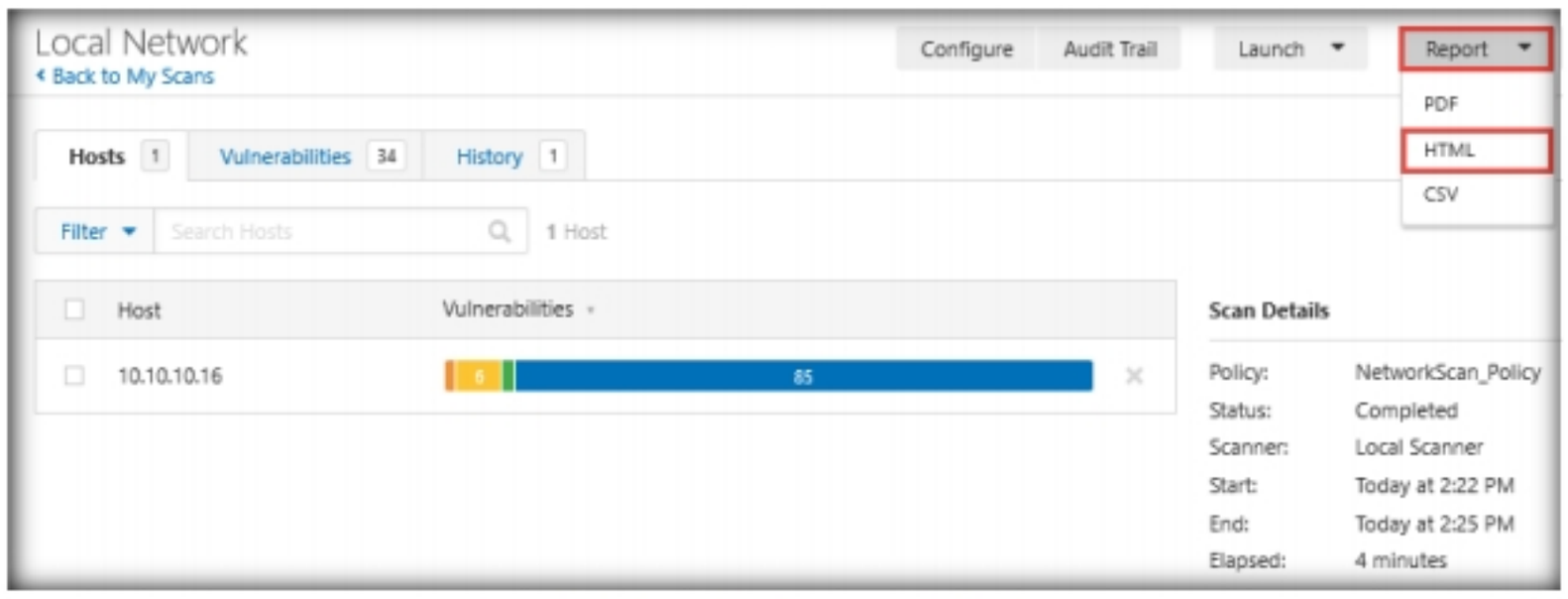


Figure 2.2.33: Exporting Report to HTML Format

40. The **Generate HTML Report** pop-up appears: leave the **Report** type option on default (**Executive Summary**). Click **Generate Report** to download the report.

Note: If the **What do you want to do with Local_Network_5cfvy7.html?** pop-up appears, click **Save**.

Note: The file name might differ in your lab environment.

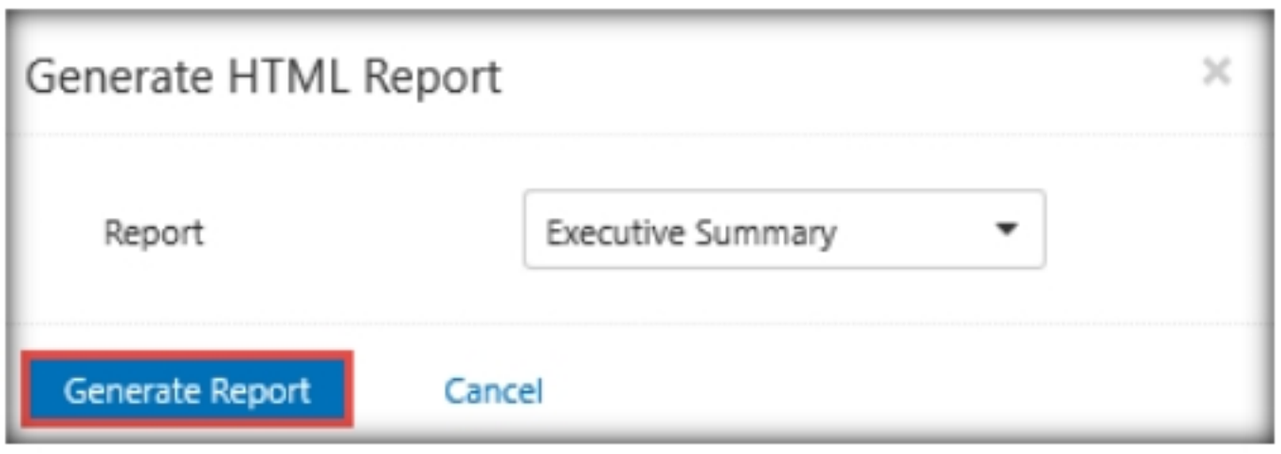


Figure 2.2.34: Export as HTML window appears

41. Once the download is finished, a pop-up appears at the bottom of the browser; click **Open**.
42. If the **How do you want to open this file?** pop-up appears, choose any browser (here, **Firefox**) to view the downloaded HTML file.

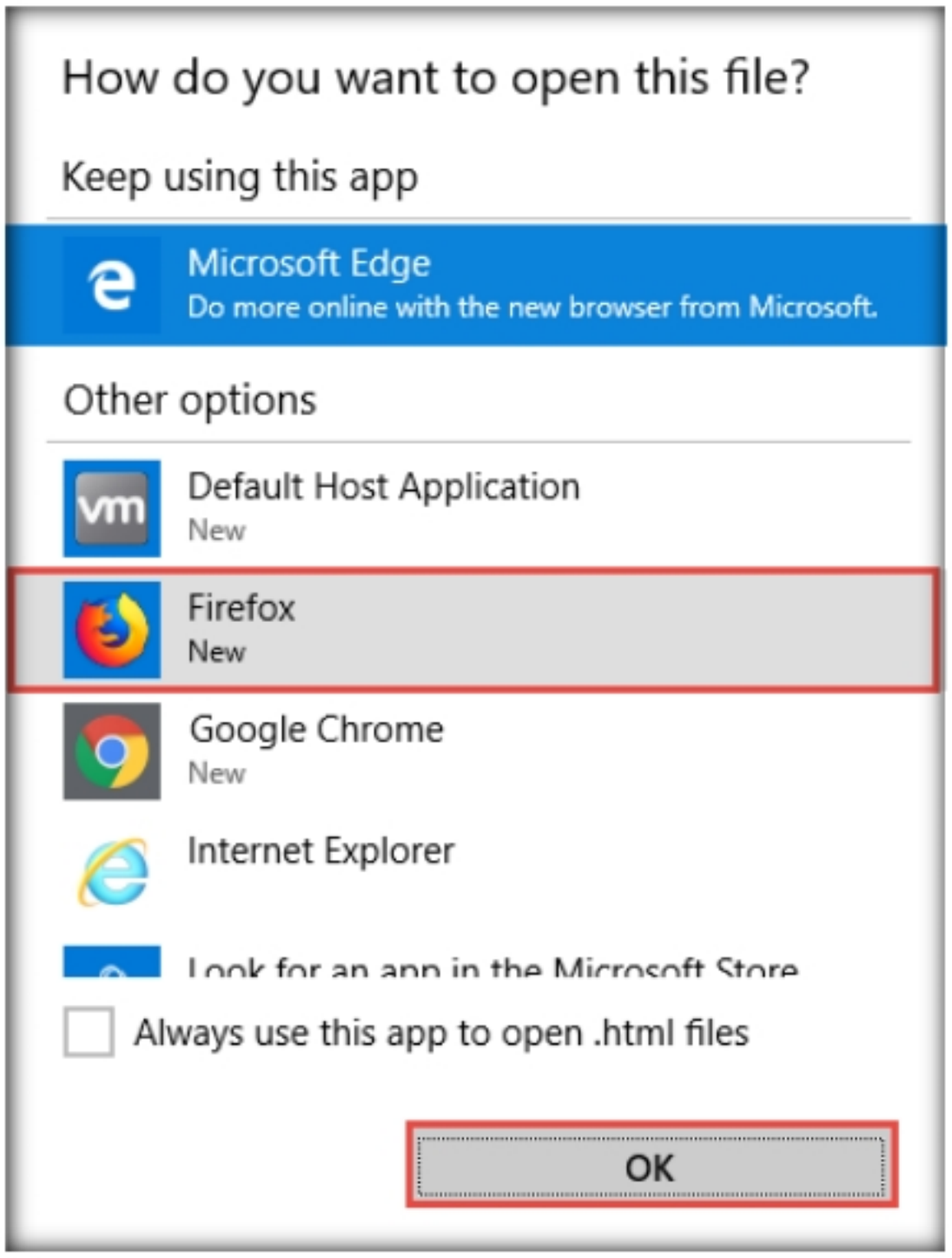


Figure 2.2.35: Choosing a browser to view the HTML

43. The Nessus scan report appears in the **Firefox** web browser, as shown in the screenshot.

Note: Screenshots might differ in your lab environment.

44. You can click the **Expand All** option to view the detailed scan report.

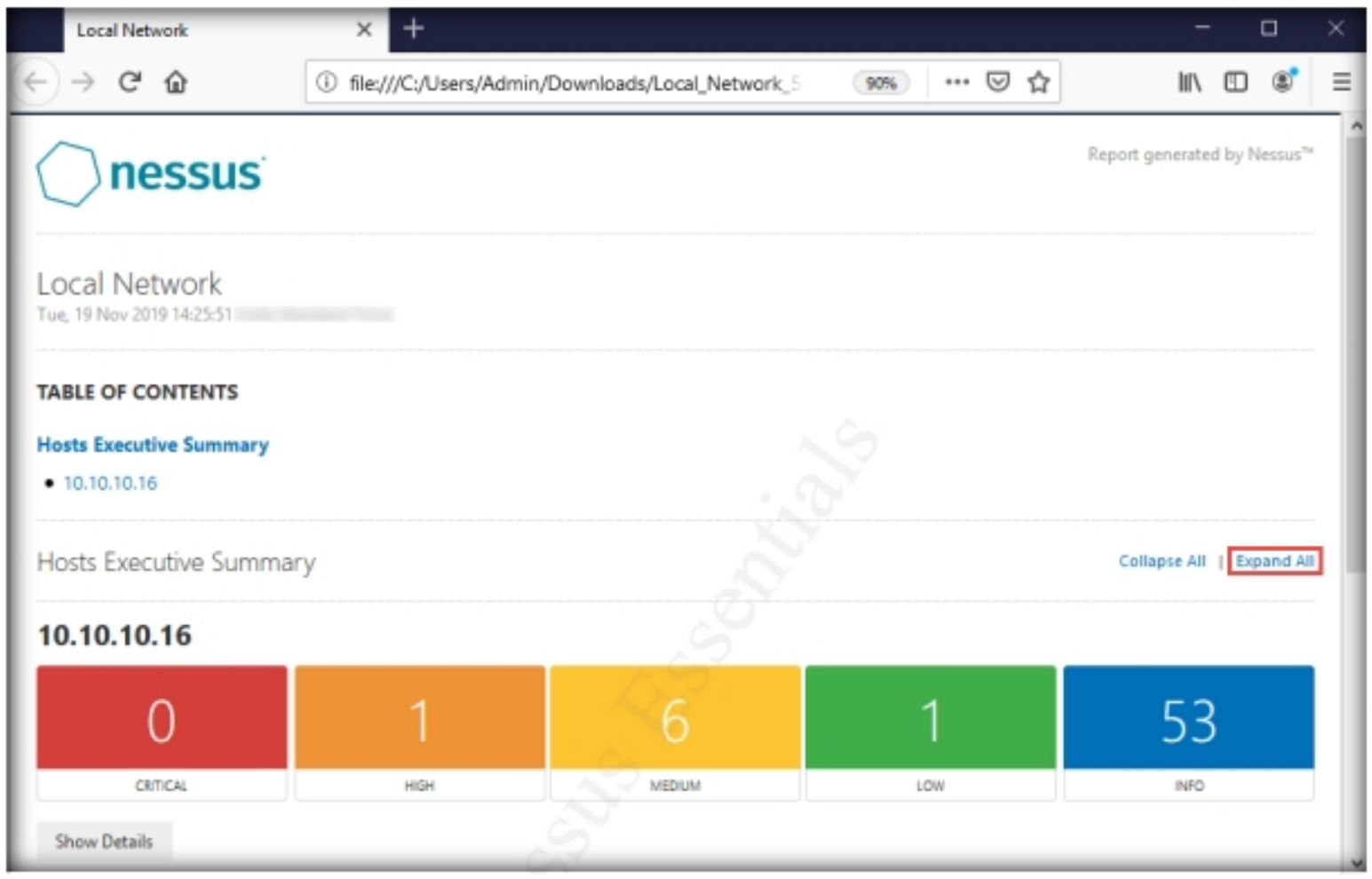


Figure 2.2.36: Vulnerability Report Displayed in HTML Format

45. A list of discovered vulnerabilities appears. You can further click on plugins (here, **41028**) to view more detailed information on the vulnerability.

Note: The results might differ in your lab environment.

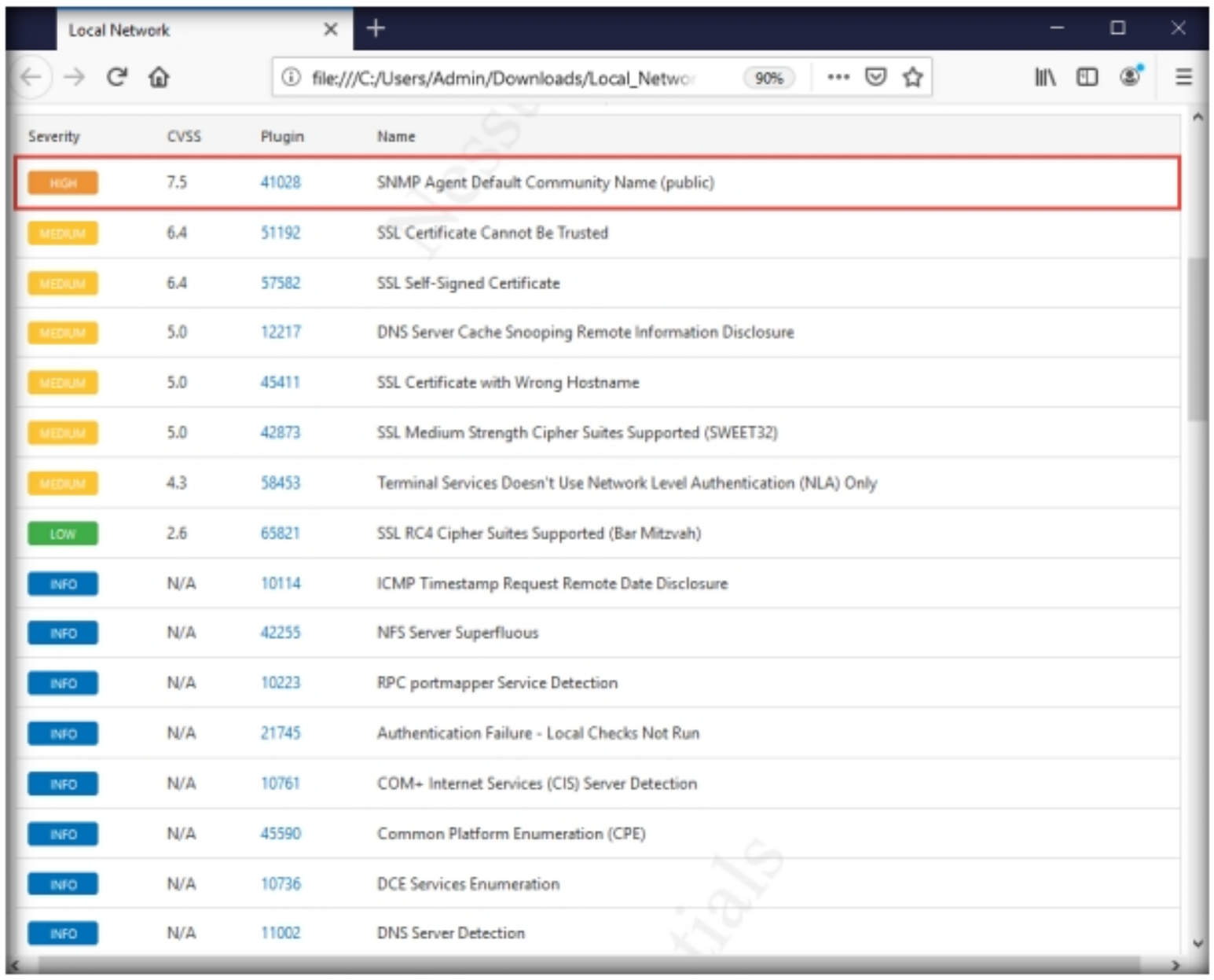


Figure 2.2.37: Viewing a Vulnerability in the Report

46. The selected plugin details are displayed, as shown in the screenshot.

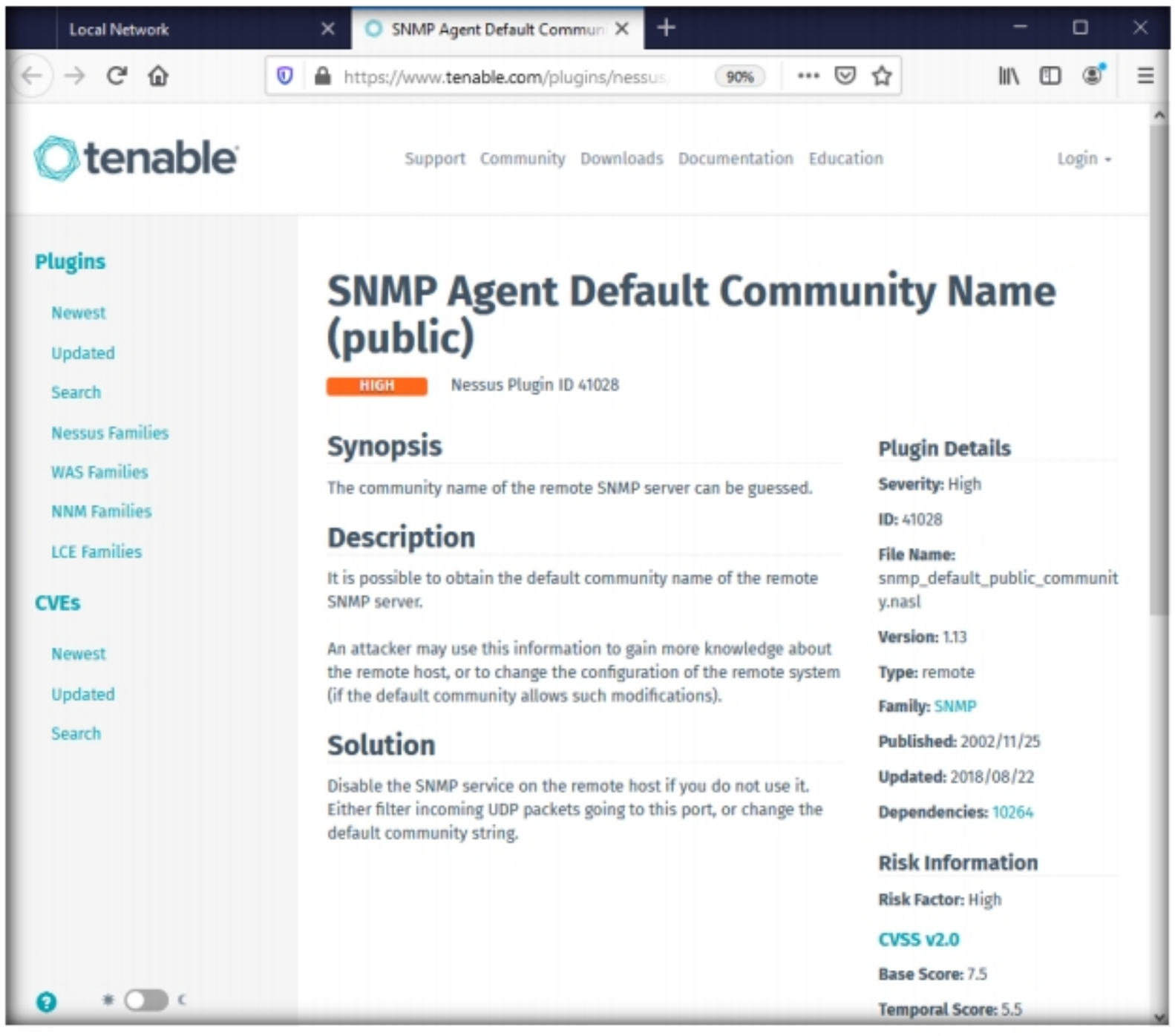


Figure 2.2.38: Details of the Selected Vulnerability

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

48. Once the vulnerability analysis is done, switch back to **Microsoft Edge** where Nessus is running and click **Admin → Sign Out** in the top-right corner.

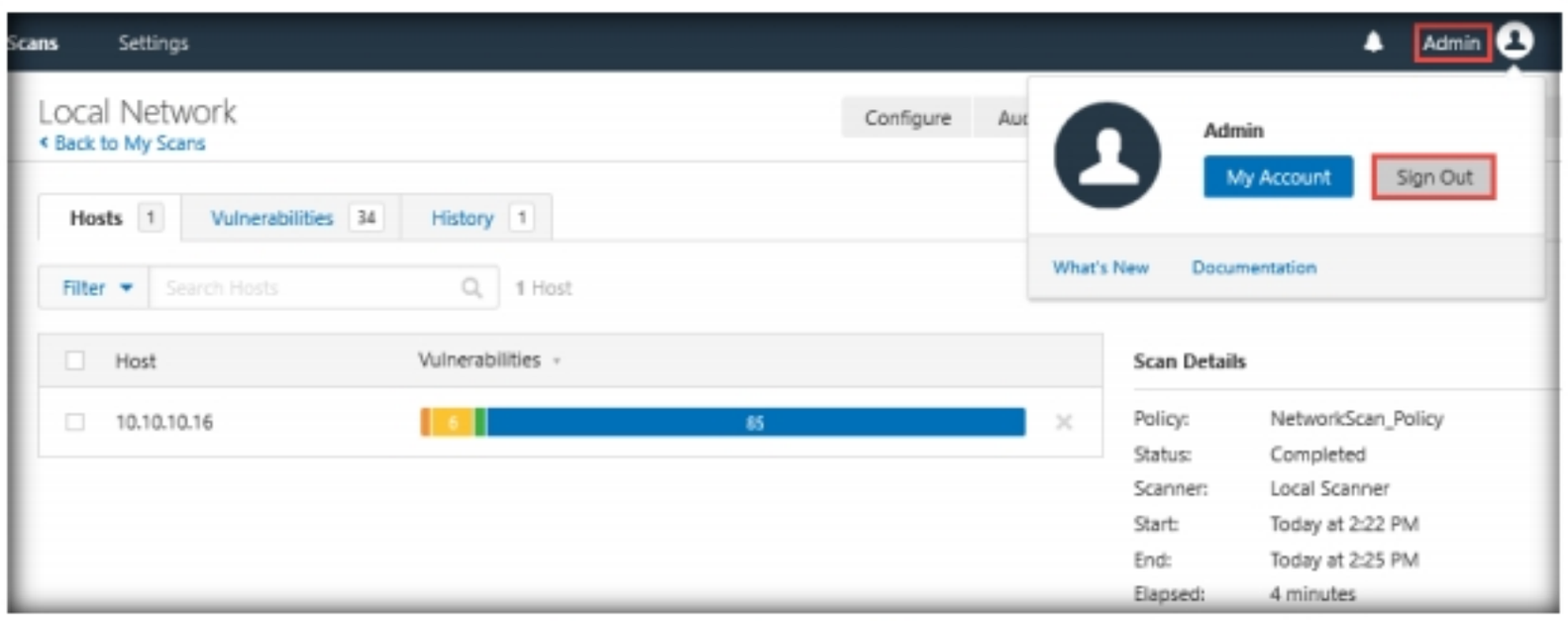


Figure 2.2.39: Signing out of Nessus

49. Once the session is successfully logged out, a **Signed out successfully. Goodbye, admin** notification appears.

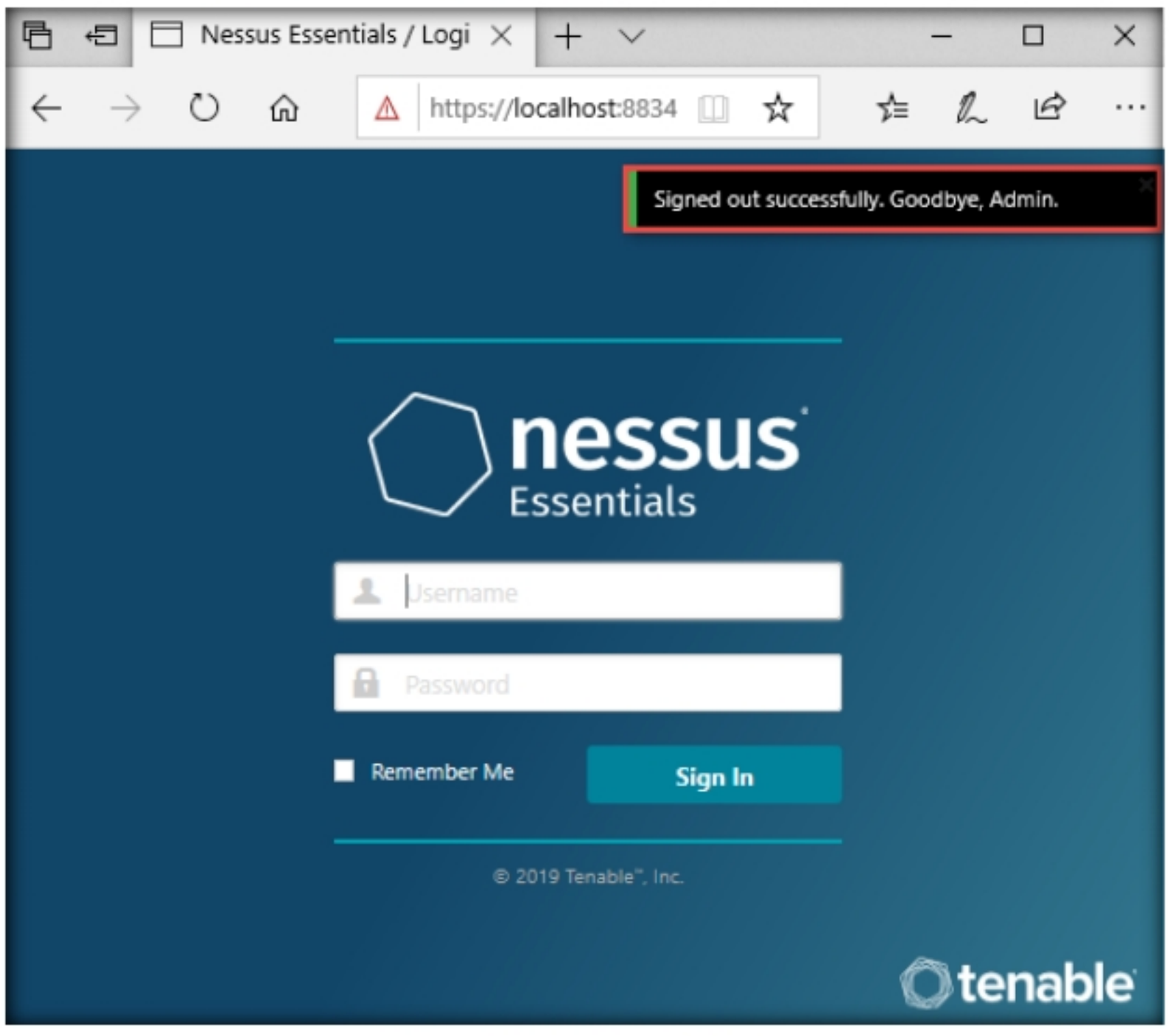


Figure 2.2.40: Signed out successfully

50. This concludes the demonstration of performing vulnerability assessment using Nessus.
51. Close all open windows and document all the acquired information.
52. Turn off the **Windows 10** virtual machine.

TASK 3 — Perform Vulnerability Scanning using GFI LanGuard

Here, we will use GFI LanGuard to perform vulnerability scanning on the target system.

1. Turn on the **Windows Server 2019** virtual machine.

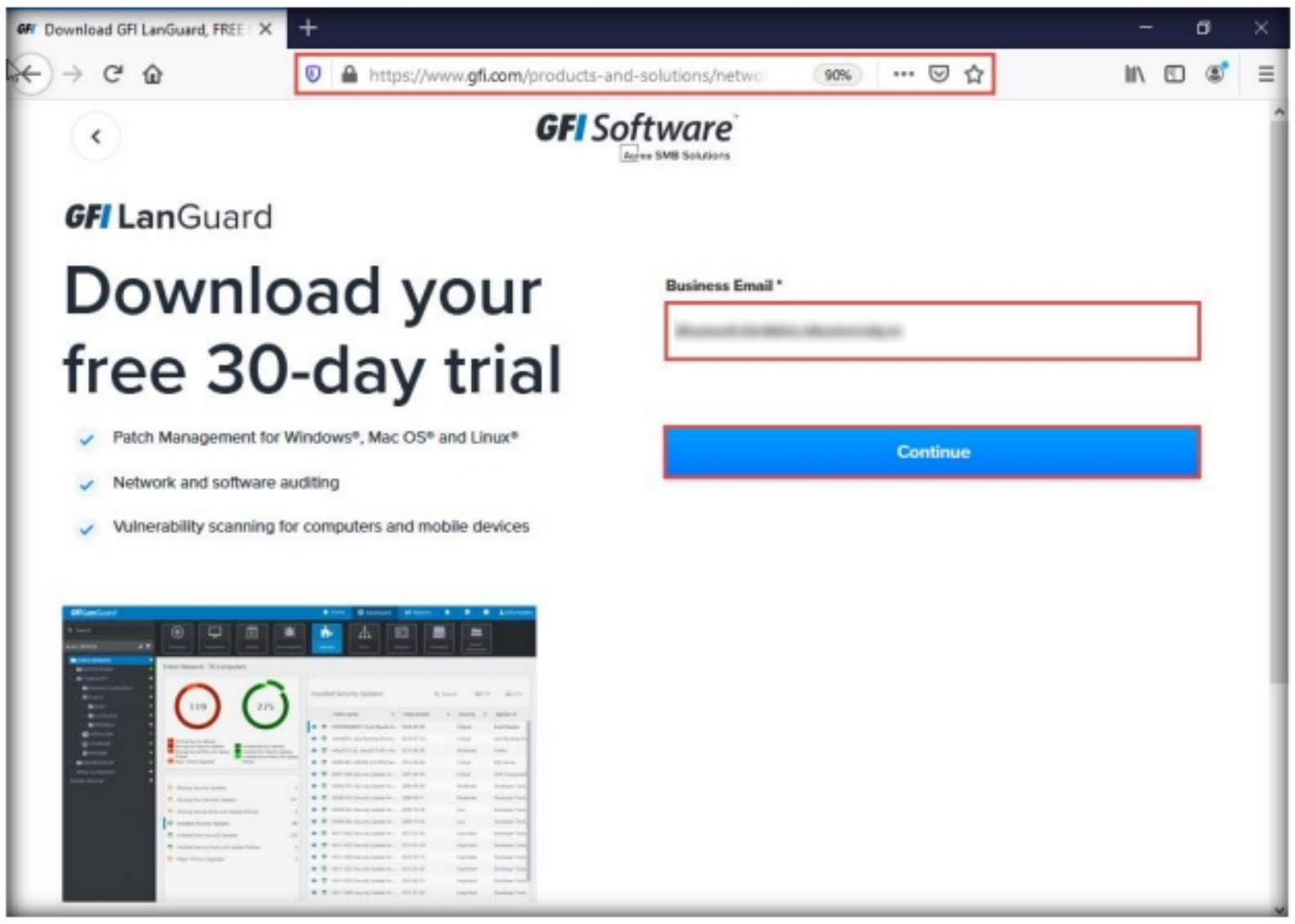
Note: Ensure that the **Windows Server 2016** virtual machine is also turned on.

2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 3.1 — Register and Download GFI LanGuard

3. Launch any web browser (here, **Mozilla Firefox**), type the URL **https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download** in the address bar and press **Enter**.

4. The **GFI LanGuard** registration page appears. Enter your business email under the **Business Email** field and click **Continue**.



GFI LanGuard scans, detects, assesses, and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort.

Figure 2.3.1: GFI LanGuard Registration page

5. On the next page, enter the required details and select the **I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process data** checkbox and click **Start my free trial**.

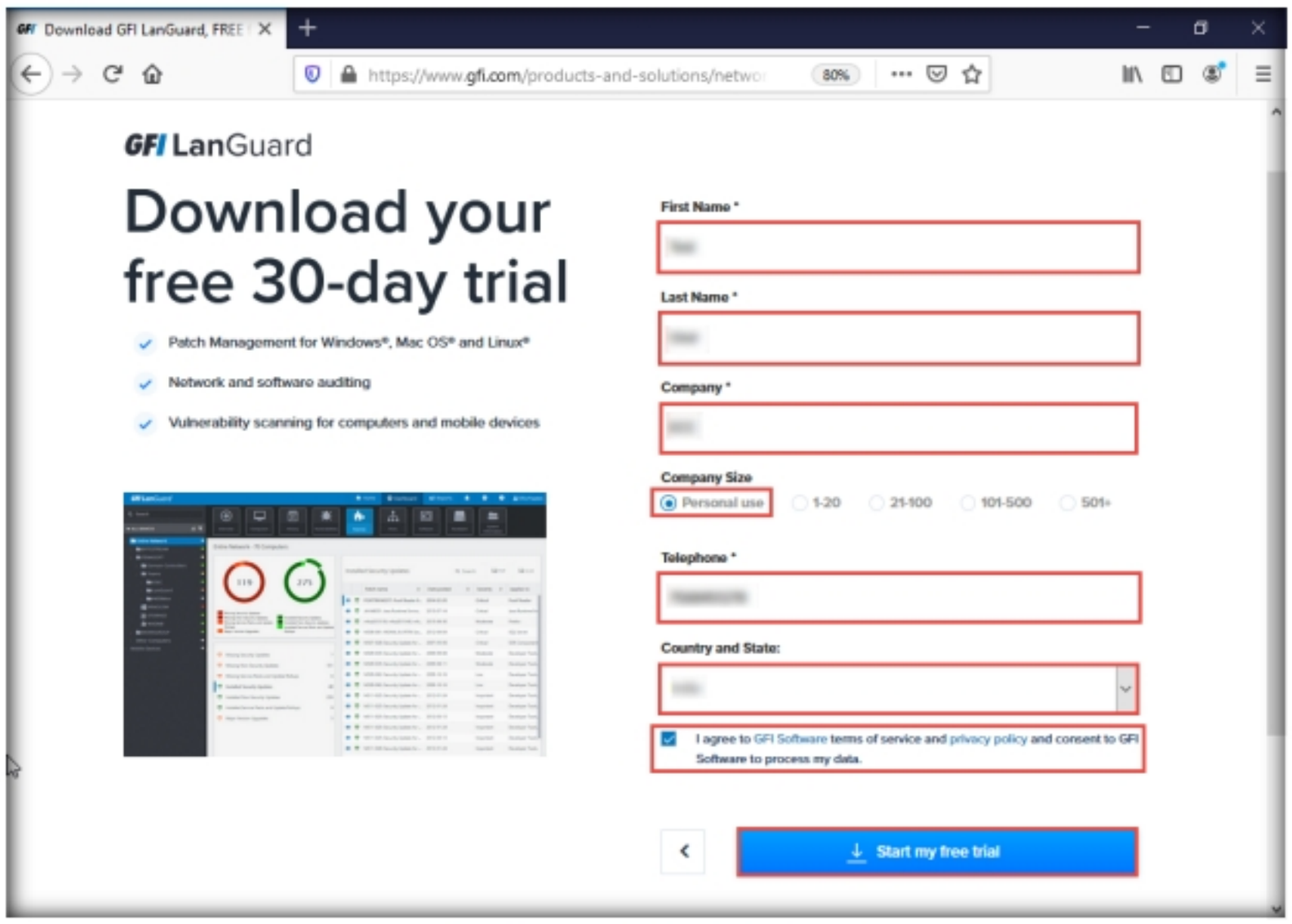


Figure 2.3.2: GFI LanGuard Download page

6. The **Download the latest version of GFI LanGuard** page appears; click the **Download Trial** button.

Note: The **Opening languard.exe** pop-up appears; click **Save File**.

GFI LanGuard scans your OSes, virtual environments, and installed applications through vulnerability check databases. It enables you to analyze the state of your network security, identify risks, and address how to take action before it is compromised.

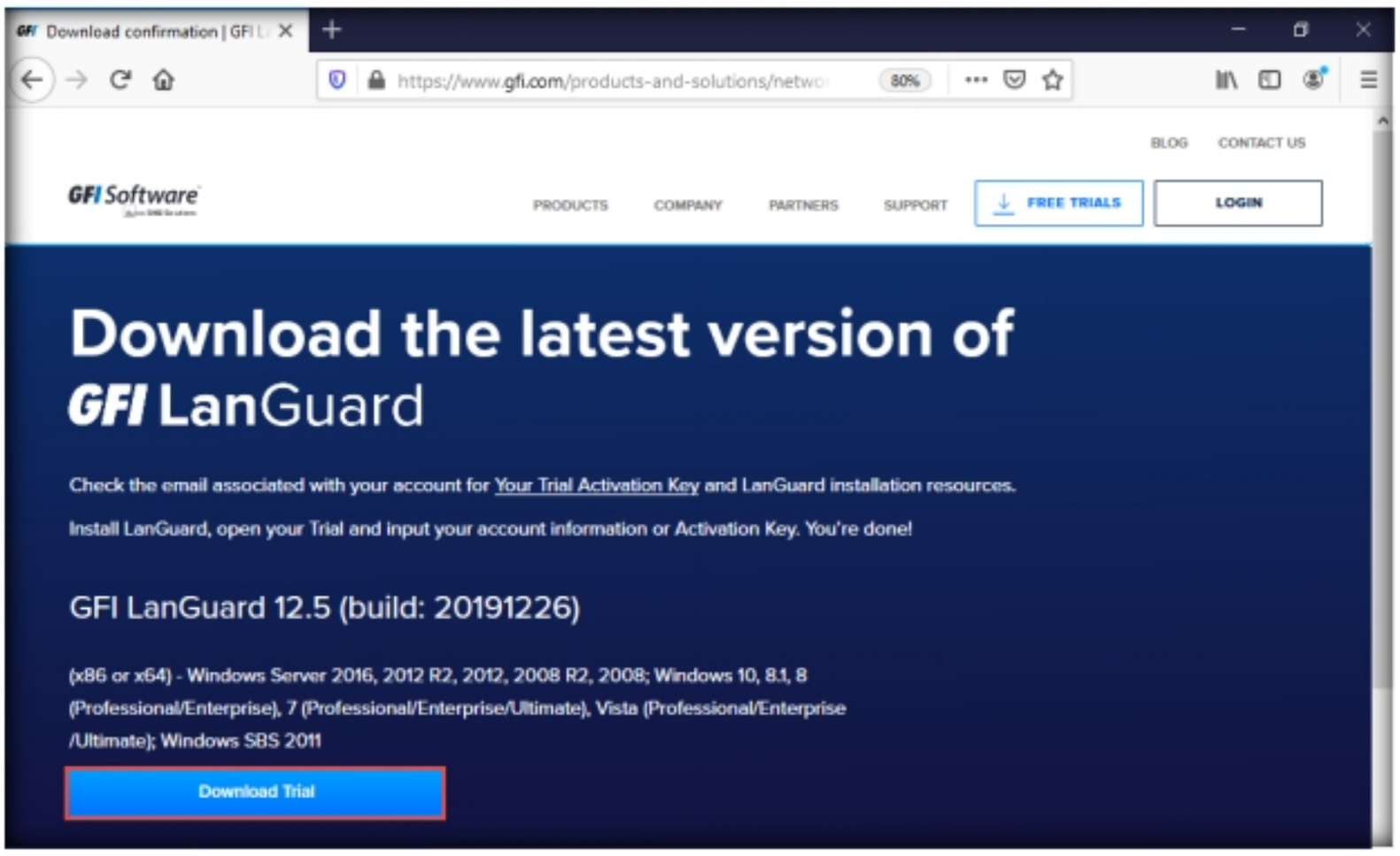


Figure 2.3.3: Complete Registration

TASK 3.2

Install GFI LanGuard

7. Now, navigate to the download location (here, **Downloads**) and double-click **languard.exe** to install.

Note: If the **User File - Security Warning** pop-up appears, click **Run**.

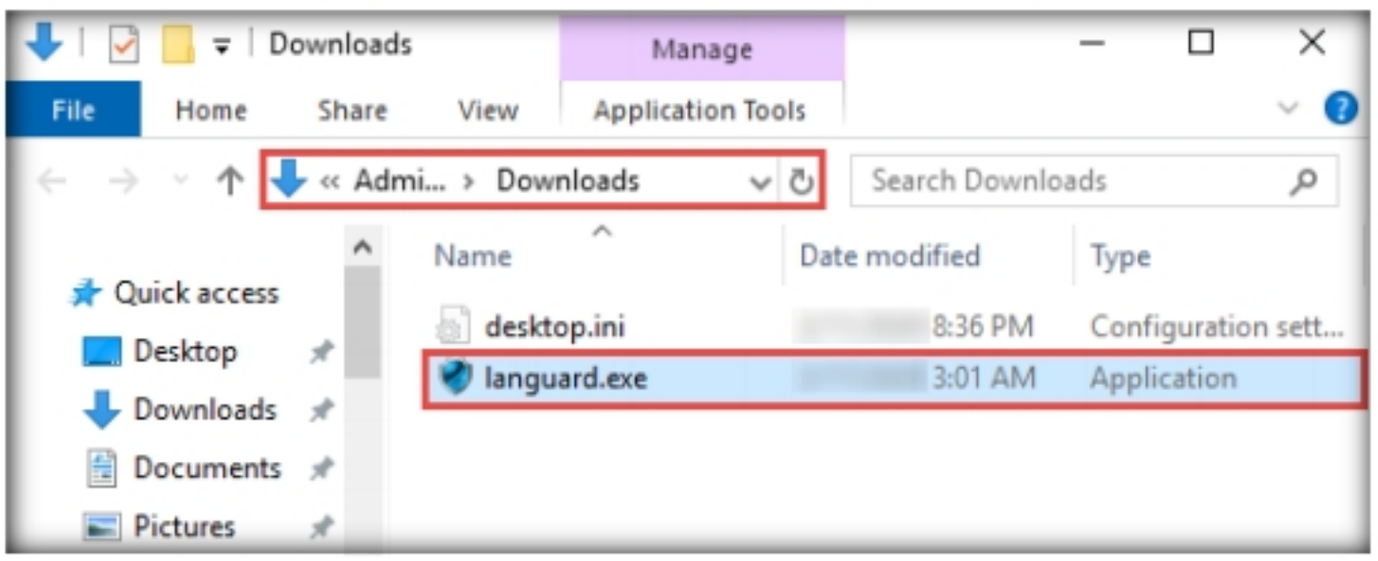


Figure 2.3.4: GFI LanGuard exe file

8. The **GFI LanGuard** dialog box appears; select preferred language (here, **English**) and click **OK**.

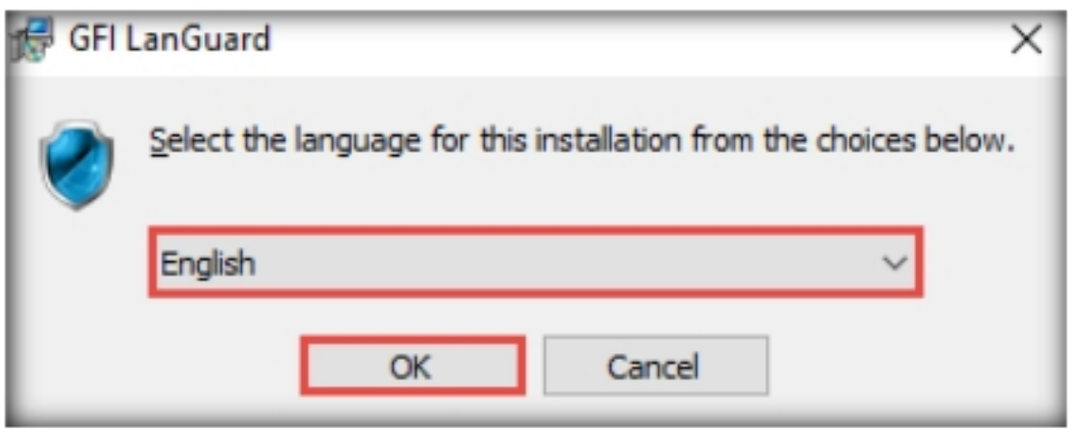


Figure 2.3.5: Selecting a language

9. The **GFI LanGuard** wizard appears with selected components for installation; click **Next** to proceed.

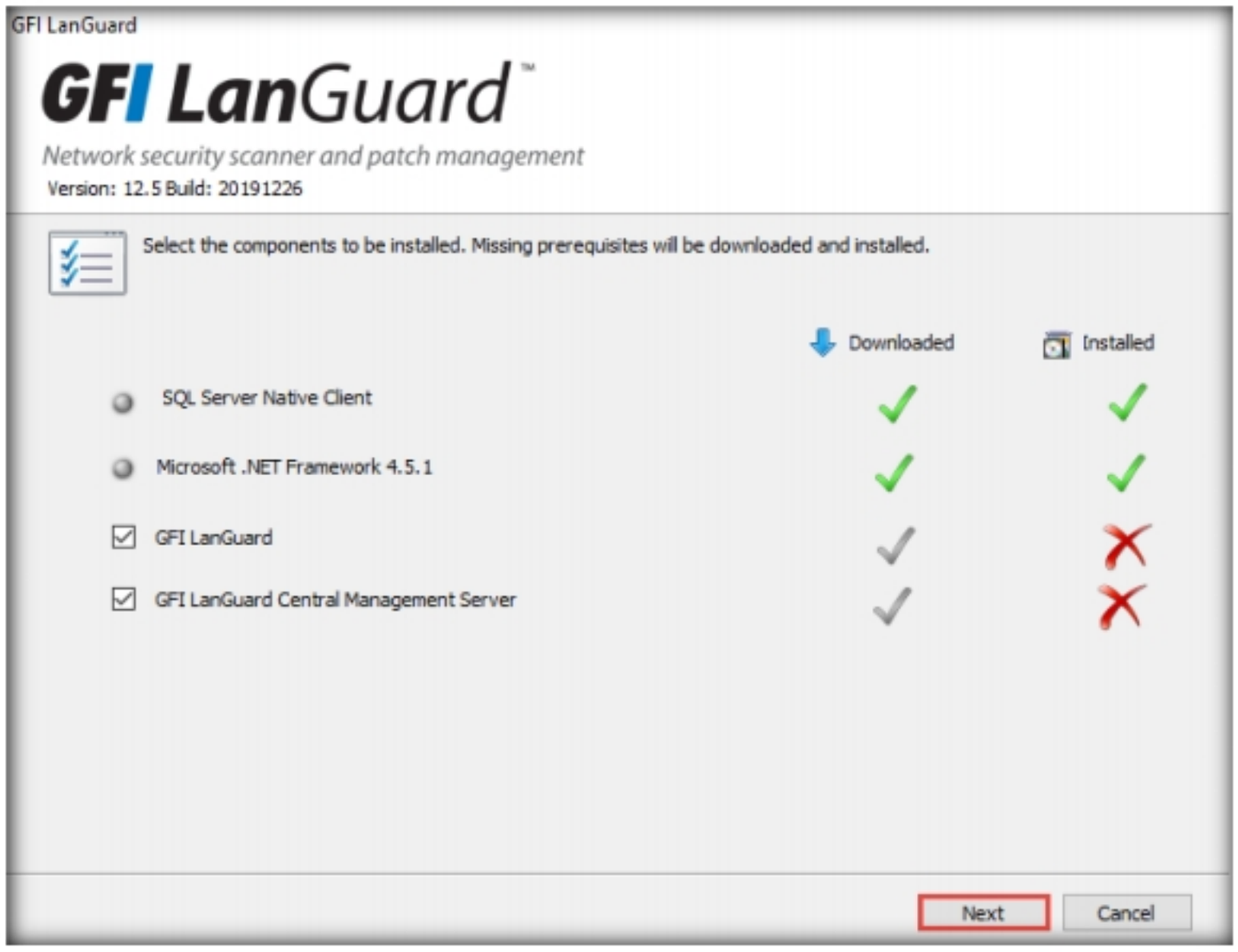


Figure 2.3.6: Installation wizard

10. The **Database Configuration** window appears. In the **SQL server name** field, type **.\SQLEXPRESS** and leave **SQL database name** as default. Ensure that the **Use Windows Authentication** checkbox is selected and click **OK**.

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

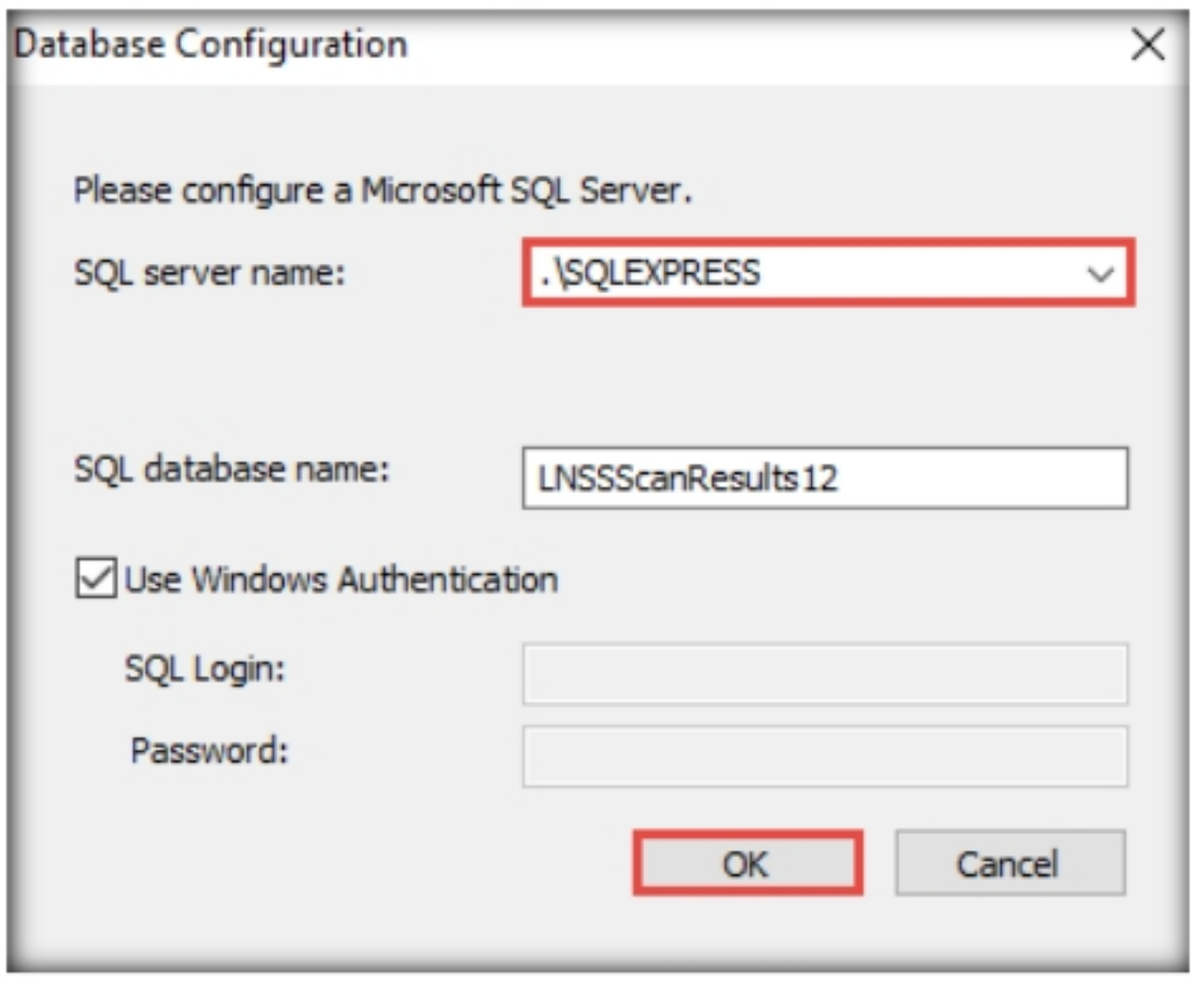


Figure 2.3.7: Database Configure window

11. Now, switch back to the **Mozilla Firefox** browser, open a new tab, and log in to your email account that you have given while registration.
12. Open an email from **GFI Downloads** and copy the activation key.

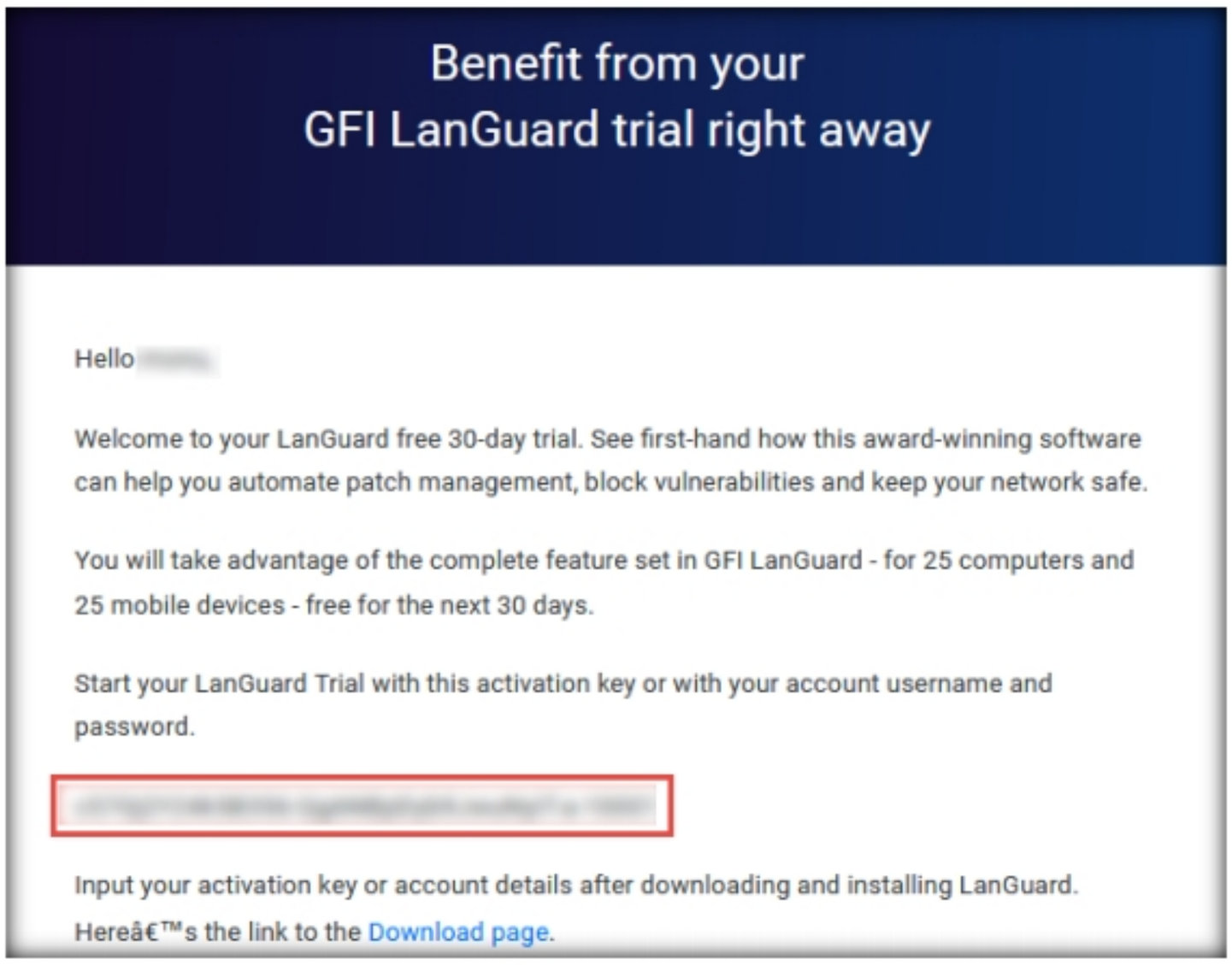


Figure 2.3.8: GFI LanGuard Trial Key

13. The **GFI LanGuard License Key** window appears. Paste the received activation key in the **Enter License Key** field and click **OK**.

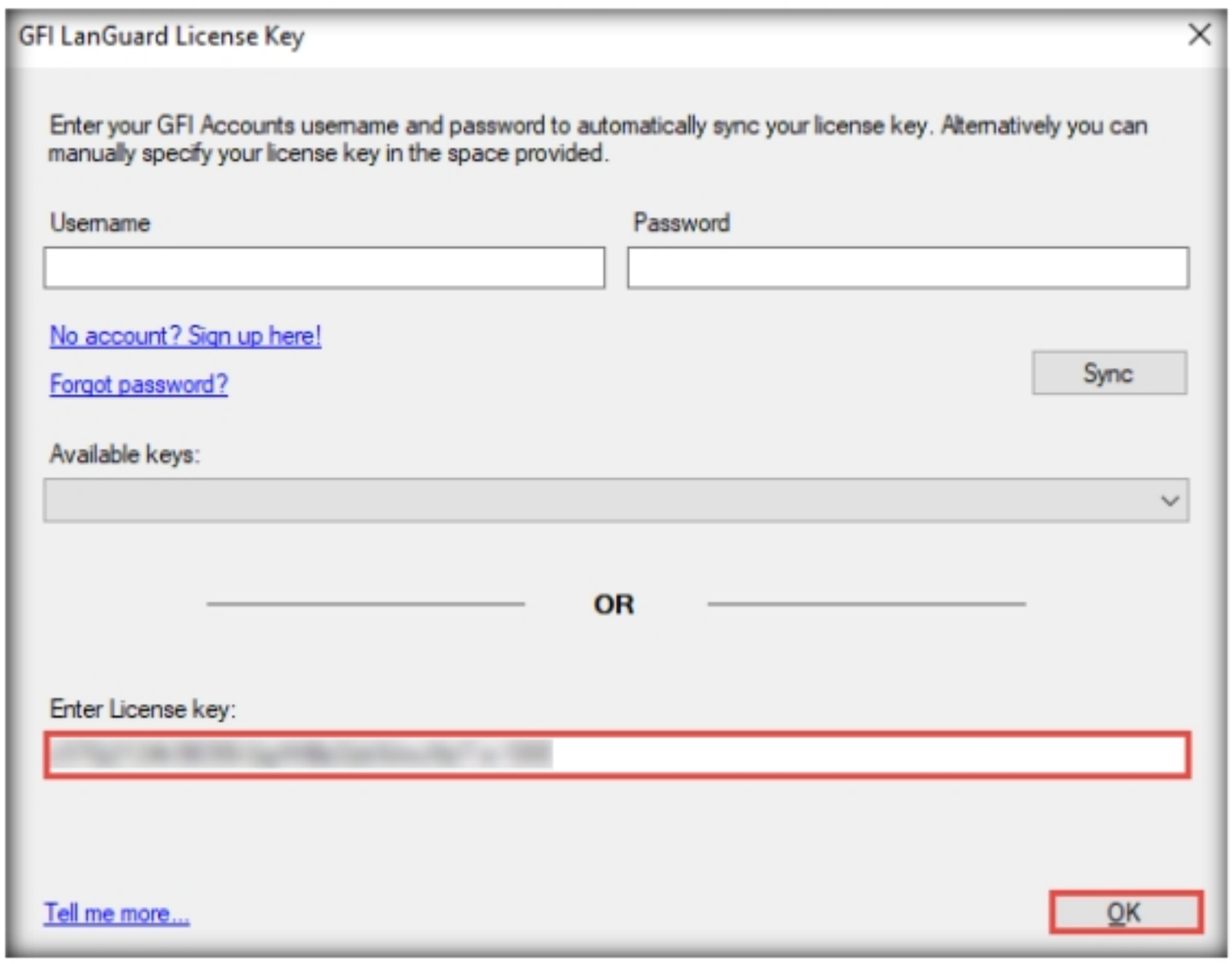


Figure 2.3.9: GFI LanGuard License window

14. GFI LanGuard starts installing after the completion of the installation; when the **GFI LanGuard Setup** window appears, click **Next**.

Figure 2.3.10: GFI LanGuard Setup window

15. The **End-User License Agreement** wizard appears; accept the terms and click **Next**.
16. In the **Attendant service credentials** wizard, leave the **Name** field as default (here, **SERVER2019\Administrator**) and enter the **Password** of the administrator account (here, **Pa$$w0rd**); then, click **Next**.

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

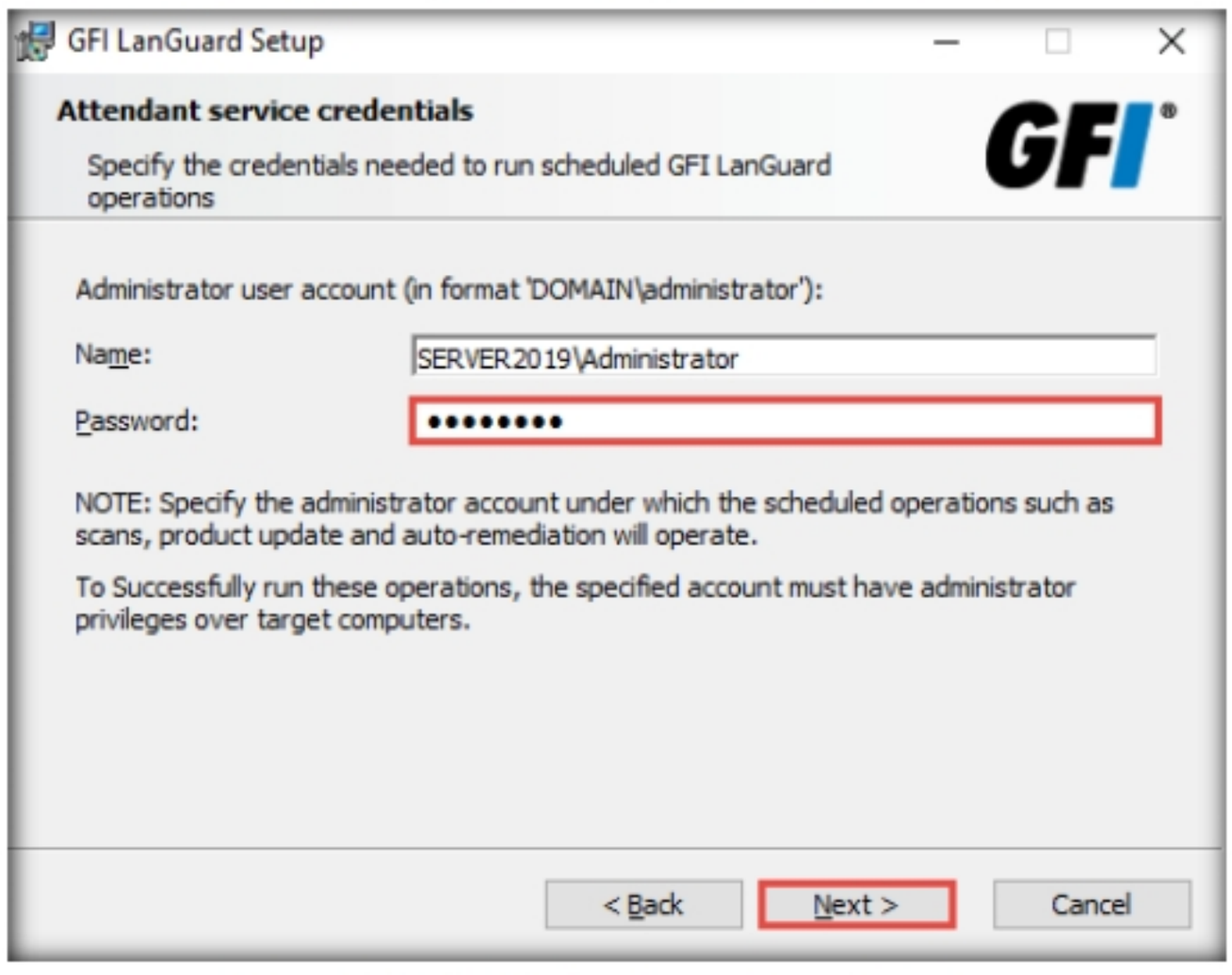


Figure 2.3.11: GFI LanGuard Attendant service credentials section

17. In the **Choose Destination Location** wizard, leave the **Folder** location set to default and click **Install**.

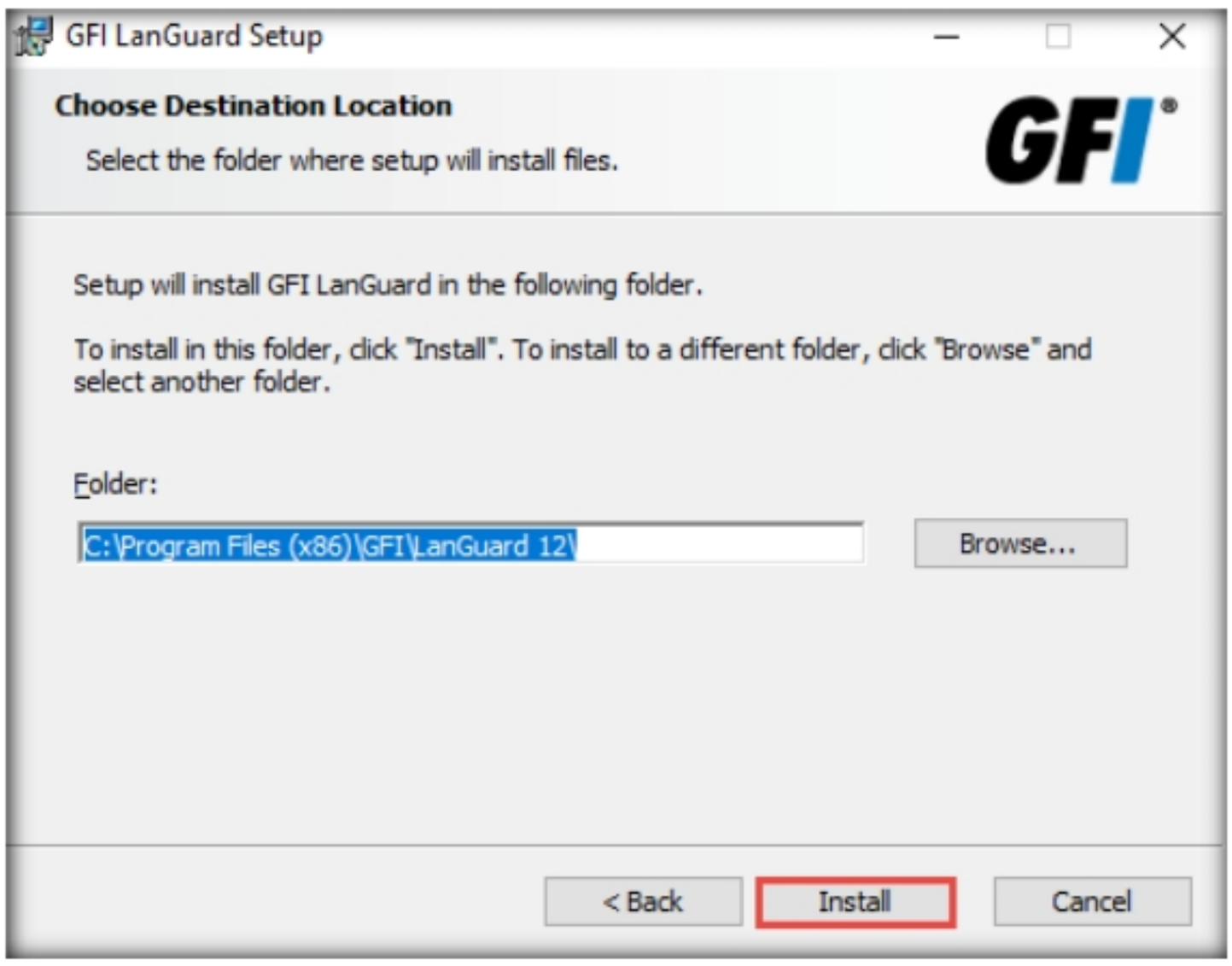


Figure 2.3.12: Choosing a folder location

18. The **Installing GFI LanGuard** wizard appears. After the completion of installation, the **GFI LanGuard Central Management Server Setup** window appears; then, click **Next**.

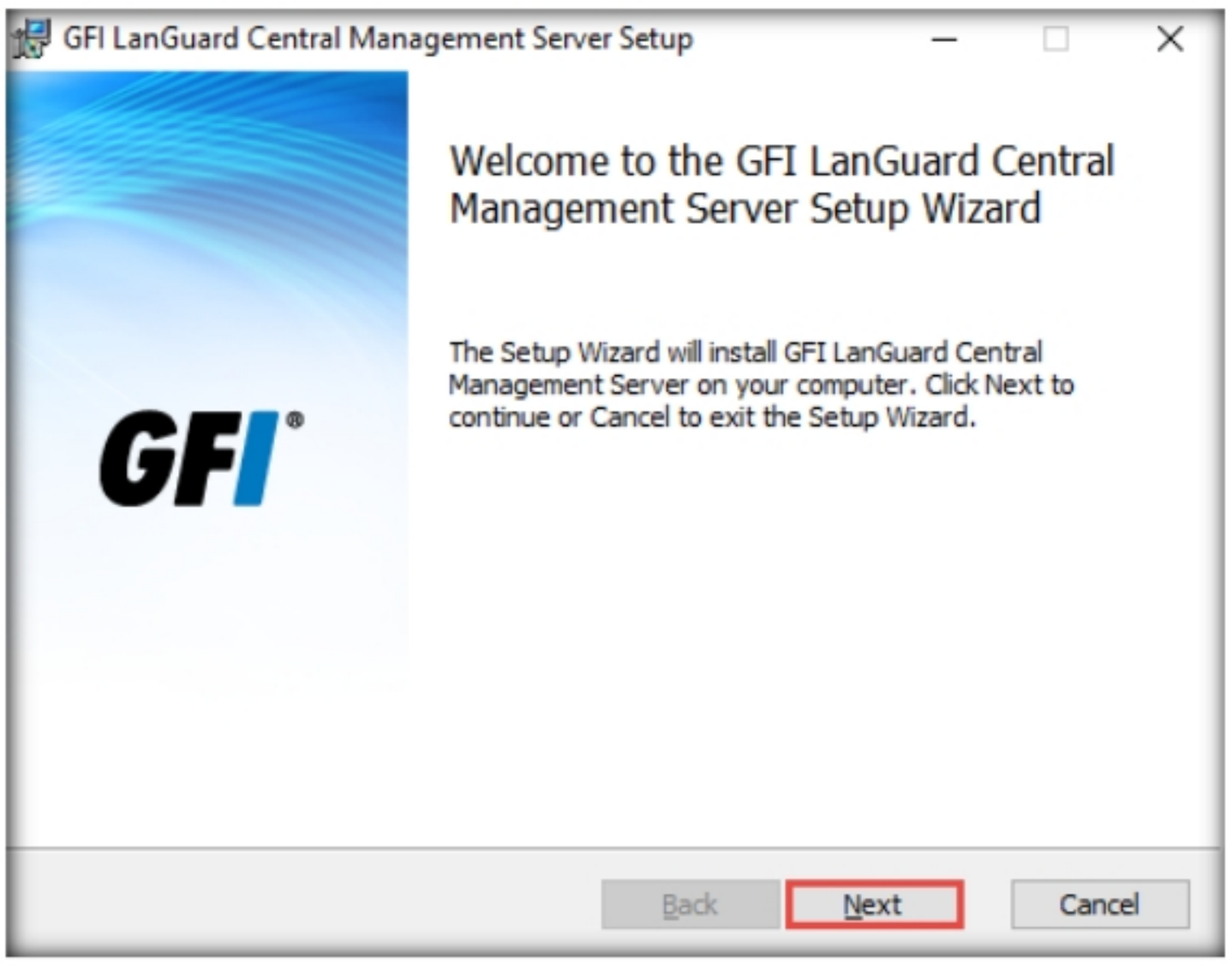


Figure 2.3.13: GFI LanGuard Central Management Server Setup window

19. In the **Service logon information** wizard, leave the **User Name** field (Administrator user account) set to its default, enter the **Password** of the administrator account (here, **Pa$$w0rd**), and click **Next**.

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

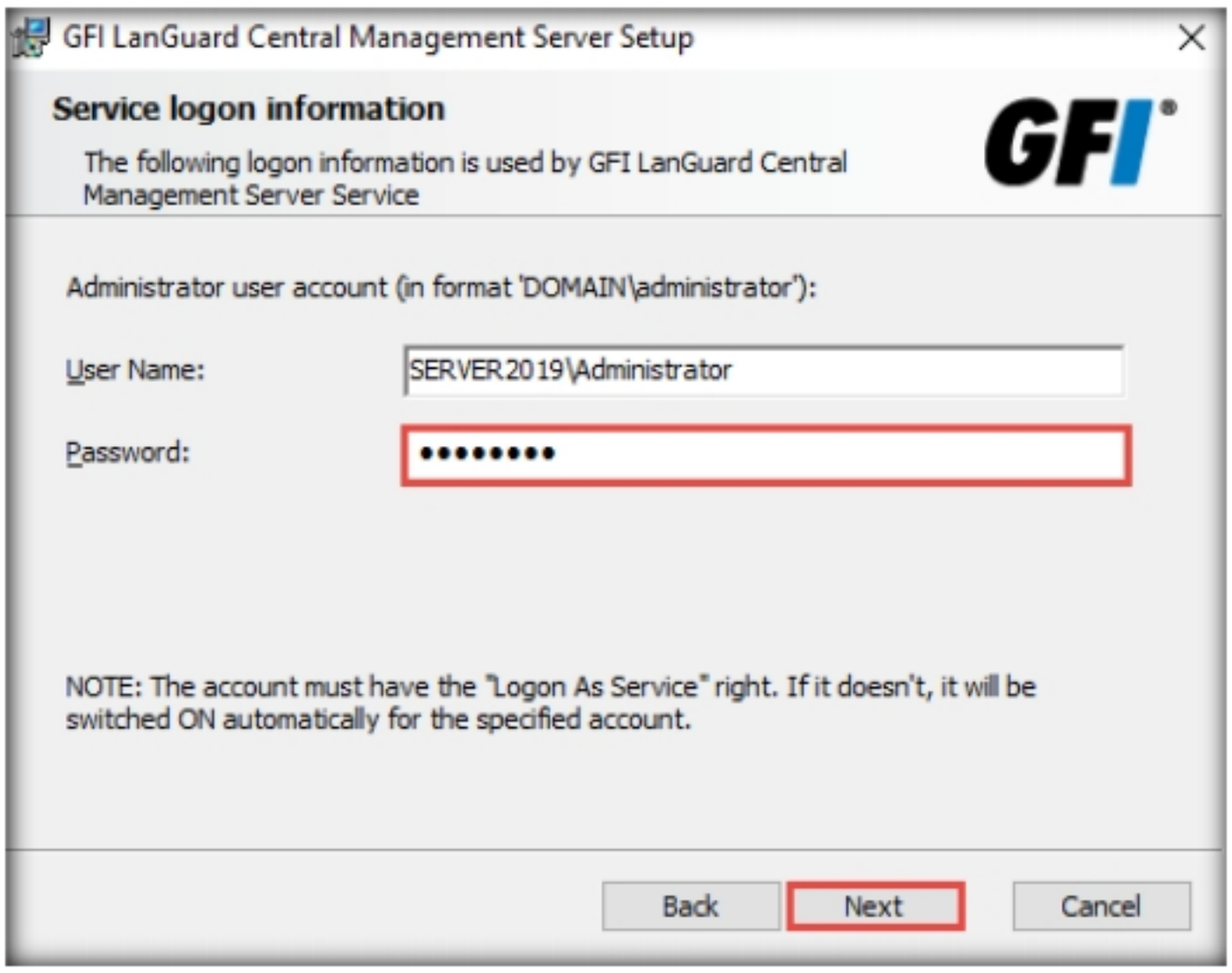


Figure 2.3.14: GFI LanGuard Service logon information section

20. The **HTTPS Settings** wizard appears; keep the name in its default and click **Next**.

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

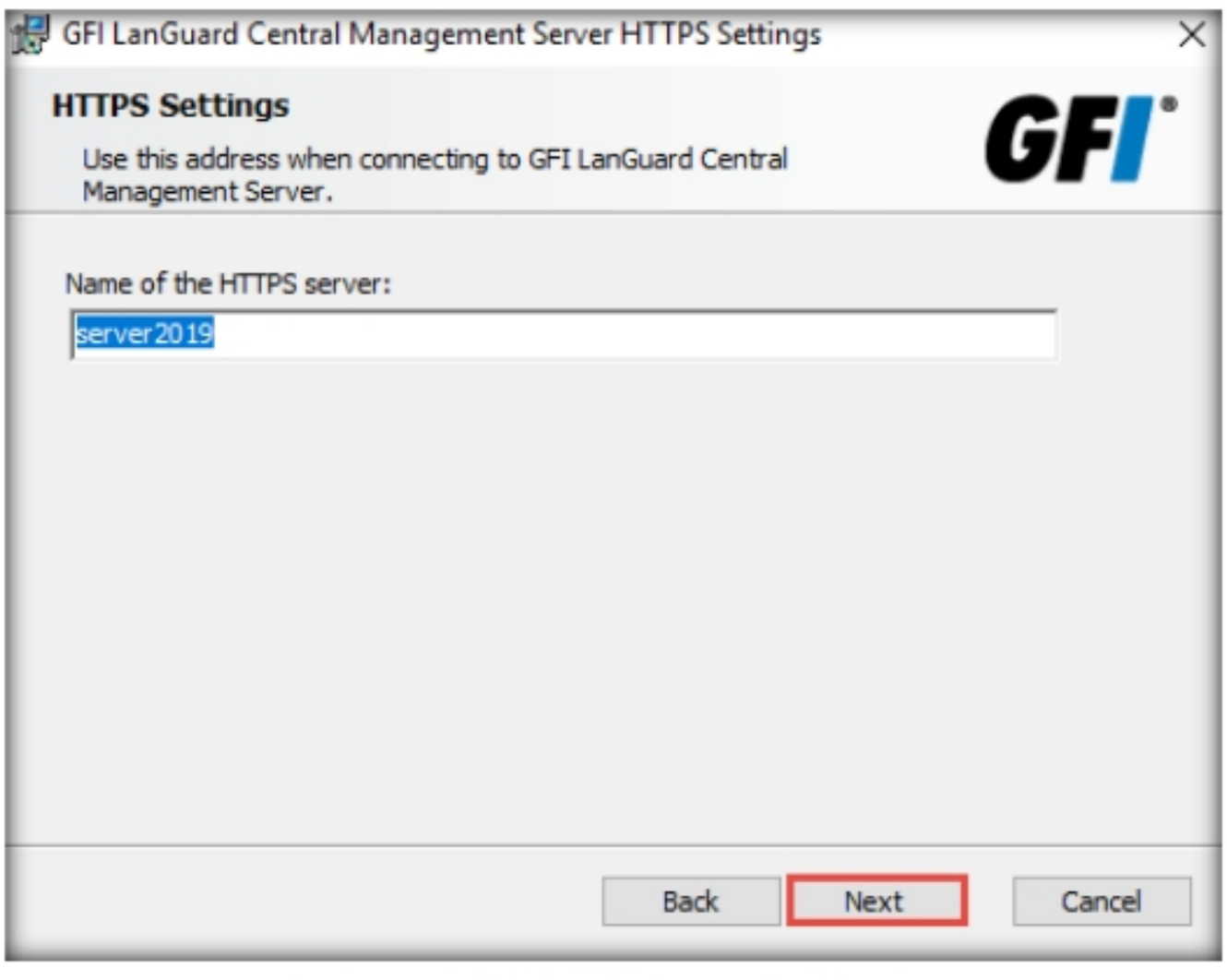


Figure 2.3.15: GFI LanGuard HTTPS Settings section

21. In the **Destination Folder** wizard, choose the location where you want to install the application (here, the default location is selected) and click **Next**.

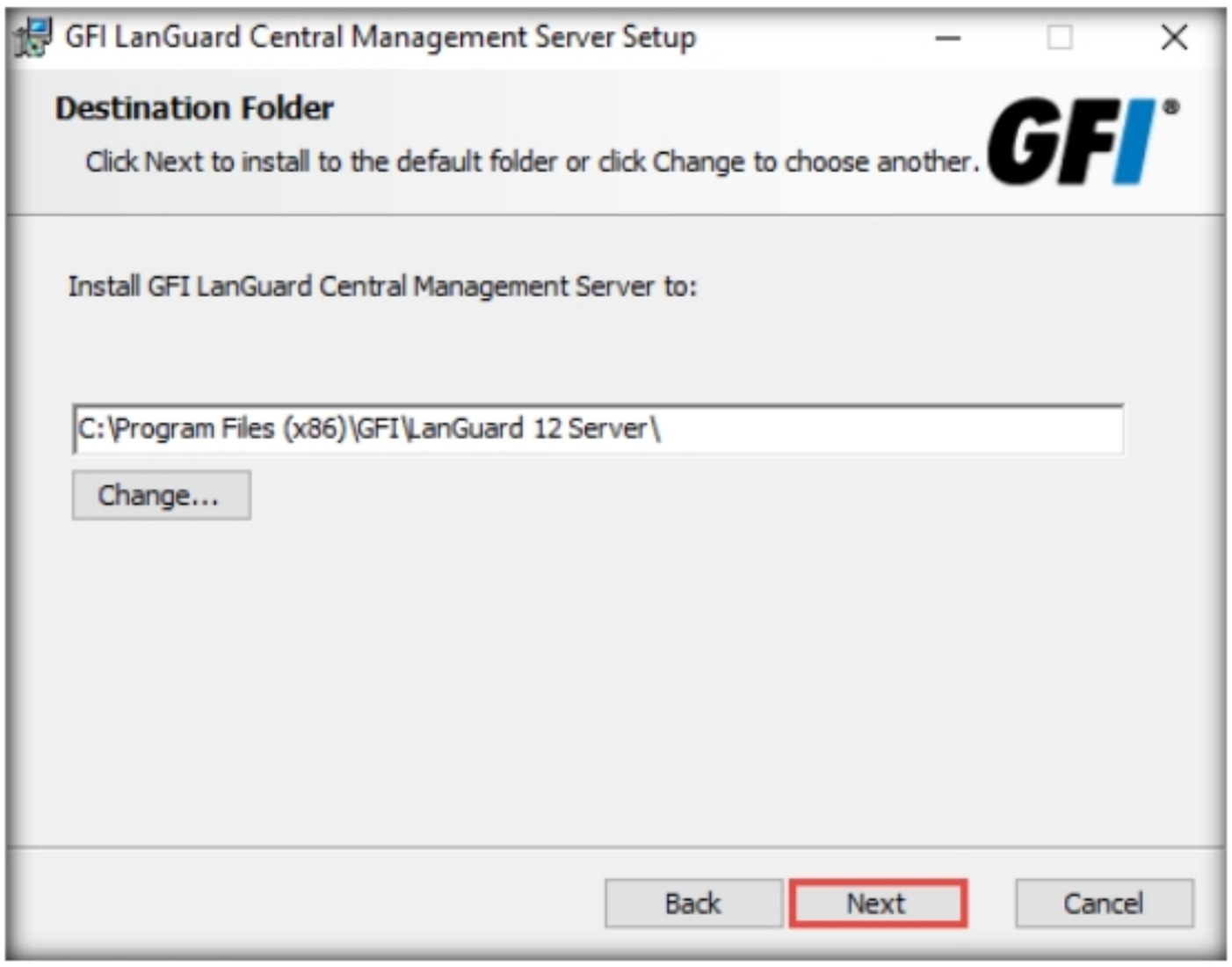


Figure 2.3.16: Choosing a folder destination

22. In the **Ready to install** wizard, click **Install** to proceed.

23. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.

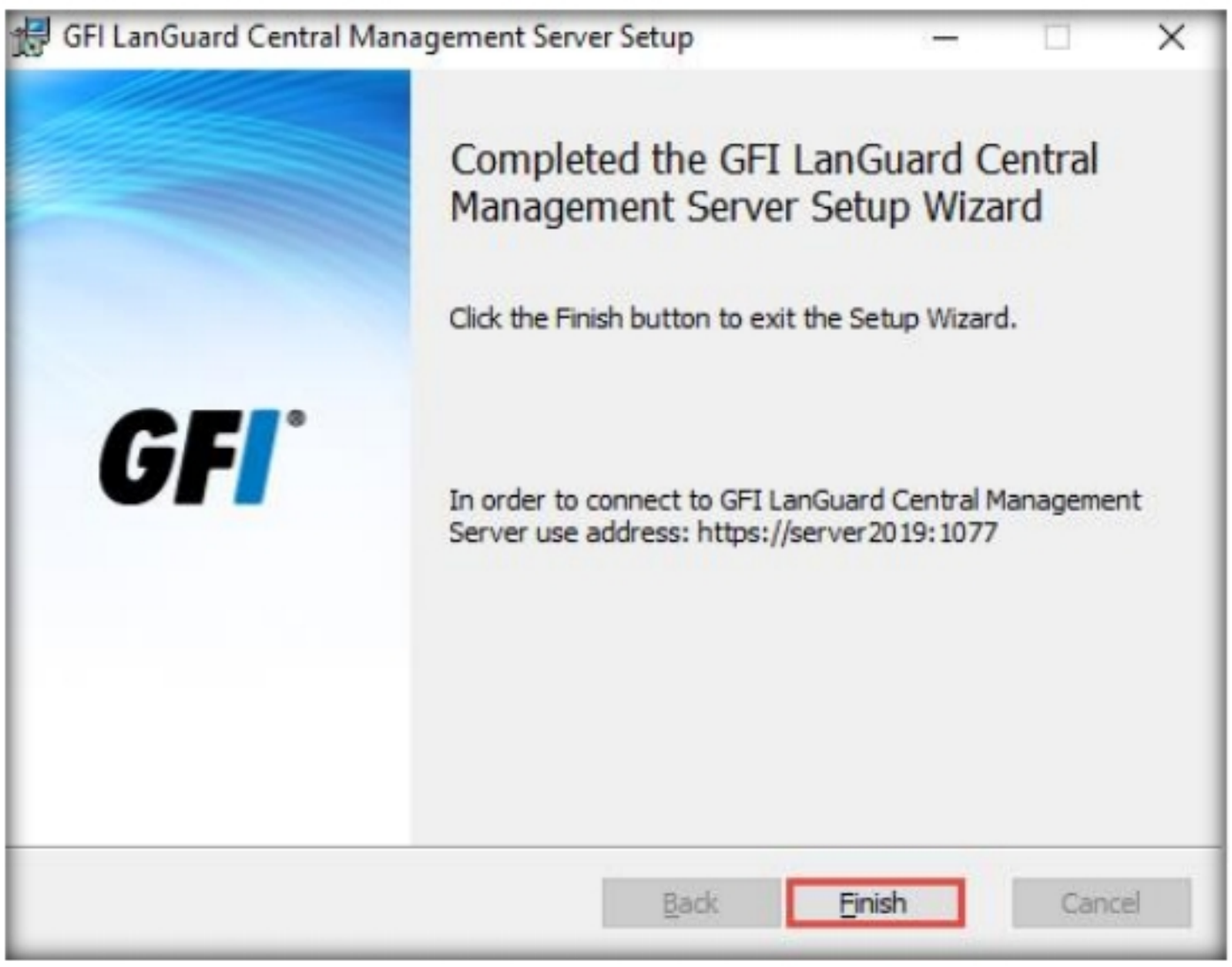


Figure 2.3.17: GFI LanGuard: click Finish

24. In the **GFI LanGuard Setup** window, ensure that the **Launch GFI LanGuard** checkbox is selected. De-select the **Launch GFI LanGuard Central Management Server** checkbox and click **Finish**.

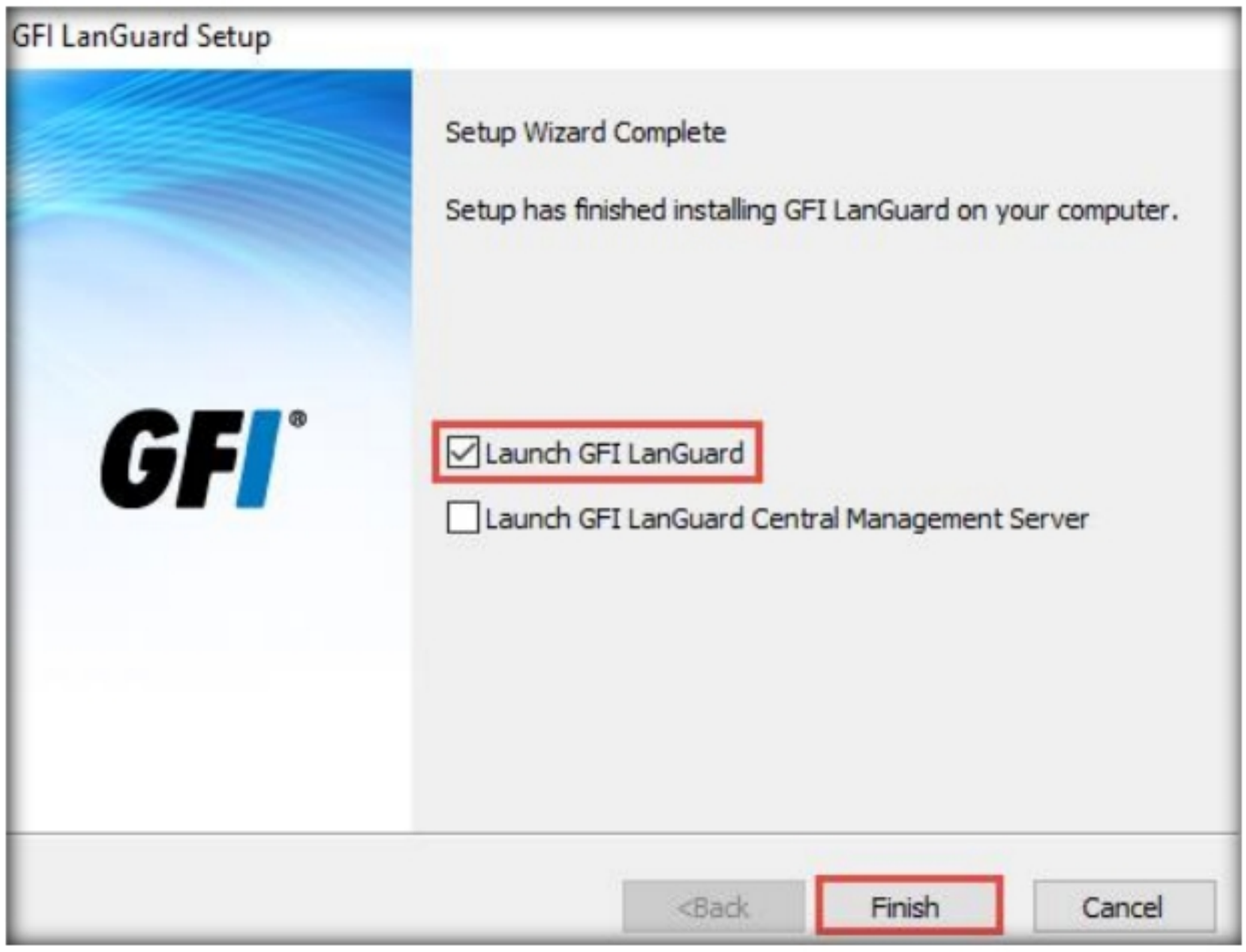


Figure 2.3.18: GFI LanGuard Setup: click Finish

25. A **GFI LanGuard** pop-up appears on the main window of the application; click **Continue evaluation**.

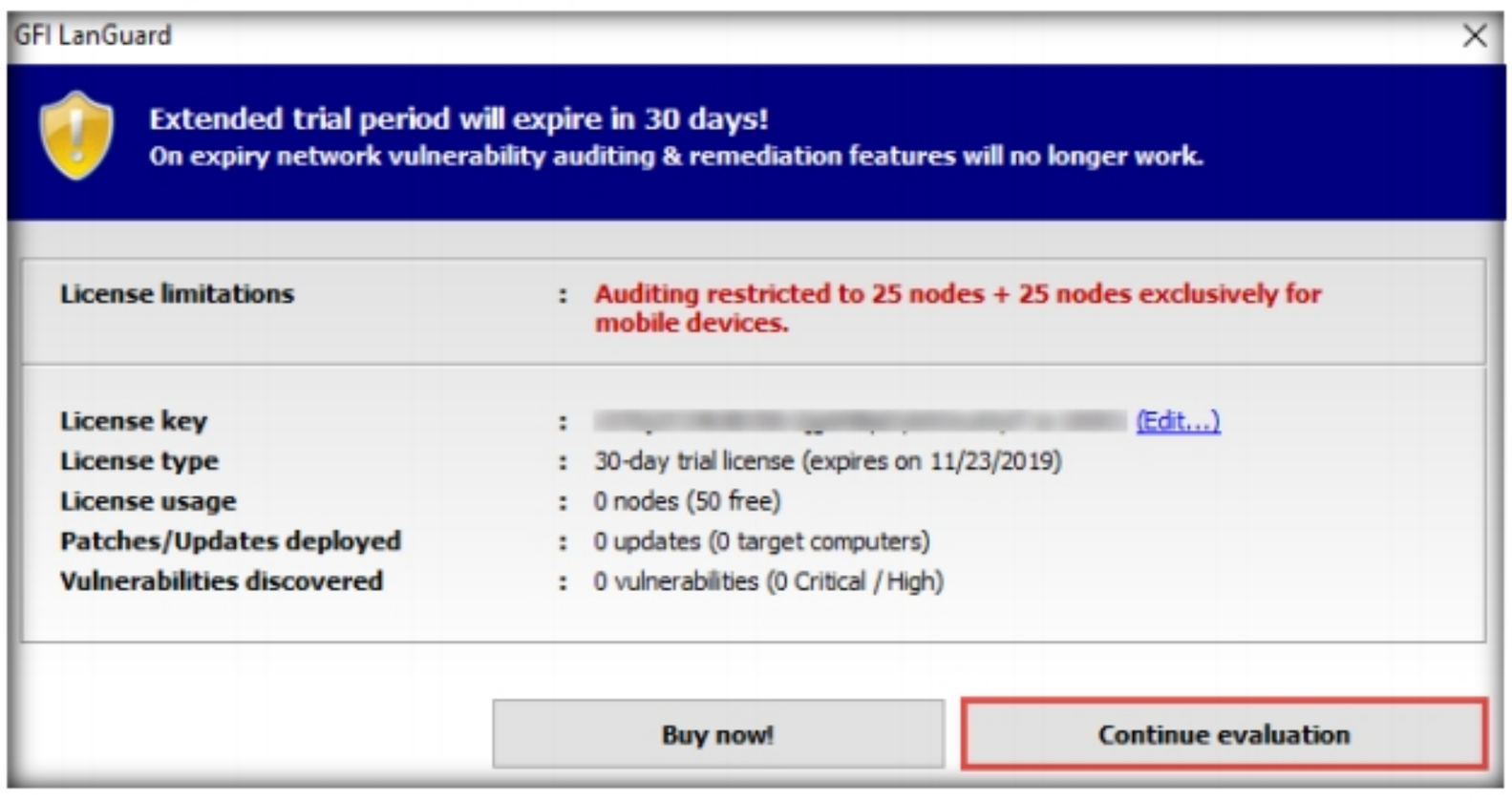


Figure 2.3.19: GFI LanGuard pop-up

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

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

Figure 2.3.20: Launching a scan in GFI LanGuard

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

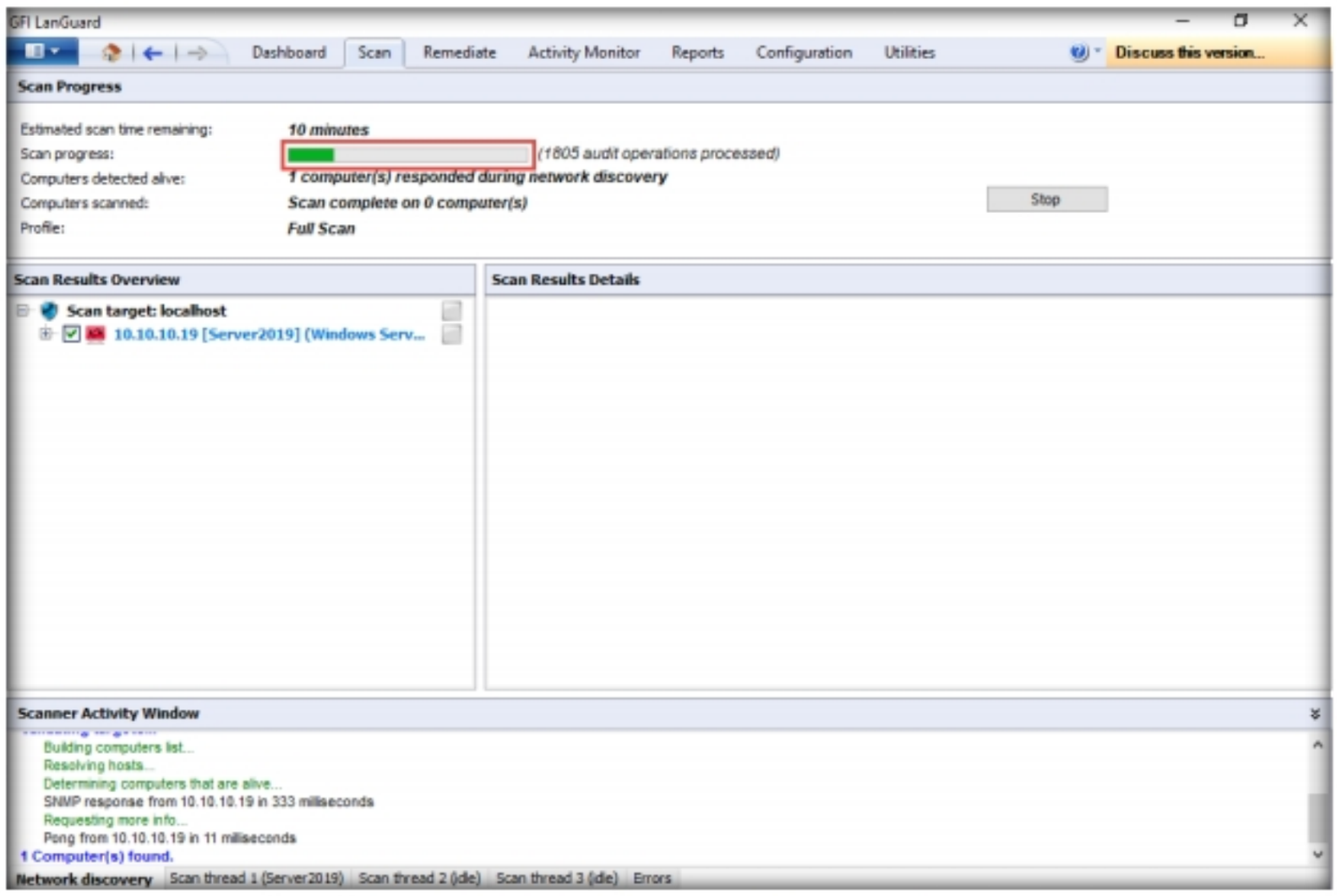


Figure 2.3.21: GFI LanGuard scanning the local machine

Note: Allow the scan to finish analyzing vulnerabilities in the host machine.

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

Note: If the **Stop scanning confirmation** pop-up appears, click **Yes**.

Note: The scan might take time to stop.

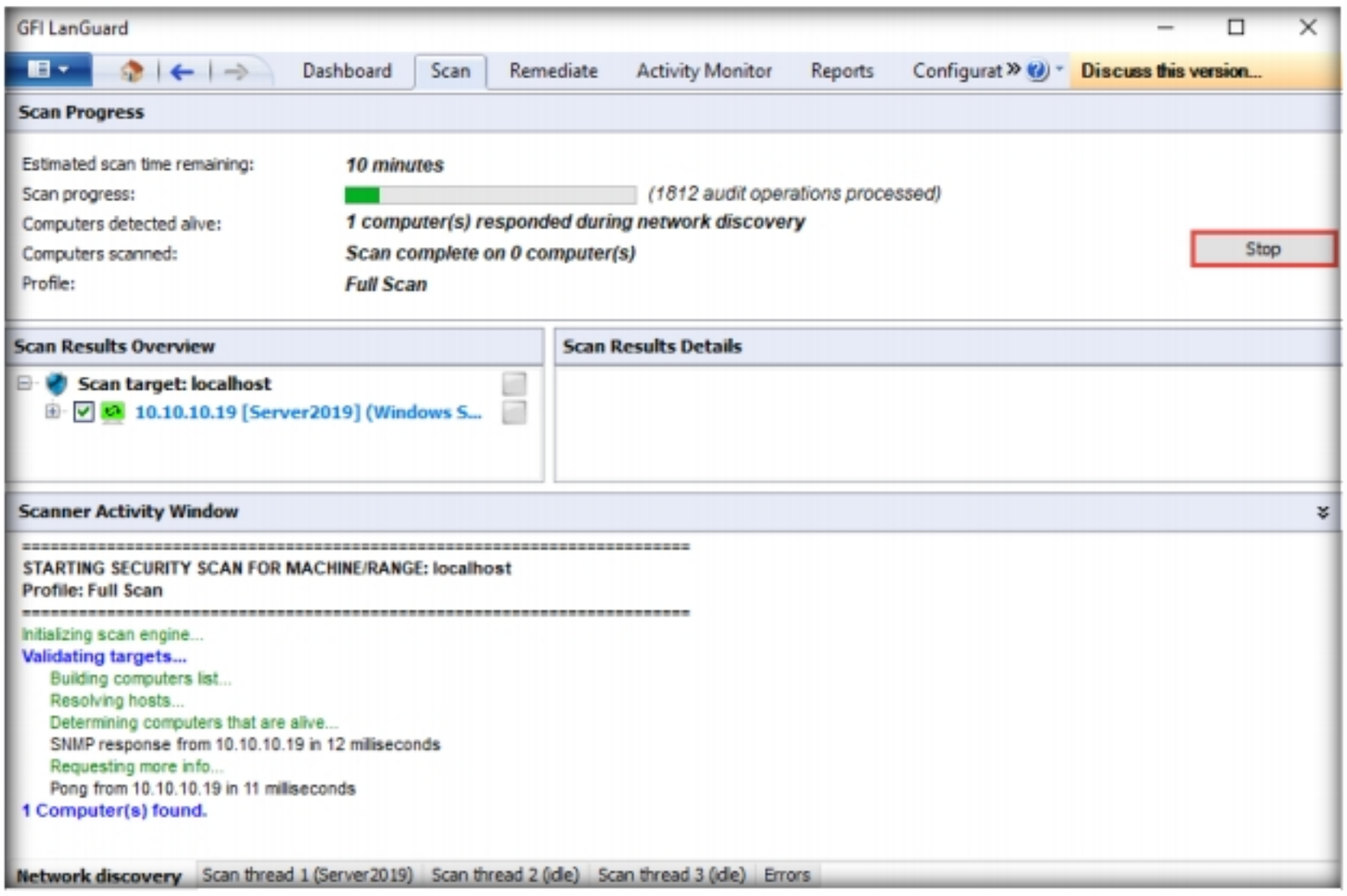


Figure 2.3.22: Stopping the scan

TASK 3.3

Scan a Target

30. The **Launch a New Scan** page appears: specify the details required to scan a target/virtual machine as follows:

- Enter the IP address of the virtual machine in the **Scan Target** field (here, the target machine is **Windows Server 2016** [**10.10.10.16**]), and ensure that the **Full Scan** option is selected from the **Profile** drop-down list.
- Ensure that **Currently logged on user** is selected in the **Credentials** drop-down list.
- Click **Scan**.

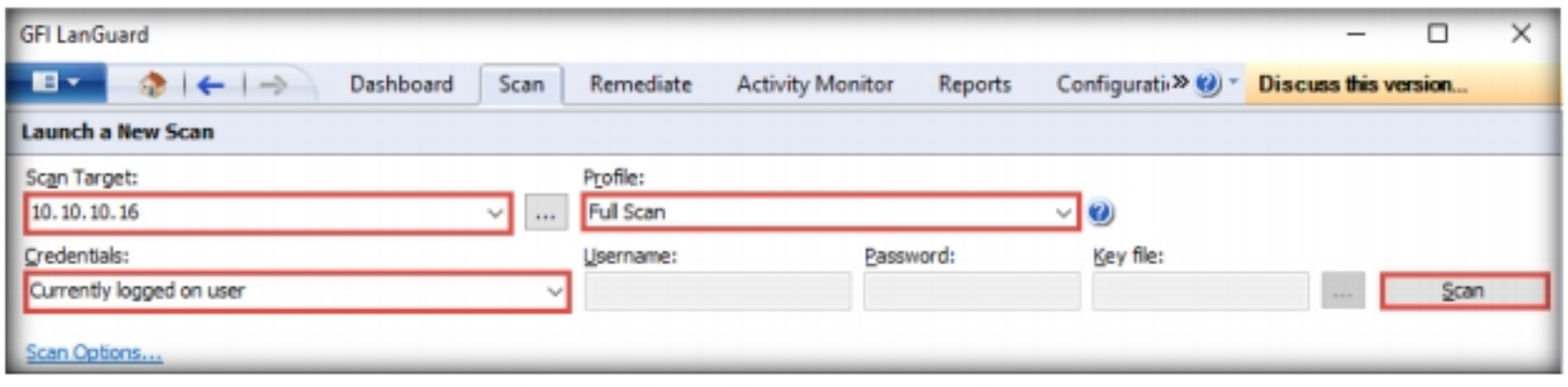


Figure 2.3.23: Customizing the scan settings

Note: This may vary in your lab environment.

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

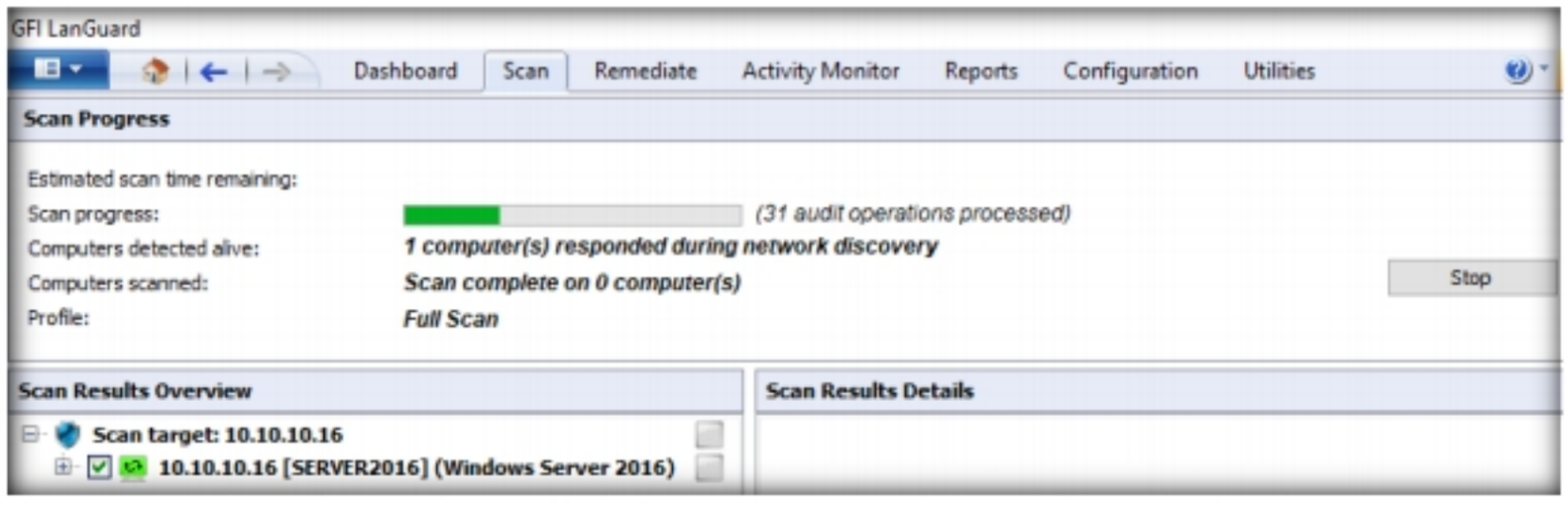


Figure 2.3.24: Vulnerability assessment being performed

32. Once the scanning is complete, a **Scan completed!** message is displayed under **Scan Results Details**, as shown in the screenshot.

Note: The scanning takes approximately 20–30 minutes to complete.

TASK 3.4

Examine the Scan Results

33. To examine the scanned result, in the left pane under **Scan Results Overview**, click the IP address (**10.10.10.16**) node to expand it. The **Vulnerability Assessment** and **Network & Software Audit** nodes are displayed, as shown in the screenshot.

Note: The results might differ in your lab environment.

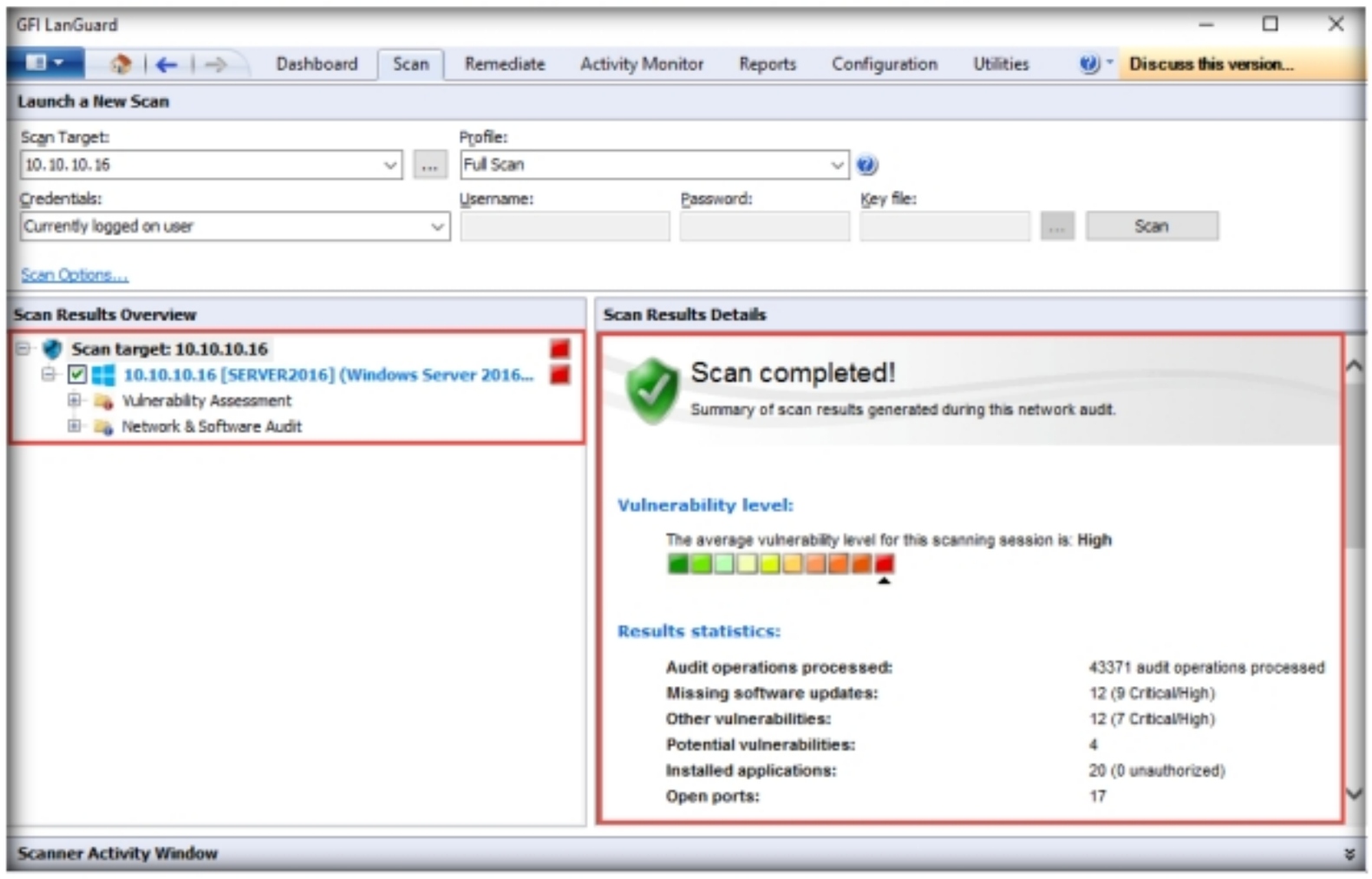


Figure 2.3.25: Viewing the scan results

34. Click the **Vulnerability Assessment** node. This shows category-wise details of assessed vulnerabilities. Click each category to view the vulnerabilities in detail.

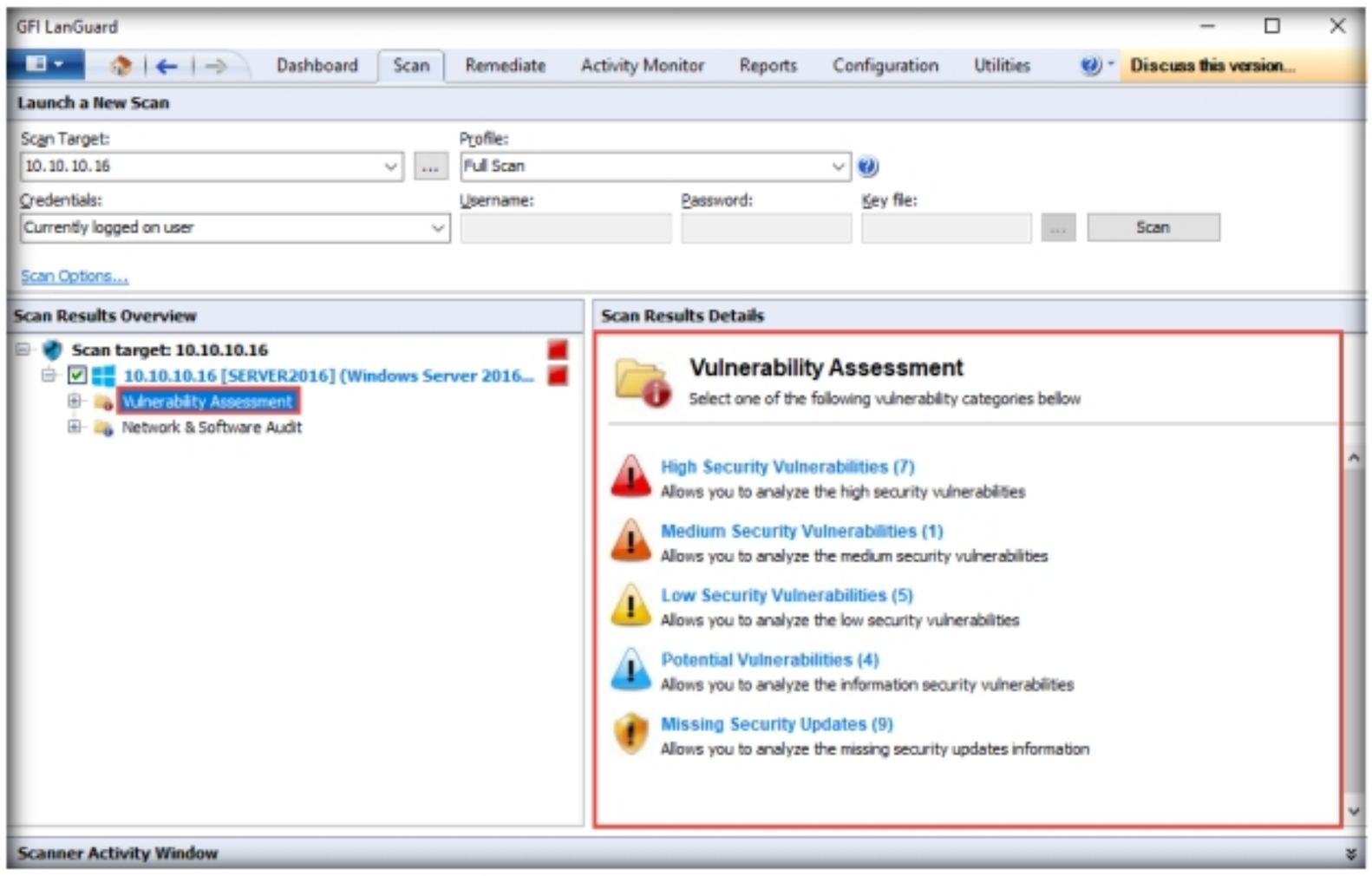


Figure 2.3.26: Vulnerability Assessment categories

35. Expand the **Network & Software Audit** node in the left pane. Click **System patching status**; detailed information regarding system patches is displayed under the **Scan Results Details** section in the right pane, as shown in the screenshot.

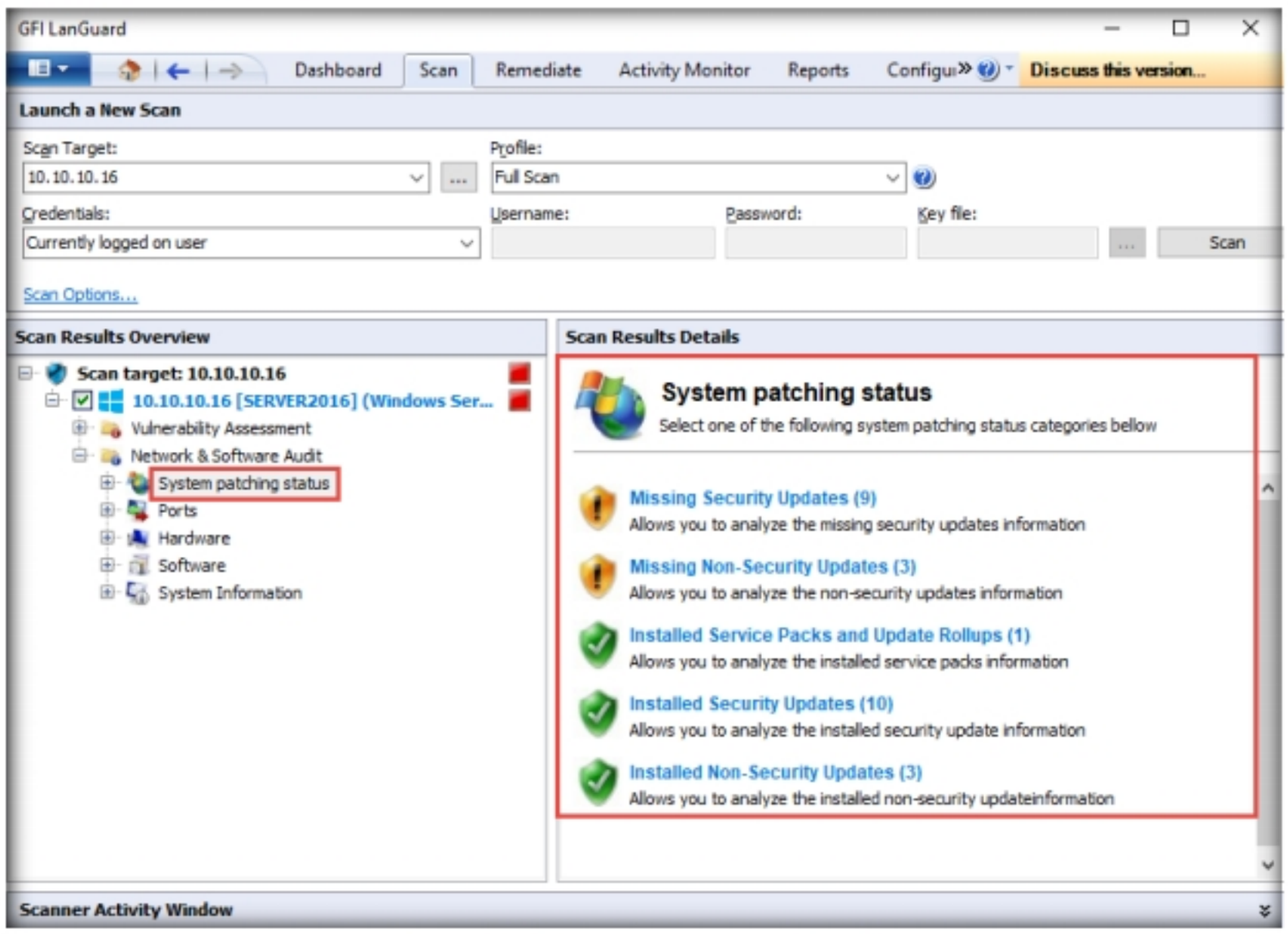


Figure 2.3.27: System patches status information

36. Expand **Ports** and click **Open TCP Ports** to view all the open TCP Ports under the **Scan Results Details** section in the right pane, as shown in the screenshot.

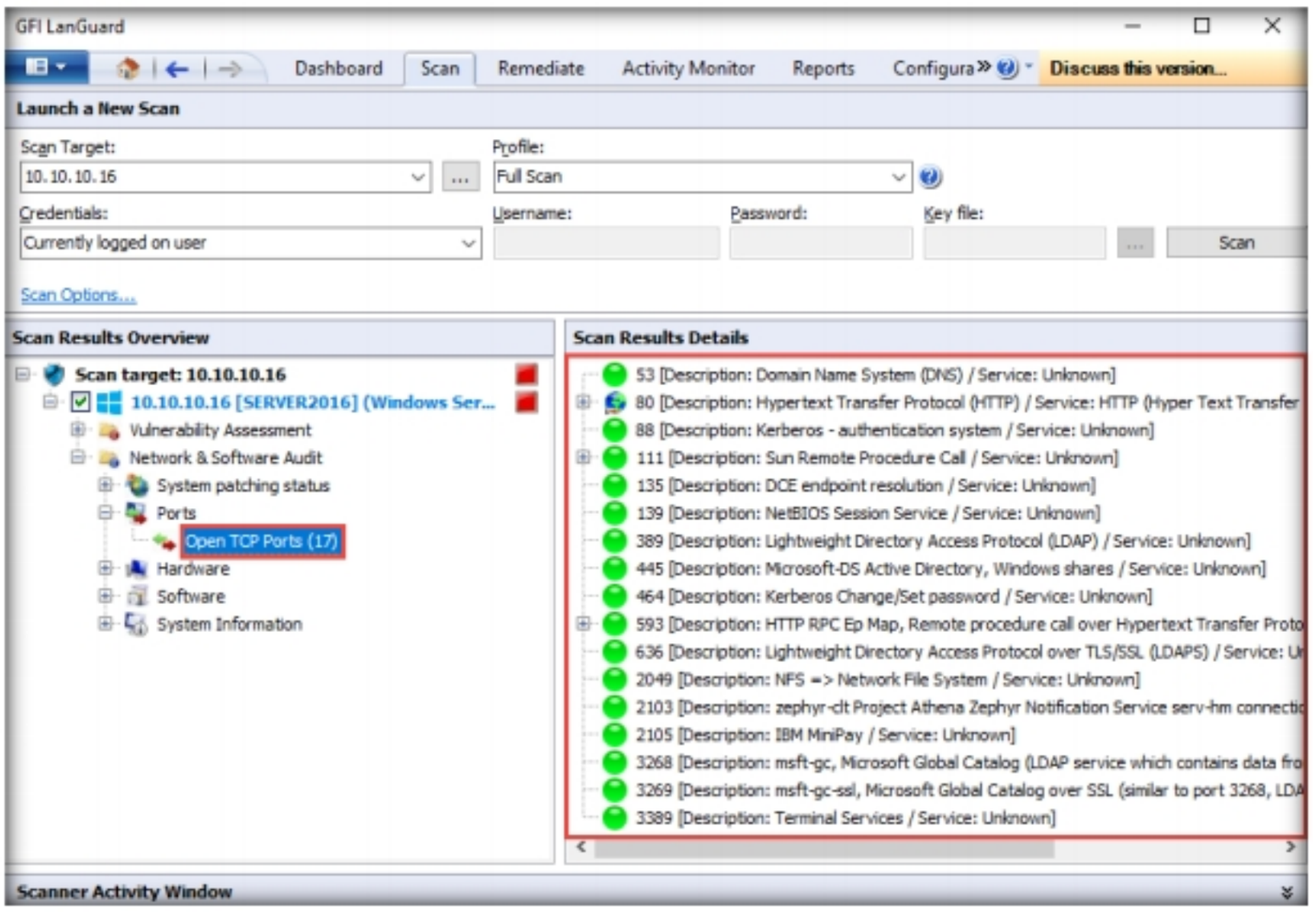


Figure 2.3.28: Scan results for open TCP Ports

37. Click **System Information** to view detailed information about the target system under the **Scan Results Details** section in the right pane.

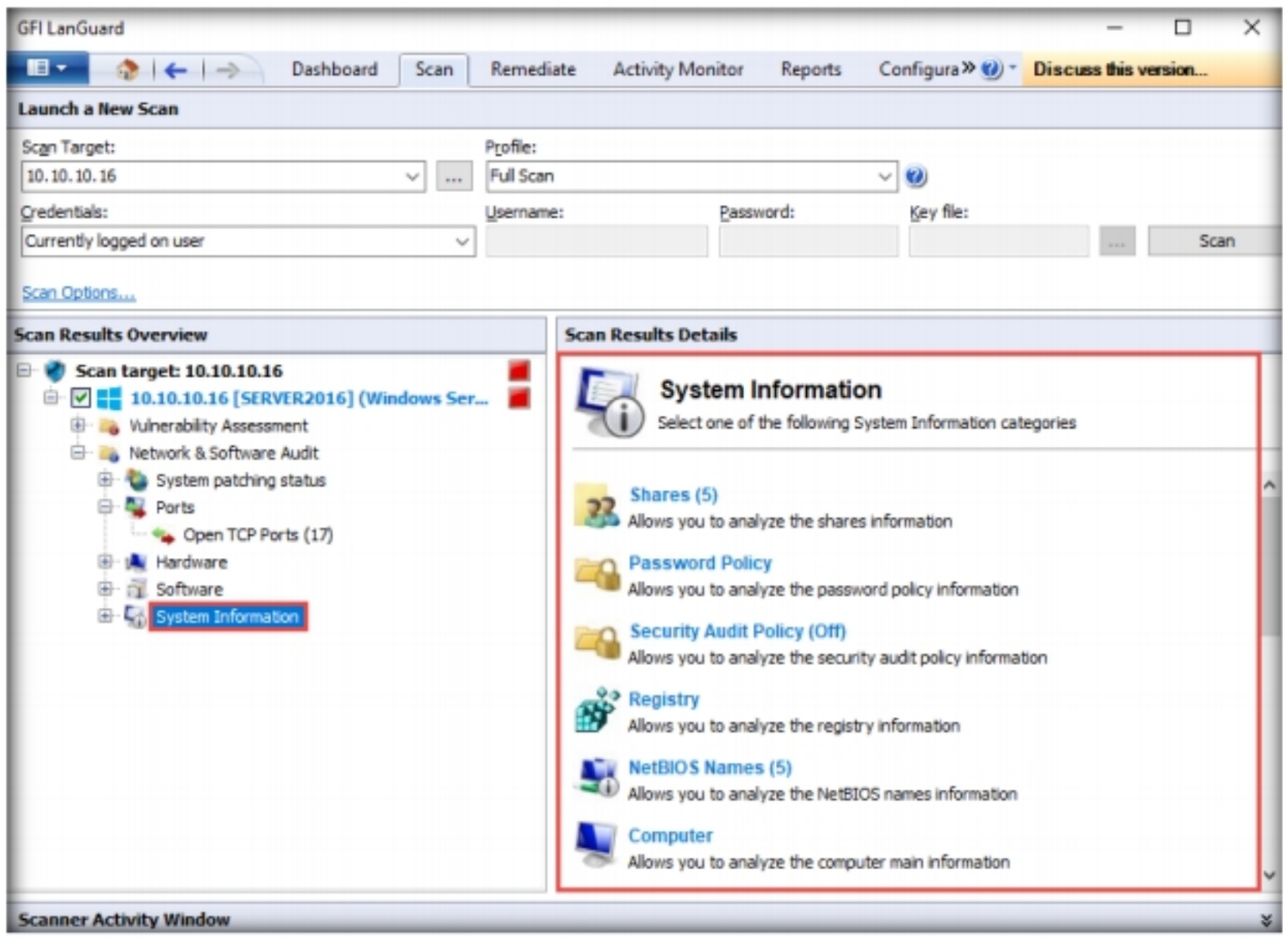


Figure 2.3.29: Scan results System Information

38. Expand the **System Information** node and click **Shares** to view the details of shared folders in the target virtual machine.

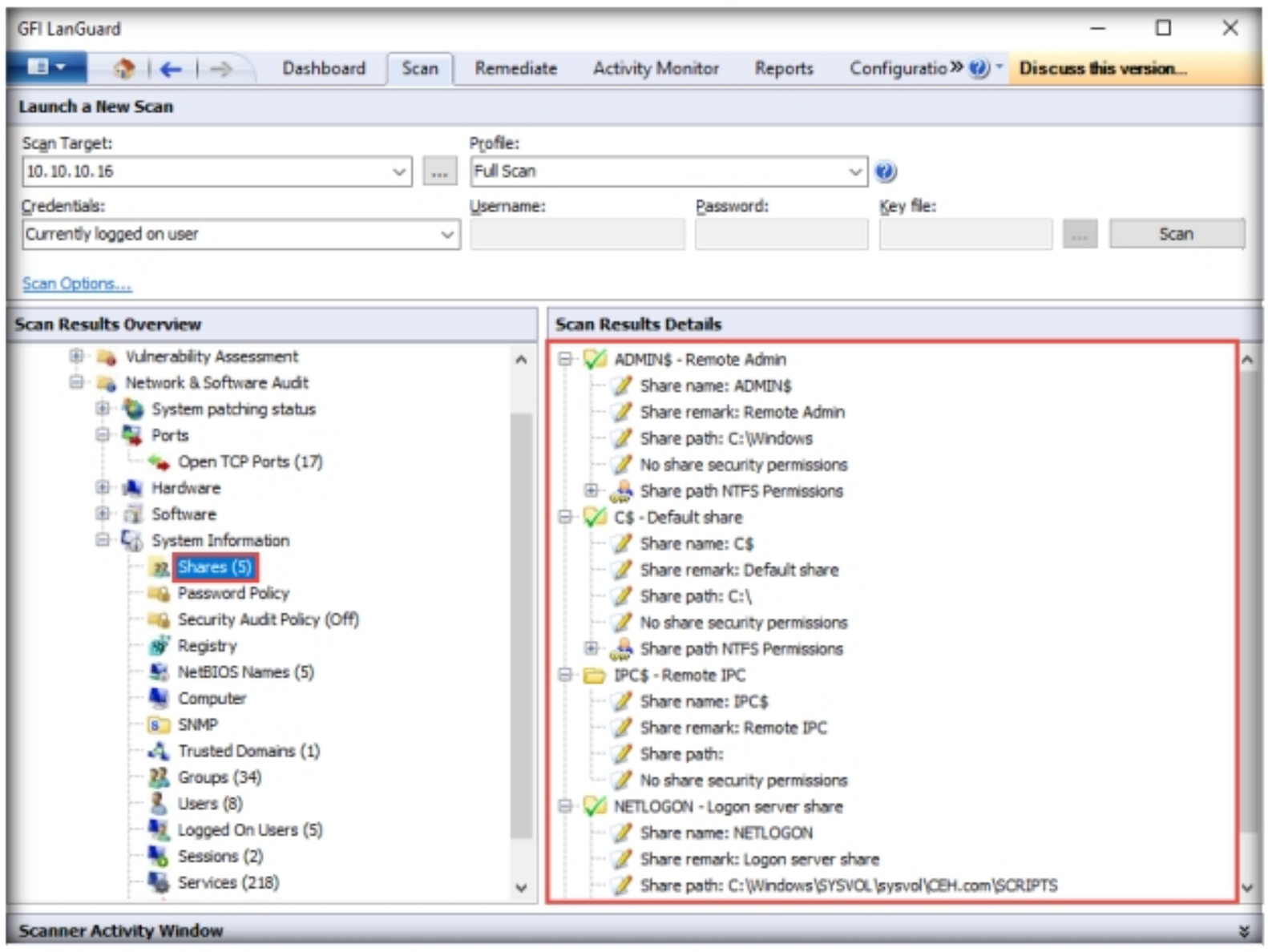


Figure 2.3.30: Scan results for Shared folders

39. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.

40. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **CEH**; then, click **SERVER2016**.

41. Detailed information such as **Vulnerability Level**, **Security Sensors**, **Computer Details**, **Scan Activity**, and **Results Statistics** are displayed in the right pane, as shown in the screenshot.

Note: In real-time, using this vulnerability information about the target systems can be used to develop and design exploits suitable to break into a network or a single target.

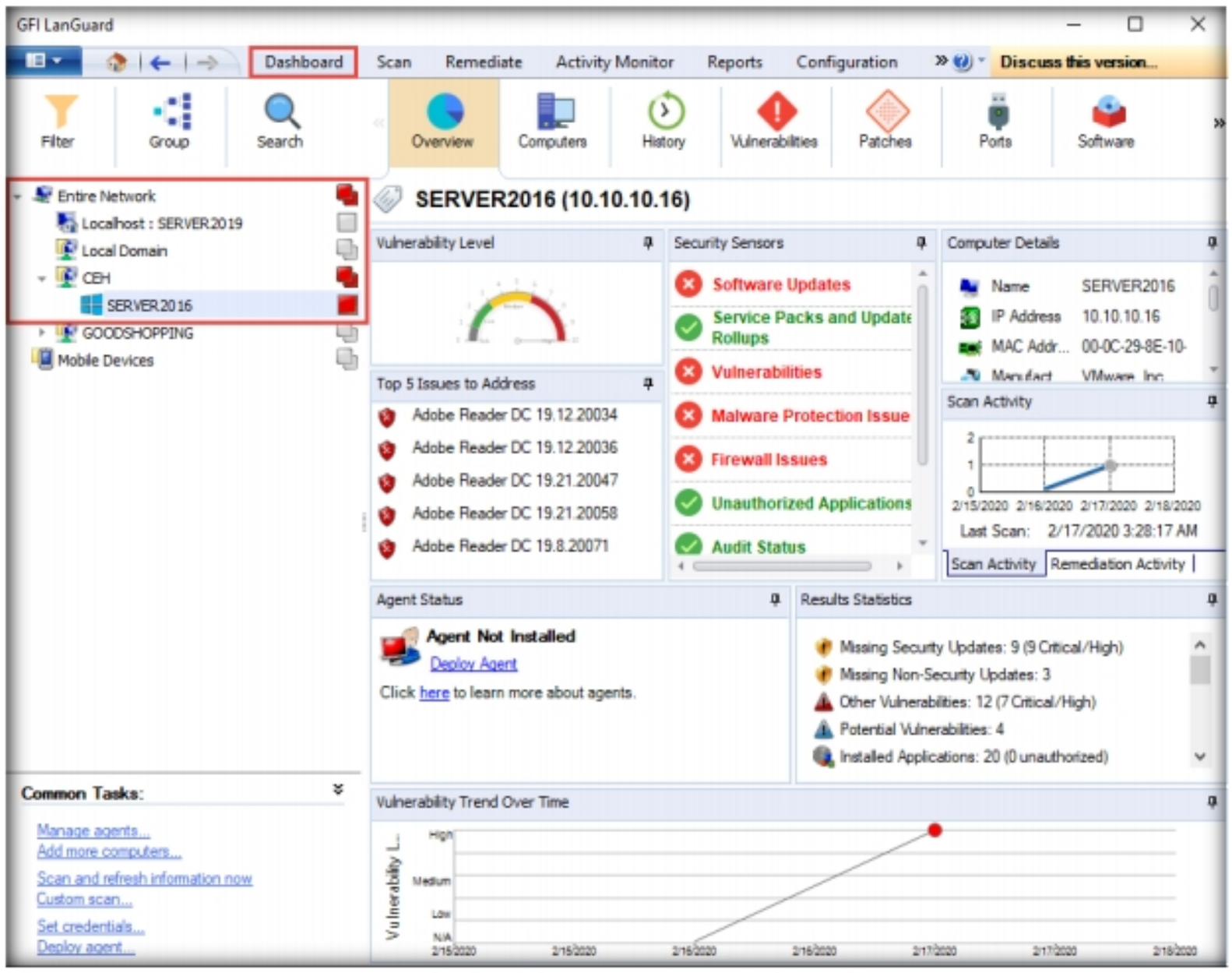


Figure 2.3.31: Overview of the Scan in Dashboard

42. You can further explore the tool by clicking on various options. For instance, click on **Software** from the options at the top to view a list of applications installed on the target machine under the **Application Category** list. You can also click on any application (here, **Google Chrome**) to view its detailed information under **Details** sections, as shown in the screenshot.

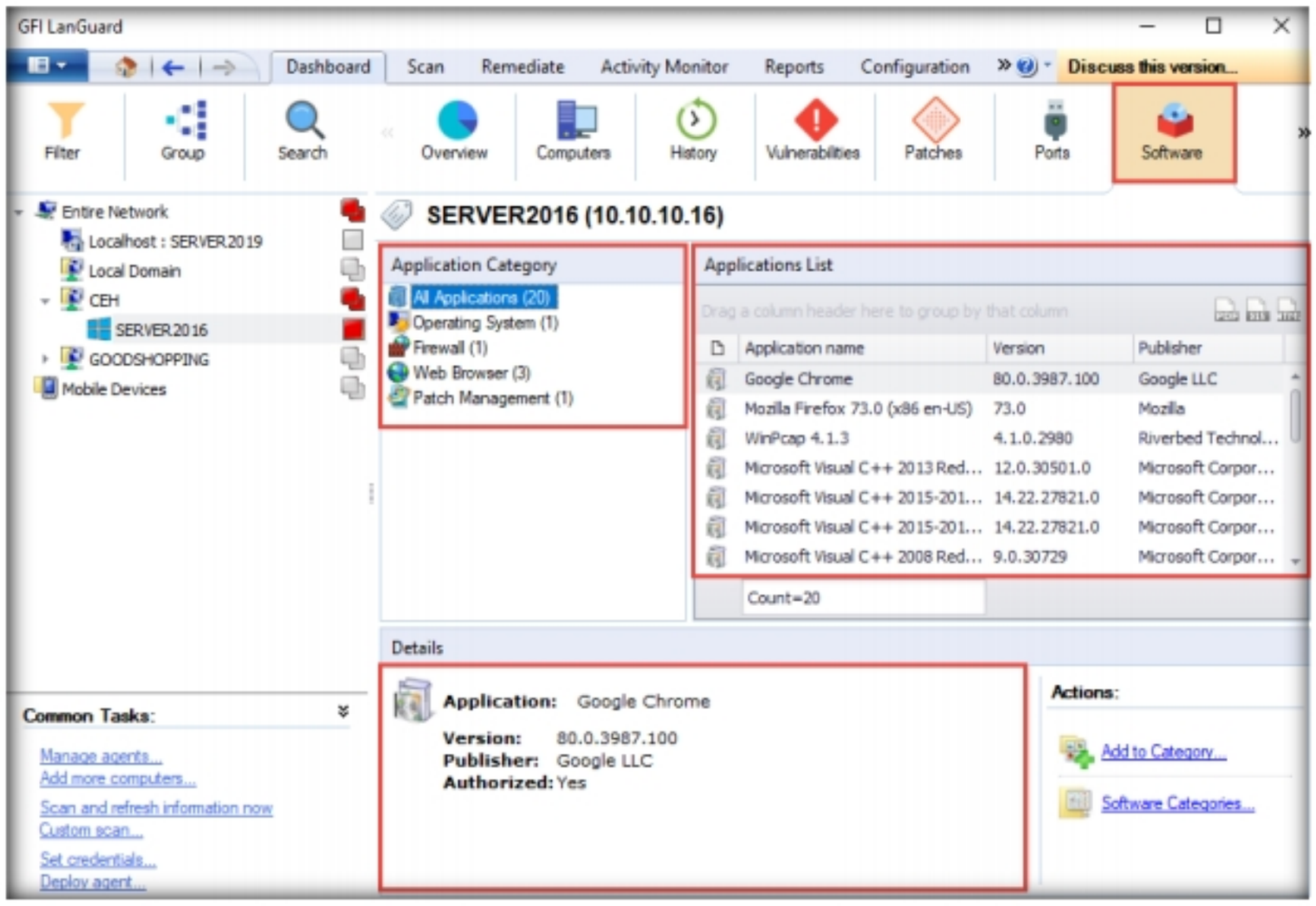


Figure 2.3.32 List of open ports

43. Click on the **Vulnerabilities** option; a list of various categories of vulnerabilities appears under the **Vulnerability Types** section. Click on any category of vulnerability (here, **High Security Vulnerabilities**): detailed information on this category is displayed under the **Details** section, and a list of vulnerabilities is displayed under the **Vulnerability List** section.

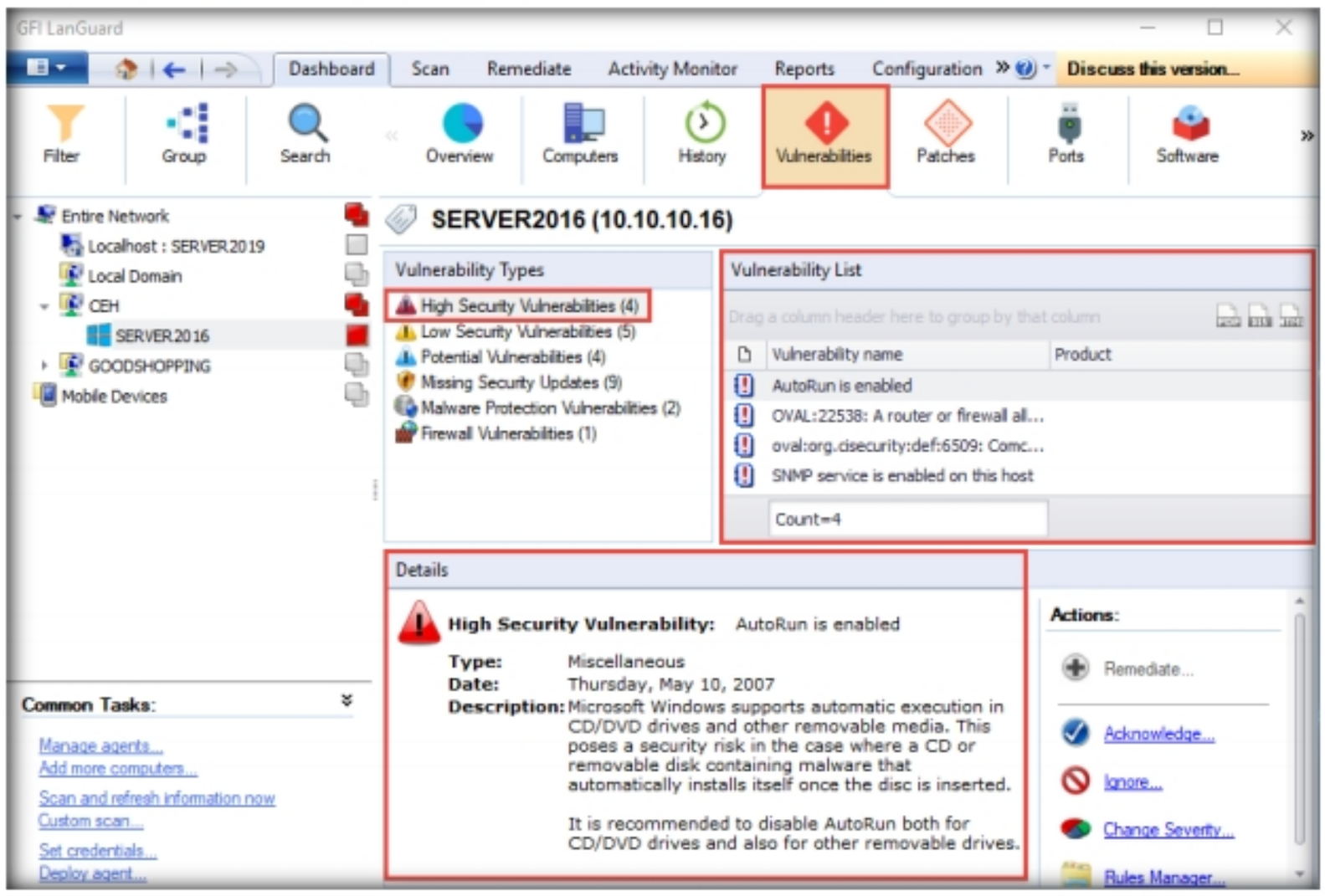


Figure 2.3.33: List of vulnerabilities

TASK 3.5

Generate Report

44. You can further explore scanned results by clicking various options such as **Patches**, **System Information**, **Hardware**, and **Ports**.

45. Now, click on the **Report** tab and click the **Vulnerability Status** type under **General Reports** from the right pane.

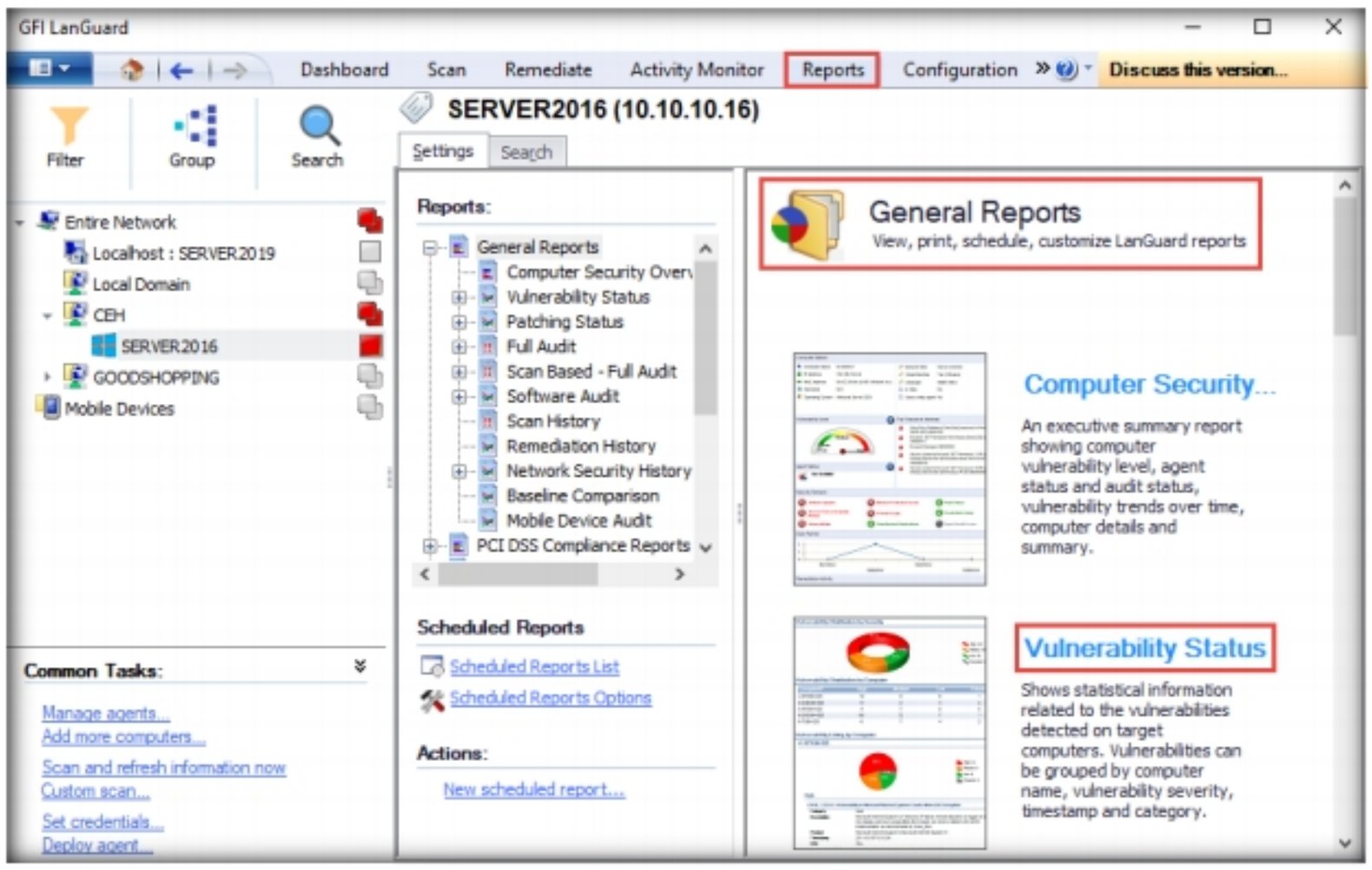


Figure 2.3.34: Generate vulnerability report

46. Information about the **Vulnerability Status** report appears in the right pane; click the **Generate Report** button to create the vulnerability report.

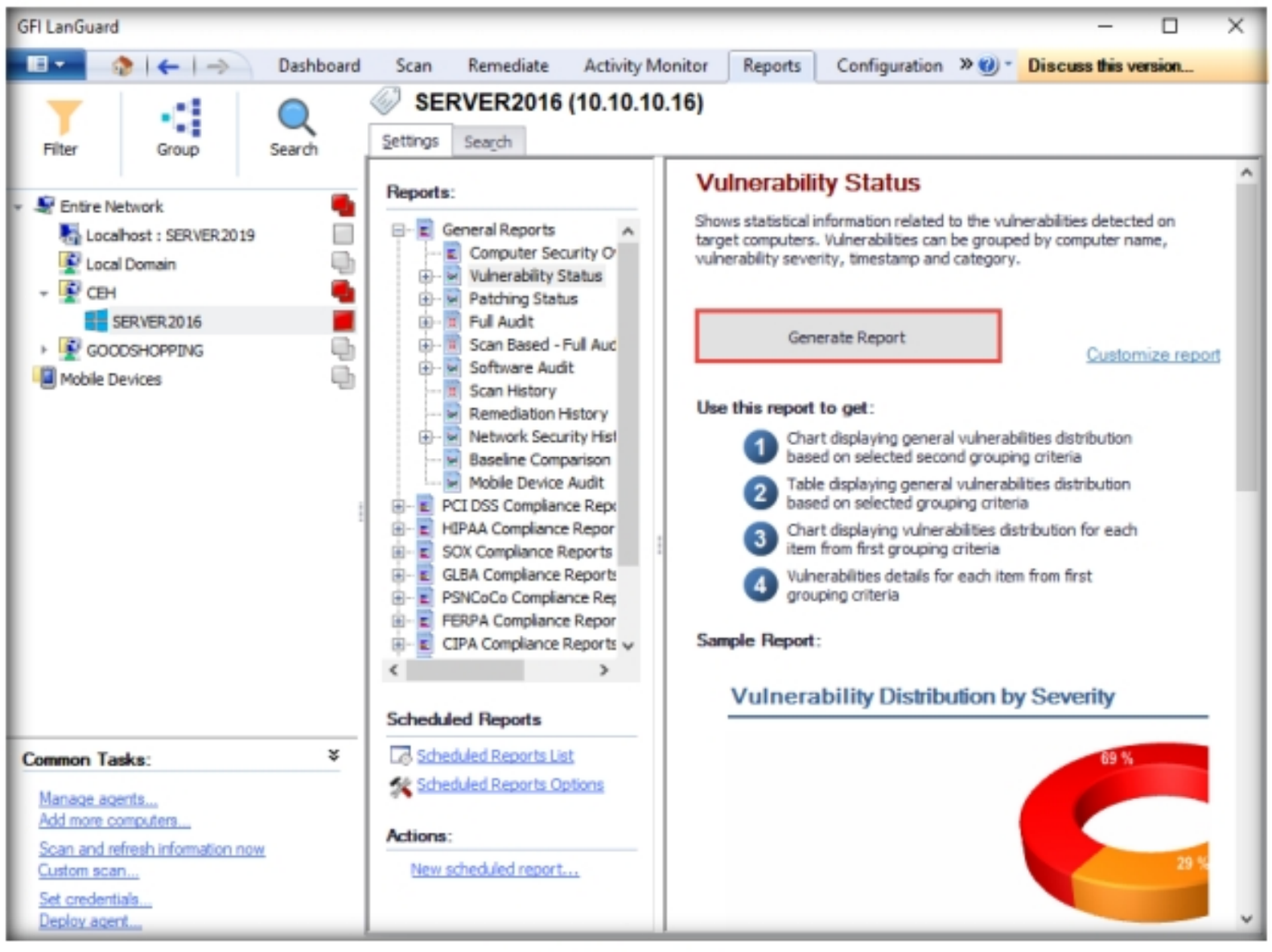


Figure 2.3.35: Generate Report

47. The **Vulnerability Status** report appears in the right pane. Click on the drop-down icon next to ( ) icon and choose the **HTML File** format.

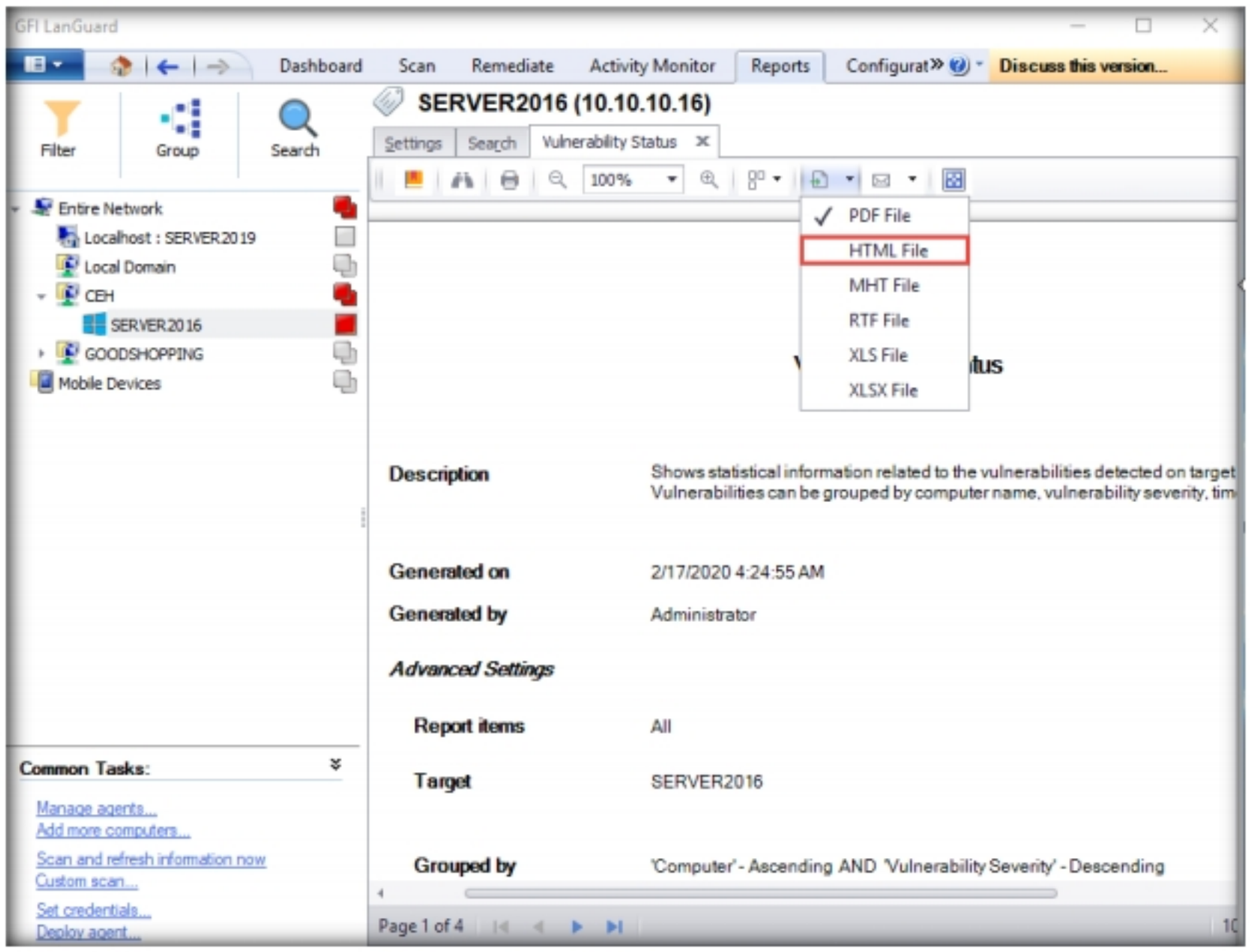


Figure 2.3.36: Report format

48. The **HTML Export Options** window appears; leave the settings to default and click **OK**.

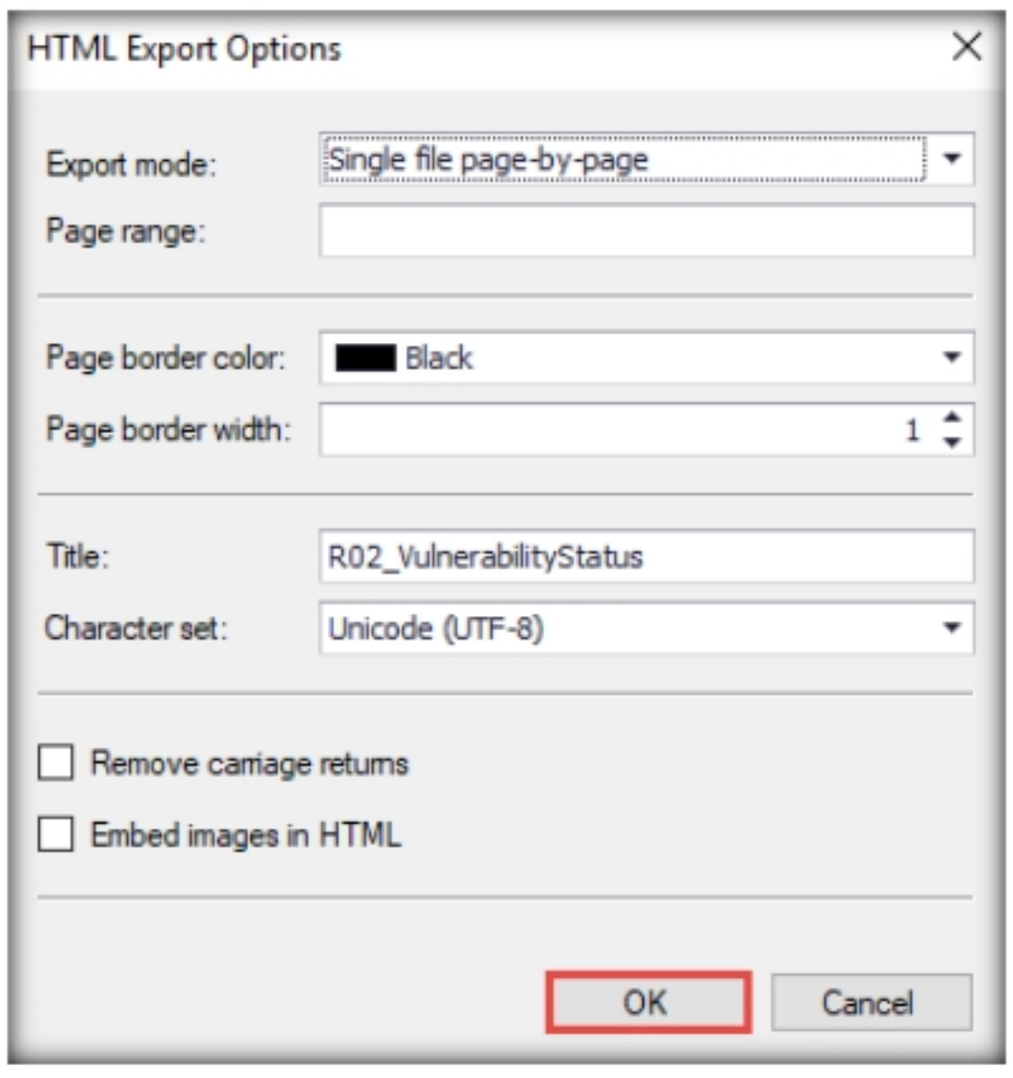


Figure 2.3.37: HTML Export Options

49. The **Save As** window appears; set the download location to **Desktop**. Rename the file to **Vulnerability Status Report.html** and click **Save**.

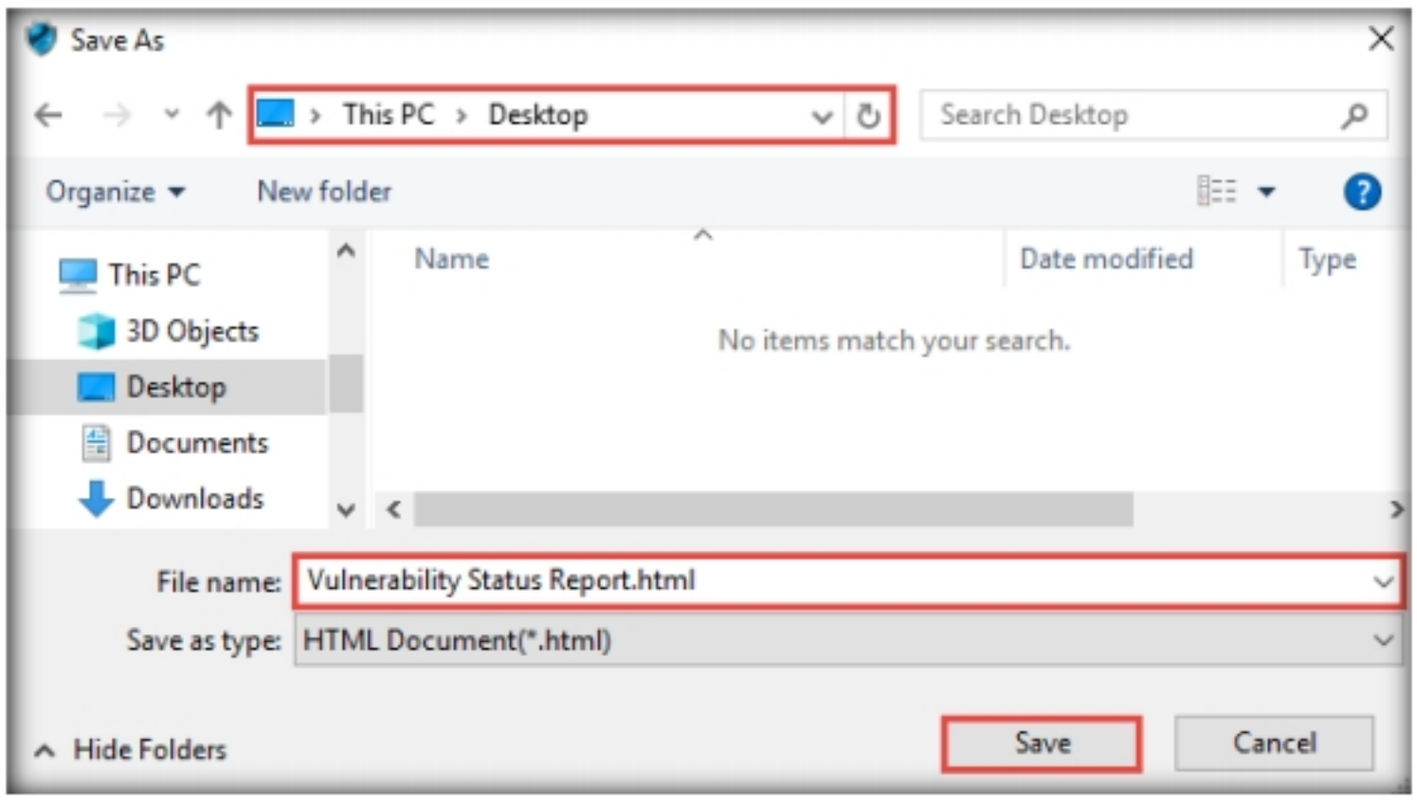


Figure 2.3.38: Save As window

50. The **GFI LanGuard** pop-up appears; click **Yes** to open the file.

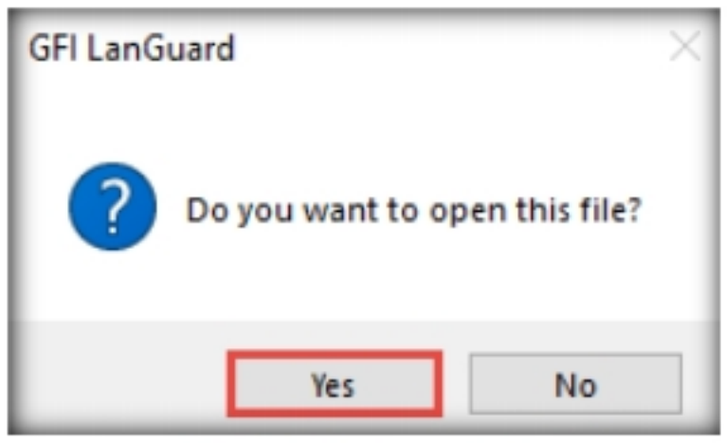


Figure 2.3.39: Open the file

51. In the **How do you want to open this file?** pop-up, select any web browser (here, **Firefox**) and click **OK**.

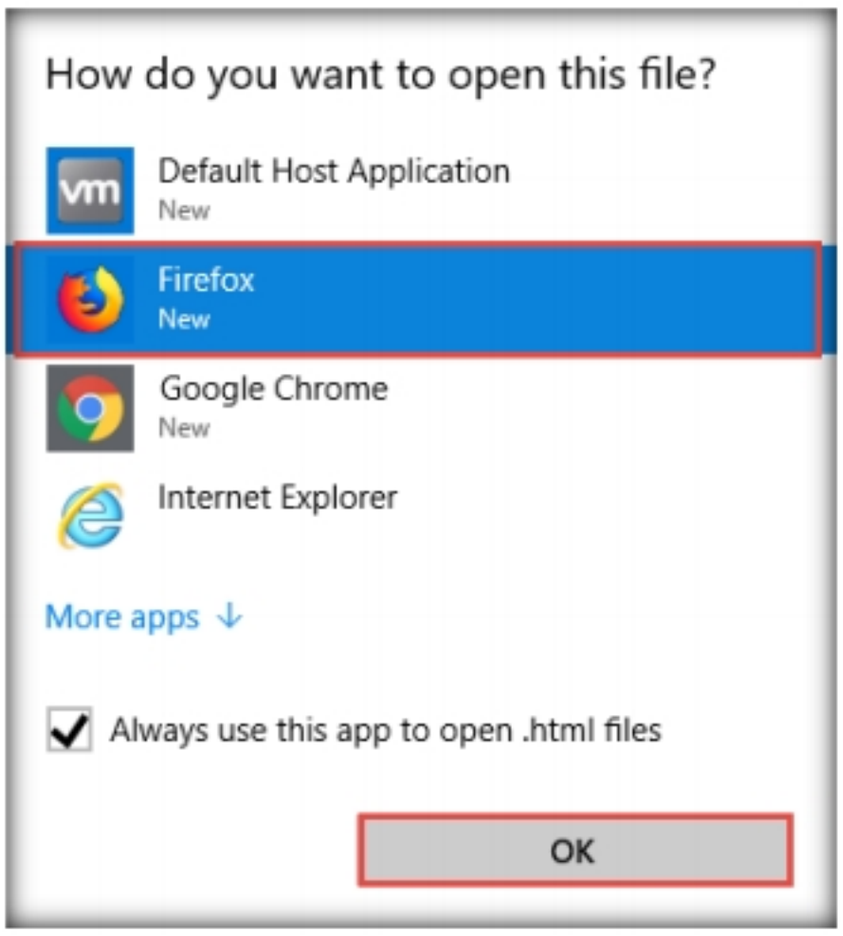


Figure 2.3.40: Selecting a web browser

52. The **Vulnerability Status** report appears; you can scroll down to view detailed information regarding discovered vulnerabilities.

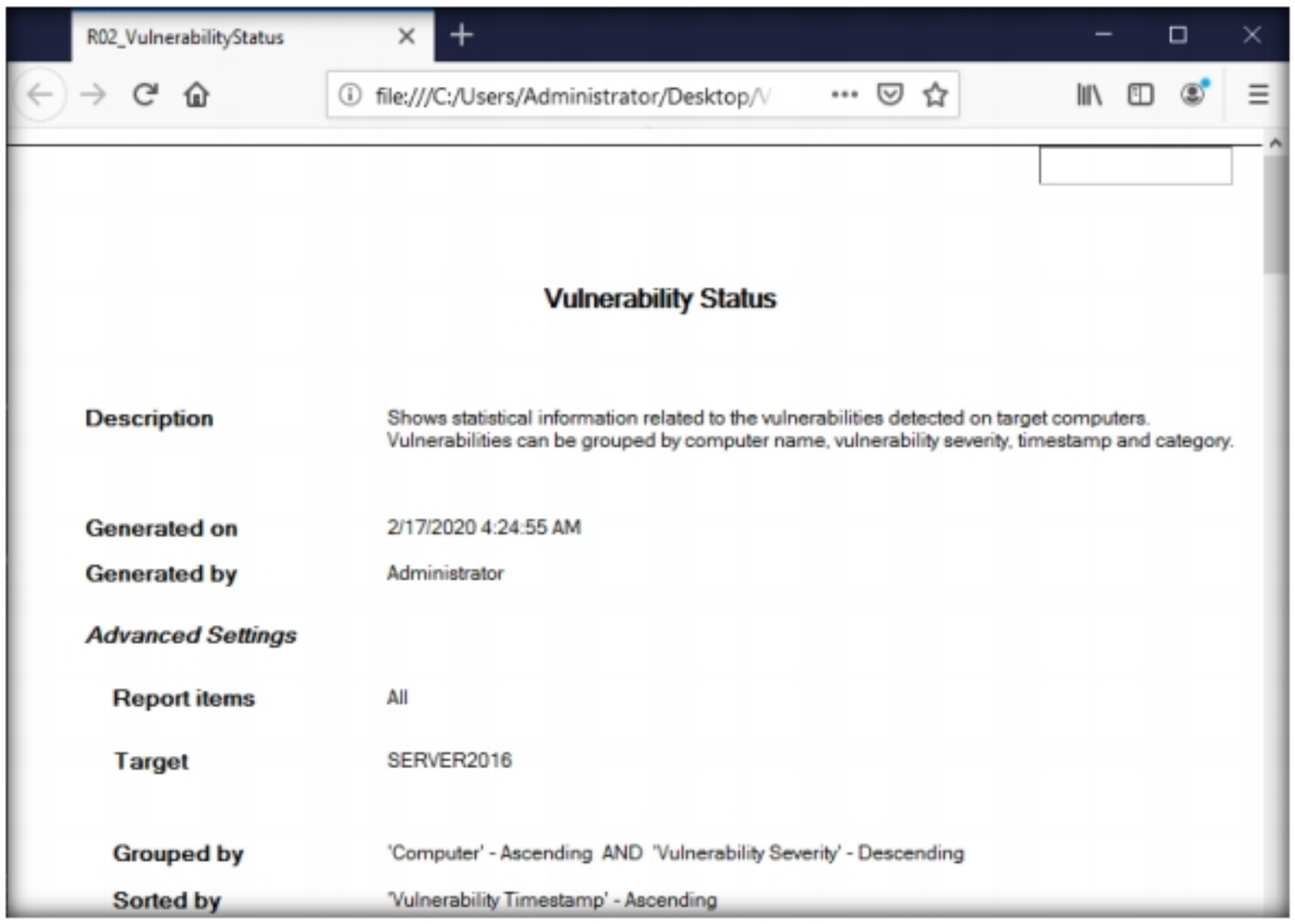


Figure 2.3.41: Vulnerability Status Report

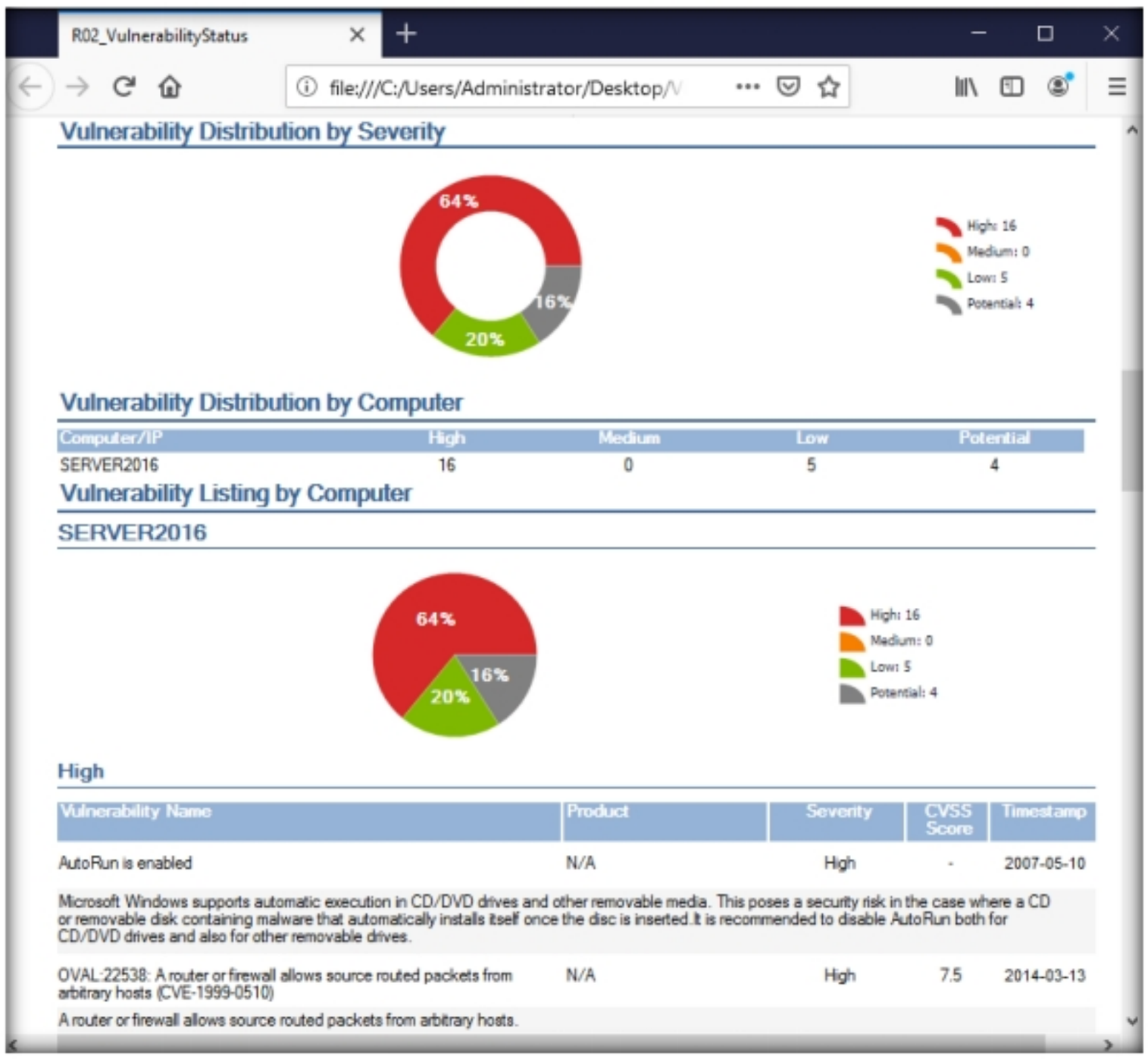


Figure 2.3.42 Vulnerability Status Report

53. This concludes the demonstration of scanning network vulnerabilities using GFI LanGuard.
54. Close all open windows and document all the acquired information.
55. Turn off the **Windows Server 2016** and **Windows Server 2019** virtual machines.

TASK 4

Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

Here, we will perform web servers and applications vulnerability scanning using CGI scanner Nikto.

Note: In this task, we will target the **www.certifiedhacker.com** website.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

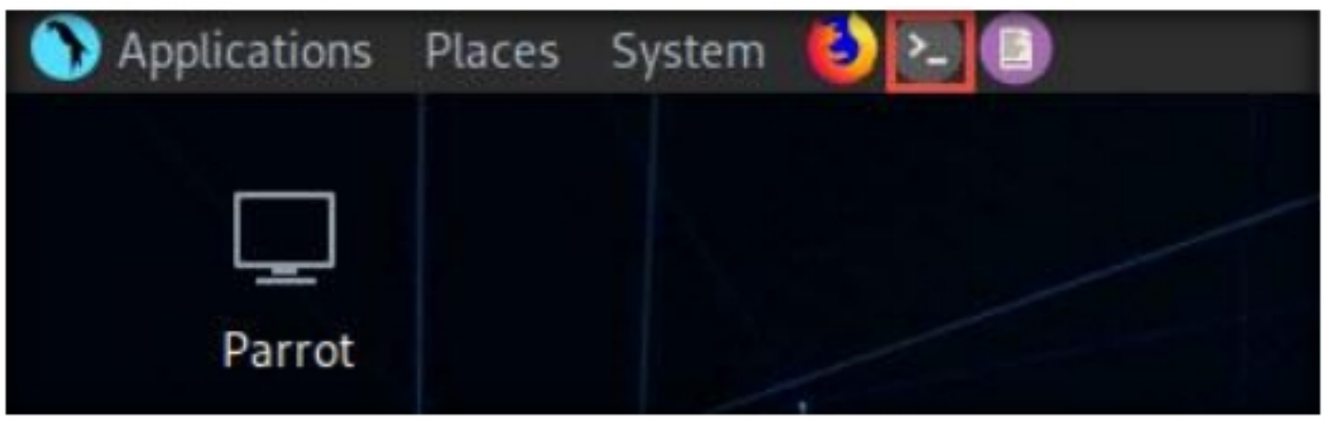


Figure 2.4.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type **nikto -H** and press **Enter** to view various available commands with full help text

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

It also checks for server configuration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

TASK 4.1

Launch Nikto Tool

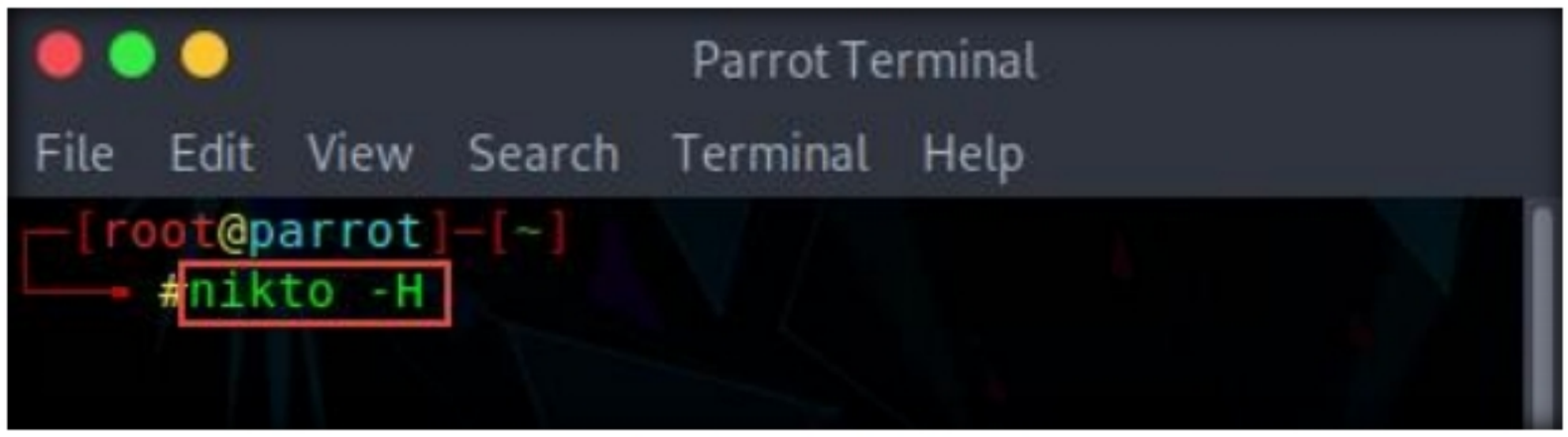


Figure 2.4.2: Nikto help command

8. The result appears, displaying various available options in Nikto. We will use the **Tuning** option to do a deeper and more comprehensive scan on the target webserver.

Note: A tuning scan can be used to decrease the number of tests performed against a target. By specifying the type of test to include or exclude, faster and focused testing can be completed. This is useful in situations where the presence of certain file types such as XSS or simply "interesting" files is undesired.

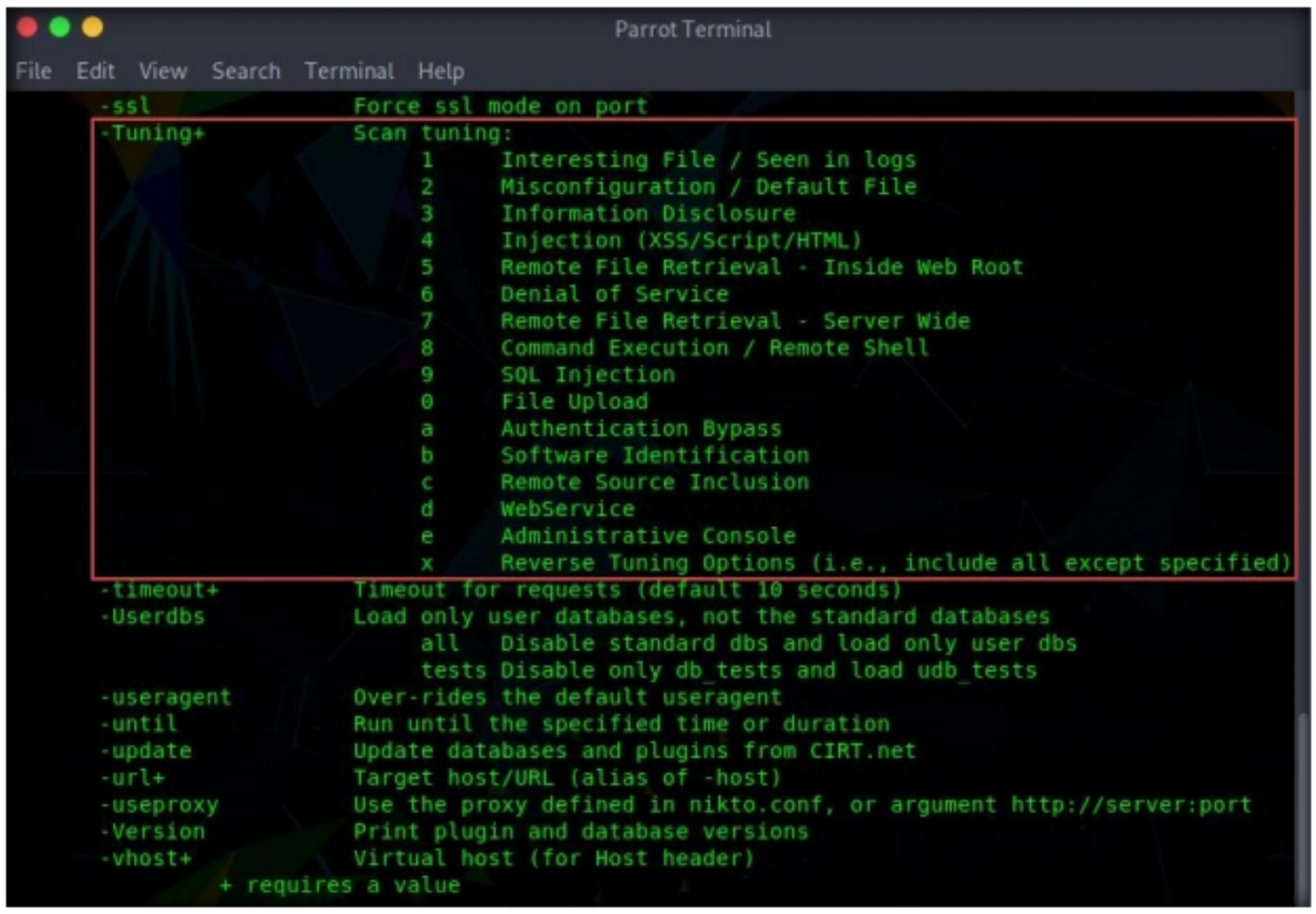


Figure 2.4.3: Nikto tuning options

9. In the terminal window, type **nikto -h <Target Website> -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

Note: **-h**: specifies the target host and **x**: specifies the Reverse Tuning Options (i.e., include all except specified)

10. The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website.

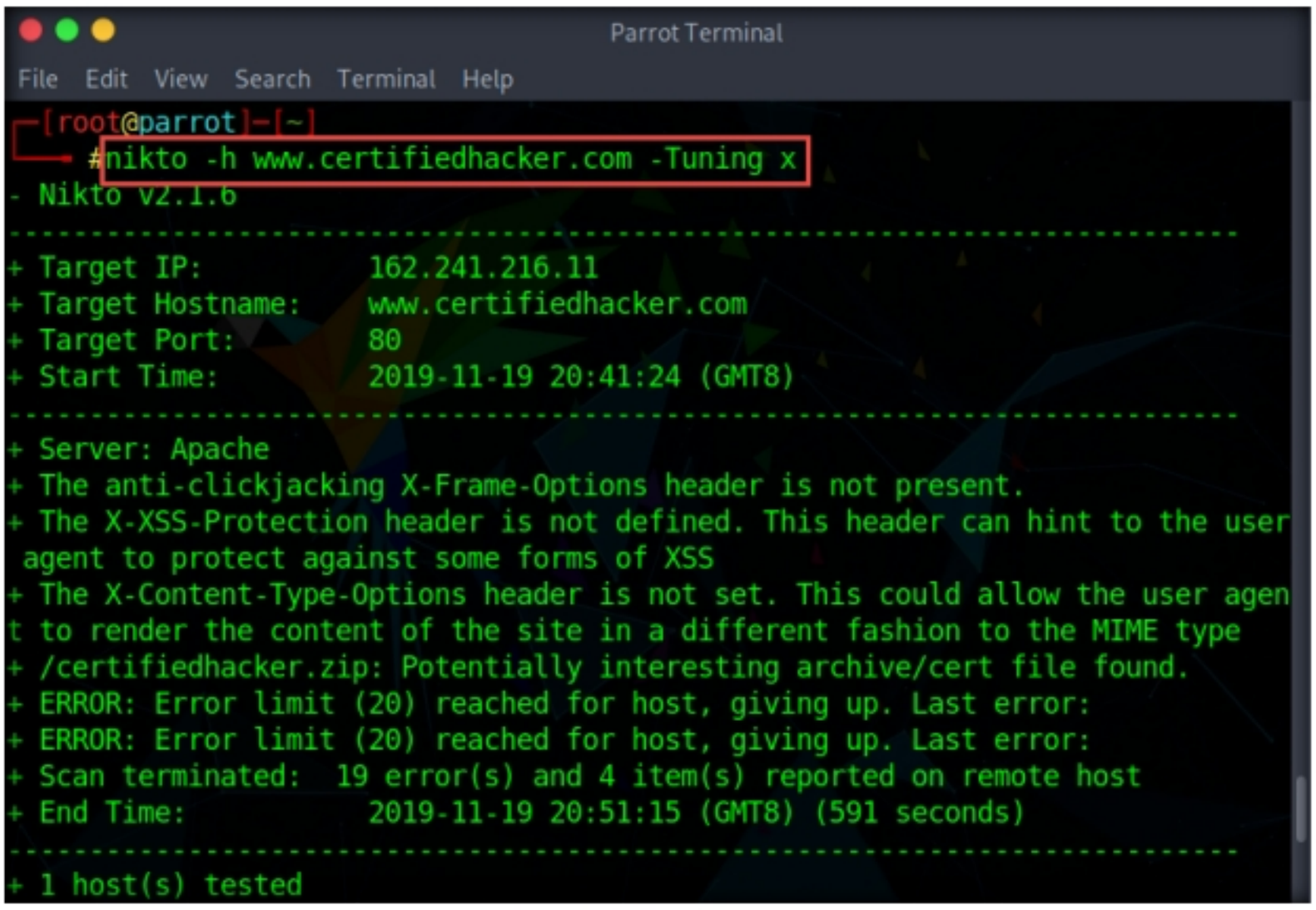


Figure 2.4.4: Nikto scan output

11. Here, we will check for cgi directories with the **-Cgidirs** option. In this option, search for specific directories or use **all** options to search for all the available directories.

12. In the terminal window, type **nikto -h <Target Website> -Cgidirs all**, (here, the target website is **www.certifiedhacker.com**) and hit **Enter**.

Note: **-Cgidirs**: scans the specified CGI directories; users can use filters such as "**none**" or "**all**" to scan all CGI directories or none).

13. The target website does not have any CGI directory; therefore, the same result as the previous scan was obtained.

Note: You can use try this command on another website to obtain information about CGI directories.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[~]
└──╼ #nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2019-11-19 20:58:20 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
 agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ ERROR: Error limit (20) reached for host, giving up. Last error: invalid HTT
P response
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  20 error(s) and 4 item(s) reported on remote host
+ End Time:           2019-11-19 21:08:20 (GMT8) (600 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 2.4.5: Nikto option to scan CGI directories

TASK 4.2

Save Scan Results

14. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd Desktop** and press **Enter**. Type **nikto -h <Target IP Address> -o <File_Name> -F txt** and press **Enter**.

Note: **-h**: specifies the target, **-o**: specifies the name of the output file, and **-F**: specifies the file format.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[~]
└──╼ #cd Desktop
┌─[root@parrot]─[~/Desktop]
└──╼ #nikto -h www.certifiedhacker.com -o Nikto_Scan_Results -F txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2019-11-19 21:25:26 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
 agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  19 error(s) and 4 item(s) reported on remote host
+ End Time:           2019-11-19 21:34:48 (GMT8) (562 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 2.4.6: Saving Vulnerability Analysis Results

15. Navigate to **/root/Desktop** and open the **Nikto_Scan_Results** file. The file appears displaying the scanned results.

Note: To navigate to the **Desktop** folder, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **/root/Desktop**

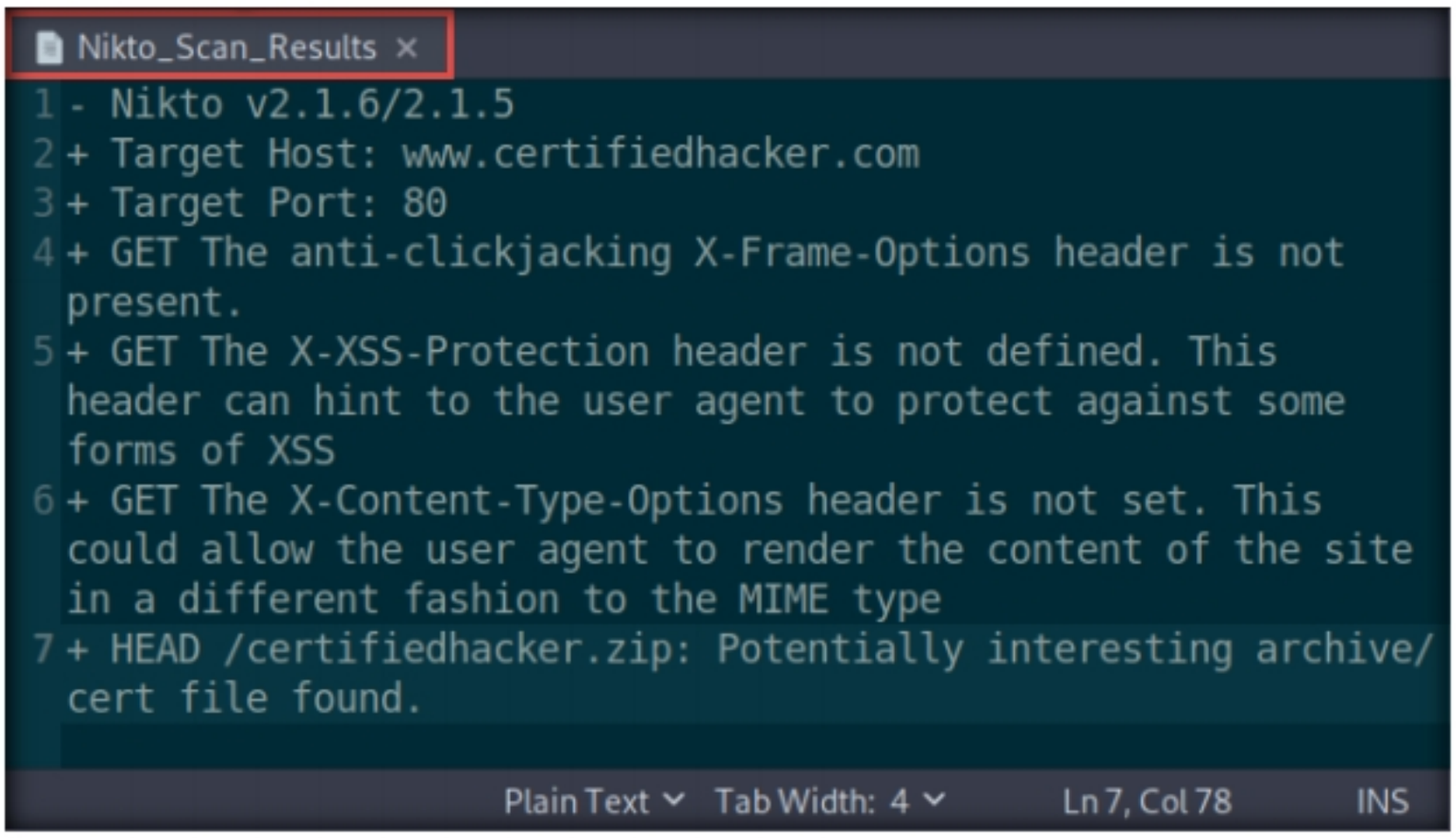


Figure 2.4.7: Nikto Scan Results File

16. This concludes the demonstration of checking vulnerabilities in the target website using Nikto.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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