Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

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

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.

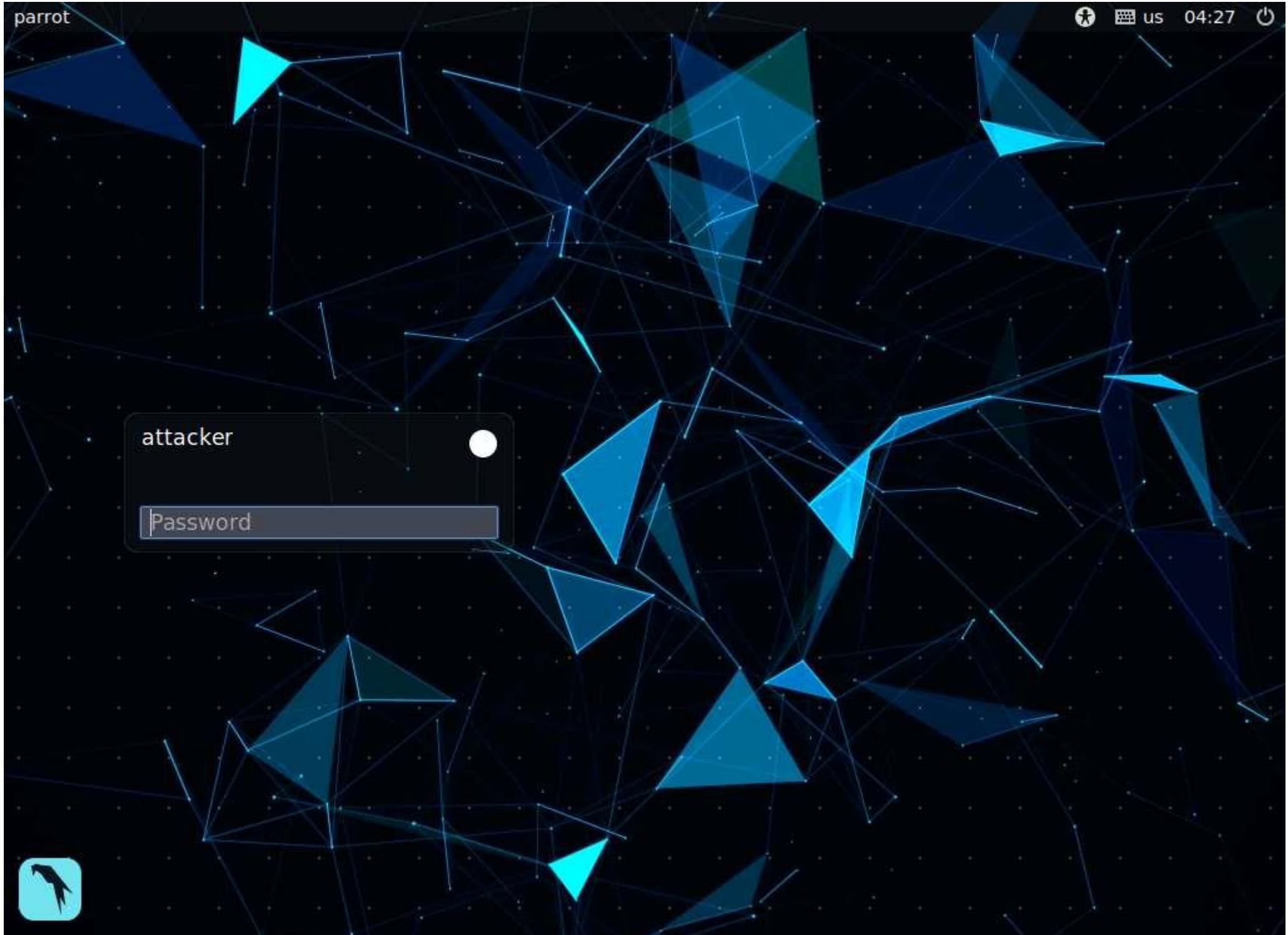
Task 1: Perform Vulnerability Analysis using OpenVAS

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

Here, we will perform a vulnerability analysis using OpenVAS.

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

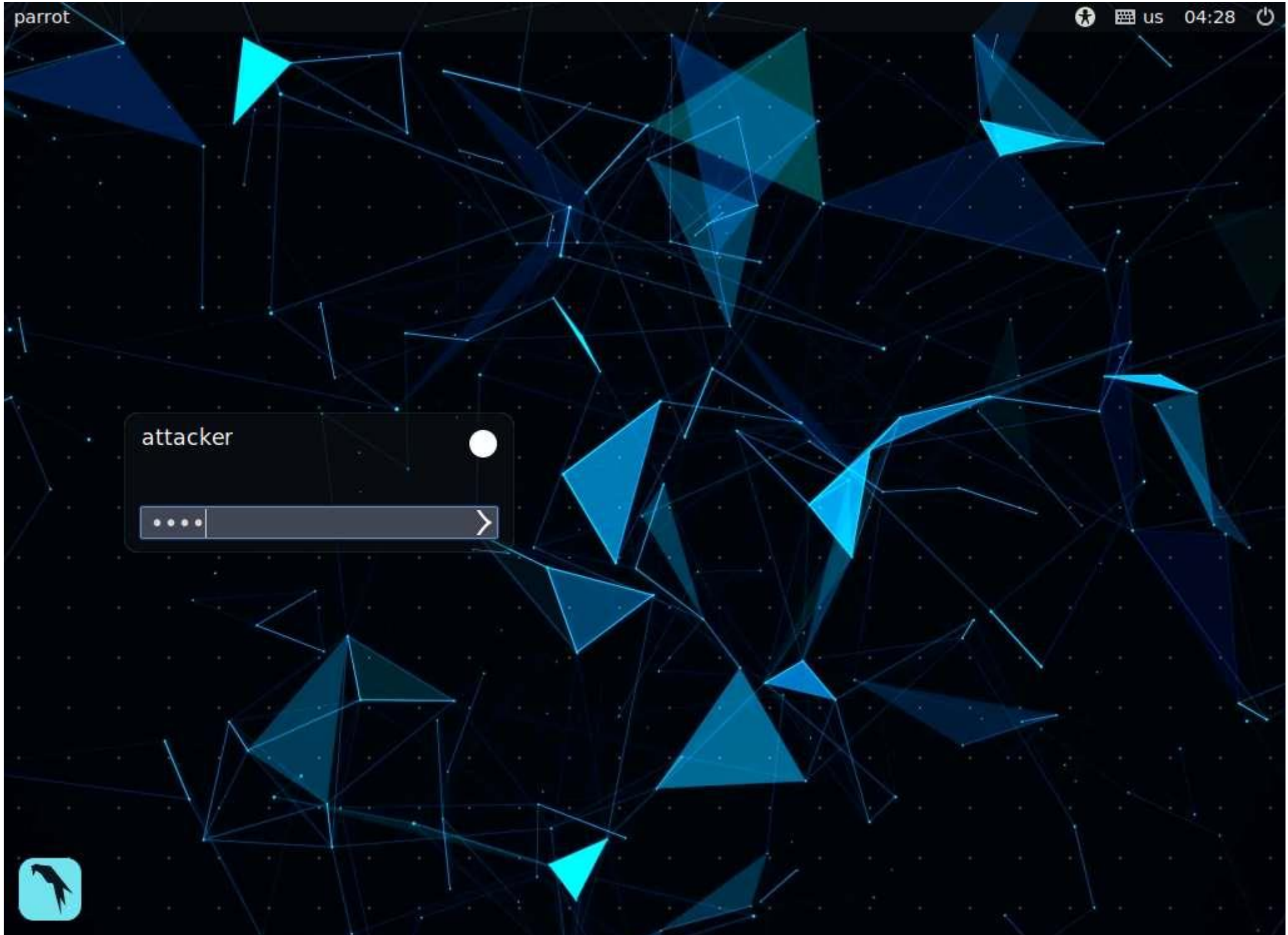
1. Click on Parrot Security to switch to the **Parrot Security** machine.


parrot
us
04:27
attacker
Password

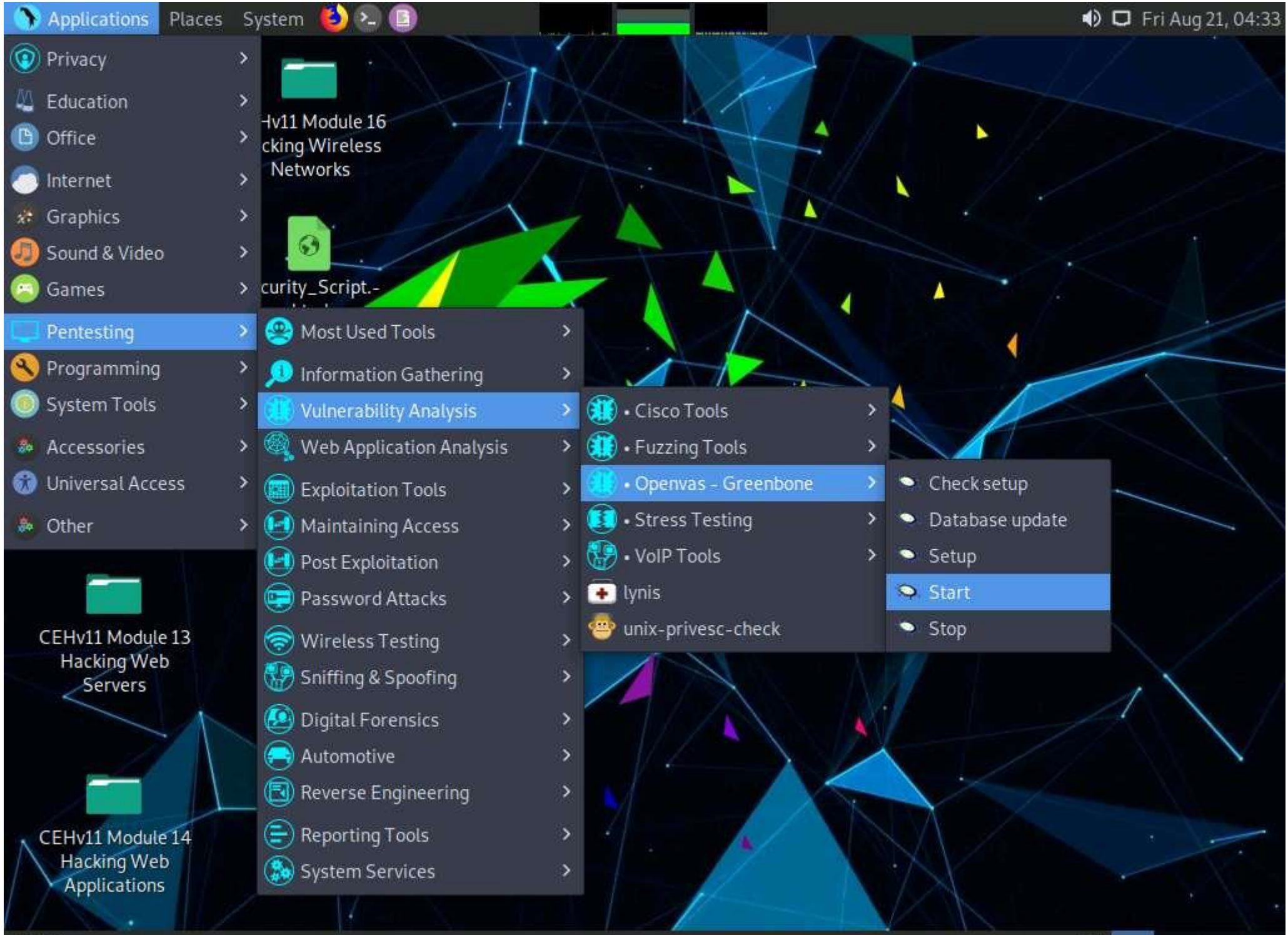
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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.

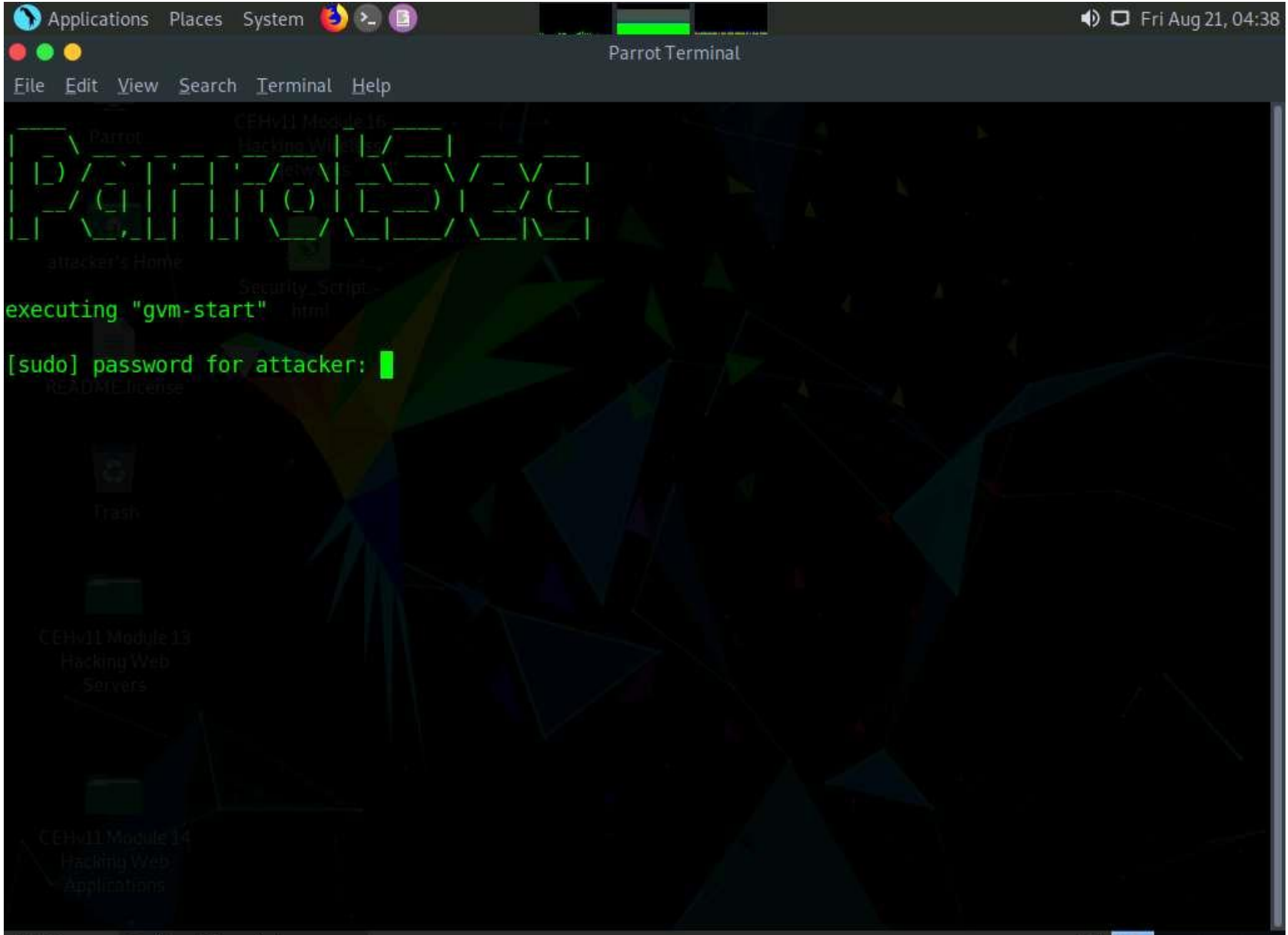

parrot
us
04:28
attacker

3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting** --> **Vulnerability Analysis** --> **Openvas - Greenbone** --> **Start** to launch OpenVAS tool.

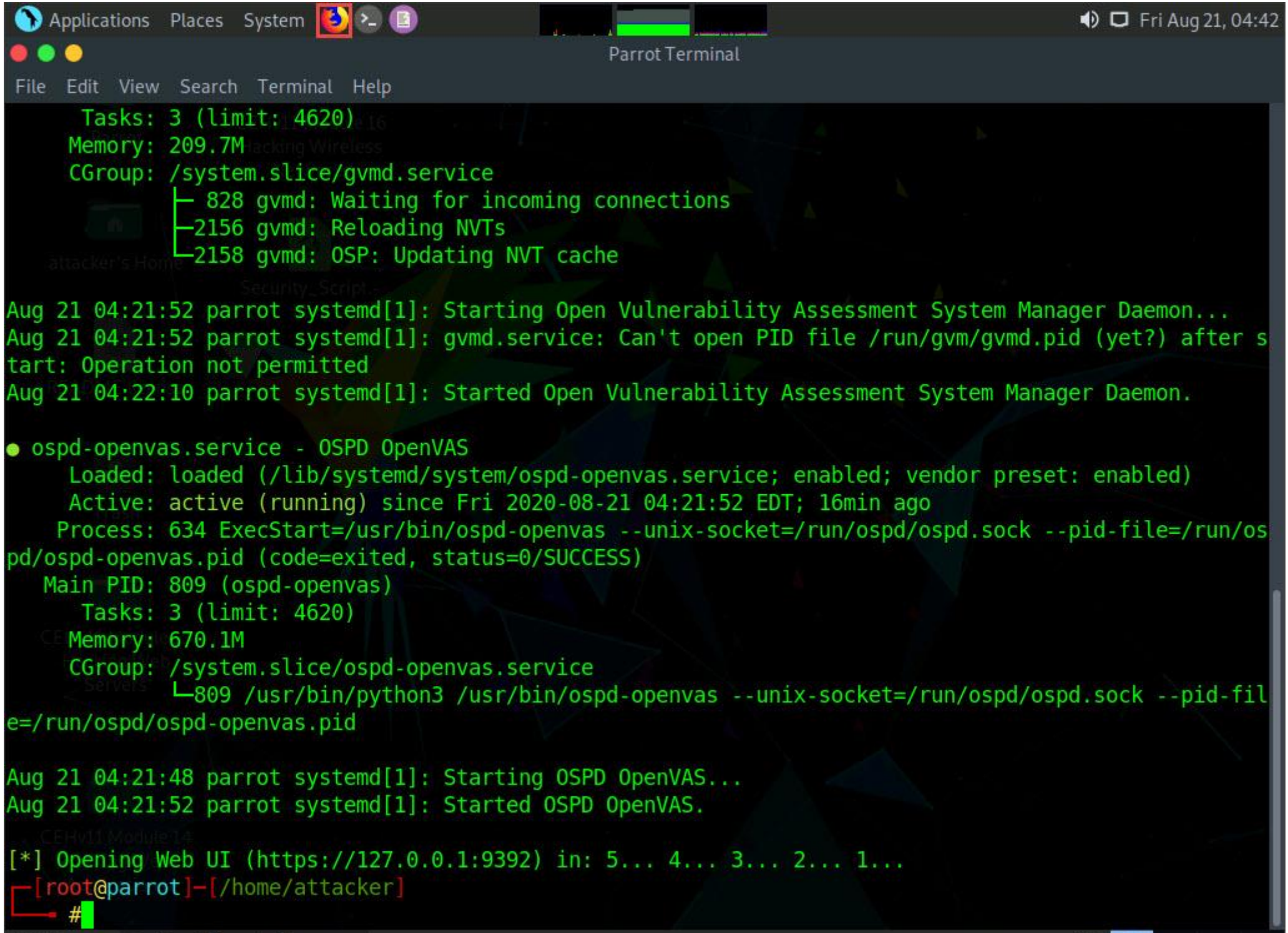

Applications
Places
System
Fri Aug 21, 04:33
Privacy
Education
Office
Internet
Graphics
Sound & Video
Games
Pentesting
Programming
System Tools
Accessories
Universal Access
Other
Most Used Tools
Information Gathering
Vulnerability Analysis
Web Application Analysis
Exploitation Tools
Maintaining Access
Post Exploitation
Password Attacks
Wireless Testing
Sniffing & Spoofing
Digital Forensics
Automotive
Reverse Engineering
Reporting Tools
System Services
• Cisco Tools
• Fuzzing Tools
• Openvas - Greenbone
• Stress Testing
• VoIP Tools
lynis
unix-privesc-check
Check setup
Database update
Setup
Start
Stop
-lv11 Module 16
cking Wireless
Networks
curity_Script.-
CEHv11 Module 13
Hacking Web
Servers
CEHv11 Module 14
Hacking Web
Applications

4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.

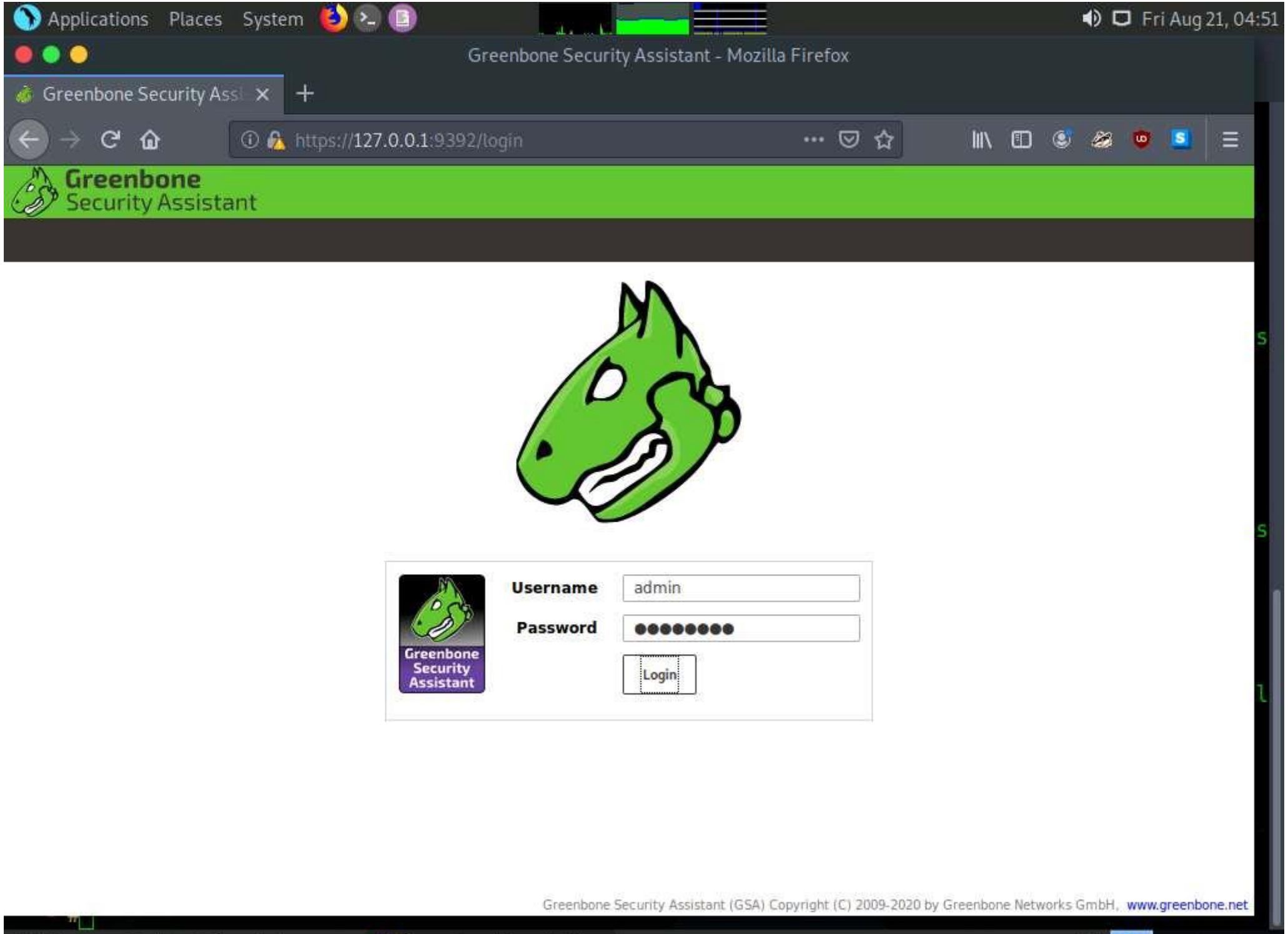
The password that you type will not be visible.


Applications
Places
System
Fri Aug 21, 04:38
Parrot Terminal
File
Edit
View
Search
Terminal
Help
executing "gvm-start"
[sudo] password for attacker:

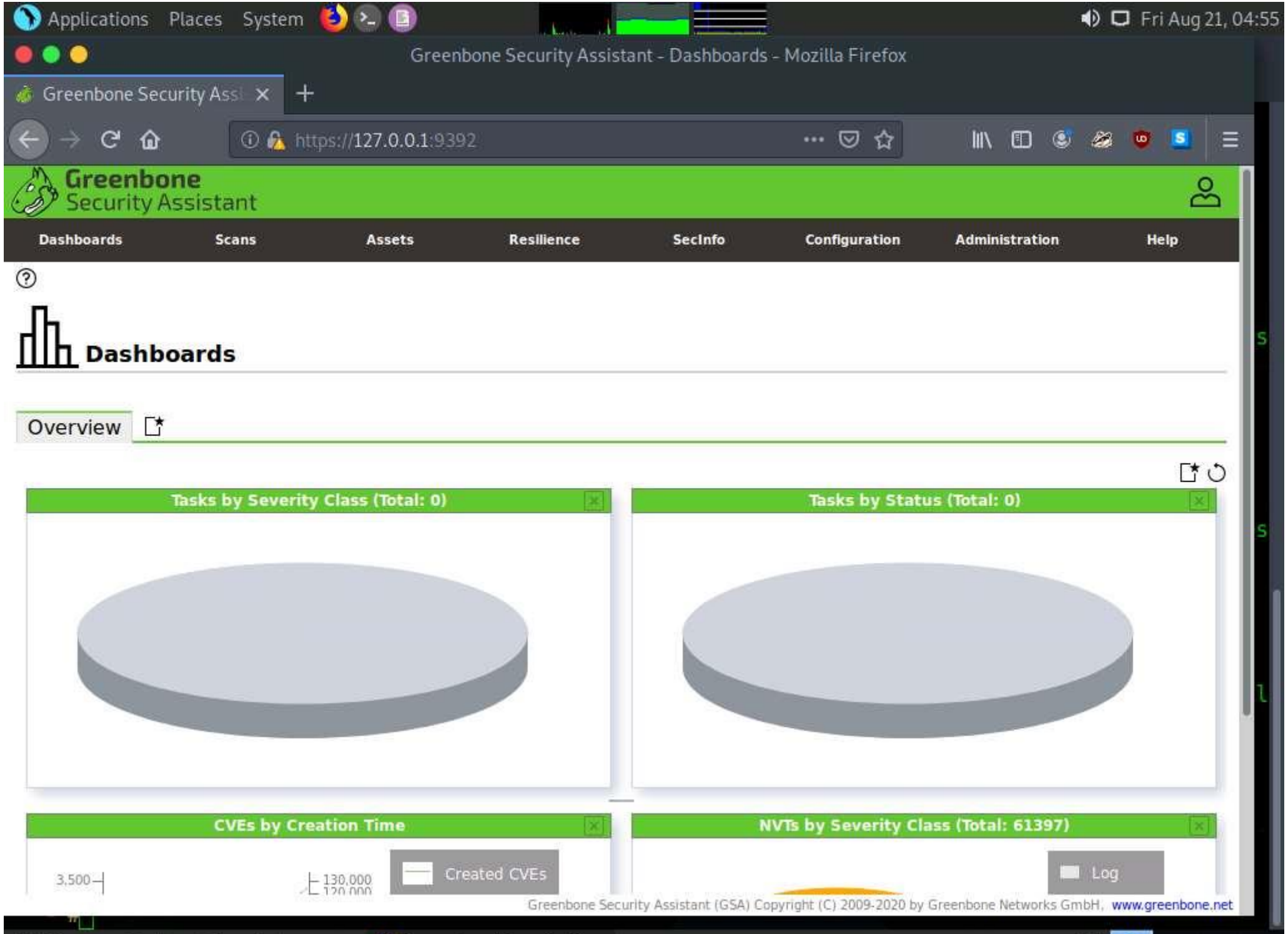
5. ☐ After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.


Applications Places System
Fri Aug 21, 04:42
Parrot Terminal
File Edit View Search Terminal Help
Tasks: 3 (limit: 4620)
Memory: 209.7M
CGroup: /system.slice/gvmd.service
├─ 828 gvmd: Waiting for incoming connections
├─2156 gvmd: Reloading NVTs
└─2158 gvmd: OSP: Updating NVT cache
Aug 21 04:21:52 parrot systemd[1]: Starting Open Vulnerability Assessment System Manager Daemon...
Aug 21 04:21:52 parrot systemd[1]: gvmd.service: Can't open PID file /run/gvm/gvmd.pid (yet?) after s
tart: Operation not permitted
Aug 21 04:22:10 parrot systemd[1]: Started Open Vulnerability Assessment System Manager Daemon.
● ospd-openvas.service - OSPD OpenVAS
Loaded: loaded (/lib/systemd/system/ospd-openvas.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2020-08-21 04:21:52 EDT; 16min ago
Process: 634 ExecStart=/usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-file=/run/os
pd/ospd-openvas.pid (code=exited, status=0/SUCCESS)
Main PID: 809 (ospd-openvas)
Tasks: 3 (limit: 4620)
Memory: 670.1M
CGroup: /system.slice/ospd-openvas.service
└─809 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-fil
e=/run/ospd/ospd-openvas.pid
Aug 21 04:21:48 parrot systemd[1]: Starting OSPD OpenVAS...
Aug 21 04:21:52 parrot systemd[1]: Started OSPD OpenVAS.
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
[root@parrot]-[/home/attacker]
#

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.

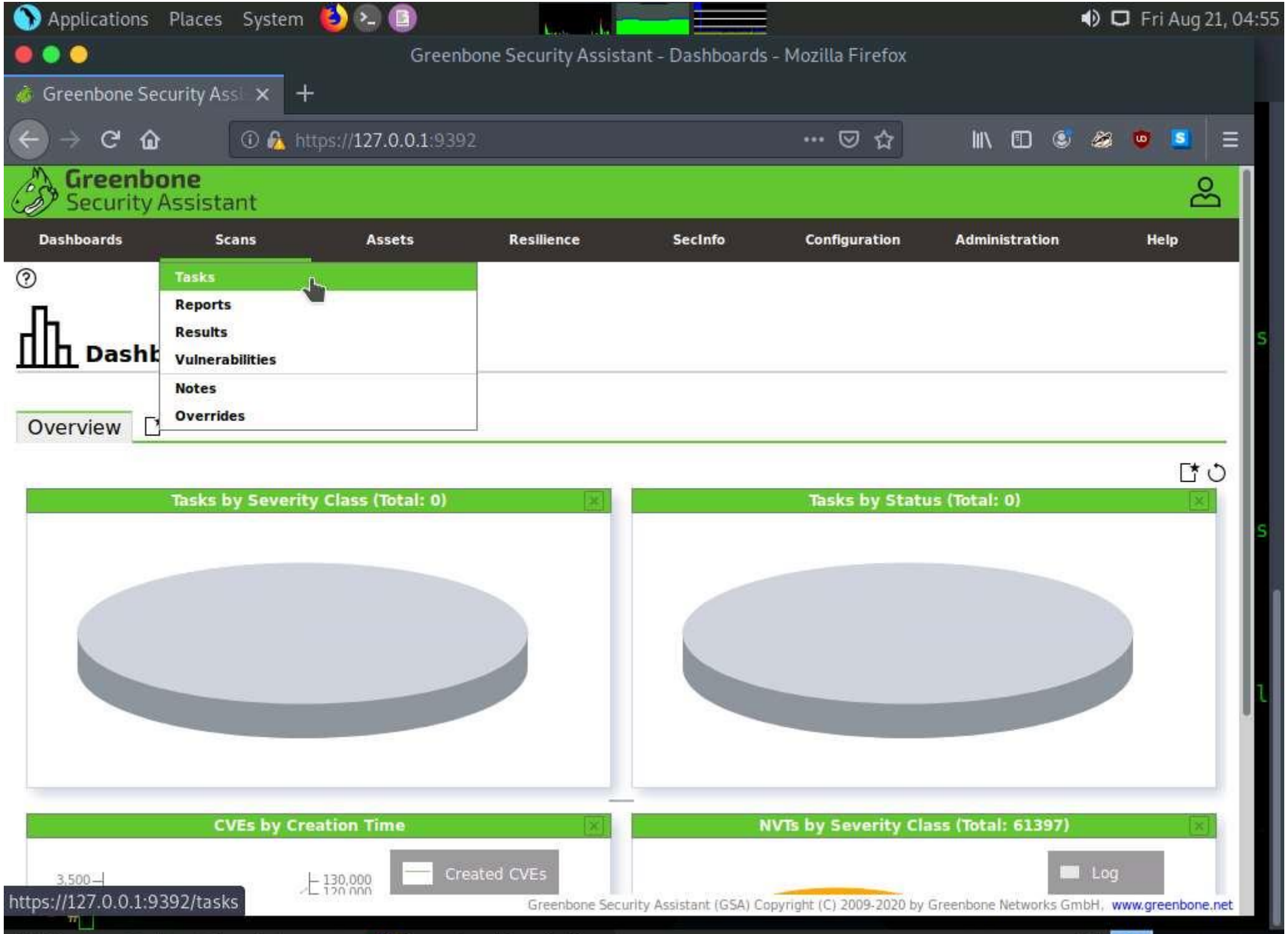

Applications
Places
System
Fri Aug 21, 04:51
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/login
Greenbone
Security Assistant
Username
admin
Password
Login
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

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

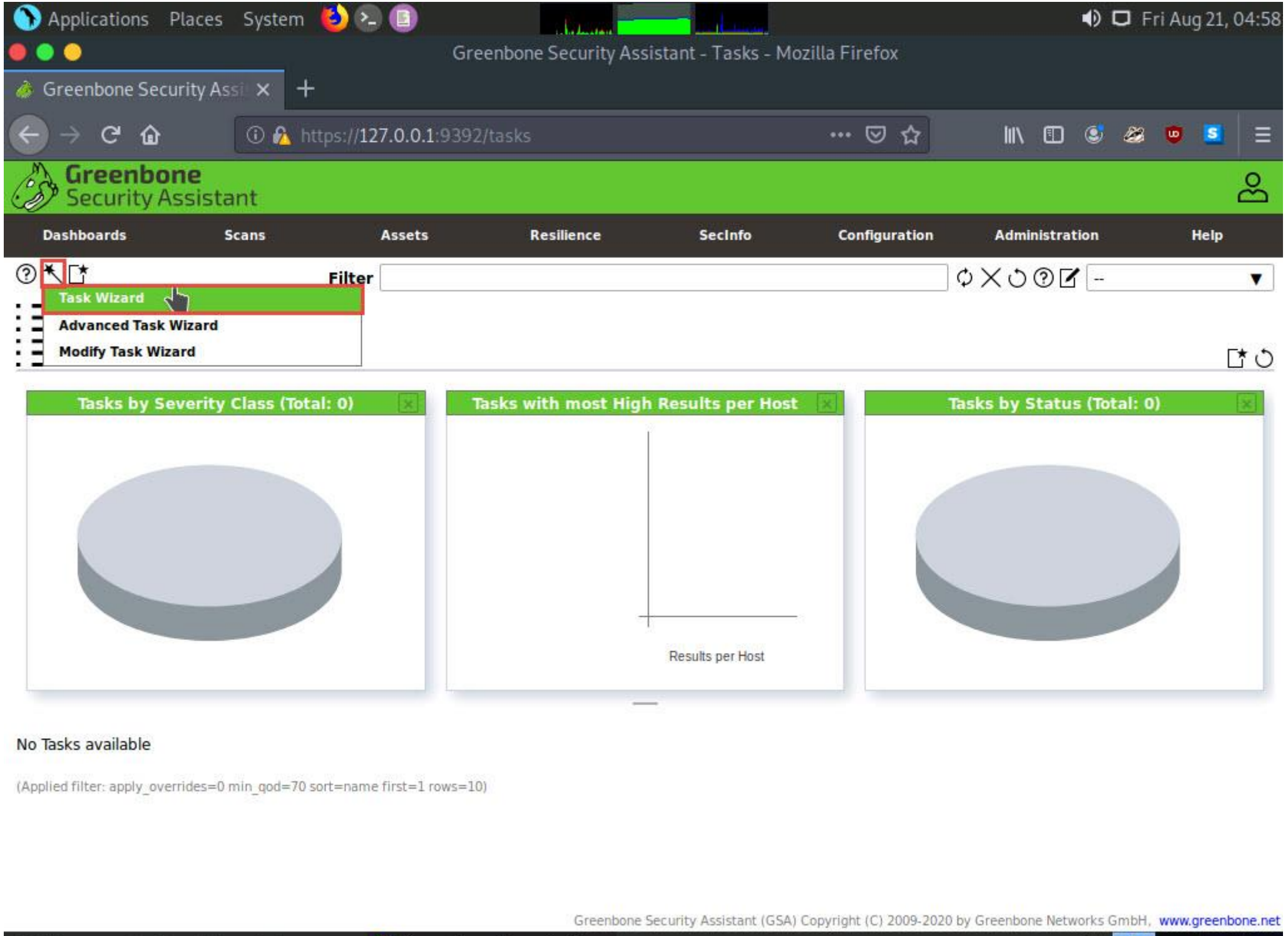

Applications
Places
System
Fri Aug 21, 04:55
Greenbone Security Assistant - Dashboards - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Dashboards
Overview
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
CVEs by Creation Time
3,500
130,000
Created CVEs
NVTs by Severity Class (Total: 61397)
Log
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

9. Navigate to **Scans --> Tasks** from the **Menu** bar.

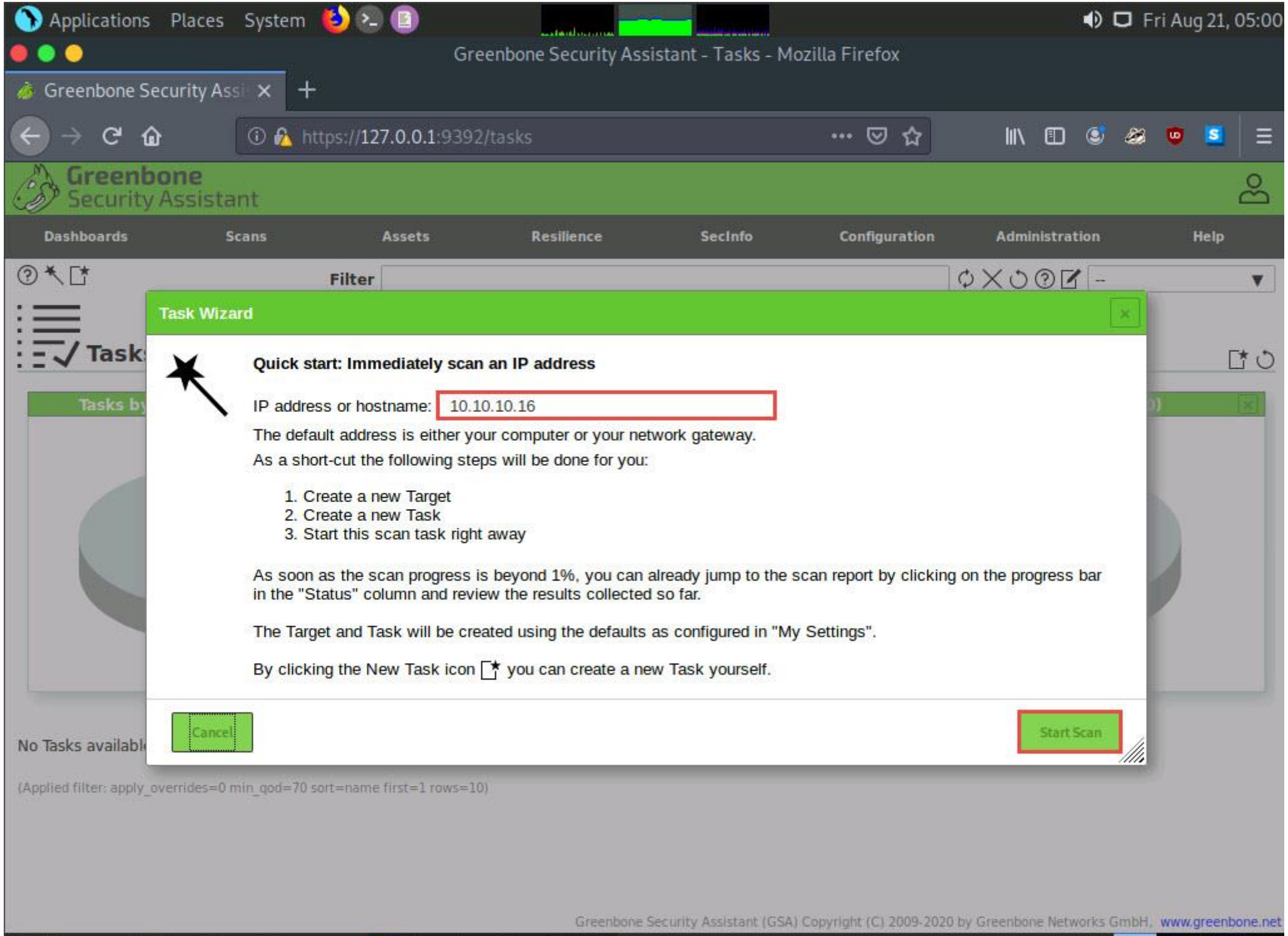
If a **Welcome to the scan management!** pop-up appears, close it.


Applications
Places
System
Fri Aug 21, 04:55
Greenbone Security Assistant - Dashboards - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Dashb
Overview
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
CVEs by Creation Time
3,500
130,000
Created CVEs
NVTs by Severity Class (Total: 61397)
Log
https://127.0.0.1:9392/tasks
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

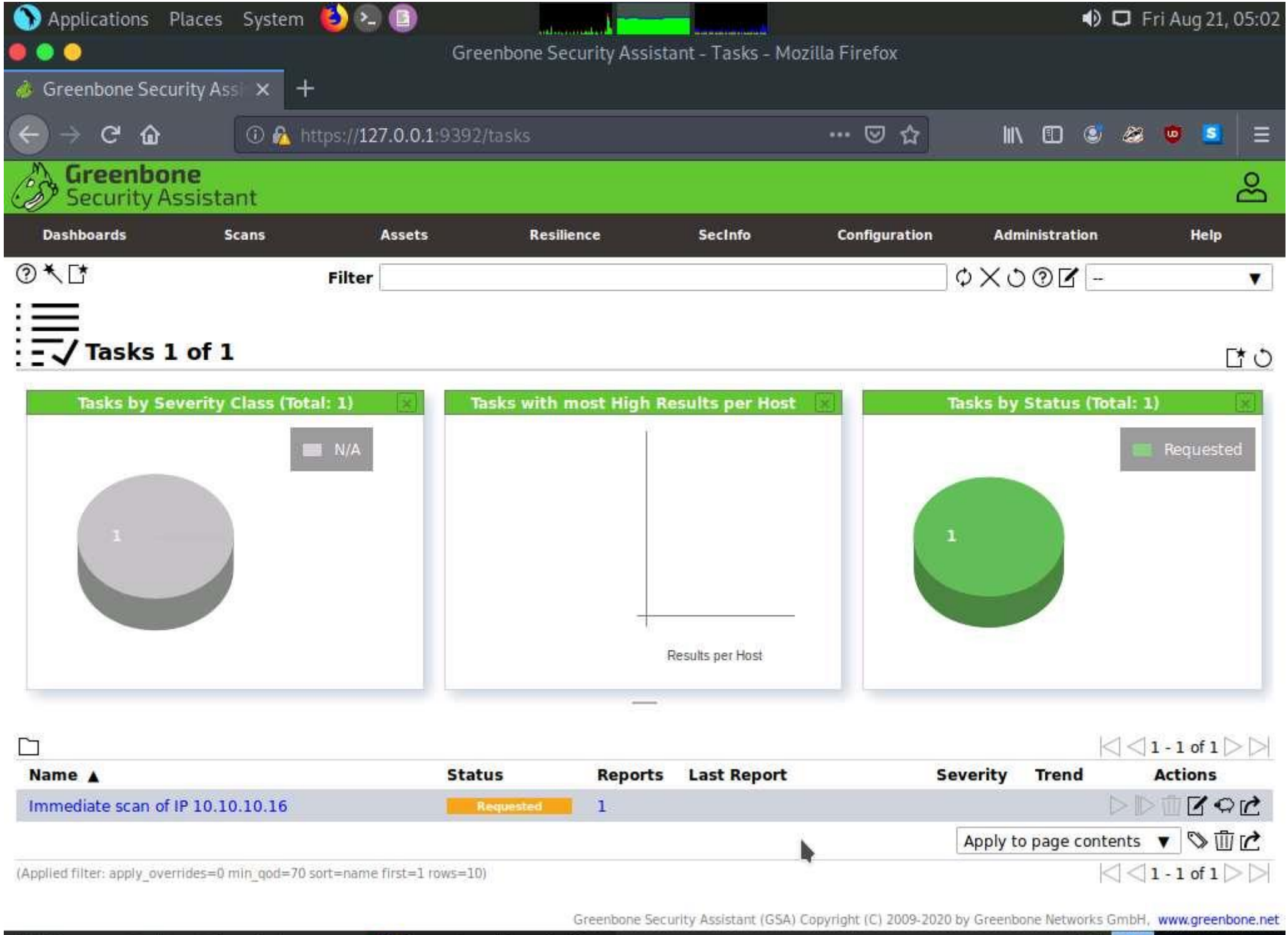
10. ☐ Hover over wand icon and click the **Task Wizard** option.


Applications
Places
System
Fri Aug 21, 04:58
Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/tasks
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Task Wizard
Advanced Task Wizard
Modify Task Wizard
Tasks by Severity Class (Total: 0)
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 0)
No Tasks available
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

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.

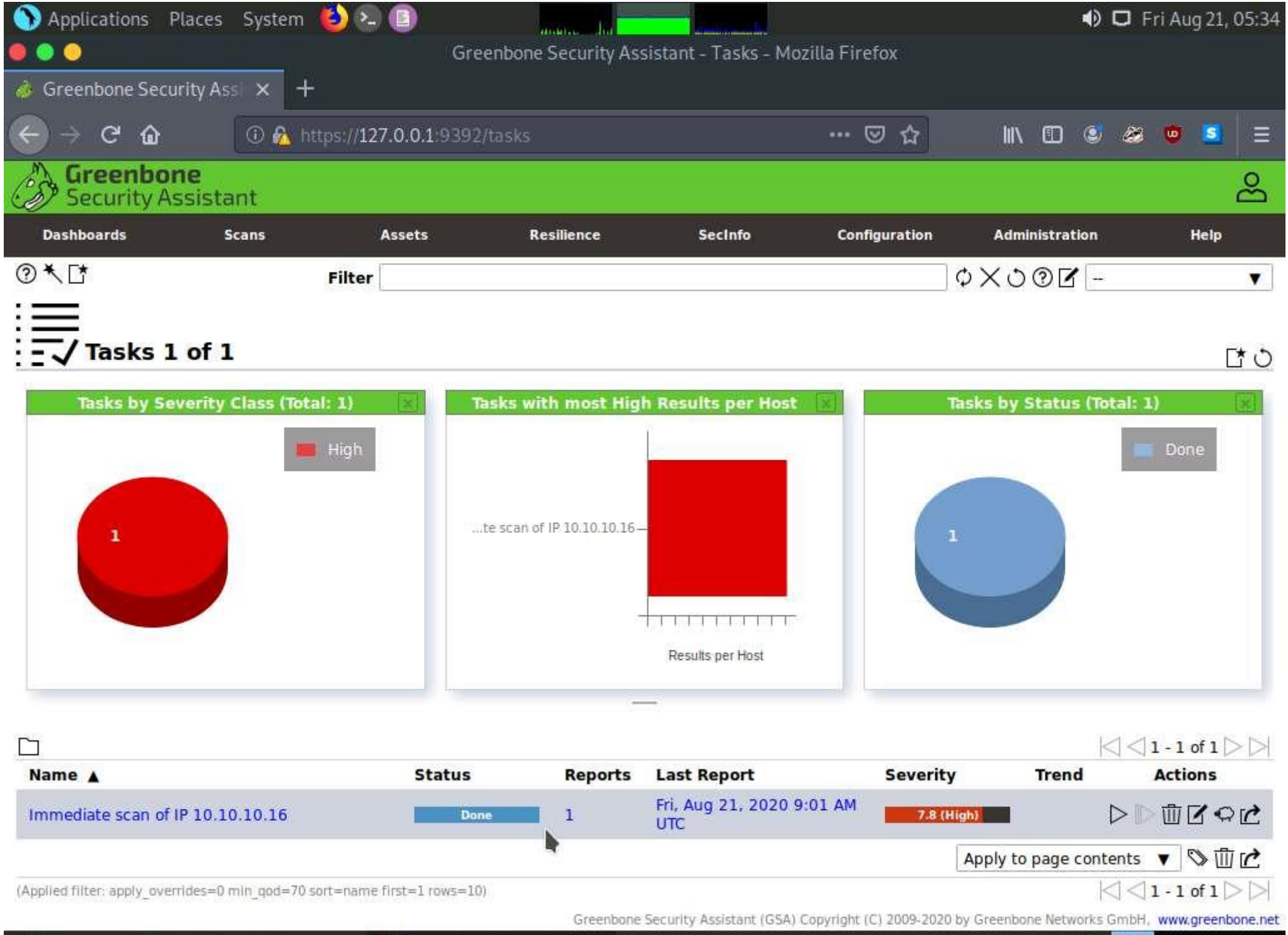

Applications Places System
Fri Aug 21, 05:00
Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Task Wizard
Quick start: Immediately scan an IP address
IP address or hostname: 10.10.10.16
The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.
The Target and Task will be created using the defaults as configured in "My Settings".
By clicking the New Task icon you can create a new Task yourself.
Cancel
Start Scan
No Tasks available
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

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

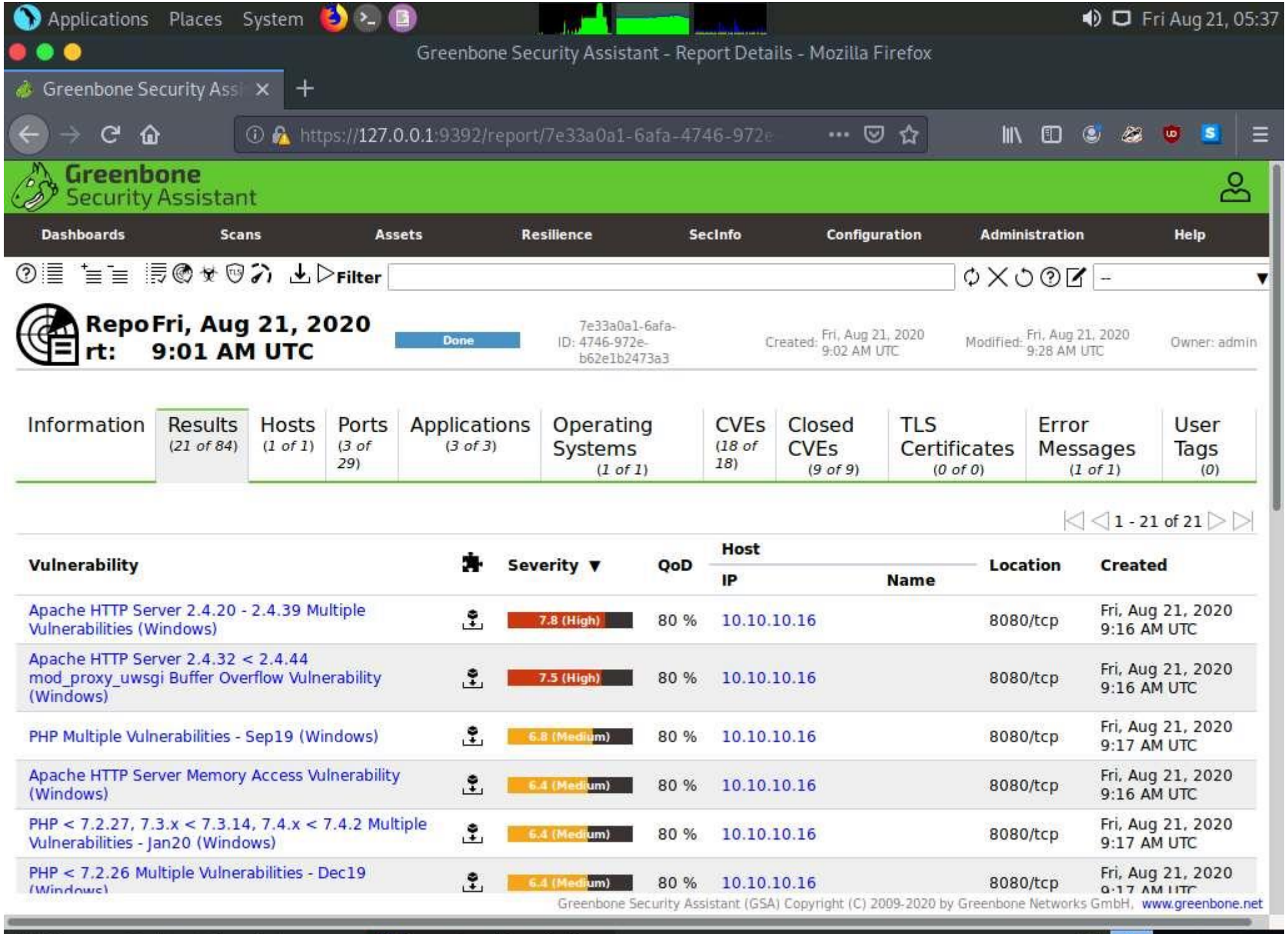

Applications Places System
Fri Aug 21, 05:02
Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
Requested
1
1 - 1 of 1
Name
Status
Reports
Last Report
Severity
Trend
Actions
Immediate scan of IP 10.10.10.16
Requested
1
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
1 - 1 of 1
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

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.

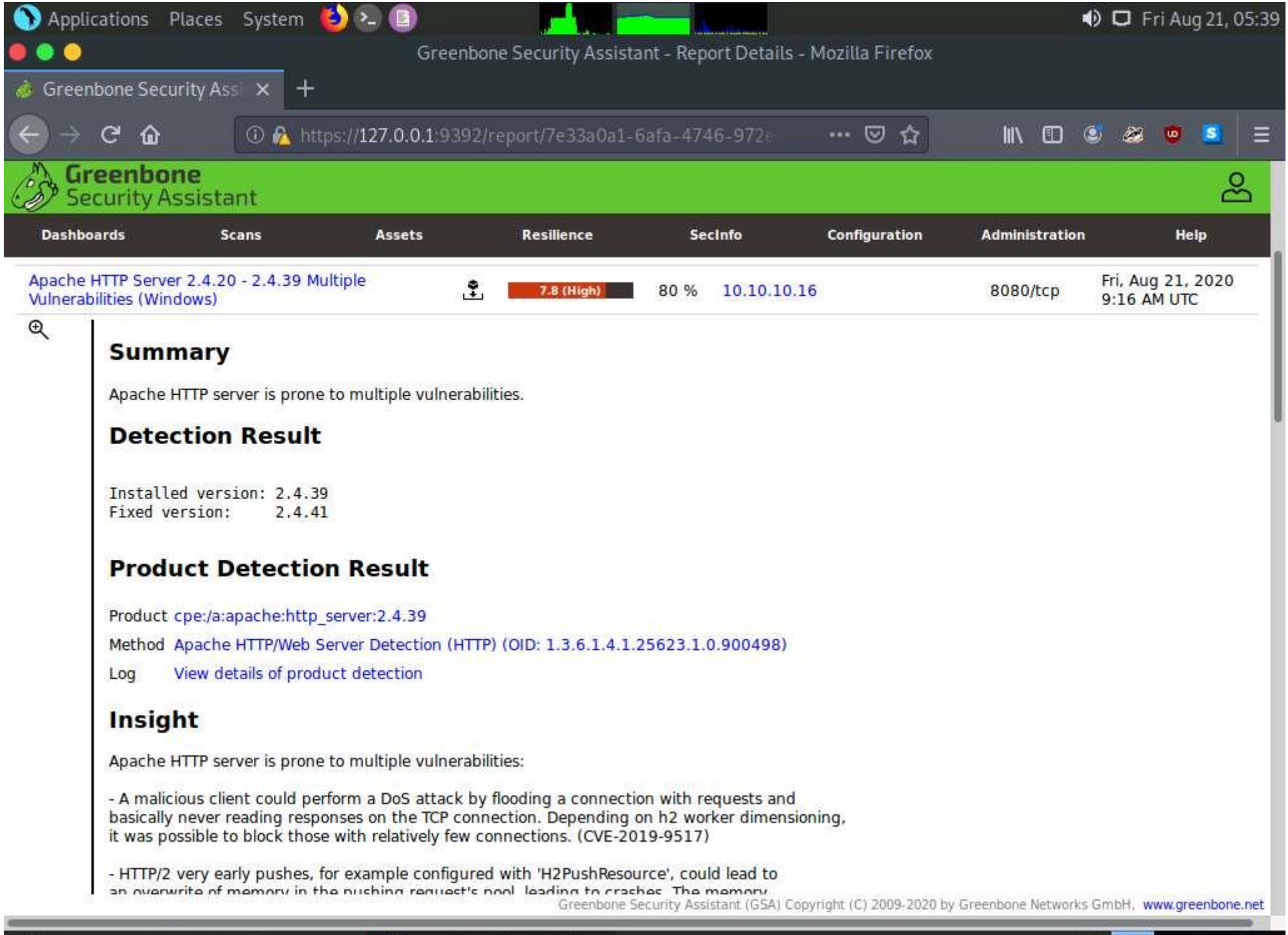
If you are logged out of the session then login again using credentials **admin**/**password**.


Applications Places System
Fri Aug 21, 05:34
Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
High
1
Tasks with most High Results per Host
...te scan of IP 10.10.10.16
Results per Host
Tasks by Status (Total: 1)
Done
1
1 - 1 of 1
Name ▲ Status Reports Last Report Severity Trend Actions
Immediate scan of IP 10.10.10.16 Done 1 Fri, Aug 21, 2020 9:01 AM UTC 7.8 (High)
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
1 - 1 of 1
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

14. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.


Applications Places System
Fri Aug 21, 05:37
Greenbone Security Assistant - Report Details - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/report/7e33a0a1-6afa-4746-972e
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report: Fri, Aug 21, 2020 9:01 AM UTC
Done
ID: 7e33a0a1-6afa-4746-972e-b62e1b2473a3
Created: Fri, Aug 21, 2020 9:02 AM UTC
Modified: Fri, Aug 21, 2020 9:28 AM UTC
Owner: admin
Information
Results (21 of 84)
Hosts (1 of 1)
Ports (3 of 29)
Applications (3 of 3)
Operating Systems (1 of 1)
CVEs (18 of 18)
Closed CVEs (9 of 9)
TLS Certificates (0 of 0)
Error Messages (1 of 1)
User Tags (0)
1 - 21 of 21
Vulnerability
Severity
QoD
Host
IP
Name
Location
Created
Apache HTTP Server 2.4.20 - 2.4.39 Multiple Vulnerabilities (Windows)
7.8 (High)
80 %
10.10.10.16
8080/tcp
Fri, Aug 21, 2020 9:16 AM UTC
Apache HTTP Server 2.4.32 < 2.4.44 mod_proxy_uwsgi Buffer Overflow Vulnerability (Windows)
7.5 (High)
80 %
10.10.10.16
8080/tcp
Fri, Aug 21, 2020 9:16 AM UTC
PHP Multiple Vulnerabilities - Sep19 (Windows)
6.8 (Medium)
80 %
10.10.10.16
8080/tcp
Fri, Aug 21, 2020 9:17 AM UTC
Apache HTTP Server Memory Access Vulnerability (Windows)
6.4 (Medium)
80 %
10.10.10.16
8080/tcp
Fri, Aug 21, 2020 9:16 AM UTC
PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)
6.4 (Medium)
80 %
10.10.10.16
8080/tcp
Fri, Aug 21, 2020 9:17 AM UTC
PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Windows)
6.4 (Medium)
80 %
10.10.10.16
8080/tcp
Fri, Aug 21, 2020
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

15. Click on any vulnerability under the **Vulnerability** column (here, **Apache HTTP Server 2.4.20 - 2.4.39 Multiple Vulnerabilities (Windows)** to view its detailed information.
16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.

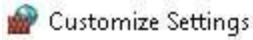

Applications Places System
Fri Aug 21, 05:39
Greenbone Security Assistant - Report Details - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/report/7e33a0a1-6afa-4746-972e
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Apache HTTP Server 2.4.20 - 2.4.39 Multiple Vulnerabilities (Windows)
7.8 (High)
80 %
10.10.10.16
8080/tcp
Fri, Aug 21, 2020 9:16 AM UTC
Summary
Apache HTTP server is prone to multiple vulnerabilities.
Detection Result
Installed version: 2.4.39
Fixed version: 2.4.41
Product Detection Result
Product cpe:/a:apache:http_server:2.4.39
Method Apache HTTP/Web Server Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900498)
Log View details of product detection
Insight
Apache HTTP server is prone to multiple vulnerabilities:
- A malicious client could perform a DoS attack by flooding a connection with requests and basically never reading responses on the TCP connection. Depending on h2 worker dimensioning, it was possible to block those with relatively few connections. (CVE-2019-9517)
- HTTP/2 very early pushes, for example configured with 'H2PushResource', could lead to
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

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** machine.
19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.
20. Click on Windows Server 2016 to switch to the **Windows Server 2016** machine and click Ctrl+Alt+Delete to activate it, by default, **Administrator** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.


CEH\Administrator

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

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



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

- (•) Turn on Windows Firewall
  - [ ] Block all incoming connections, including those in the list of allowed apps
  - [ ] Notify me when Windows Firewall blocks a new app
- ( ) Turn off Windows Firewall (not recommended)

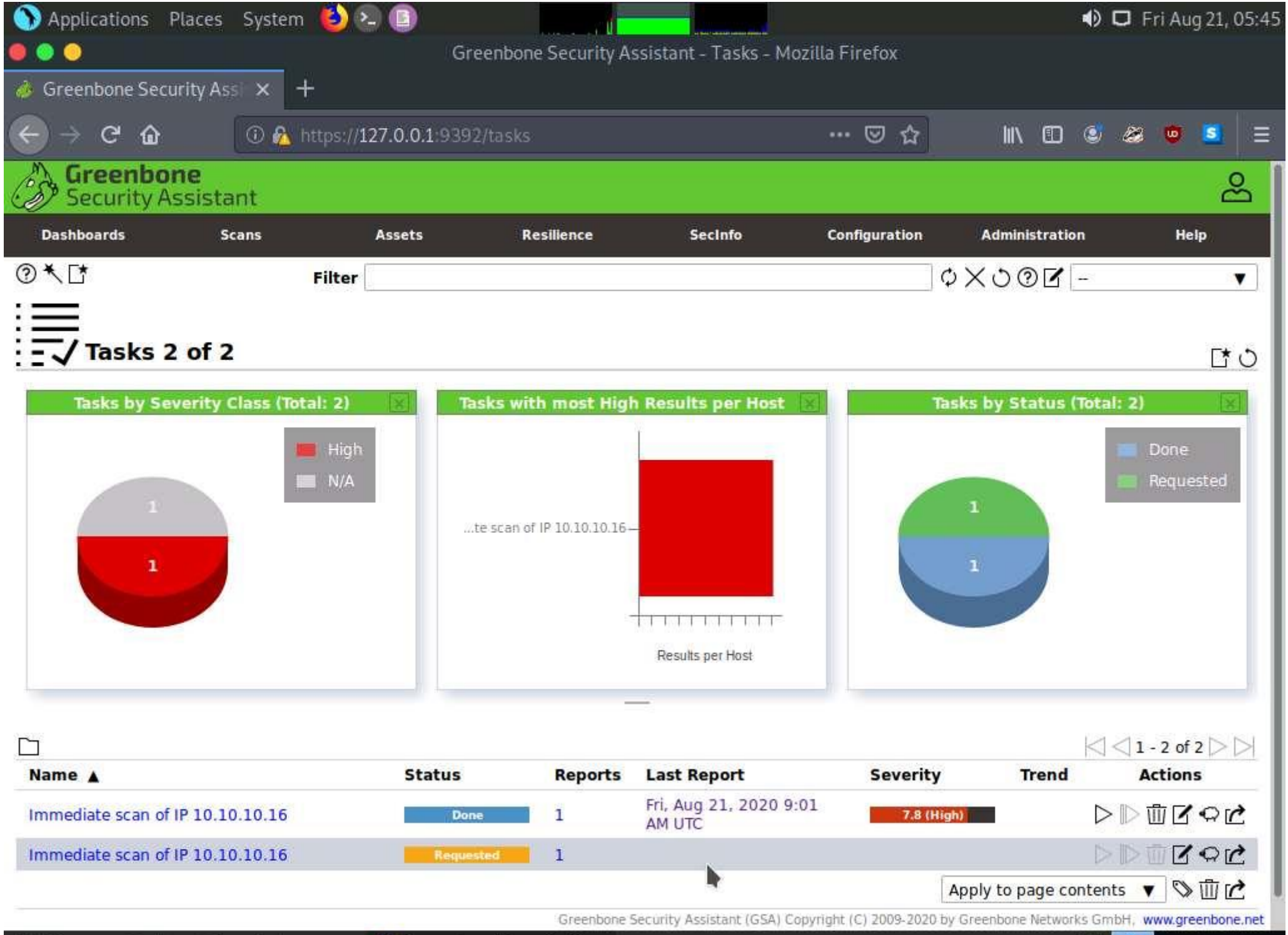
Private network settings

- (•) Turn on Windows Firewall
  - [ ] Block all incoming connections, including those in the list of allowed apps
  - [ ] Notify me when Windows Firewall blocks a new app
- ( ) Turn off Windows Firewall (not recommended)

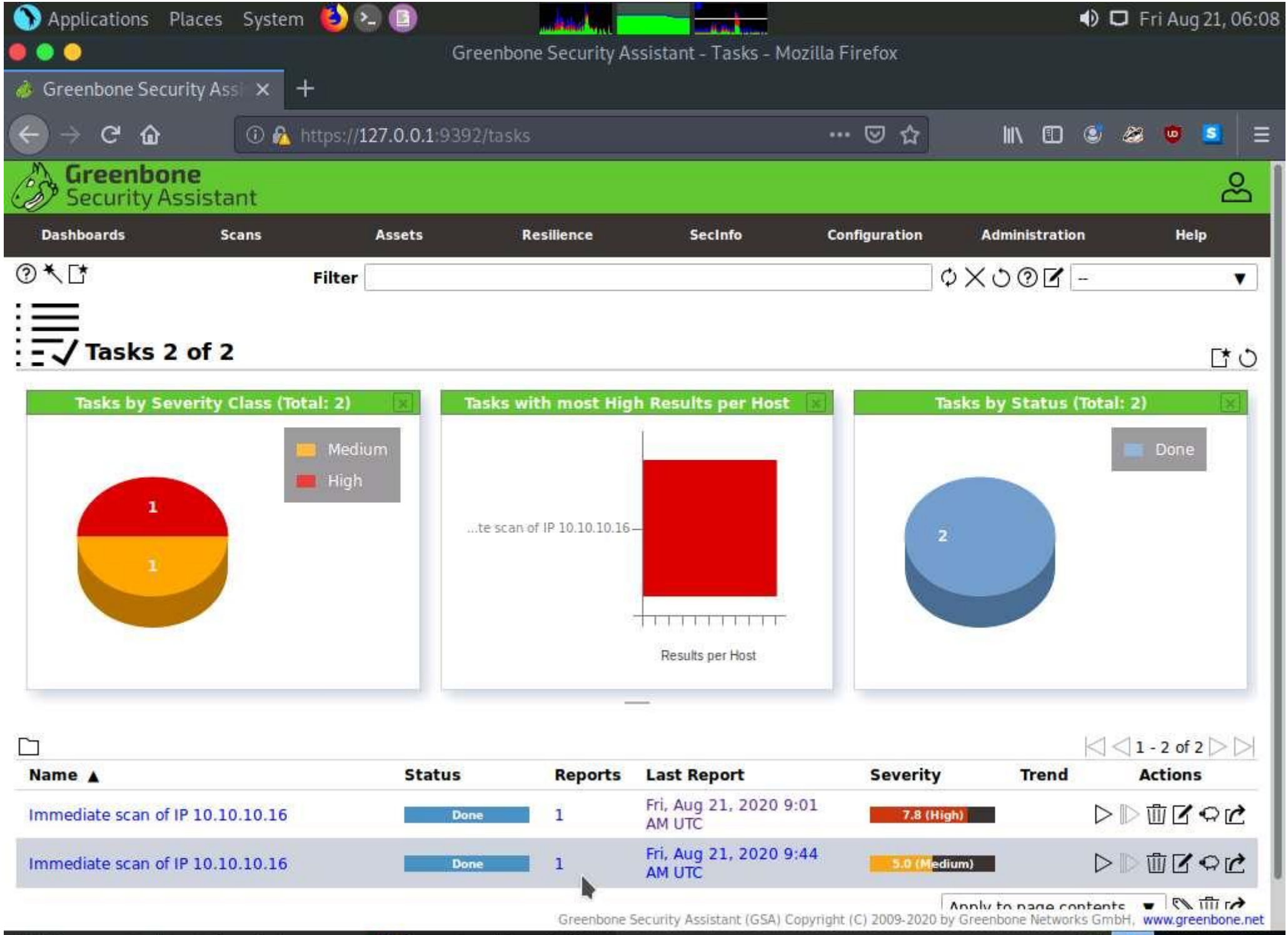
Public network settings

- (•) Turn on Windows Firewall
  - [ ] Block all incoming connections, including those in the list of allowed apps
  - [ ] Notify me when Windows Firewall blocks a new app
- ( ) Turn off Windows Firewall (not recommended)

22. ☐ click on Parrot Security to switch to **Parrot Security** machine and 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.

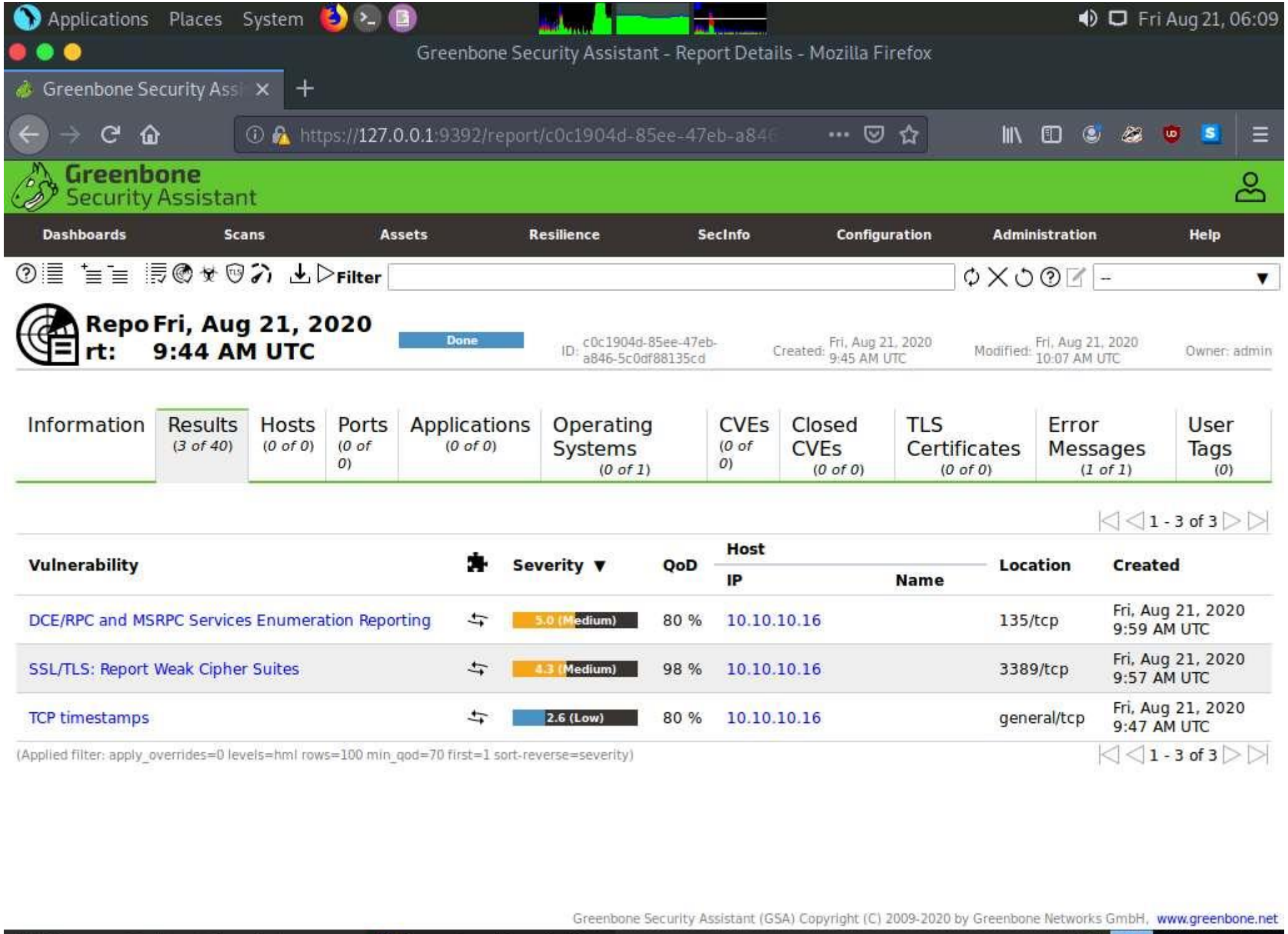

Applications Places System
Fri Aug 21, 05:45
Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Tasks 2 of 2
Tasks by Severity Class (Total: 2)
High
N/A
1
1
Tasks with most High Results per Host
...te scan of IP 10.10.10.16
Results per Host
Tasks by Status (Total: 2)
Done
Requested
1
1
1 - 2 of 2
Name ▲ Status Reports Last Report Severity Trend Actions
Immediate scan of IP 10.10.10.16 Done 1 Fri, Aug 21, 2020 9:01 AM UTC 7.8 (High)
Immediate scan of IP 10.10.10.16 Requested 1
Apply to page contents
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

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


Applications Places System
Fri Aug 21, 06:08
Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Tasks 2 of 2
Tasks by Severity Class (Total: 2)
Medium
High
1
1
Tasks with most High Results per Host
...te scan of IP 10.10.10.16
Results per Host
Tasks by Status (Total: 2)
Done
2
1 - 2 of 2
Name ▲ Status Reports Last Report Severity Trend Actions
Immediate scan of IP 10.10.10.16 Done 1 Fri, Aug 21, 2020 9:01 AM UTC 7.8 (High)
Immediate scan of IP 10.10.10.16 Done 1 Fri, Aug 21, 2020 9:44 AM UTC 5.0 (Medium)
Apply to page contents
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

25. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

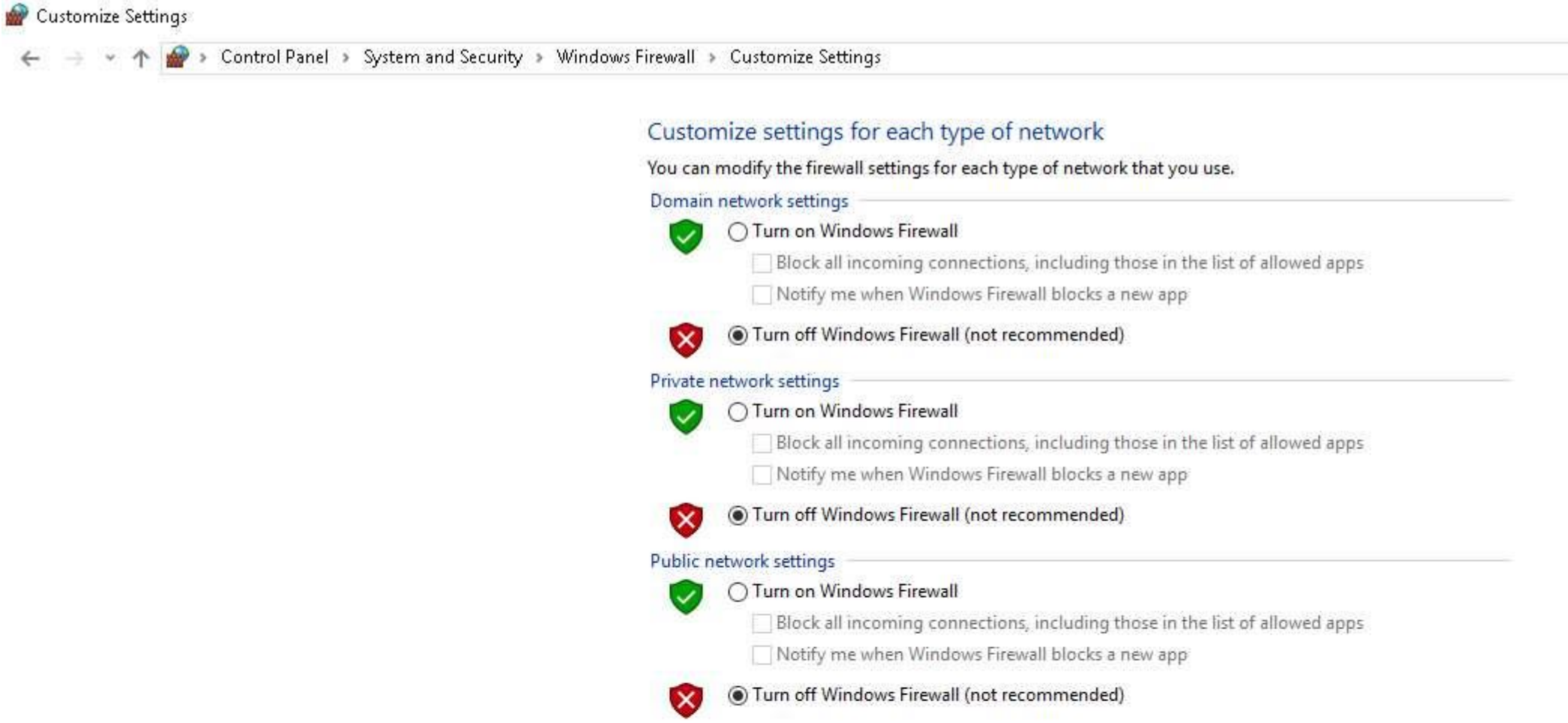
The results might vary in your lab environment.


Applications Places System
Fri Aug 21, 06:09
Greenbone Security Assistant - Report Details - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/report/c0c1904d-85ee-47eb-a84
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report: Fri, Aug 21, 2020 9:44 AM UTC
Done
ID: c0c1904d-85ee-47eb-a846-5c0df88135cd
Created: Fri, Aug 21, 2020 9:45 AM UTC
Modified: Fri, Aug 21, 2020 10:07 AM UTC
Owner: admin
Information
Results (3 of 40)
Hosts (0 of 0)
Ports (0 of 0)
Applications (0 of 0)
Operating Systems (0 of 1)
CVEs (0 of 0)
Closed CVEs (0 of 0)
TLS Certificates (0 of 0)
Error Messages (1 of 1)
User Tags (0)
1 - 3 of 3
Vulnerability
Severity
QoD
Host
IP
Name
Location
Created
DCE/RPC and MSRPC Services Enumeration Reporting
5.0 (Medium)
80 %
10.10.10.16
135/tcp
Fri, Aug 21, 2020 9:59 AM UTC
SSL/TLS: Report Weak Cipher Suites
4.3 (Medium)
98 %
10.10.10.16
3389/tcp
Fri, Aug 21, 2020 9:57 AM UTC
TCP timestamps
2.6 (Low)
80 %
10.10.10.16
general/tcp
Fri, Aug 21, 2020 9:47 AM UTC
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 3 of 3
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

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. Click on Windows Server 2016 to switch to the **Windows Server 2016** machine and click Ctrl+Alt+Delete to activate it, by default, **Administrator** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.


CEH\Administrator

30. ☐ Navigate to **Control Panel** --> **System and Security** --> **Windows Firewall** --> **Turn Windows Firewall on or off**, disable Windows Firewall, and click **OK**.


Customize Settings
Control Panel › System and Security › Windows Firewall › Customize Settings
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Domain network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
Private network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
Public network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)

Task 2: Perform Vulnerability Scanning using Nessus

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

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

1. Click on Windows 10 to switch to **Windows 10** machine.
2. Launch any browser, (here, **Microsoft Edge**). In the address bar of the browser place your mouse cursor and click https://localhost:8834/ and press **Enter**
3. **This site is not secure** page appears, expand the **Details** section and click **Go on to the webpage**

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

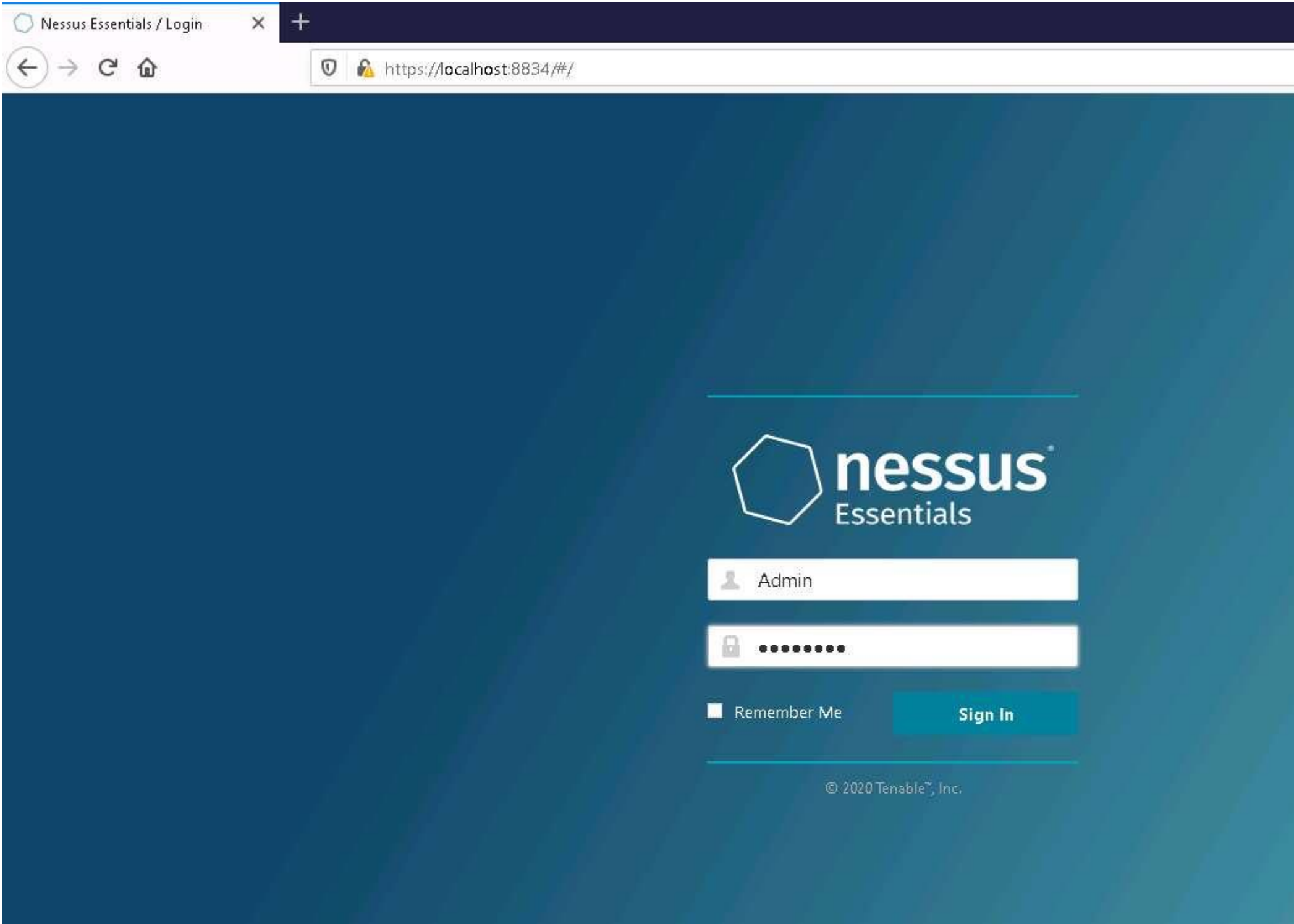
Details

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

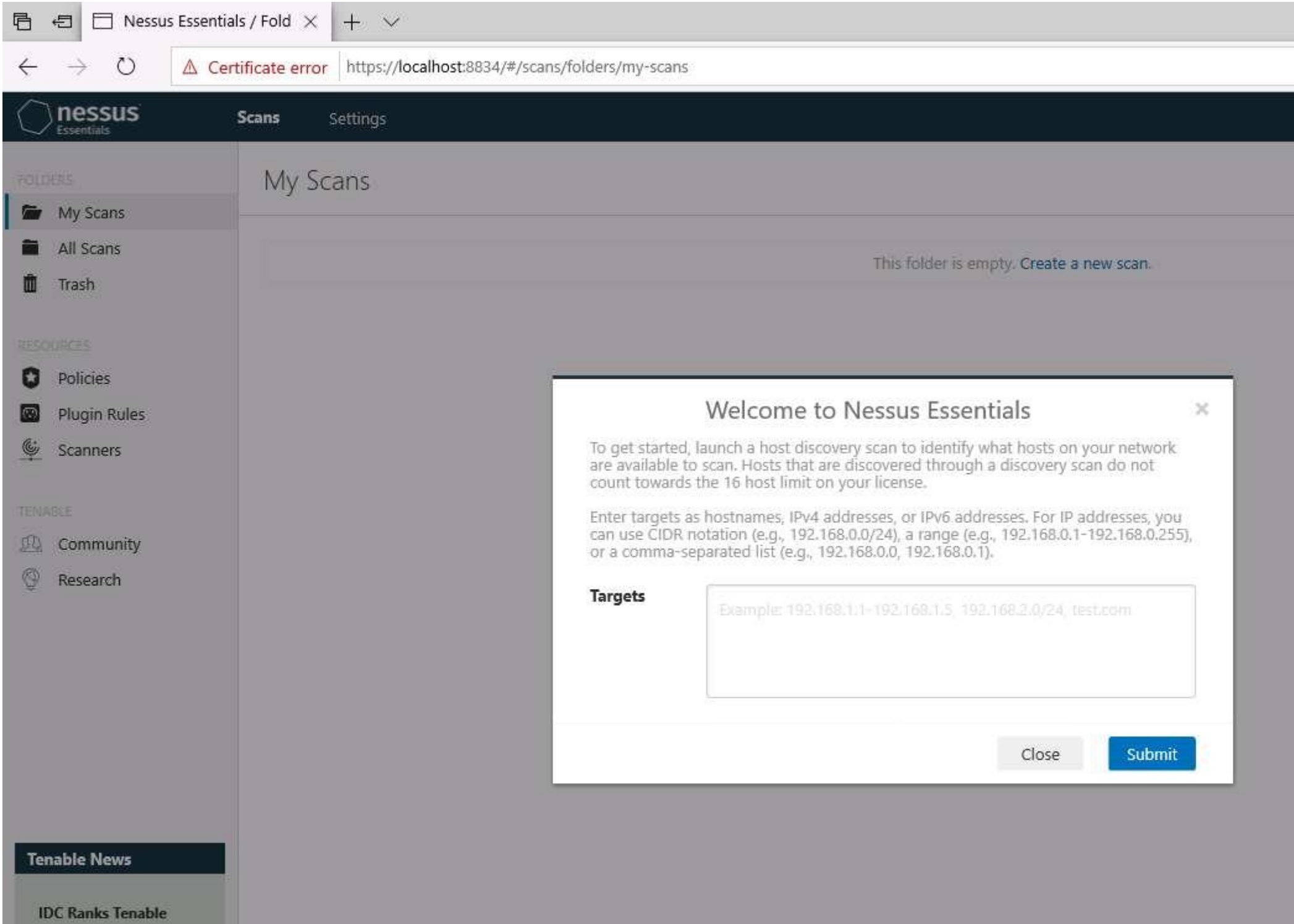
Go on to the webpage (Not recommended)

4. ☐ In the Nessus login page use **Admin** as the username and **password** as Password and click **Sign In**

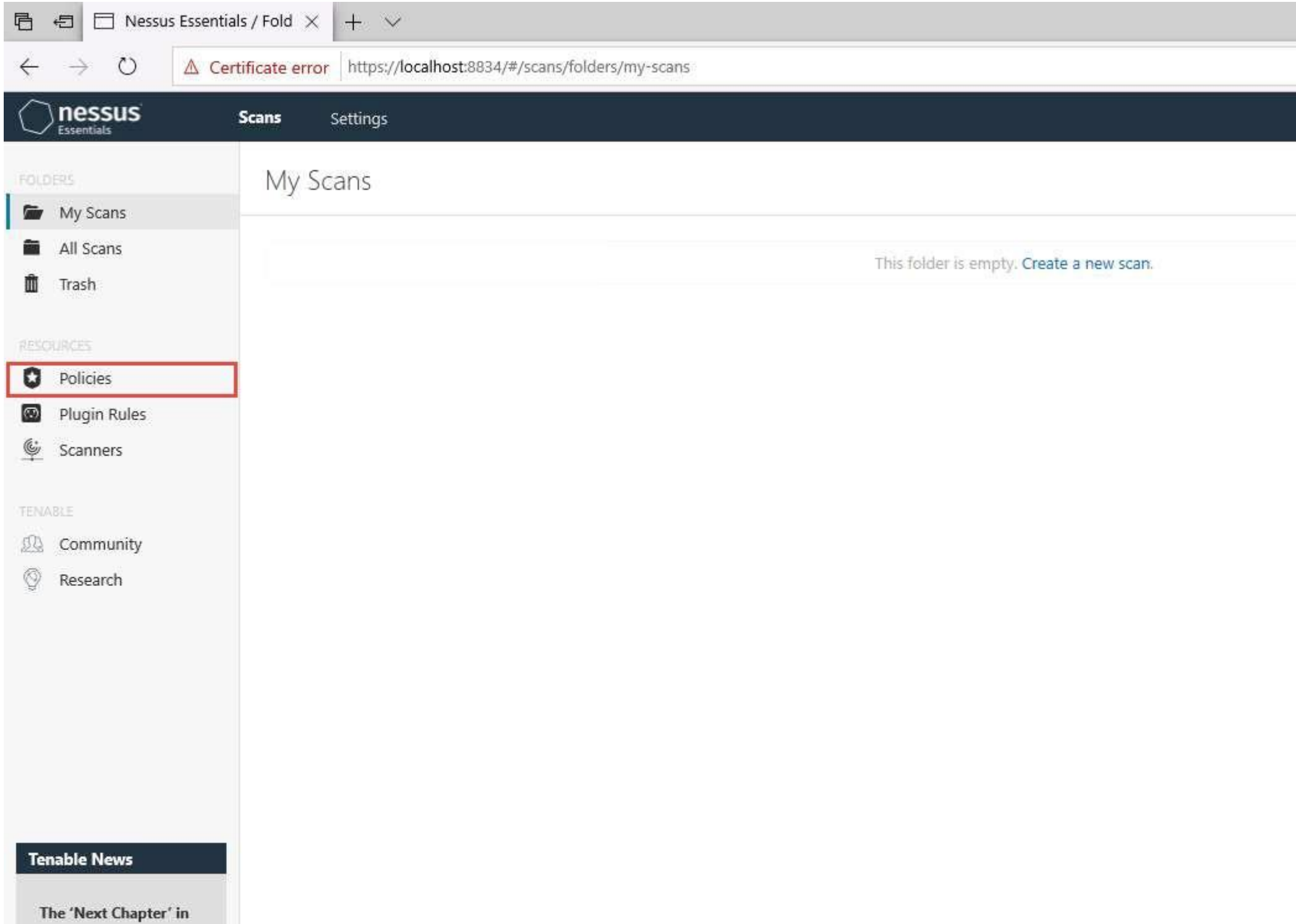

Nessus Essentials / Login
https://localhost:8834/#/
nessus
Essentials
Admin
Remember Me
Sign In
© 2020 Tenable™, Inc.

5. 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.

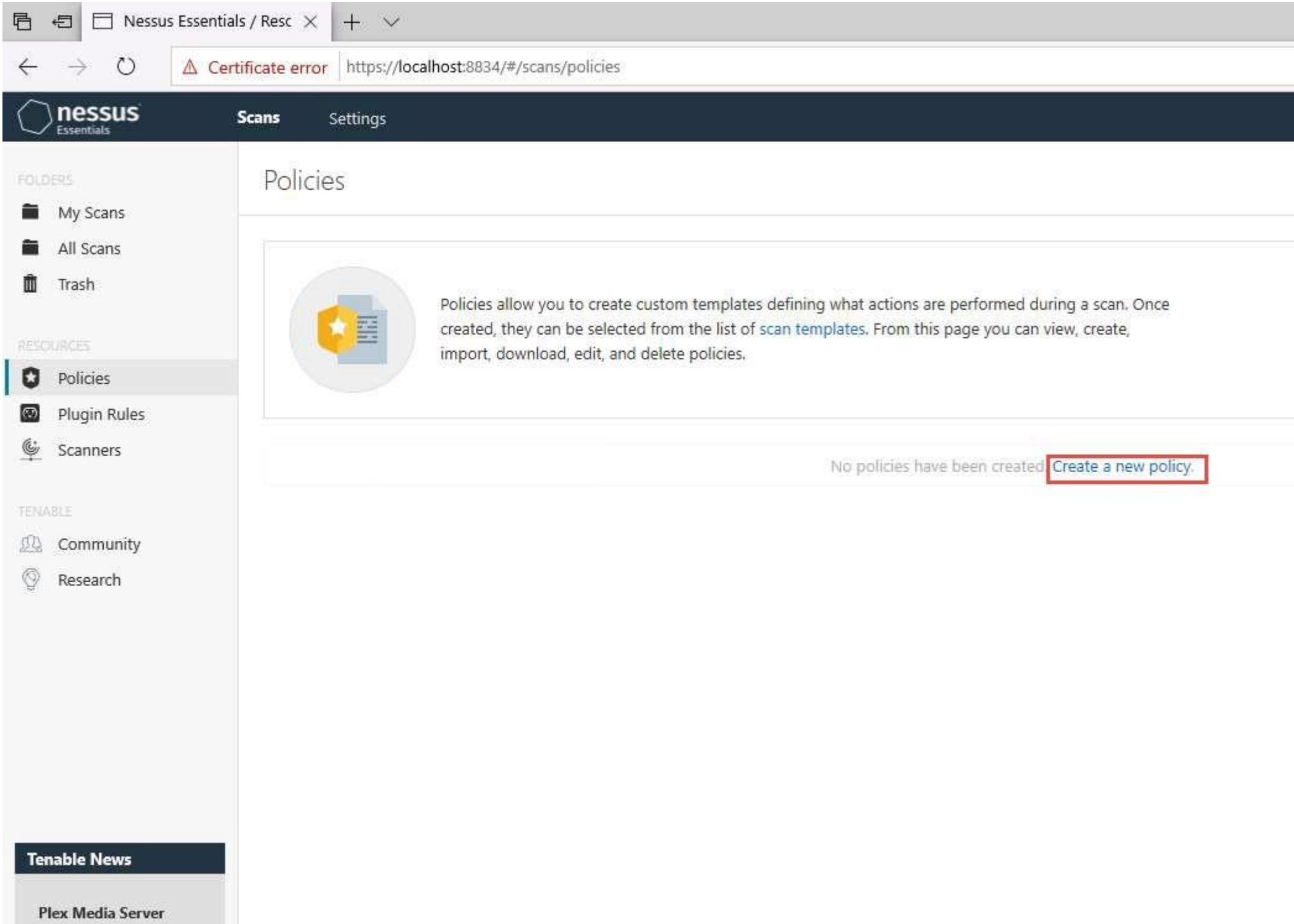
In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/folders/my-scans
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
IDC Ranks Tenable
My Scans
This folder is empty. Create a new scan.
Welcome to Nessus Essentials
To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
Close
Submit

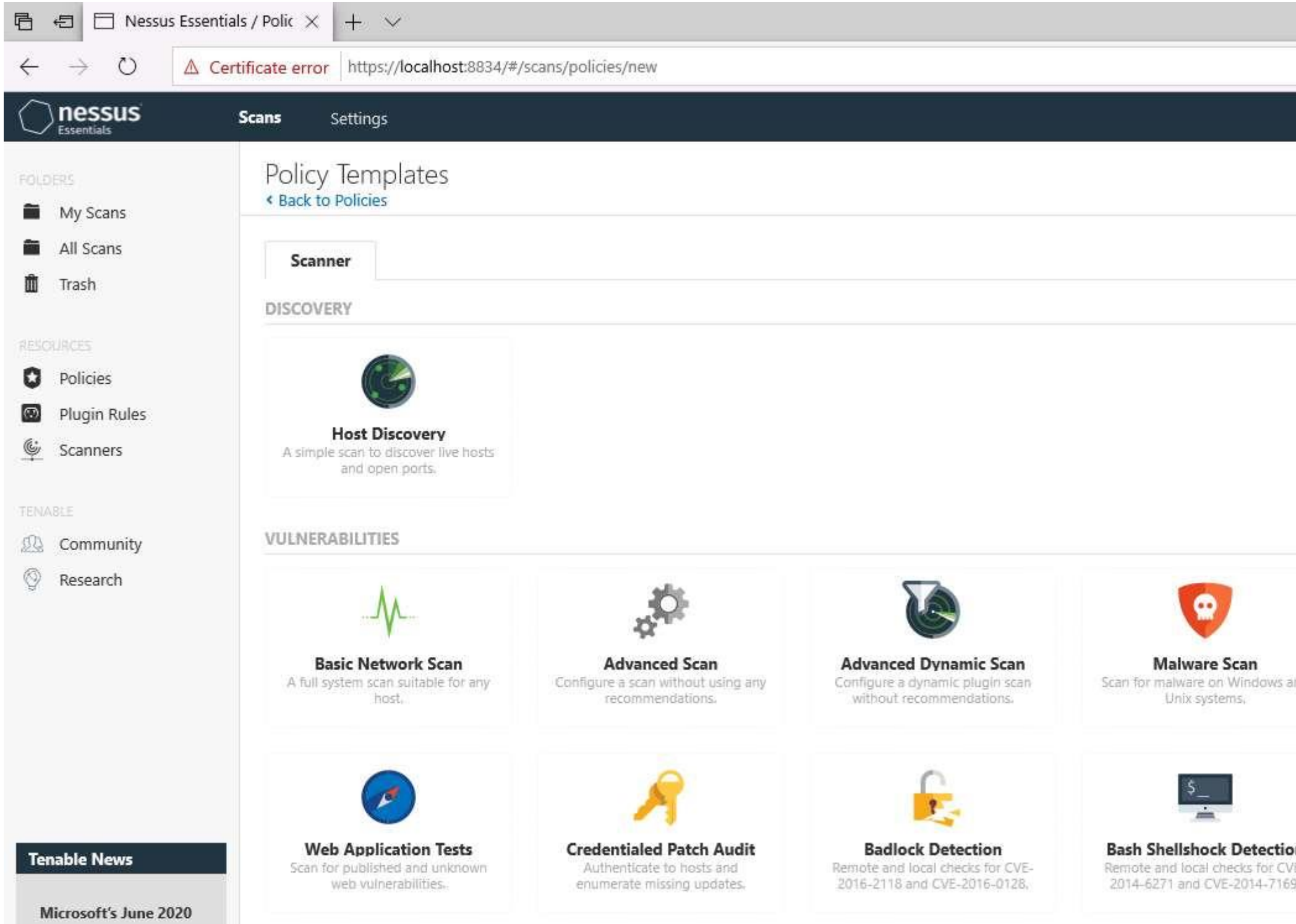
6. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/folders/my-scans
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
My Scans
This folder is empty. Create a new scan.
Tenable News
The 'Next Chapter' in

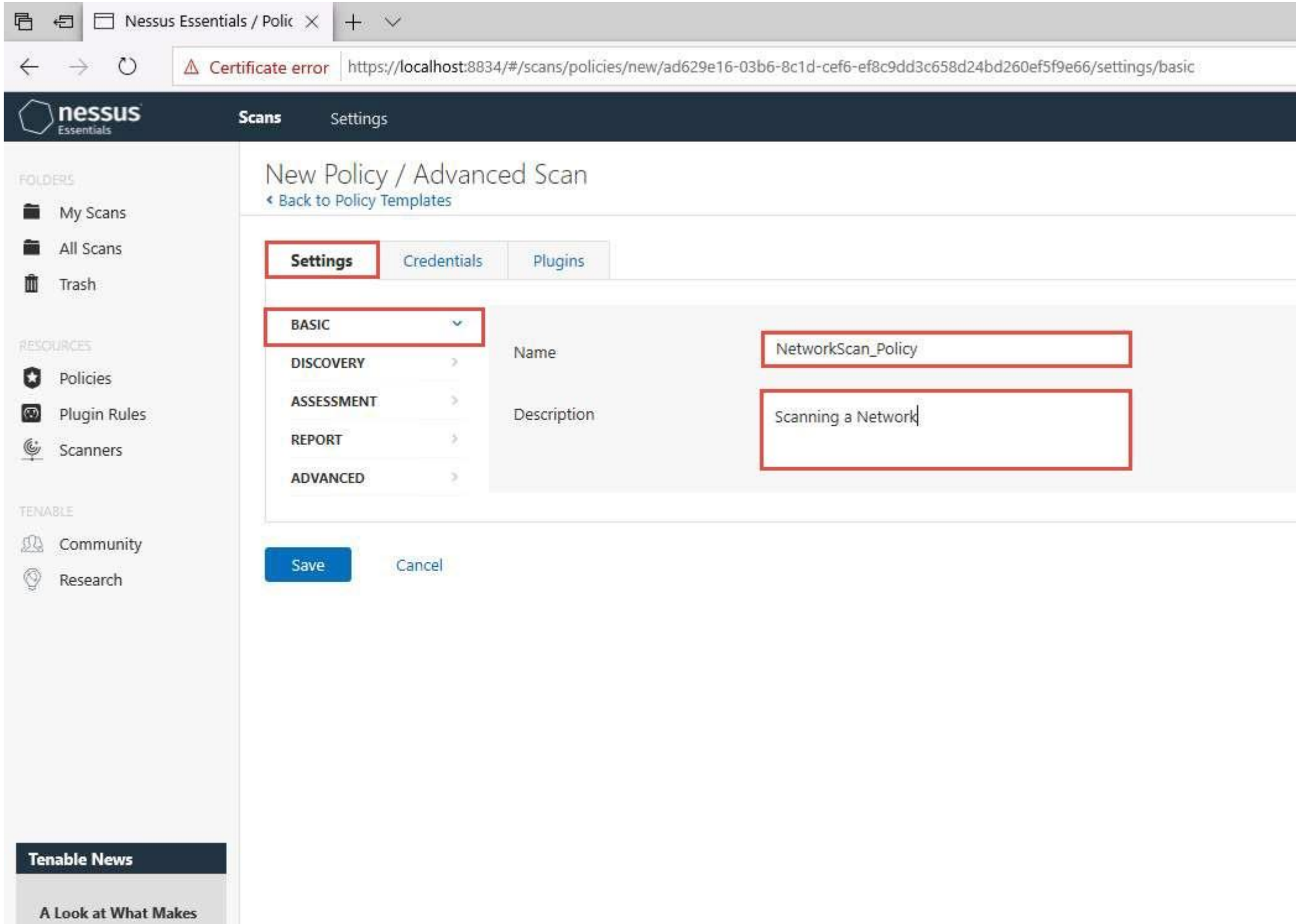
7. ☐ The **Policies** window appears; **click Create a new policy**.


Nessus Essentials / Resc
Certificate error
https://localhost:8834/#/scans/policies
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Plex Media Server
Policies
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
No policies have been created. Create a new policy.

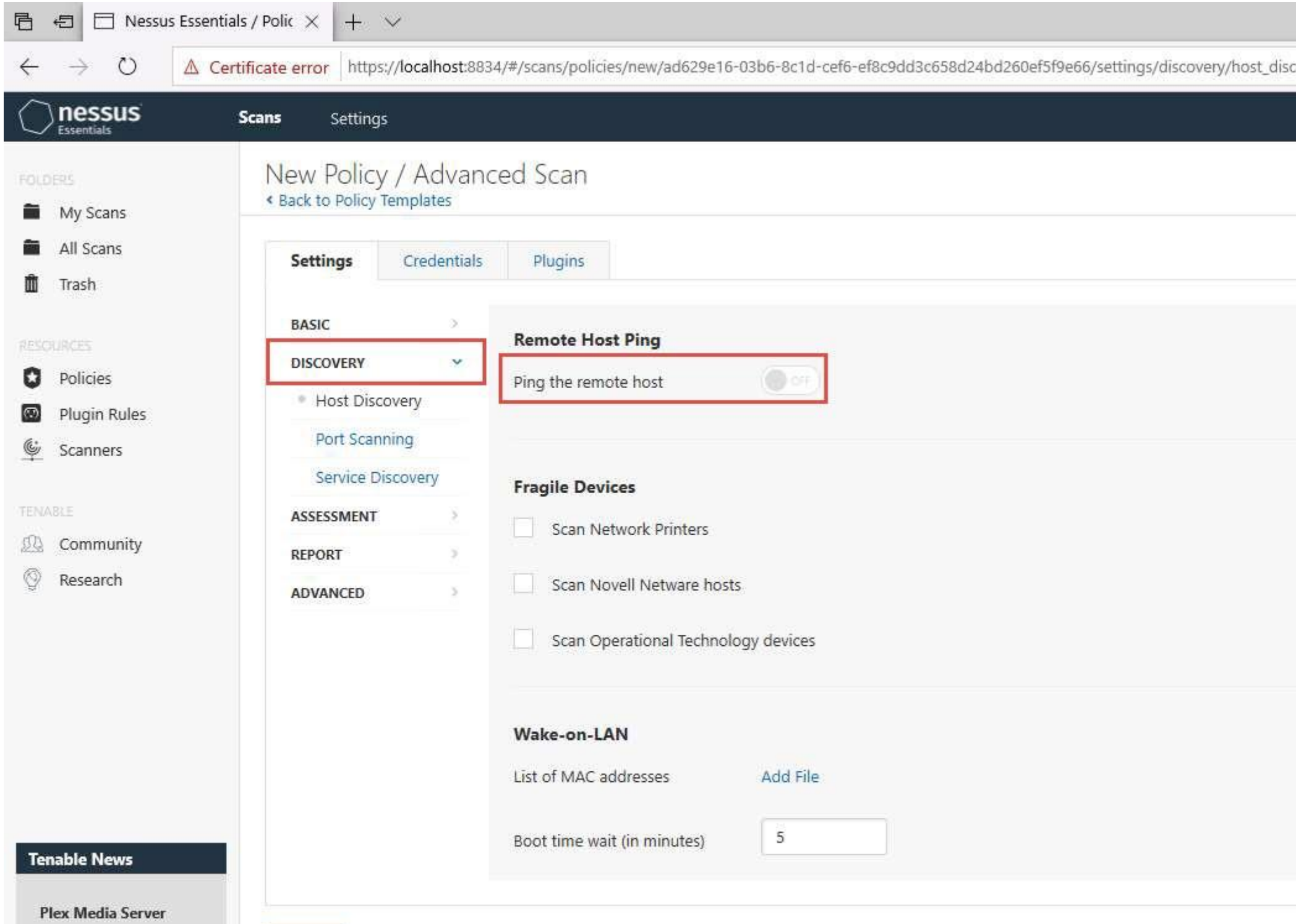
8. The **Policy Templates** window appears; click **Advanced Scan**.


Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Microsoft's June 2020
Policy Templates
Back to Policies
Scanner
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows a
Unix systems.
Web Application Tests
Scan for published and unknown web vulnerabilities.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detectio
Remote and local checks for CV
2014-6271 and CVE-2014-7169

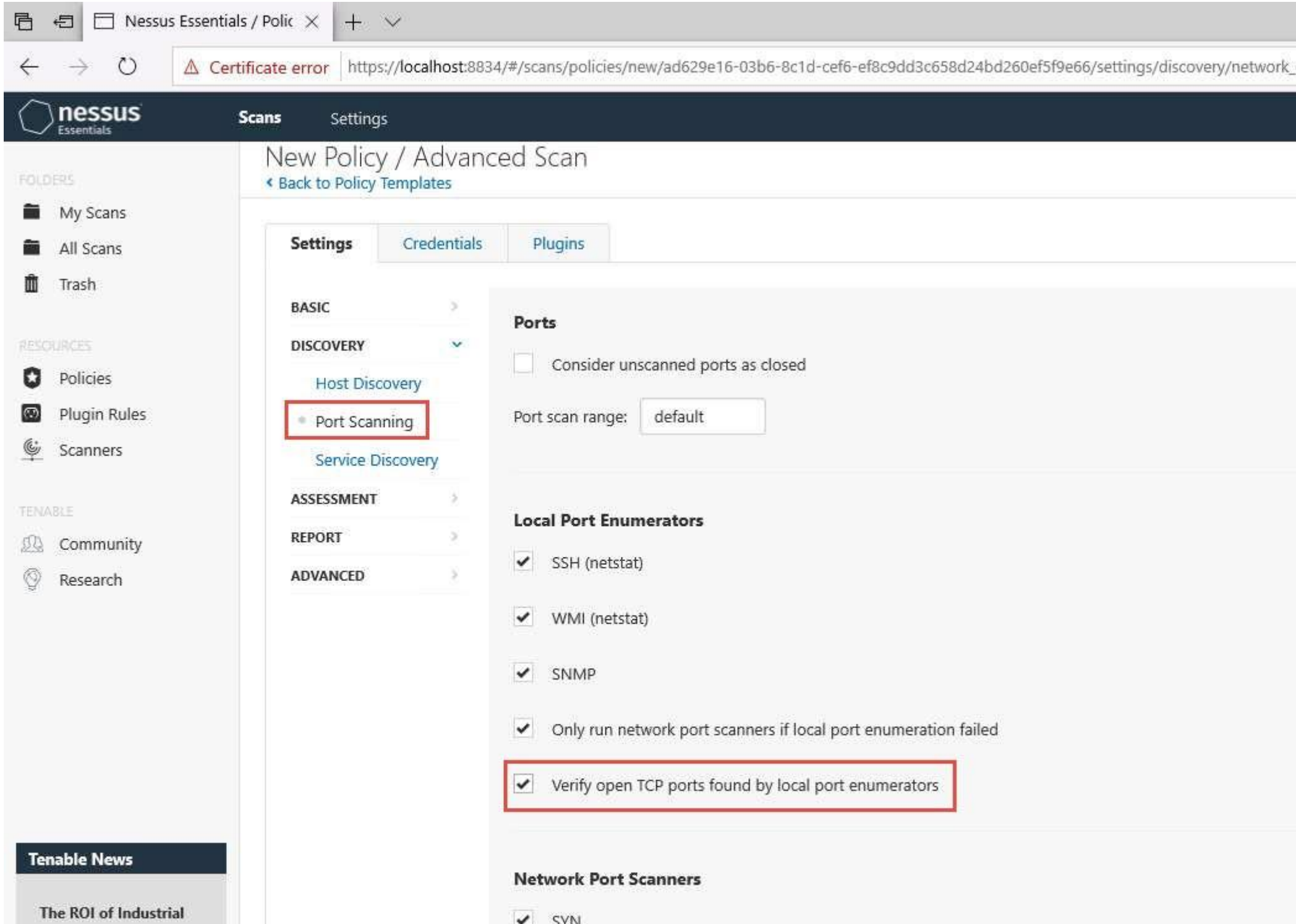
9. The **New Policy / Advanced Scan** section appears.
10. In the **Settings** tab under the **BASIC** setting type, specify a policy name in the **Name** field (here, **NetworkScan_Policy**), and give a **Description** about the policy (here, **Scanning a Network**).


Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/basic
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
A Look at What Makes
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
NetworkScan_Policy
Description
Scanning a Network
Save
Cancel

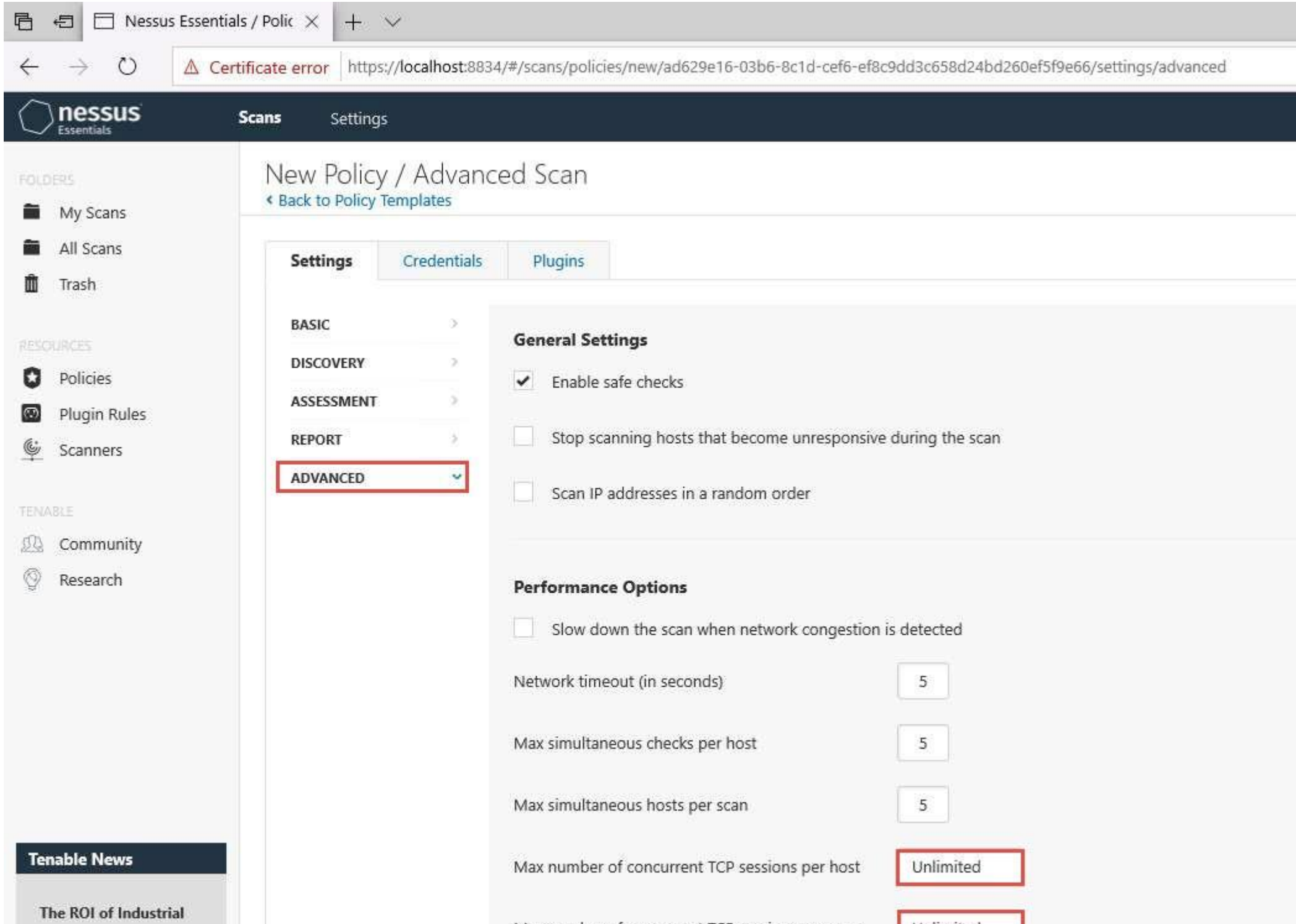
11. ☐ In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.


Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/discovery/host_disc
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Plex Media Server
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Remote Host Ping
Ping the remote host
OFF
Fragile Devices
Scan Network Printers
Scan Novell Netware hosts
Scan Operational Technology devices
Wake-on-LAN
List of MAC addresses
Add File
Boot time wait (in minutes)
5

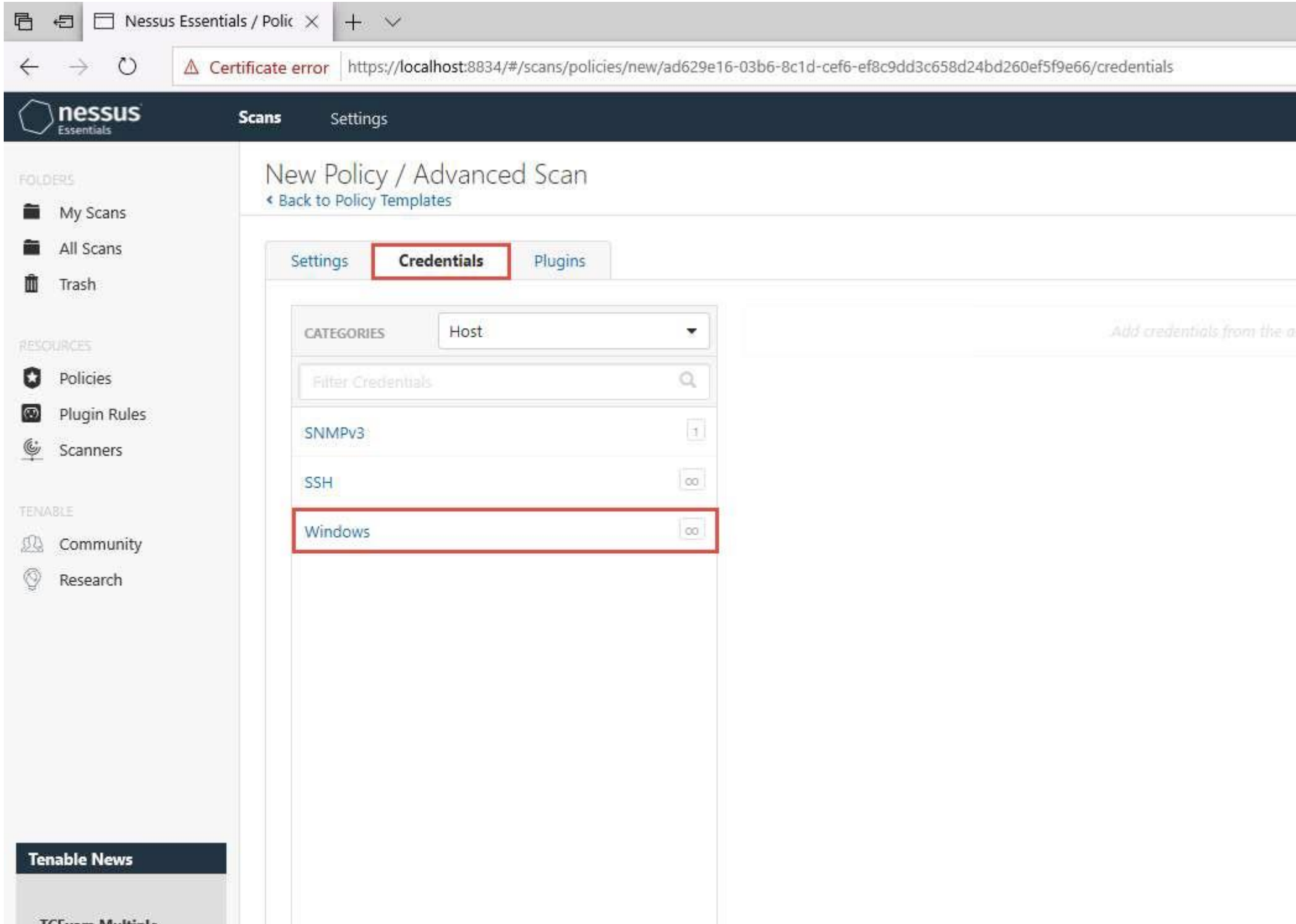
12. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox. Leave the other fields with default options, as shown in the screenshot.


Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/discovery/network_
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
The ROI of Industrial
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Ports
Consider unscanned ports as closed
Port scan range:
default
Local Port Enumerators
SSH (netstat)
WMI (netstat)
SNMP
Only run network port scanners if local port enumeration failed
Verify open TCP ports found by local port enumerators
Network Port Scanners
SYN

13. 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**.

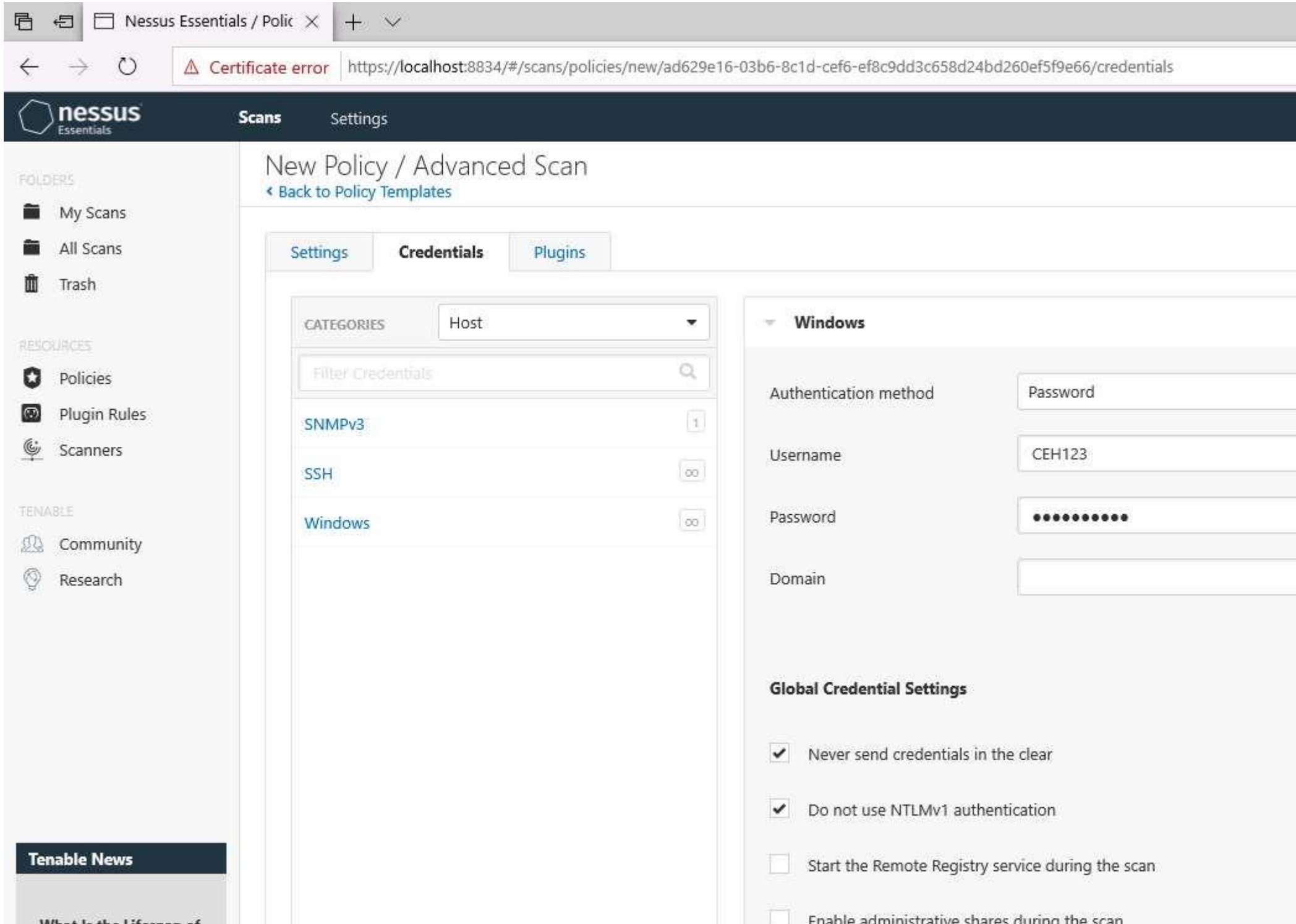

Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/advanced
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
The ROI of Industrial
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
General Settings
Enable safe checks
Stop scanning hosts that become unresponsive during the scan
Scan IP addresses in a random order
Performance Options
Slow down the scan when network congestion is detected
Network timeout (in seconds)
5
Max simultaneous checks per host
5
Max simultaneous hosts per scan
5
Max number of concurrent TCP sessions per host
Unlimited

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

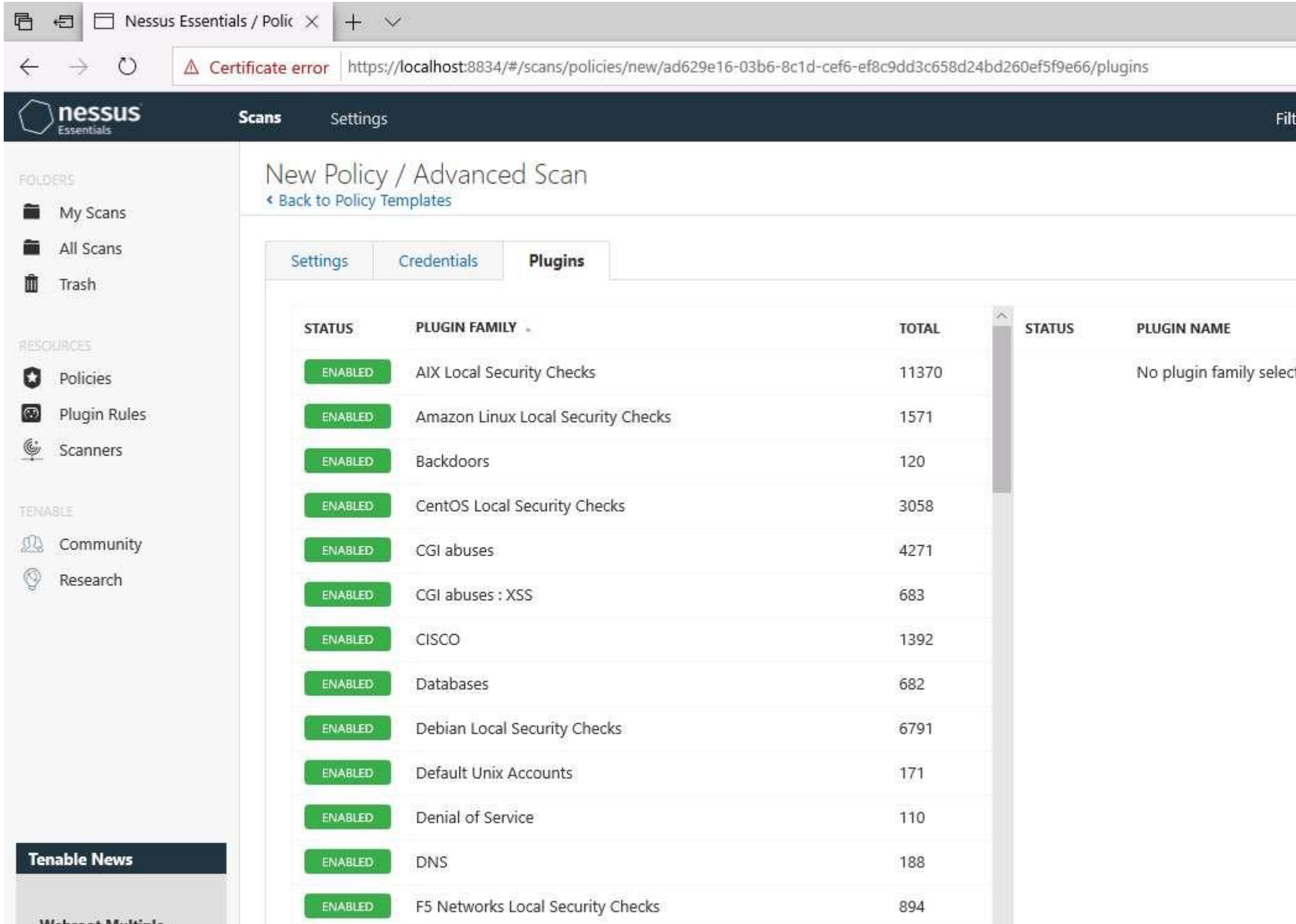

Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/credentials
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows

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

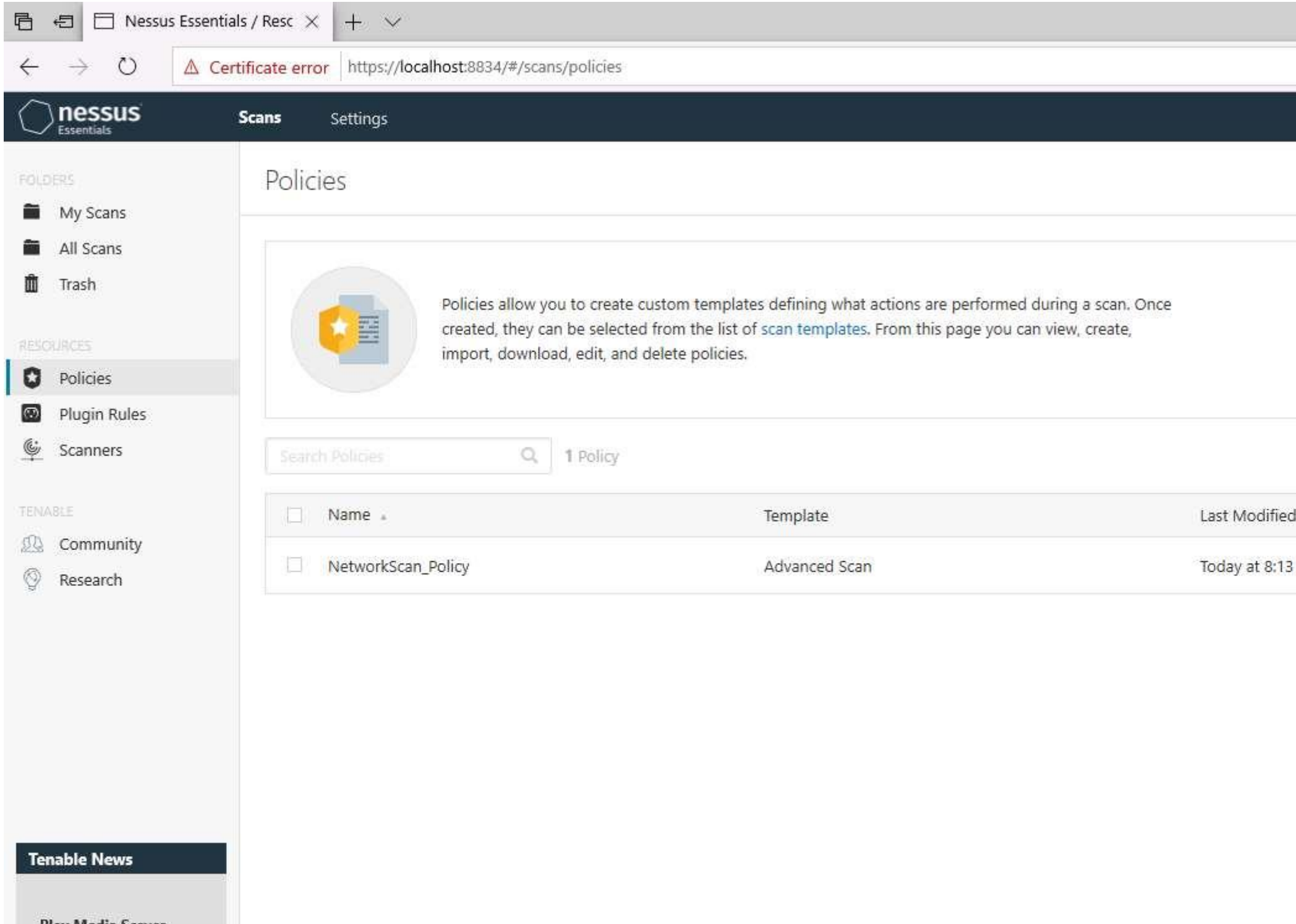
Re-enter the created user account credentials, **Admin/password**, if session timeout notification pop-up appears.


Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/credentials
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
Windows
Authentication method
Password
Username
CEH123
Password
Domain
Global Credential Settings
Never send credentials in the clear
Do not use NTLMv1 authentication
Start the Remote Registry service during the scan

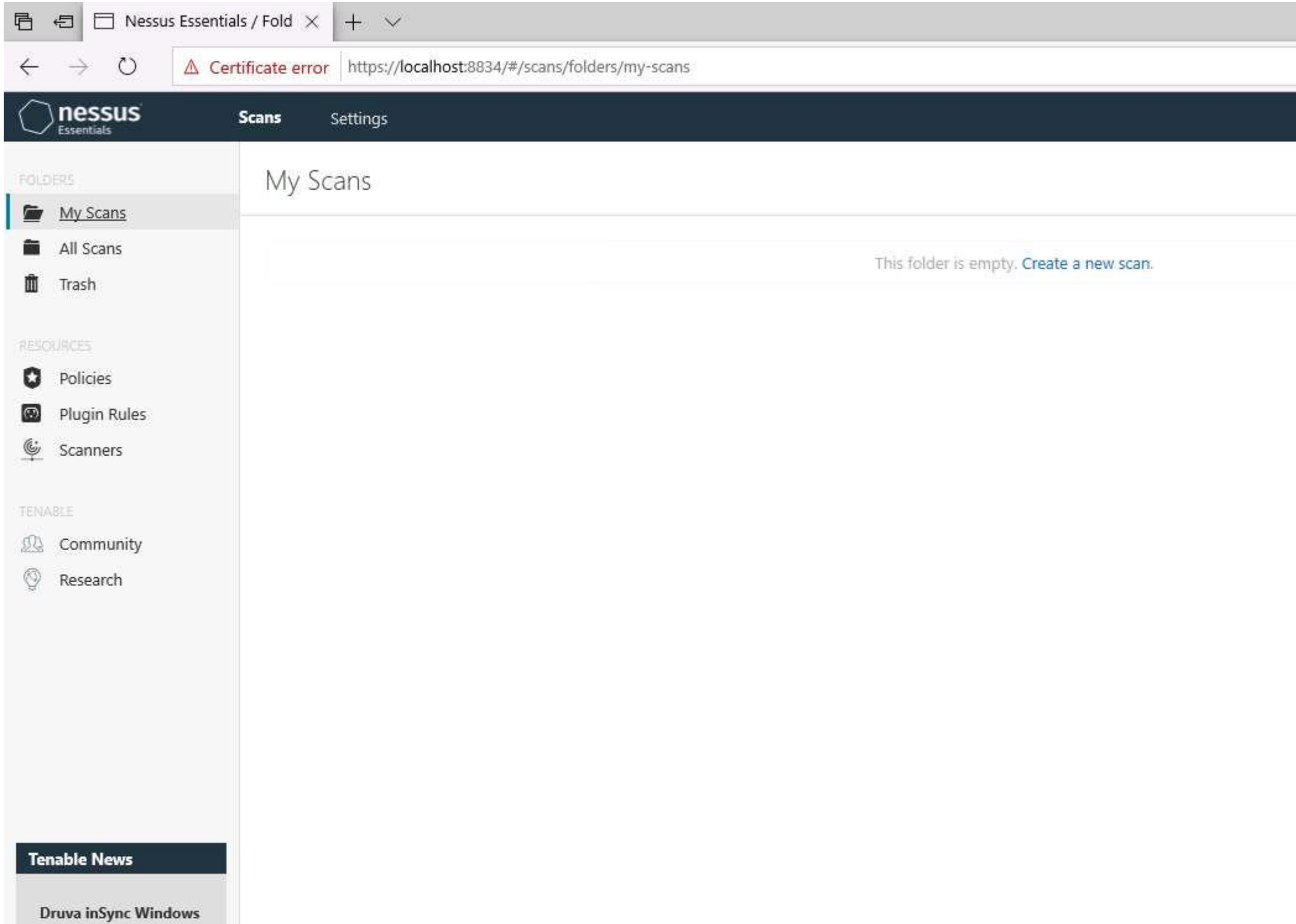
16. ☐ Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.


Nessus Essentials / Polic
Certificate error
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/plugins
nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
STATUS
PLUGIN FAMILY
TOTAL
ENABLED AIX Local Security Checks 11370
ENABLED Amazon Linux Local Security Checks 1571
ENABLED Backdoors 120
ENABLED CentOS Local Security Checks 3058
ENABLED CGI abuses 4271
ENABLED CGI abuses : XSS 683
ENABLED CISCO 1392
ENABLED Databases 682
ENABLED Debian Local Security Checks 6791
ENABLED Default Unix Accounts 171
ENABLED Denial of Service 110
ENABLED DNS 188
ENABLED F5 Networks Local Security Checks 894
STATUS
PLUGIN NAME
No plugin family select

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

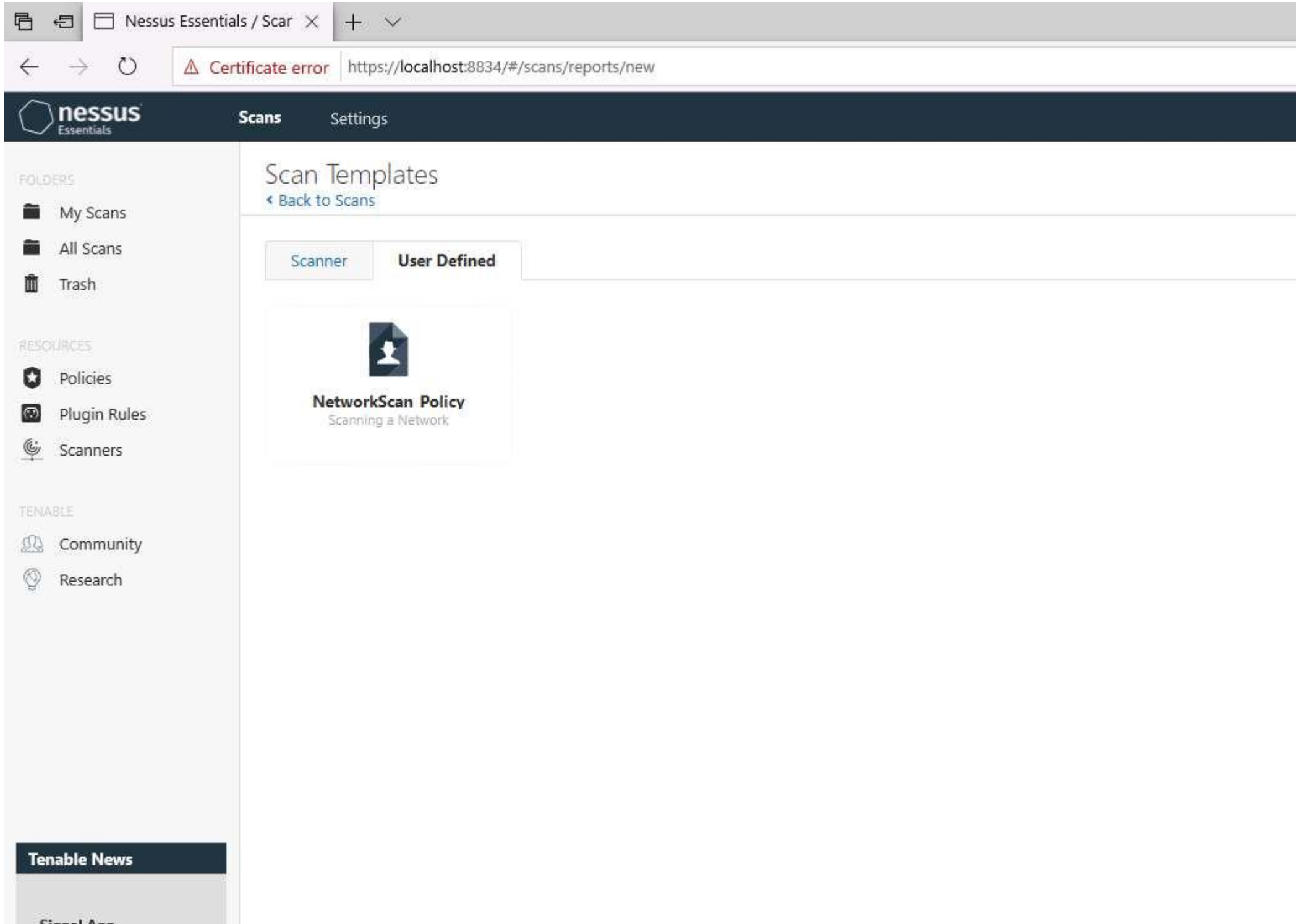

Nessus Essentials / Resc
Certificate error
https://localhost:8834/#/scans/policies
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Policies
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
Search Policies
1 Policy
Name
Template
Last Modified
NetworkScan_Policy
Advanced Scan
Today at 8:13

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


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/folders/my-scans
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
My Scans
This folder is empty. Create a new scan.
Tenable News
Druva inSync Windows

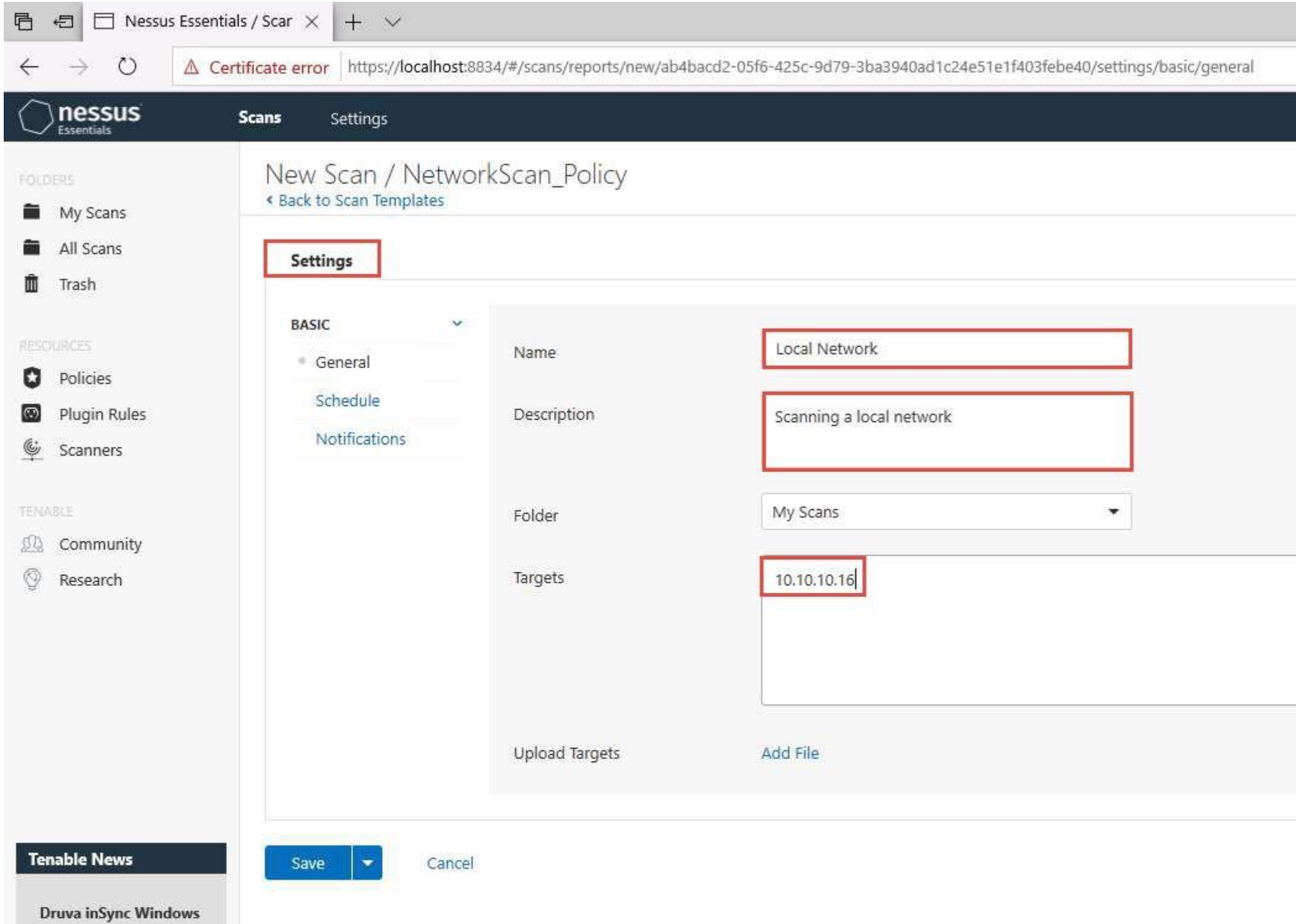
19. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan Policy**.

If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin/password**), if it still shows the API Disabled error then clear the cache of the browser by clicking on the three dots at the top right of the browser --> Click on History --> Clear History and make sure that cache and cookies are checked and click on clear and login to the **Nessus Essentials** again.

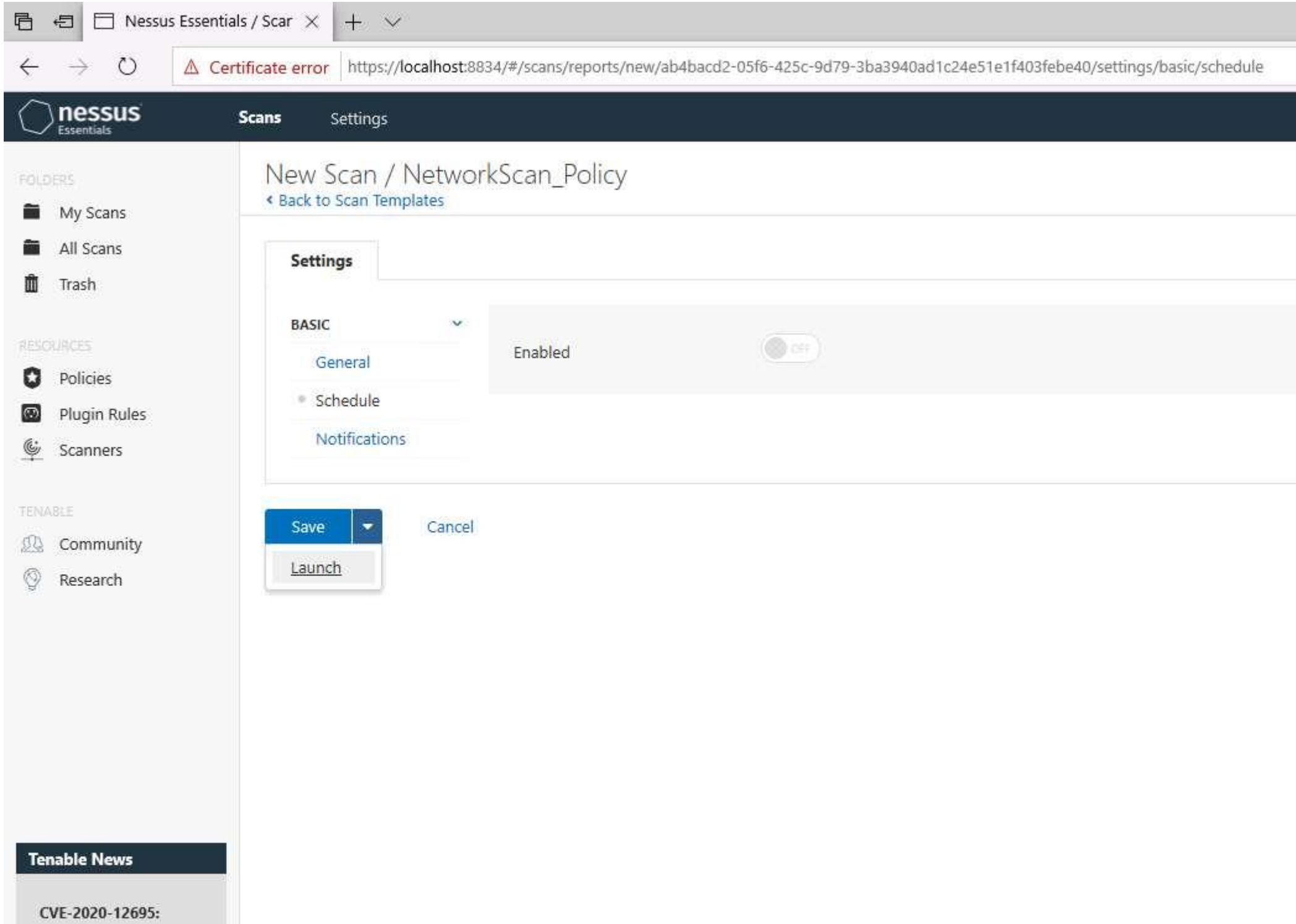

Nessus Essentials / Scar
Certificate error
https://localhost:8834/#/scans/reports/new
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Scan Templates
Back to Scans
Scanner
User Defined
NetworkScan Policy
Scanning a Network

20. 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)**.

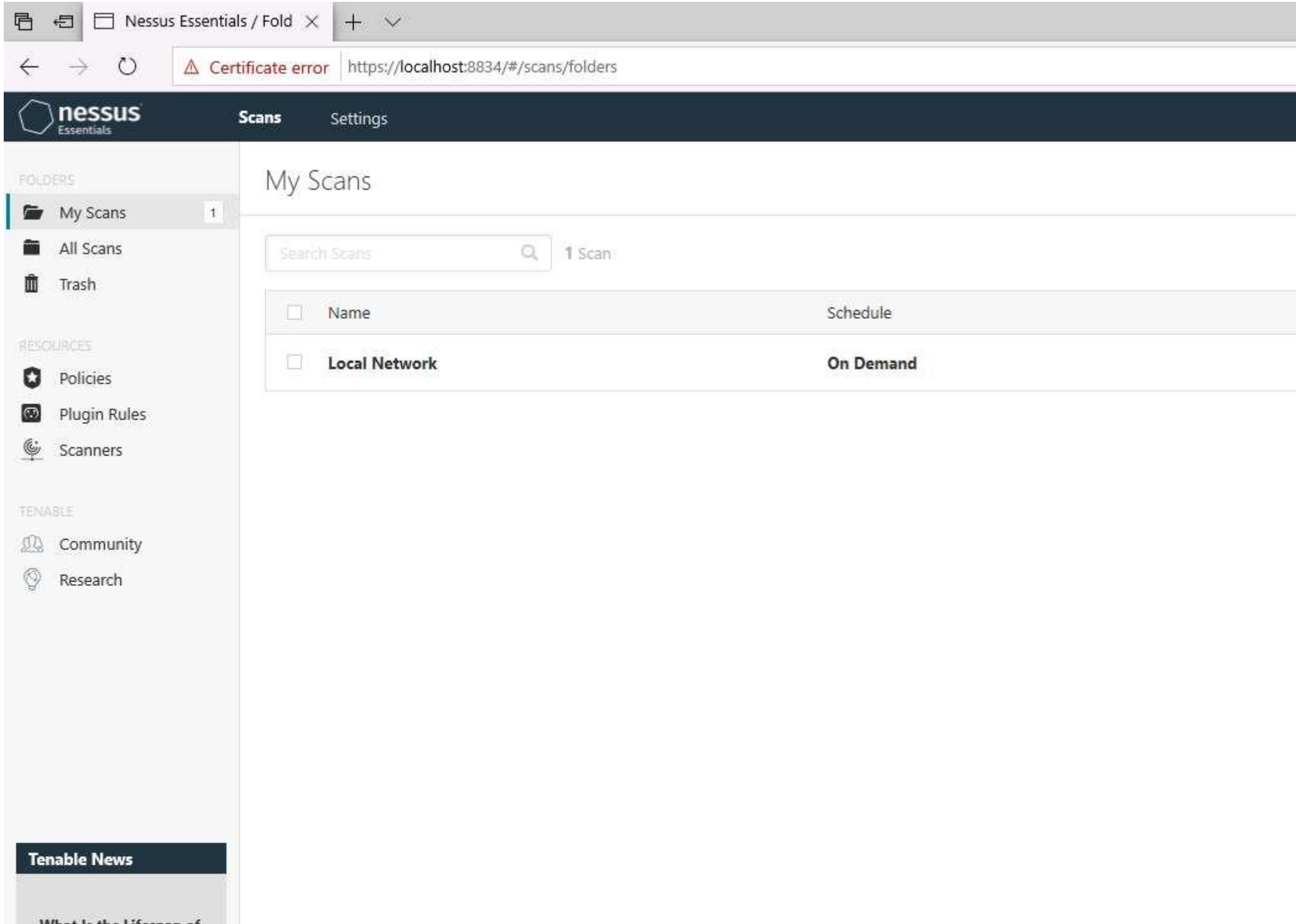
The IP addresses may vary in your lab environment.


Nessus Essentials / Scar
Certificate error
https://localhost:8834/#/scans/reports/new/ab4bacd2-05f6-425c-9d79-3ba3940ad1c24e51e1f403febe40/settings/basic/general
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Druva inSync Windows
New Scan / NetworkScan_Policy
Back to Scan Templates
Settings
BASIC
General
Schedule
Notifications
Name
Local Network
Description
Scanning a local network
Folder
My Scans
Targets
10.10.10.16
Upload Targets
Add File
Save
Cancel

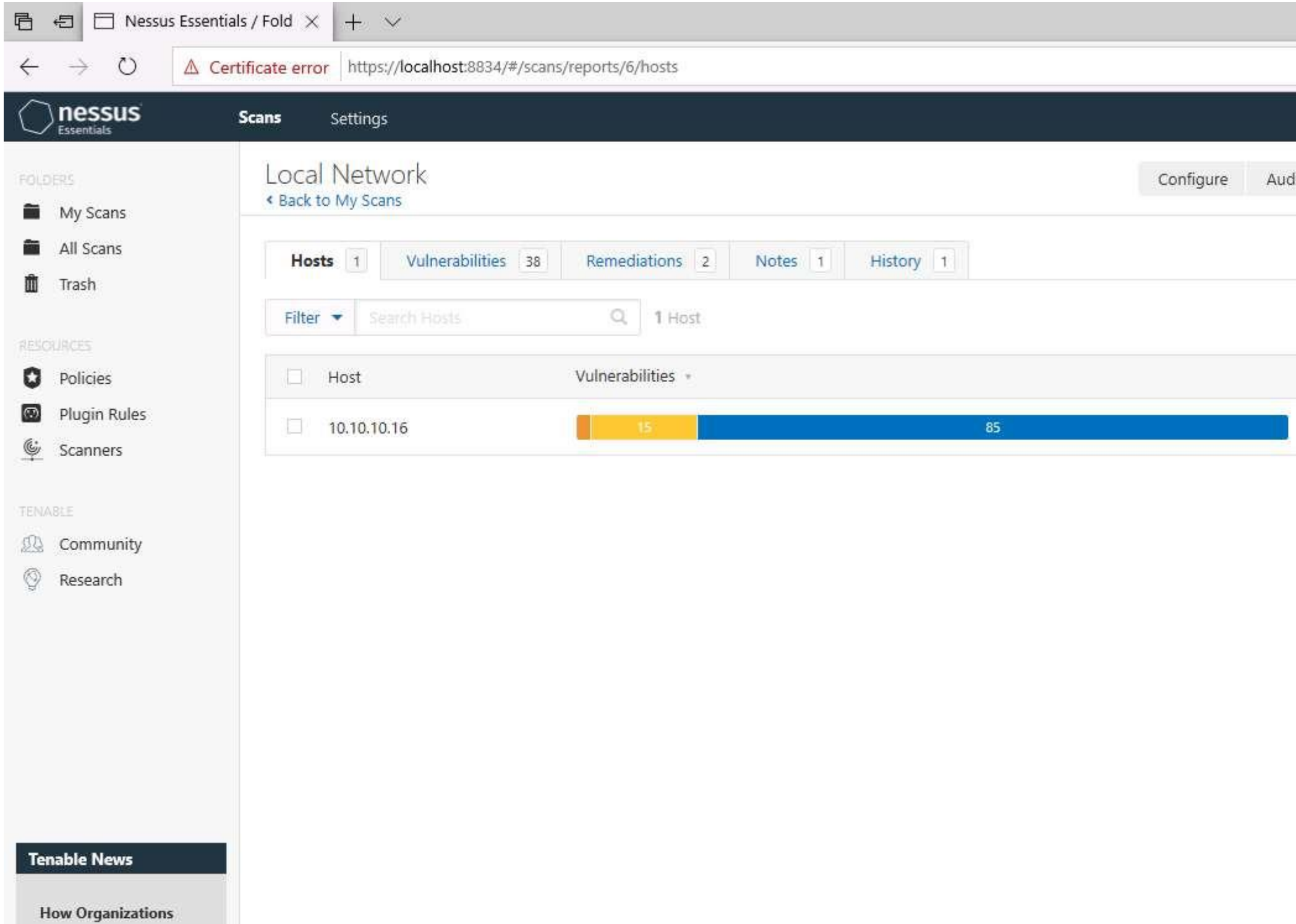
21. ☐ Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.


Nessus Essentials / Scar
Certificate error
https://localhost:8834/#/scans/reports/new/ab4bacd2-05f6-425c-9d79-3ba3940ad1c24e51e1f403febe40/settings/basic/schedule
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
New Scan / NetworkScan_Policy
Back to Scan Templates
Settings
BASIC
General
Schedule
Notifications
Enabled
OFF
Save
Launch
Cancel
Tenable News
CVE-2020-12695:

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


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/folders
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
My Scans
Search Scans
1 Scan
Name
Schedule
Local Network
On Demand

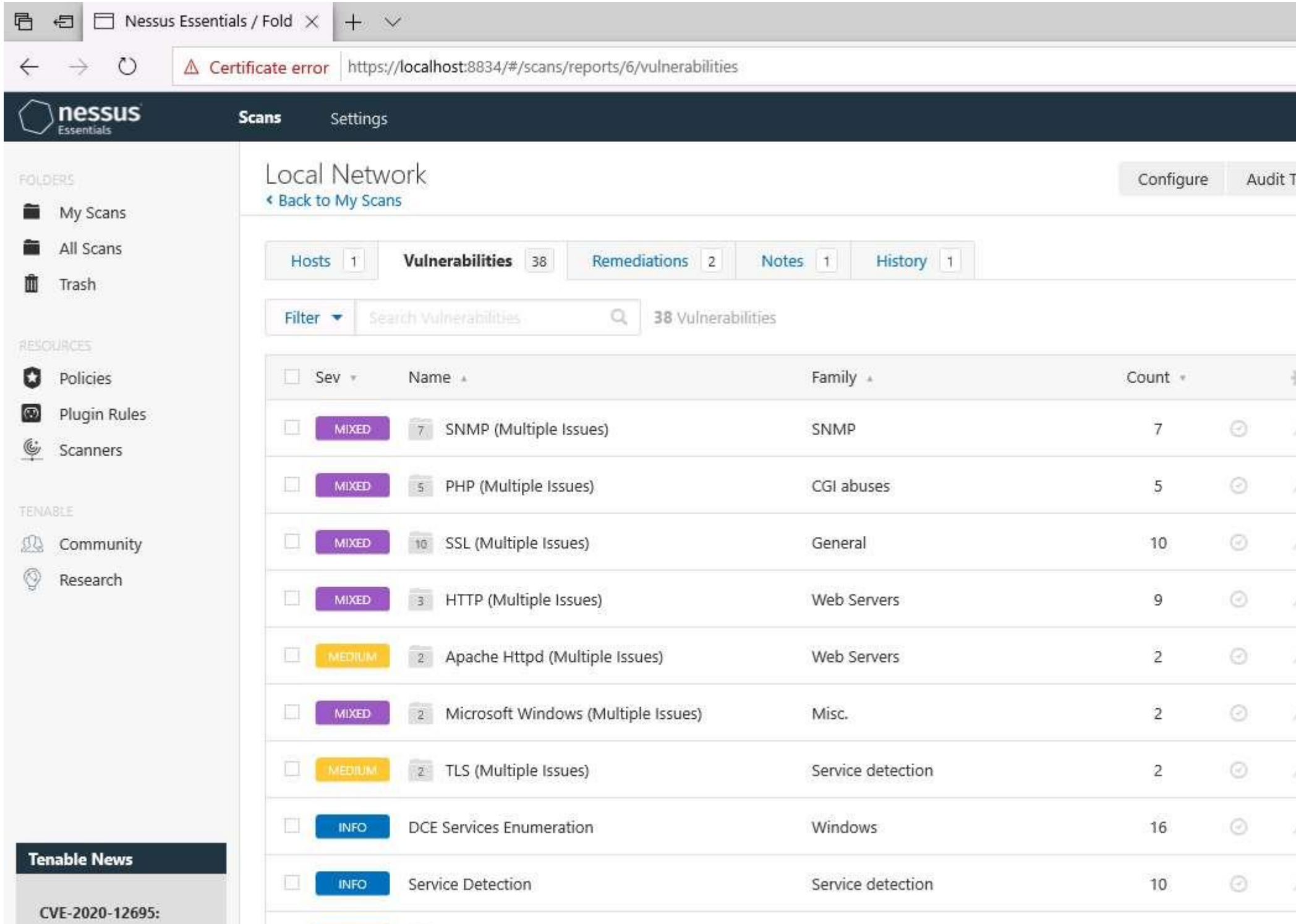
23. ☐ After the completion of the scan: click **Local Network** to view the detailed results.
24. ☐ The **Local Network** window appears, displaying the summary of target hosts, as well as the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab, as shown in the screenshot.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/reports/6/hosts
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
How Organizations
Local Network
Back to My Scans
Configure
Aud
Hosts 1
Vulnerabilities 38
Remediations 2
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
10.10.10.16
15
85

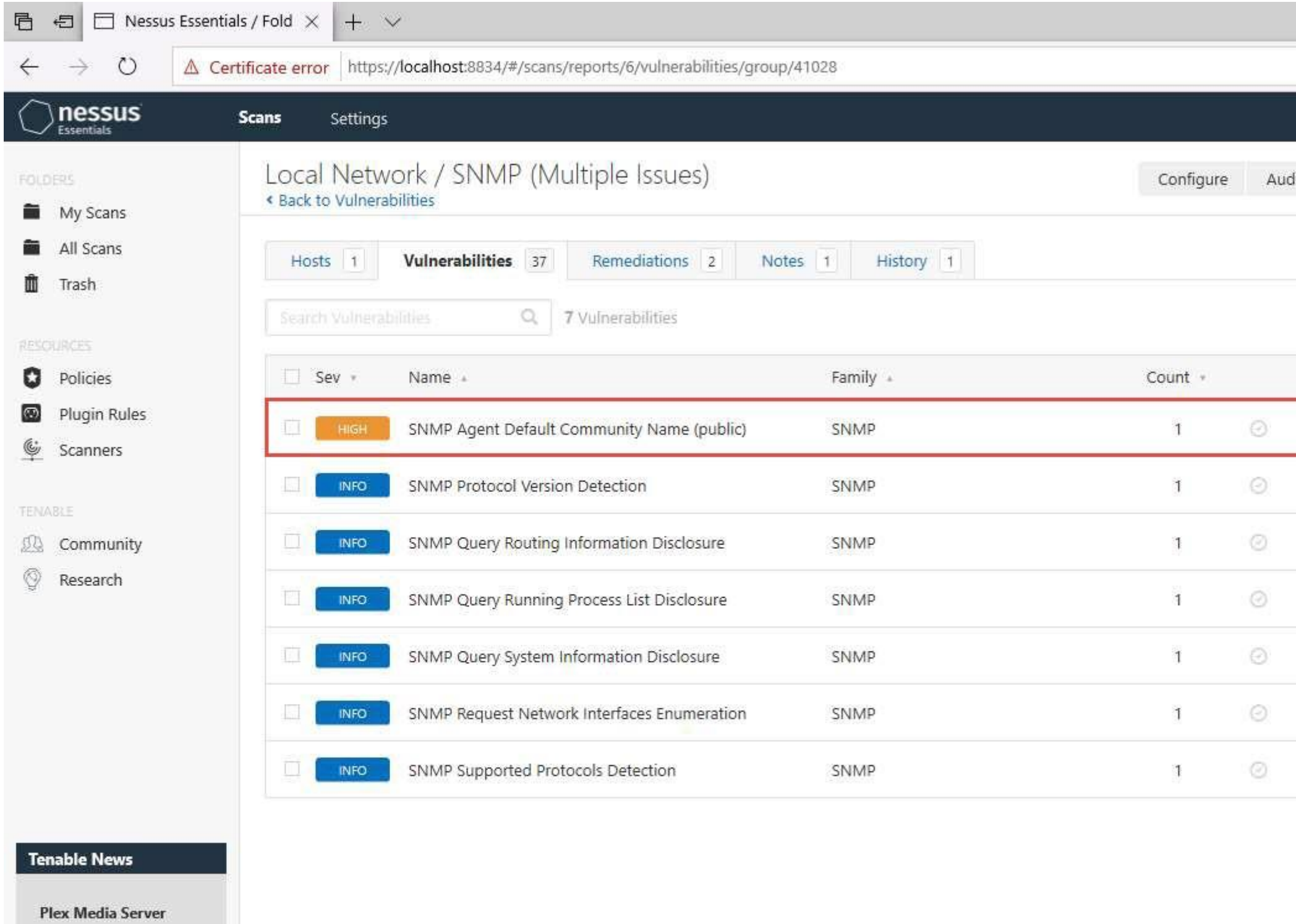
25. ☐ Click the **Vulnerabilities** tab, and scroll down to view all the vulnerabilities associated with the target machine.

The list of vulnerabilities may differ in your lab environment.

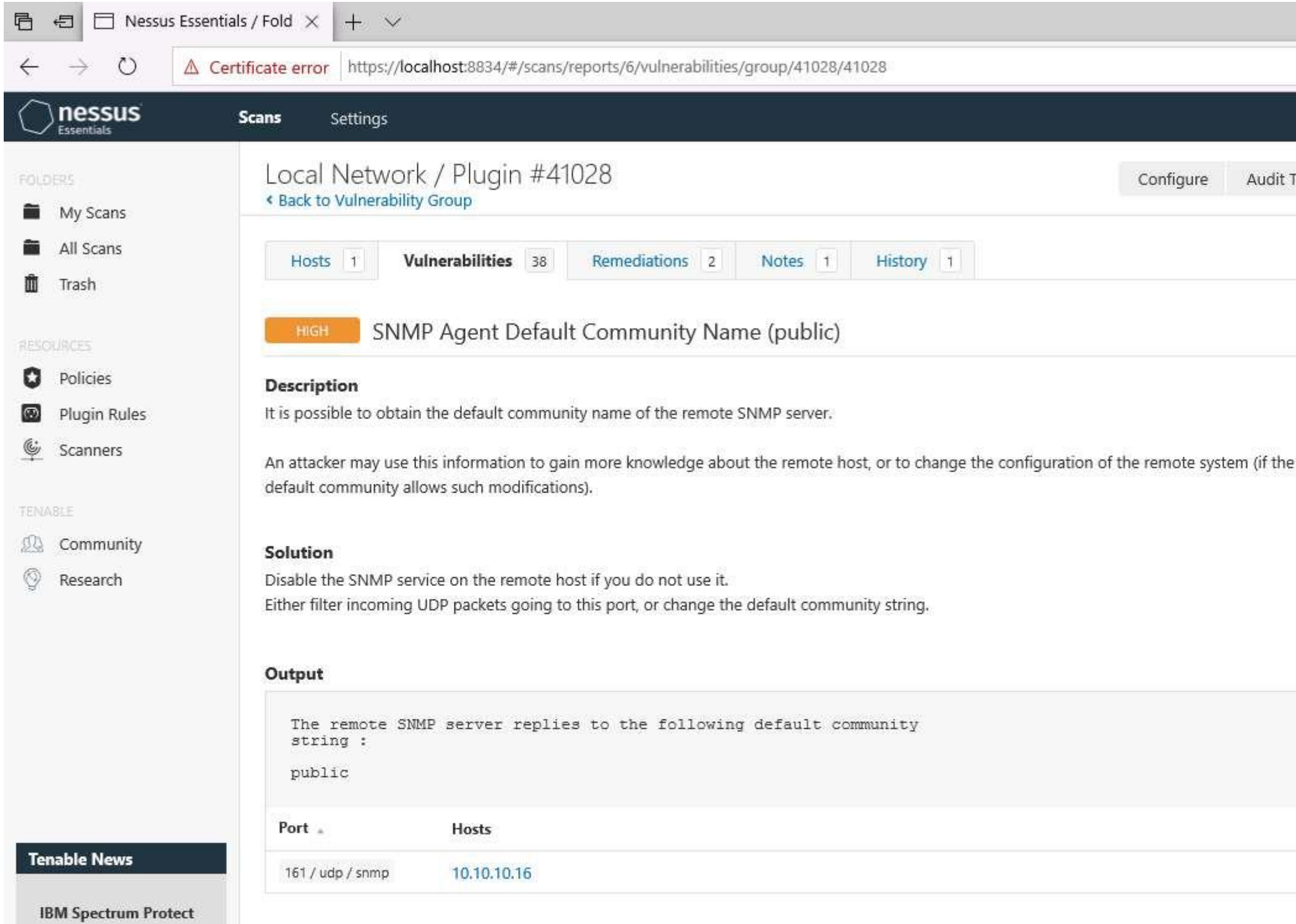
26. ☐ Click these vulnerabilities to view detailed reports about each. For instance, in this lab, we are selecting the first vulnerability in the list, that is, **SNMP (Multiple Issues)**.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/reports/6/vulnerabilities
nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
CVE-2020-12695:
Local Network
Back to My Scans
Configure
Audit T
Hosts 1
Vulnerabilities 38
Remediations 2
Notes 1
History 1
Filter
Search Vulnerabilities
38 Vulnerabilities
Sev
Name
Family
Count
MIXED 7 SNMP (Multiple Issues) SNMP 7
MIXED 5 PHP (Multiple Issues) CGI abuses 5
MIXED 10 SSL (Multiple Issues) General 10
MIXED 3 HTTP (Multiple Issues) Web Servers 9
MEDIUM 2 Apache Httpd (Multiple Issues) Web Servers 2
MIXED 2 Microsoft Windows (Multiple Issues) Misc. 2
MEDIUM 2 TLS (Multiple Issues) Service detection 2
INFO DCE Services Enumeration Windows 16
INFO Service Detection Service detection 10

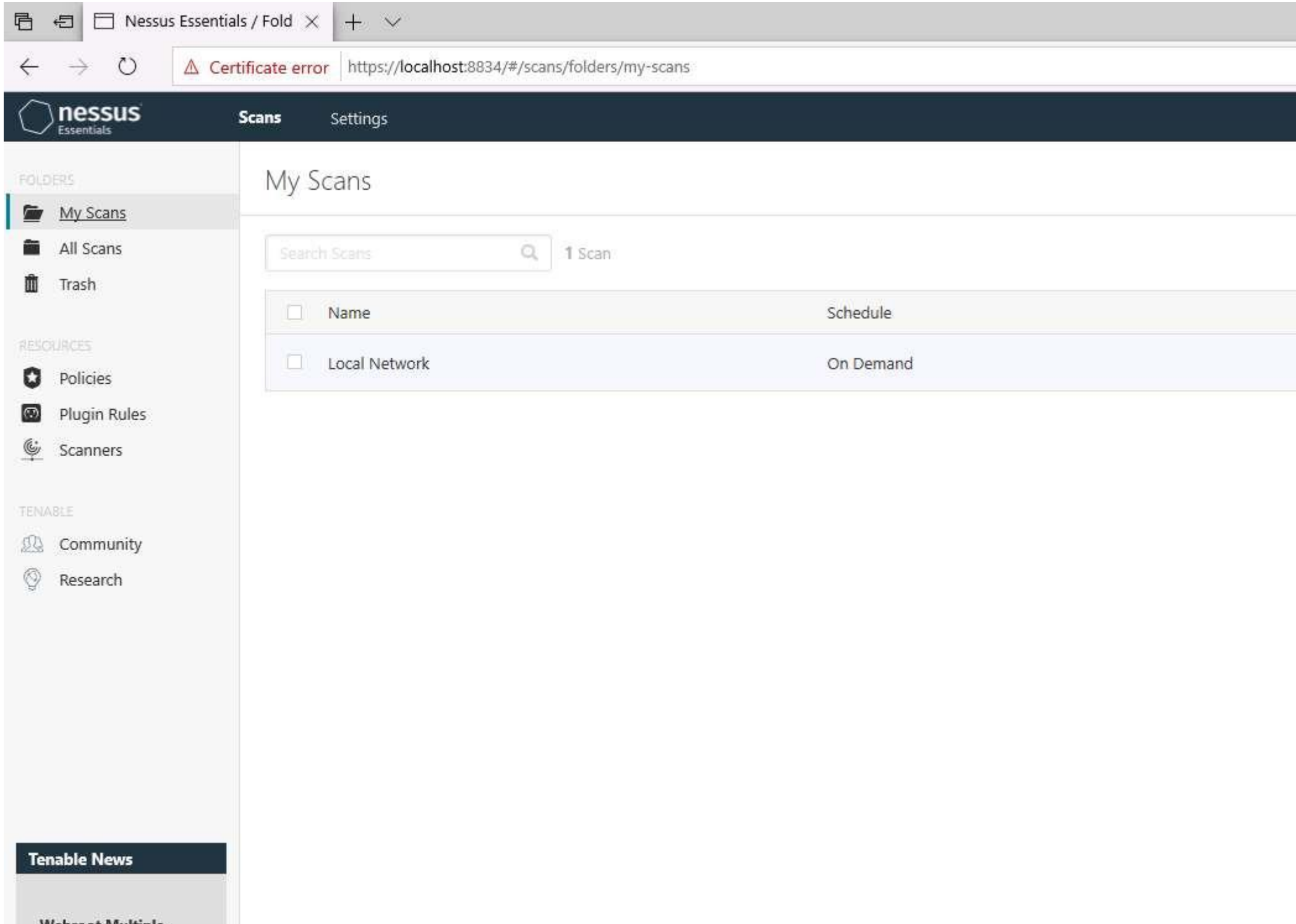
27. The **Local Network** / **SNMP (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SNMP Agent Default**) to view its detailed information.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/reports/6/vulnerabilities/group/41028
nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Plex Media Server
Local Network / SNMP (Multiple Issues)
Back to Vulnerabilities
Configure
Aud
Hosts 1
Vulnerabilities 37
Remediations 2
Notes 1
History 1
Search Vulnerabilities
7 Vulnerabilities
Sev
Name
Family
Count
HIGH SNMP Agent Default Community Name (public) SNMP 1
INFO SNMP Protocol Version Detection SNMP 1
INFO SNMP Query Routing Information Disclosure SNMP 1
INFO SNMP Query Running Process List Disclosure SNMP 1
INFO SNMP Query System Information Disclosure SNMP 1
INFO SNMP Request Network Interfaces Enumeration SNMP 1
INFO SNMP Supported Protocols Detection SNMP 1

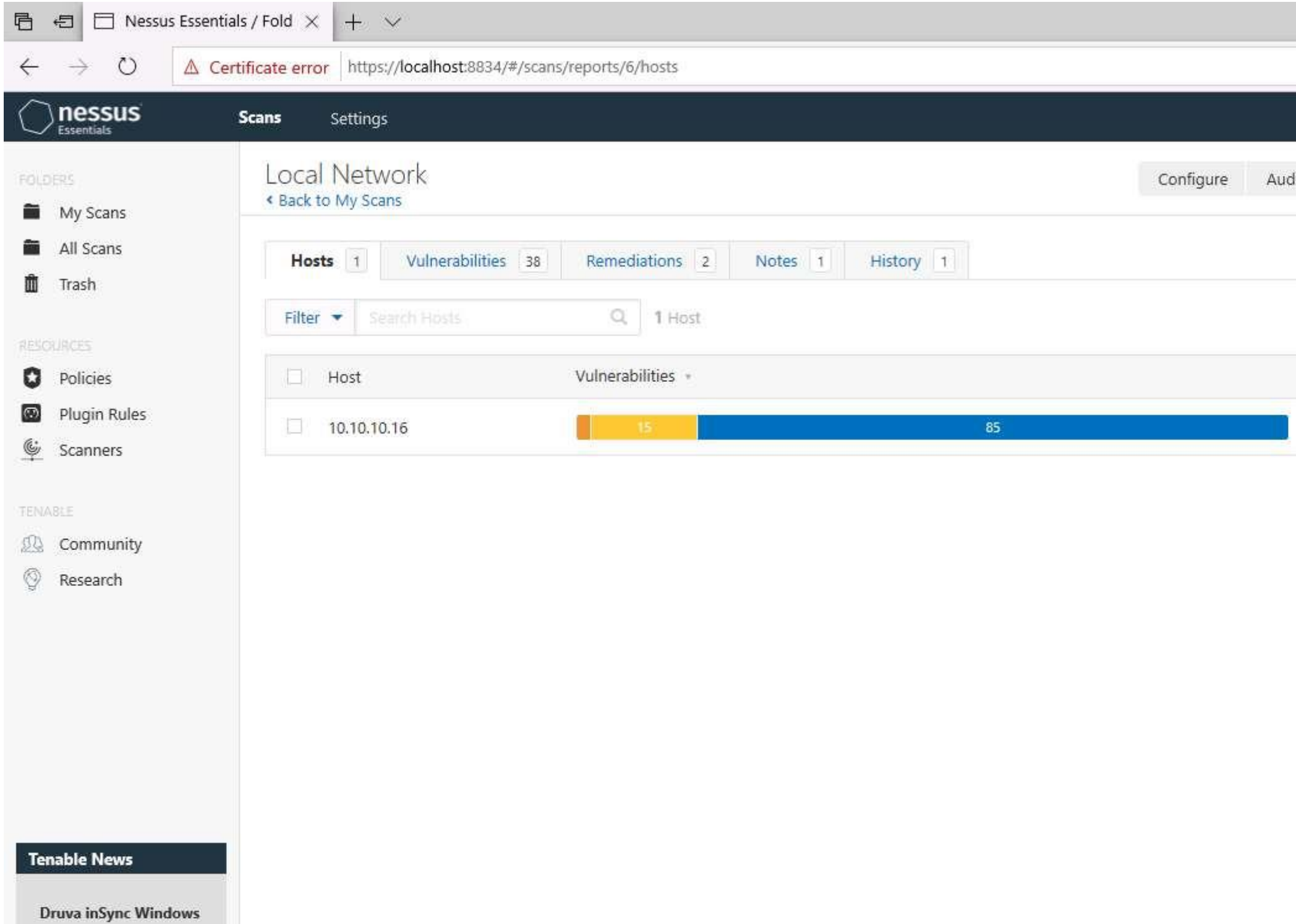
28. ☐ The report regarding selected vulnerability **SNMP Agent Default Community Name (public)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/reports/6/vulnerabilities/group/41028/41028
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
IBM Spectrum Protect
Local Network / Plugin #41028
Back to Vulnerability Group
Configure
Audit T
Hosts 1
Vulnerabilities 38
Remediations 2
Notes 1
History 1
HIGH
SNMP Agent Default Community Name (public)
Description
It is possible to obtain the default community name of the remote SNMP server.
An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).
Solution
Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.
Output
The remote SNMP server replies to the following default community string :
public
Port
Hosts
161 / udp / snmp
10.10.10.16

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


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/folders/my-scans
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
My Scans
Search Scans
1 Scan
Name
Schedule
Local Network
On Demand

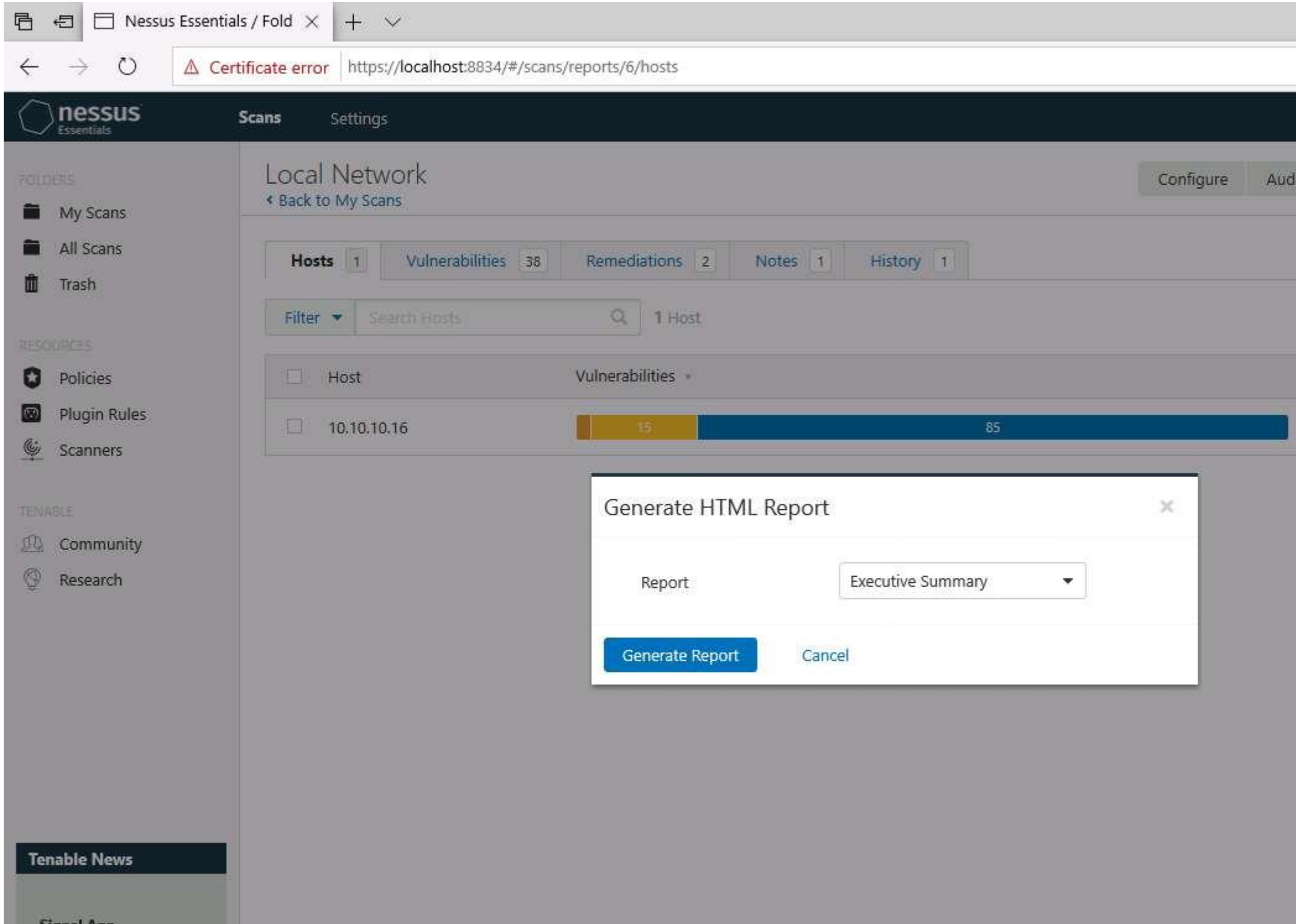
30. In the **Local Network** window, click the **Report** tab from the top-right corner, and choose a file format (here, **HTML**) from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/reports/6/hosts
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Druva inSync Windows
Local Network
Back to My Scans
Configure
Aud
Hosts 1
Vulnerabilities 38
Remediations 2
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
10.10.10.16
15
85

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

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

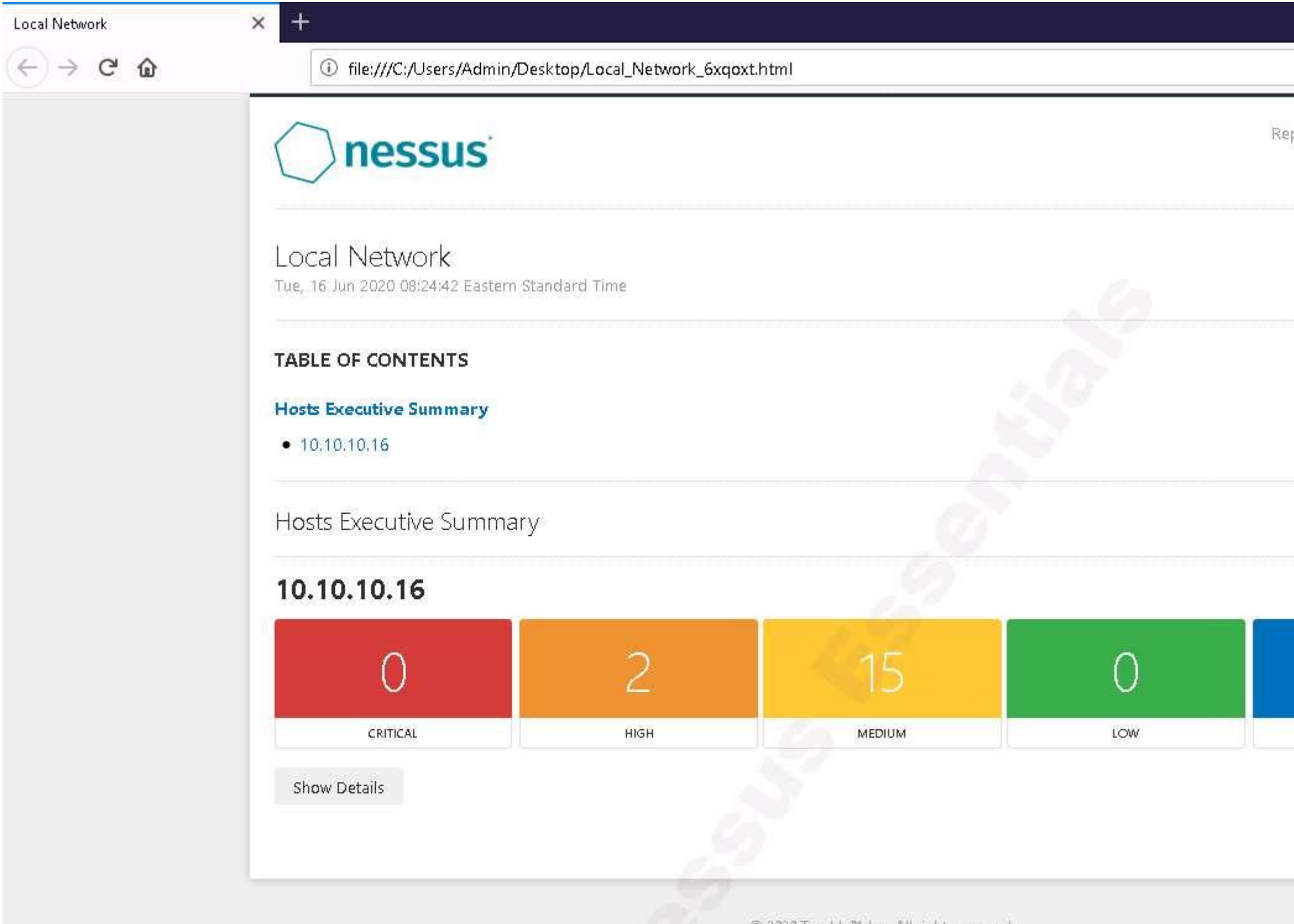
The file name might differ in your lab environment


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/reports/6/hosts
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Local Network
Back to My Scans
Configure
Aud
Hosts 1
Vulnerabilities 38
Remediations 2
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
10.10.10.16
15
85
Generate HTML Report
Report
Executive Summary
Generate Report
Cancel

32. Once the download is finished, a pop-up appears at the bottom of the browser; click **Open**.
33. If the **How do you want to open this file?** pop-up appears, choose any browser (here, **Firefox**) to view the downloaded HTML file.
34. The Nessus scan report appears in the **Firefox** web browser, as shown in the screenshot.

Screenshots and browser might differ in your lab environment.

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


Local Network
file:///C:/Users/Admin/Desktop/Local_Network_6xqoxt.html
nessus
Local Network
Tue, 16 Jun 2020 08:24:42 Eastern Standard Time
TABLE OF CONTENTS
Hosts Executive Summary
10.10.10.16
Hosts Executive Summary
10.10.10.16
0
CRITICAL
2
HIGH
15
MEDIUM
0
LOW
Show Details

36. ☐ A list of discovered vulnerabilities appears. You can further click on plugins (here, **130276**) to view more detailed information on the vulnerability

The results might differ in your lab environment.

CRITICAL	HIGH	MEDIUM	LOW

Severity	CVSS	Plugin	Name
HIGH	7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.4	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities
MEDIUM	6.4	125639	PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.
MEDIUM	6.4	134162	PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities
MEDIUM	6.4	135926	PHP 7.2.x < 7.2.30 Multiple Vulnerabilities
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.8	135290	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities
MEDIUM	5.8	127131	PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname

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

Plugins

Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families

CVEs

Newest
Updated
Search

PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remo Vulnerability.

HIGH Nessus Plugin ID 130276

Synopsis

An application installed on the remote host is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP running on the remote web server is prior to 7.1.33, 7.2.x prior to 7.2.24, or 7.3.x prior to 7.3.11. It is, therefore, affected by a remote code execution vulnerability due to insufficient validation of user input. An unauthenticated, remote attacker can exploit this, by sending a specially crafted request, to cause the execution of arbitrary code by breaking the fastcgi_split_path_info directive.

Solution

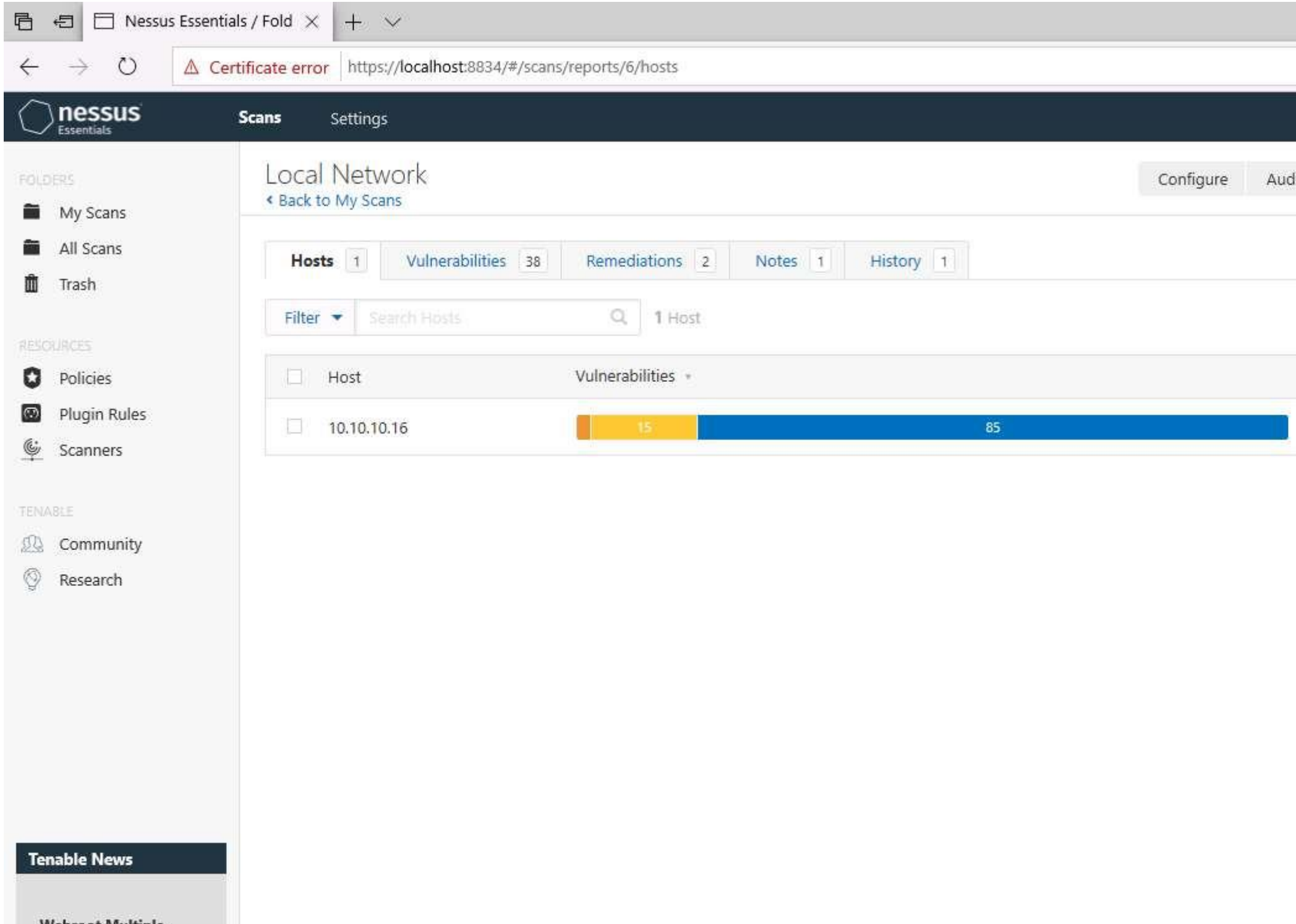
Upgrade to PHP version 7.3.11 or later.

See Also

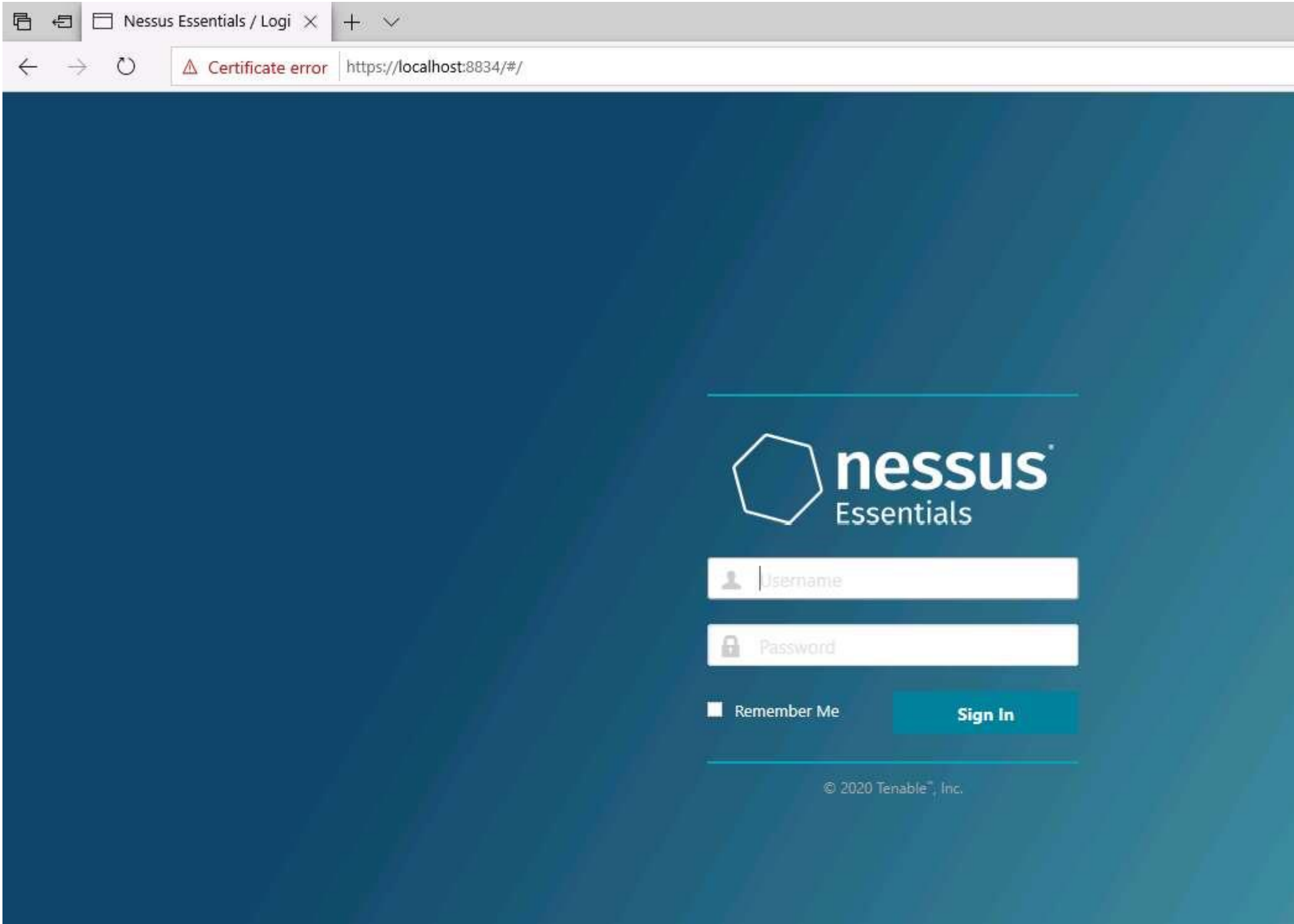
https://www.php.net/ChangeLog-7.php#7.3.11

https://www.php.net/ChangeLog-7.php#7.2.24

38. ☐ In this way, you can select a vulnerability of your choice to view the complete details.
39. ☐ 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.


Nessus Essentials / Fold
Certificate error
https://localhost:8834/#/scans/reports/6/hosts
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Local Network
Back to My Scans
Configure
Aud
Hosts 1
Vulnerabilities 38
Remediations 2
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
10.10.10.16
15
85

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


Nessus Essentials / Logi
Certificate error
https://localhost:8834/#/
nessus
Essentials
Username
Password
Remember Me
Sign In
© 2020 Tenable™, Inc.

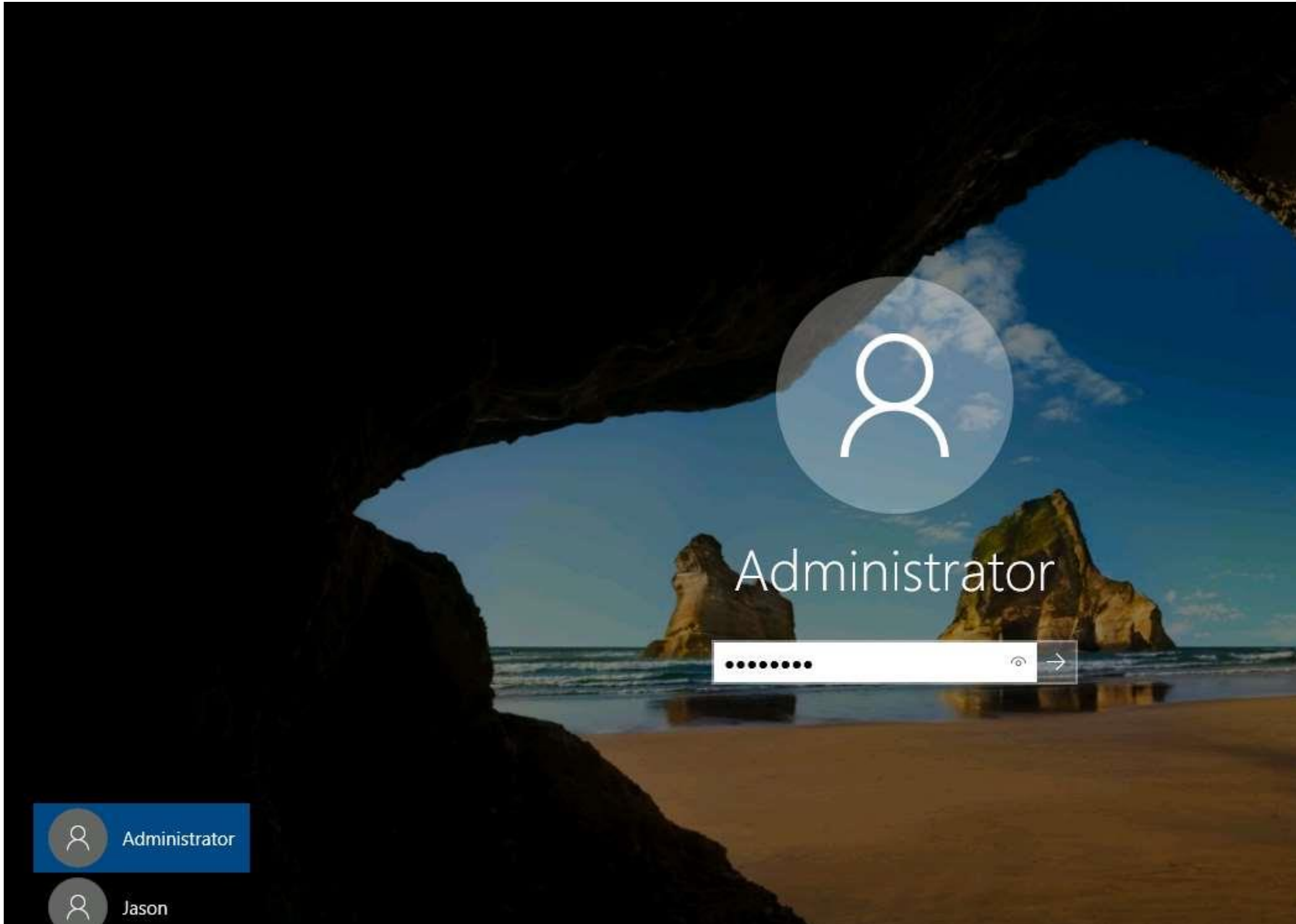
41. ☐ This concludes the demonstration of performing vulnerability assessment using Nessus.
42. ☐ Close all open windows and document all the acquired information.

Task 3: Perform Vulnerability Scanning using GFI LanGuard

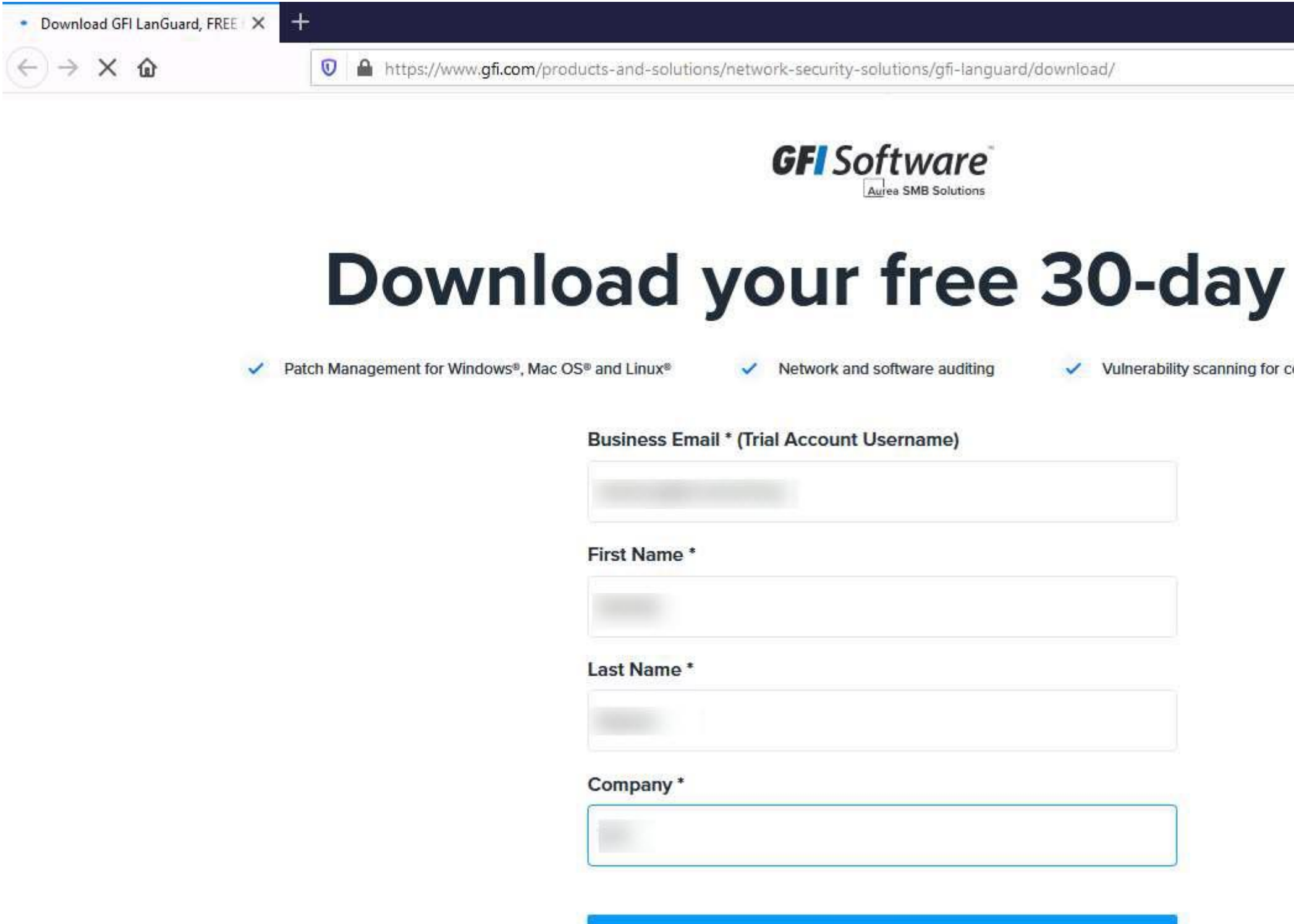
GFI LanGuard scans, detects, assesses, and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort. It scans your OSes, virtual environments, and installed applications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

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

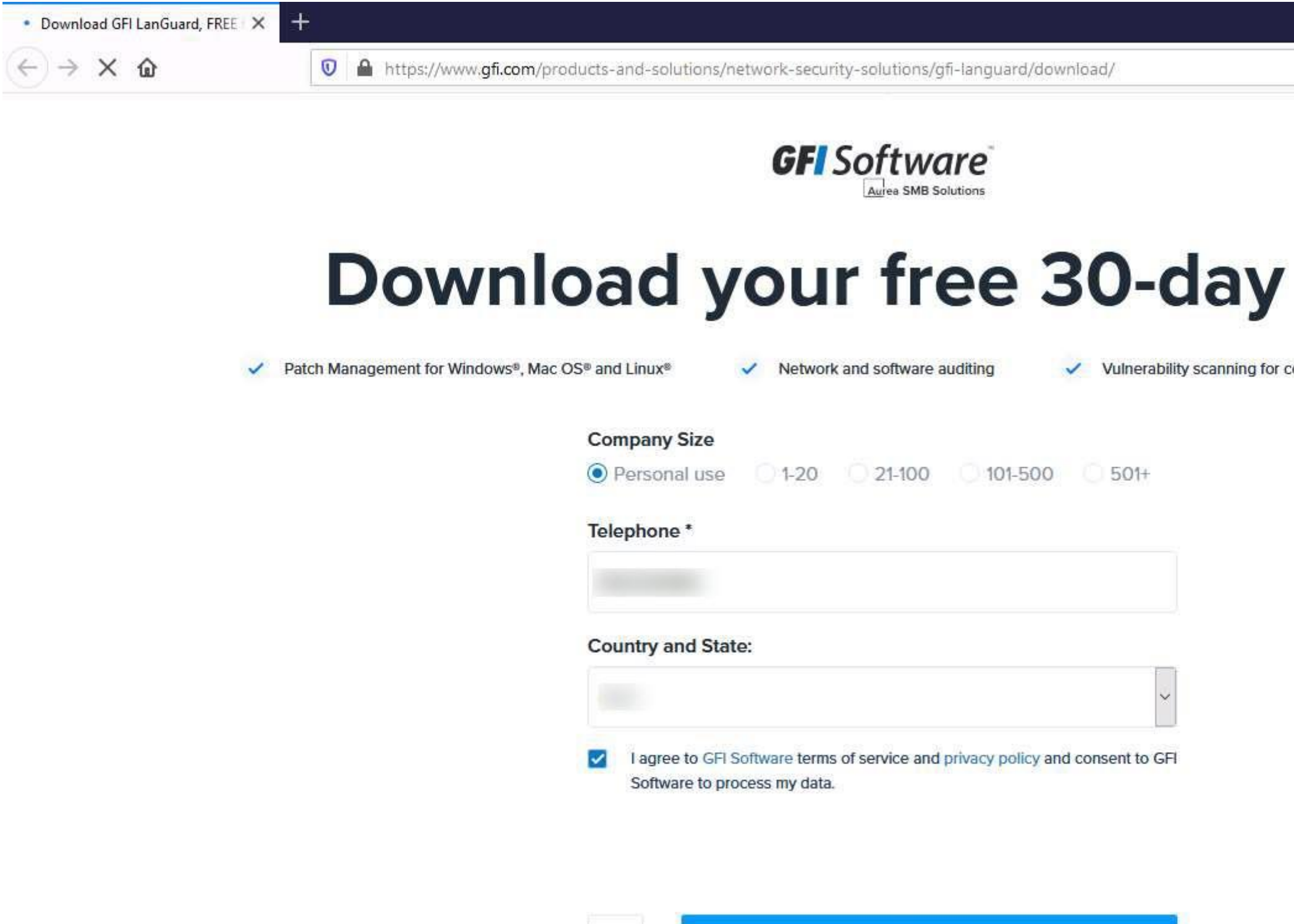
1. ☐ Click on Windows Server 2019 to switch to the **Windows Server 2019** machine, click Ctrl+Alt+Delete to activate the machine. By default, **Administrator** user account is selected and click on Pa$$w0rd to enter the password and press **Enter**.

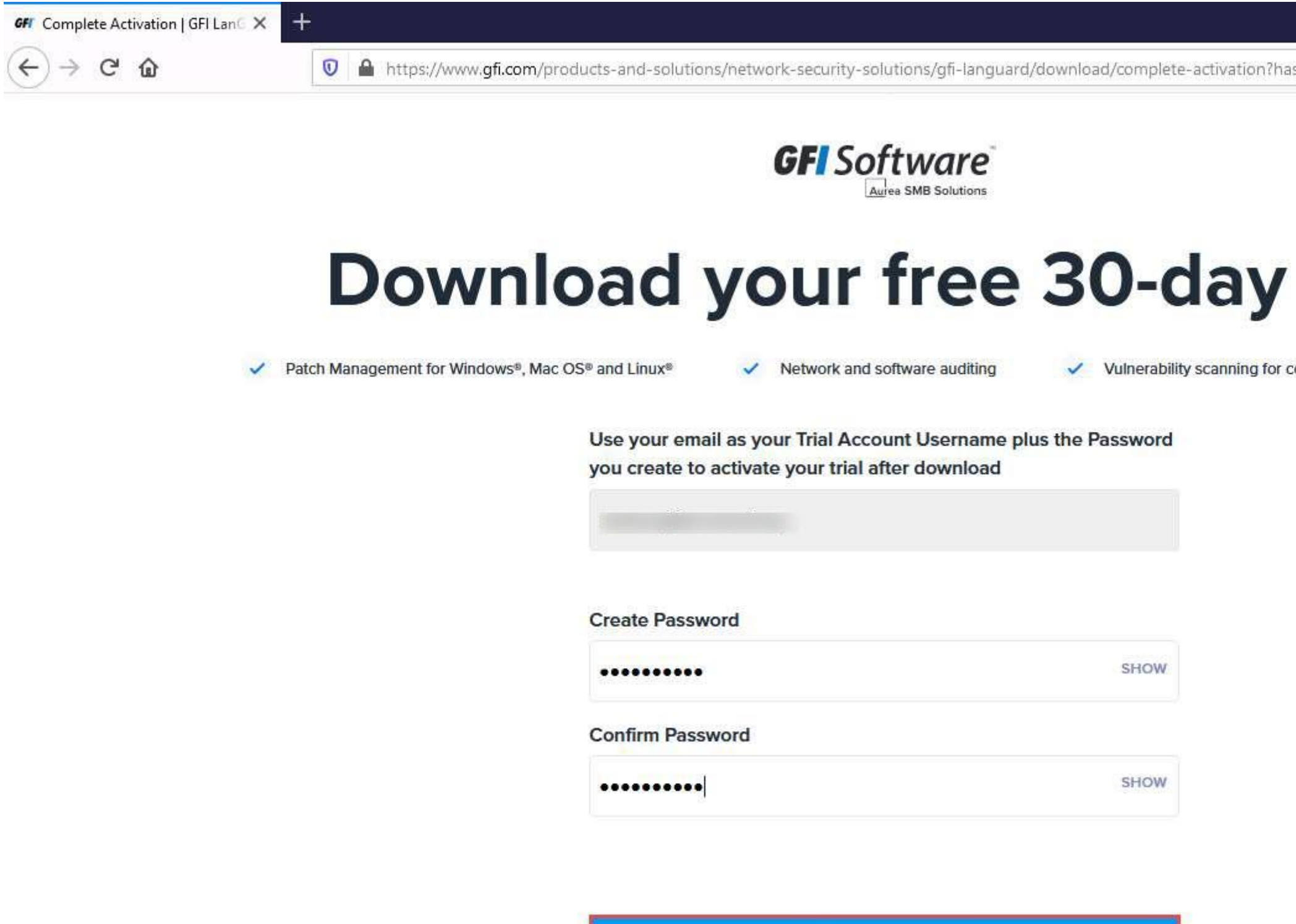

Administrator
Administrator
Jason

2. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/ and press **Enter**
3. The **GFI LanGuard** registration page appears. Enter your details and business email under the **Business Email** field and click **Continue**.


Download GFI LanGuard, FREE
https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/
GFI Software
Aurea SMB Solutions
Download your free 30-day
Patch Management for Windows®, Mac OS® and Linux®
Network and software auditing
Vulnerability scanning for c
Business Email * (Trial Account Username)
First Name *
Last Name *
Company *

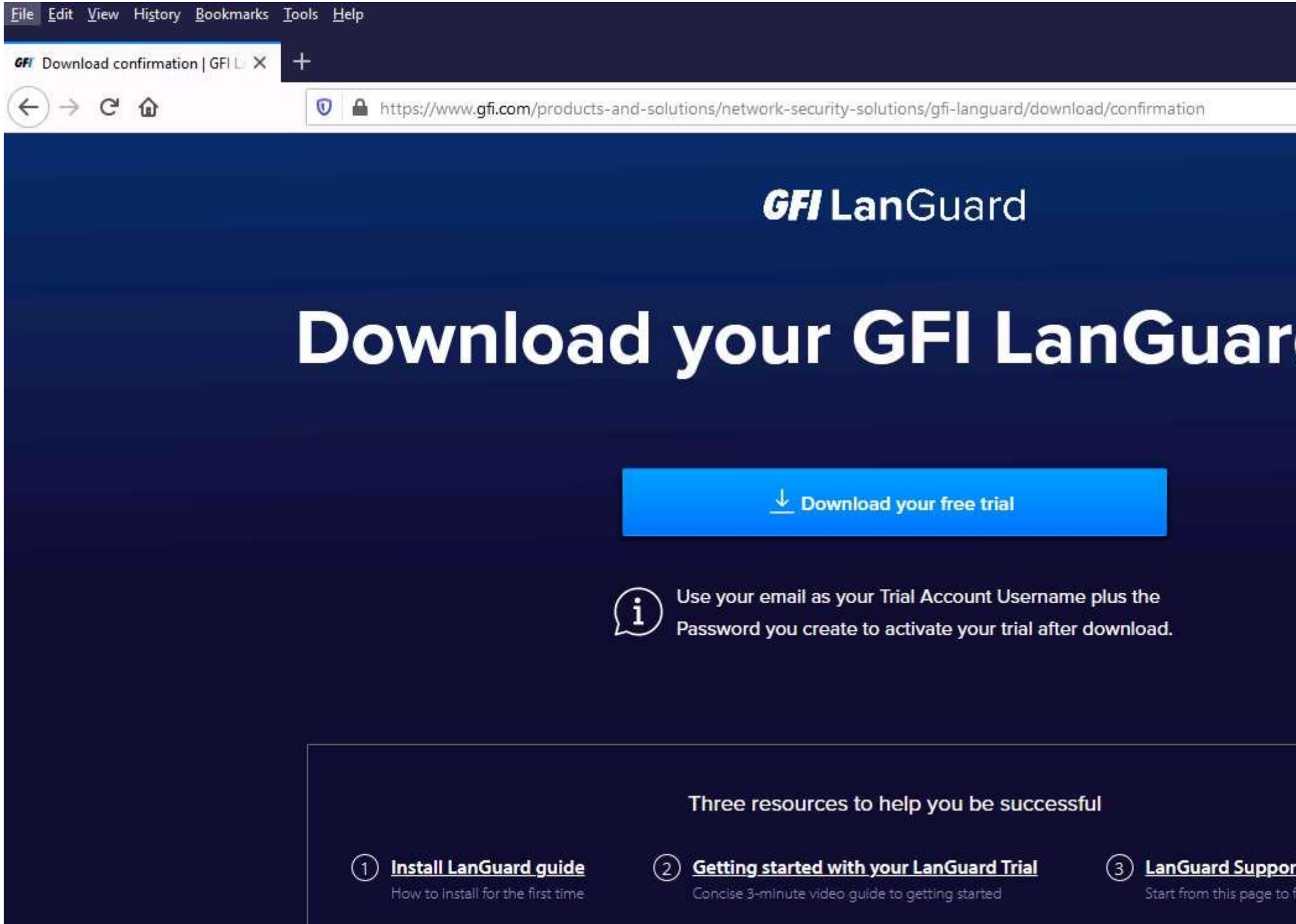
4. On the next page, enter the required details and select the **I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process data** checkbox and click **Start my free trial**


Download GFI LanGuard, FREE
https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/
GFI Software
Aurea SMB Solutions
Download your free 30-day
Patch Management for Windows®, Mac OS® and Linux®
Network and software auditing
Vulnerability scanning for c
Company Size
Personal use
1-20
21-100
101-500
501+
Telephone *
Country and State:
I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process my data.


Complete Activation | GFI Lan
https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/complete-activation?has
GFI Software
Aurea SMB Solutions
Download your free 30-day
Patch Management for Windows®, Mac OS® and Linux®
Network and software auditing
Vulnerability scanning for c
Use your email as your Trial Account Username plus the Password you create to activate your trial after download
Create Password
SHOW
Confirm Password
SHOW

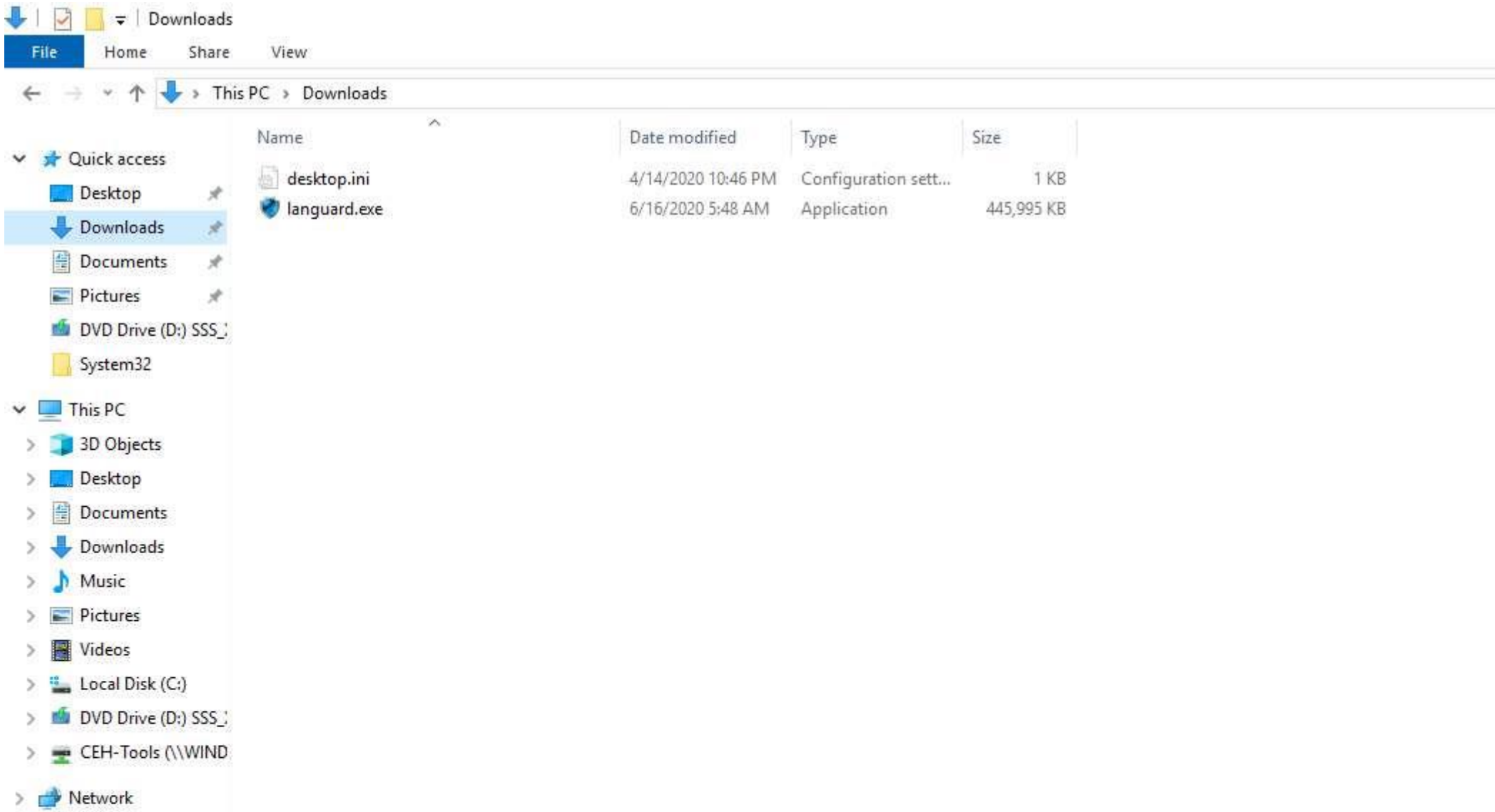
5. The **Download your GFI LanGuard trial** page appears; click the **Download your free trial** button.

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

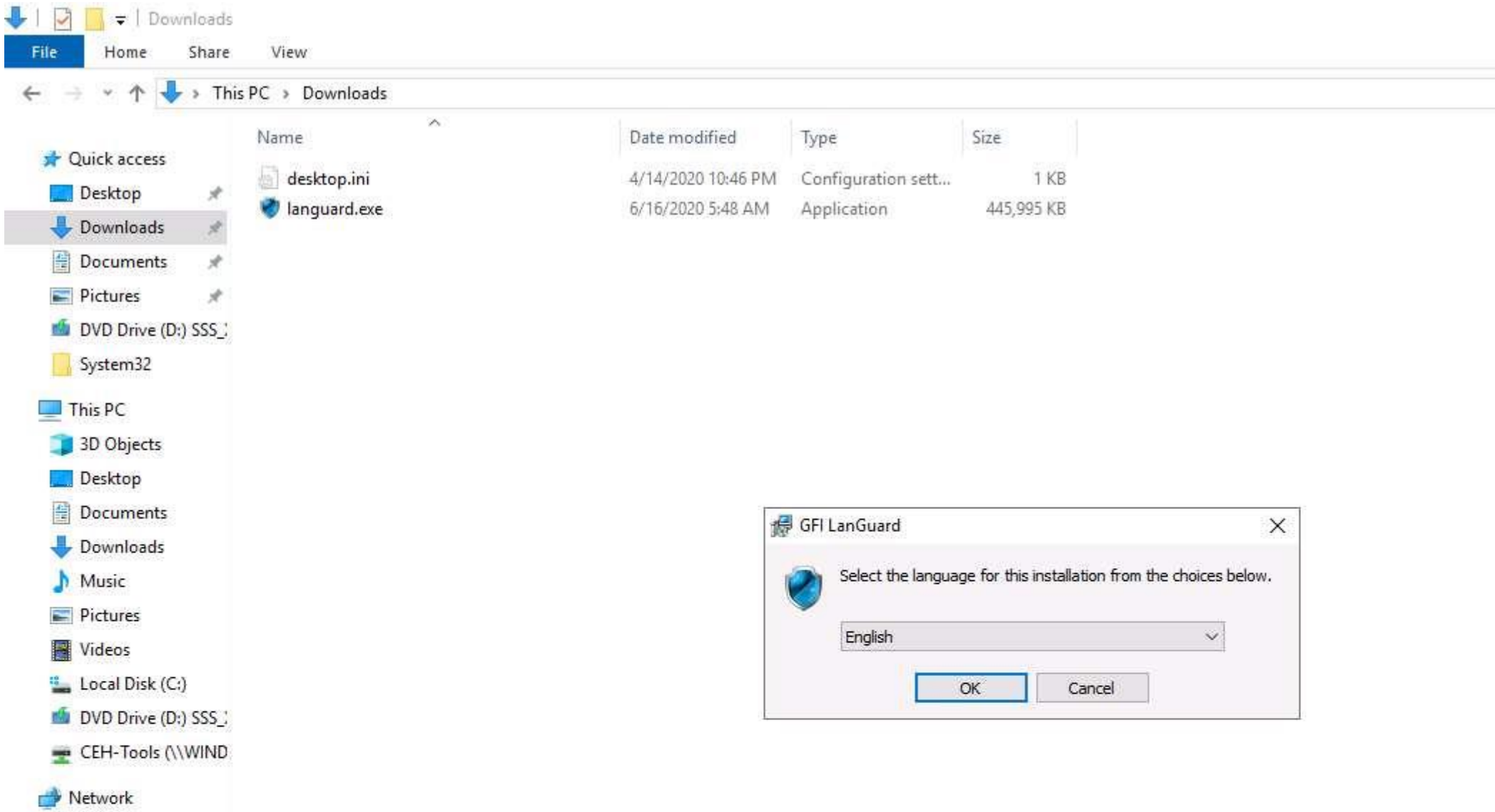

File Edit View History Bookmarks Tools Help
Download confirmation | GFI L
https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/confirmation
GFI LanGuard
Download your GFI LanGuar
Download your free trial
Use your email as your Trial Account Username plus the
Password you create to activate your trial after download.
Three resources to help you be successful
1 Install LanGuard guide
How to install for the first time
2 Getting started with your LanGuard Trial
Concise 3-minute video guide to getting started
3 LanGuard Suppor
Start from this page to

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

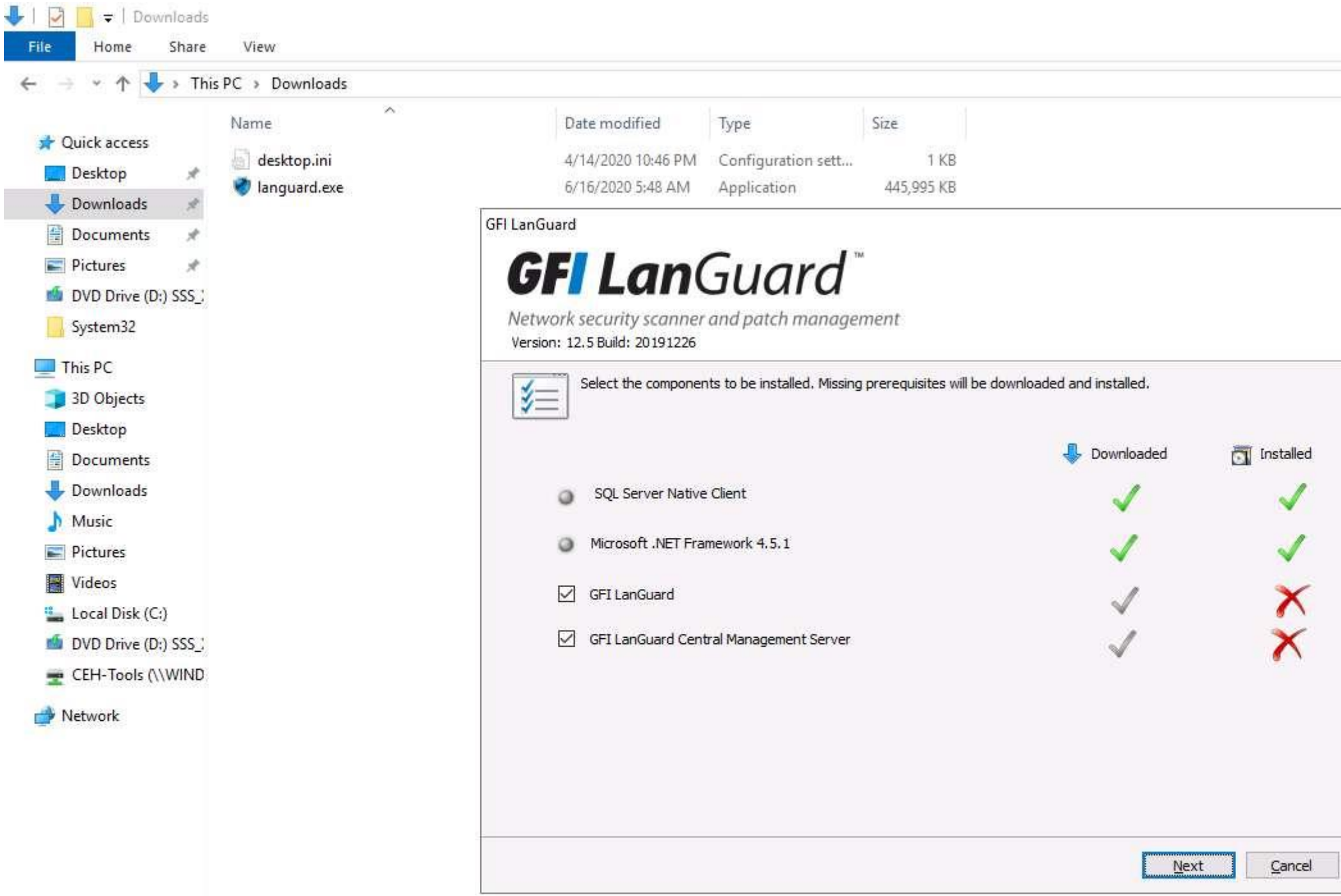
   If the **User File - Security Warning** pop-up appears, click **Run**.


Downloads
File
Home
Share
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
desktop.ini
4/14/2020 10:46 PM
Configuration sett...
1 KB
languard.exe
6/16/2020 5:48 AM
Application
445,995 KB

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

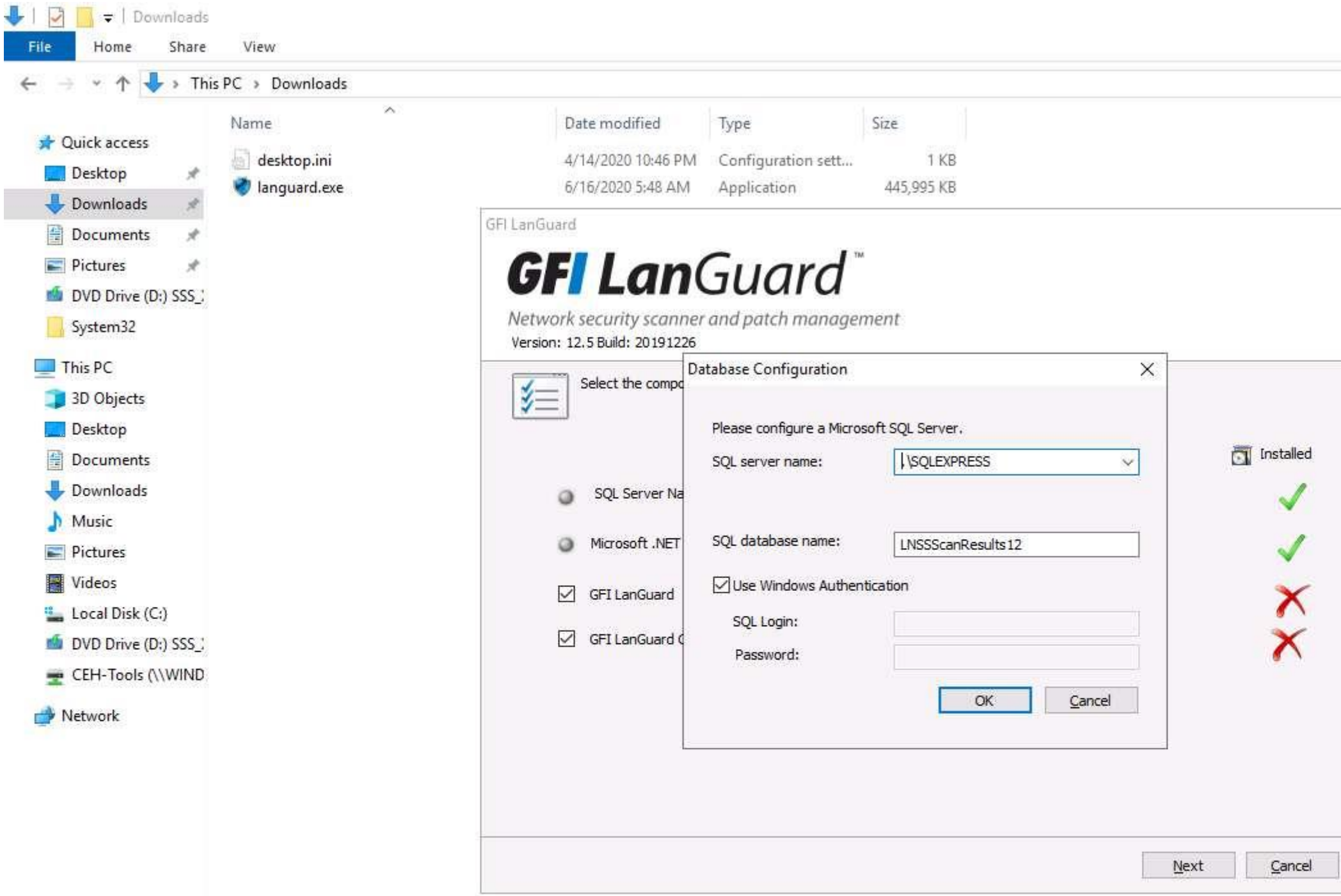

Downloads
File
Home
Share
View
This PC › Downloads
Name
Date modified
Type
Size
desktop.ini
4/14/2020 10:46 PM
Configuration sett...
1 KB
languard.exe
6/16/2020 5:48 AM
Application
445,995 KB
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
GFI LanGuard
Select the language for this installation from the choices below.
English
OK
Cancel

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

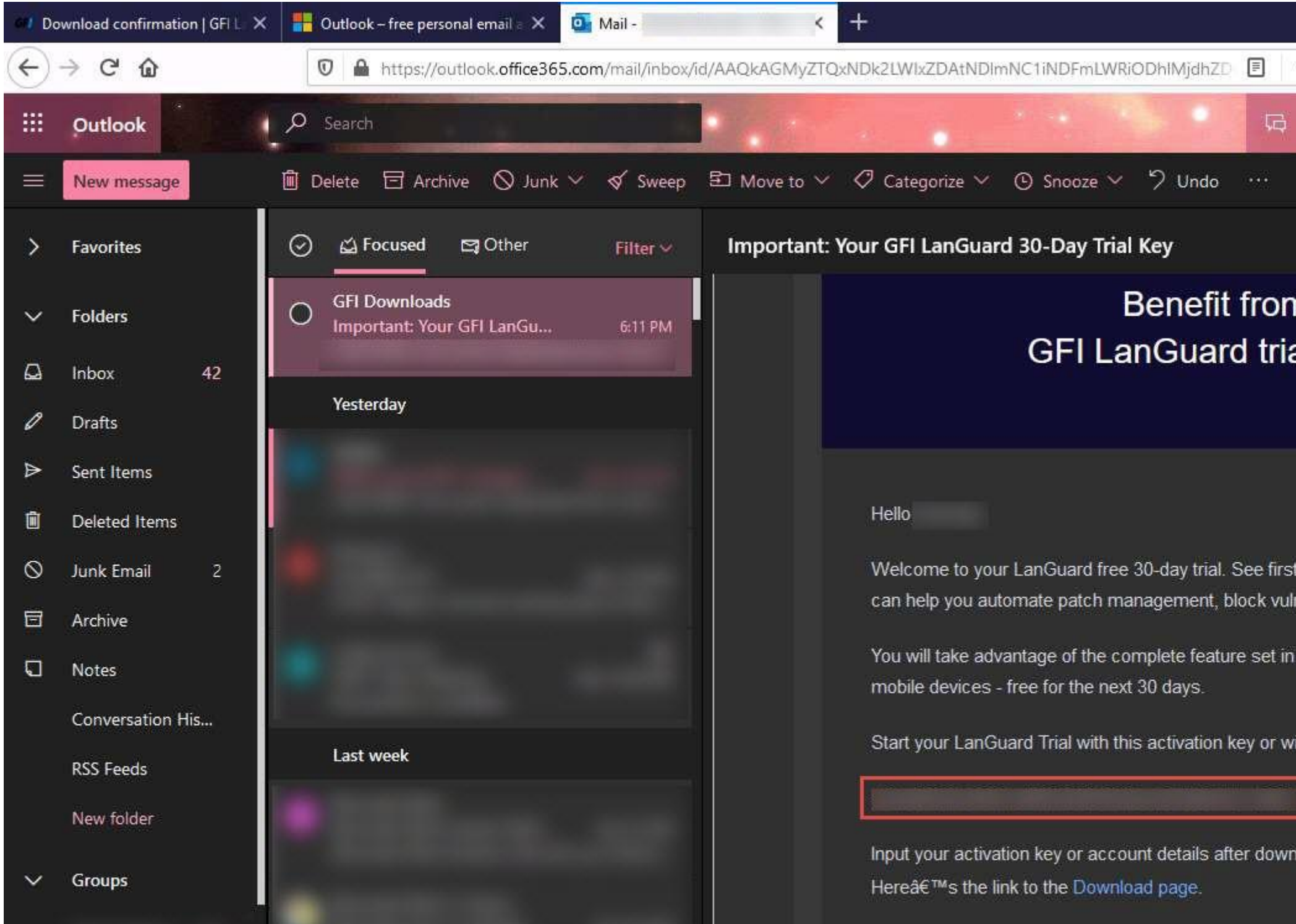

Downloads
File
Home
Share
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
desktop.ini
4/14/2020 10:46 PM
Configuration sett...
1 KB
languard.exe
6/16/2020 5:48 AM
Application
445,995 KB
GFI LanGuard
GFI LanGuard
Network security scanner and patch management
Version: 12.5 Build: 20191226
Select the components to be installed. Missing prerequisites will be downloaded and installed.
Downloaded
Installed
SQL Server Native Client
Microsoft .NET Framework 4.5.1
GFI LanGuard
GFI LanGuard Central Management Server
Next
Cancel

9. 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**.

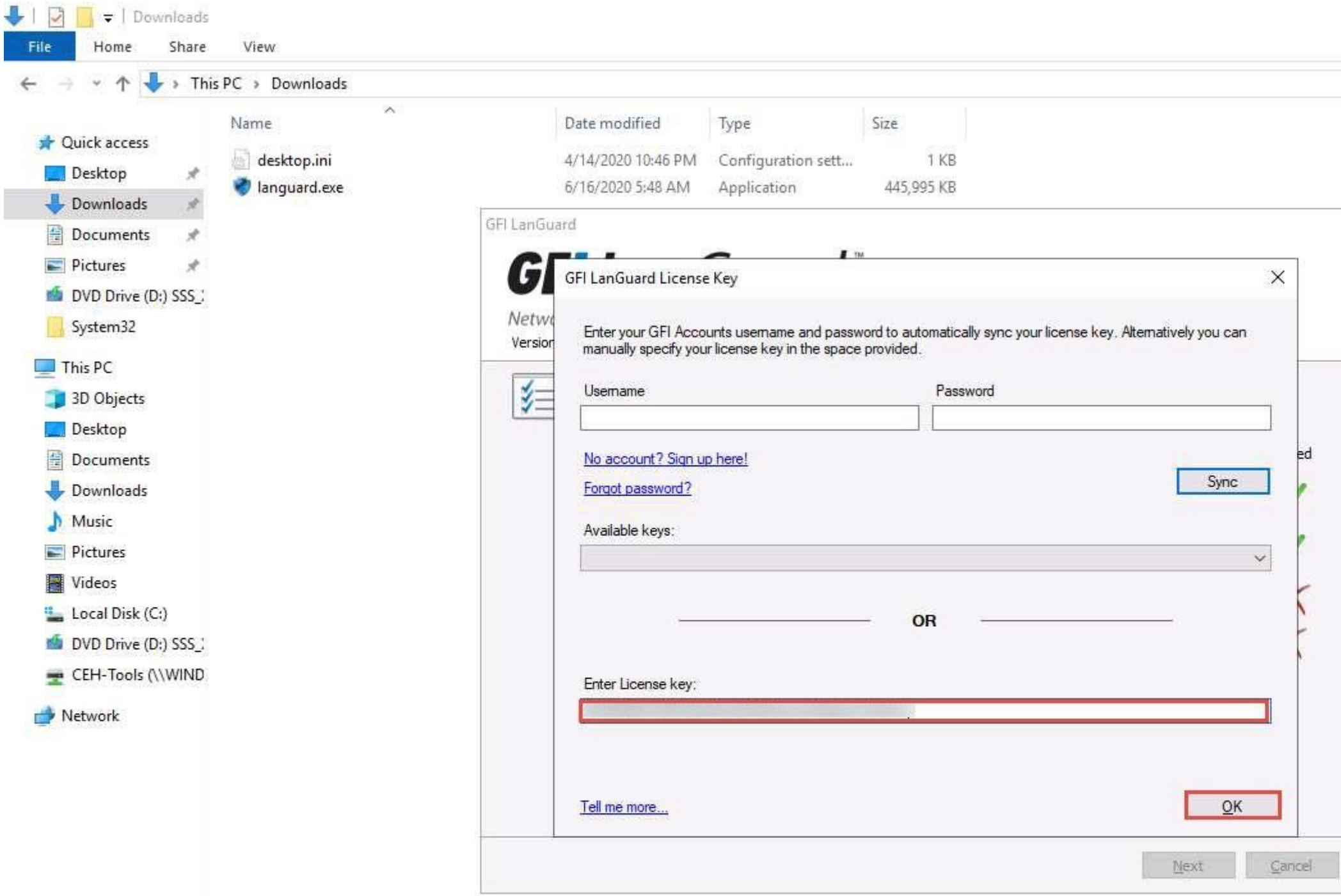
> The SQL server name might differ in your lab environment.


Downloads
File
Home
Share
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
desktop.ini
4/14/2020 10:46 PM
Configuration sett...
1 KB
languard.exe
6/16/2020 5:48 AM
Application
445,995 KB
GFI LanGuard
GFI LanGuard
Network security scanner and patch management
Version: 12.5 Build: 20191226
Select the compo
SQL Server Na
Microsoft .NET
GFI LanGuard
GFI LanGuard C
Installed
Database Configuration
Please configure a Microsoft SQL Server.
SQL server name:
\SQLEXPRESS
SQL database name:
LNSSScanResults12
Use Windows Authentication
SQL Login:
Password:
OK
Cancel
Next
Cancel

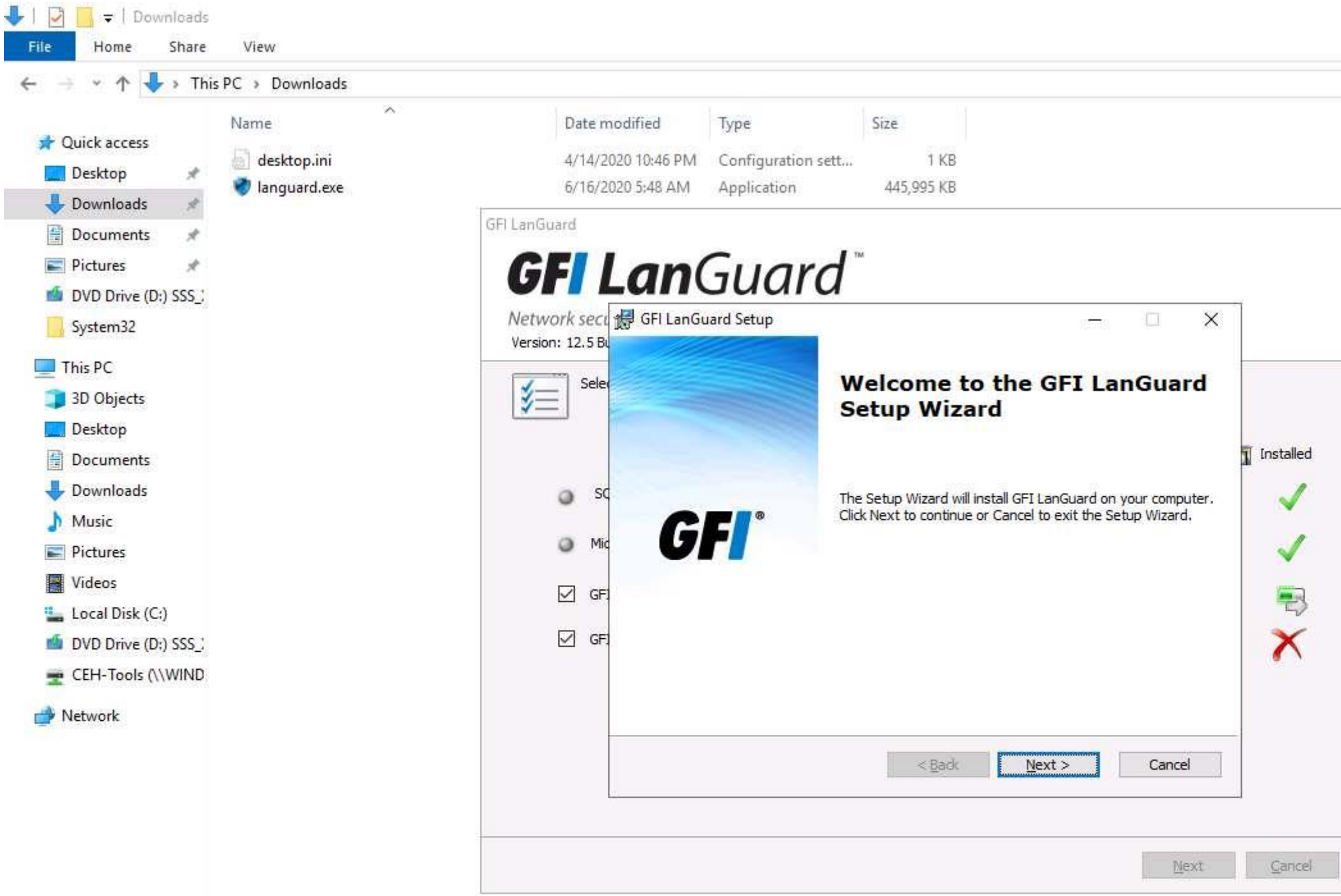
10. ☐ Now, switch back to the **Mozilla Firefox** browser, open a new tab, and log in to your email account that you have given while registration.
11. ☐ Open an email from **GFI Downloads** and copy the activation key.


Download confirmation | GFI L
Outlook – free personal email a
Mail -
https://outlook.office365.com/mail/inbox/id/AAQkAGMyZTQxNDk2LWIxZDAtNDImNC1iNDFmLWRiODhlMjdhZD
Outlook
Search
New message
Delete
Archive
Junk
Sweep
Move to
Categorize
Snooze
Undo
Favorites
Folders
Inbox 42
Drafts
Sent Items
Deleted Items
Junk Email 2
Archive
Notes
Conversation His...
RSS Feeds
New folder
Groups
Focused
Other
Filter
GFI Downloads
Important: Your GFI LanGu...
6:11 PM
Yesterday
Last week
Important: Your GFI LanGuard 30-Day Trial Key
Benefit from
GFI LanGuard tria
Hello
Welcome to your LanGuard free 30-day trial. See first
can help you automate patch management, block vul
You will take advantage of the complete feature set in
mobile devices - free for the next 30 days.
Start your LanGuard Trial with this activation key or w
Input your activation key or account details after down
Hereâ€™s the link to the Download page.

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

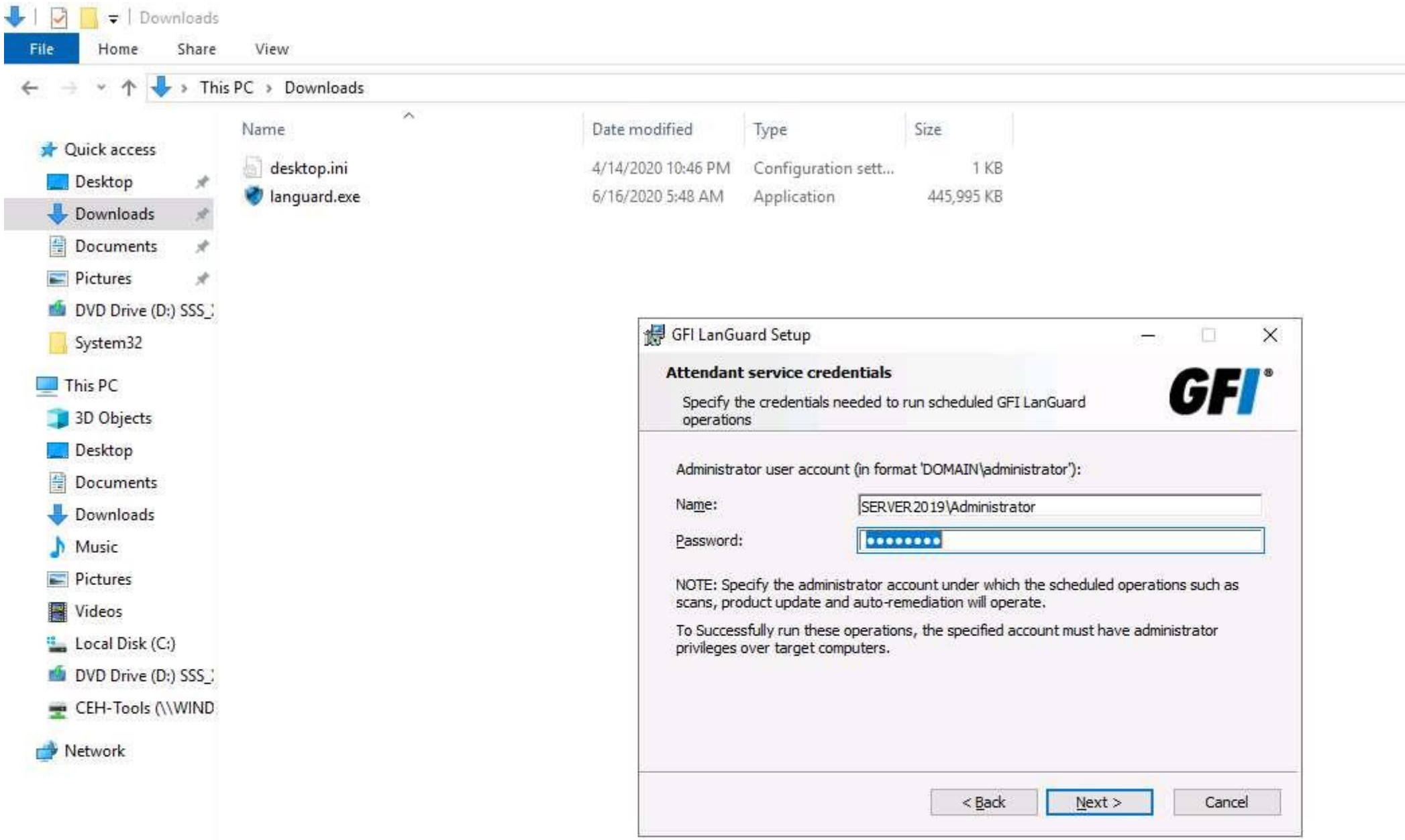

Downloads
File
Home
Share
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
desktop.ini
4/14/2020 10:46 PM
Configuration sett...
1 KB
languard.exe
6/16/2020 5:48 AM
Application
445,995 KB
GFI LanGuard
GFI LanGuard License Key
Enter your GFI Accounts username and password to automatically sync your license key. Alternatively you can manually specify your license key in the space provided.
Username
Password
No account? Sign up here!
Forgot password?
Sync
Available keys:
OR
Enter License key:
Tell me more...
OK
Next
Cancel

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


Downloads
File
Home
Share
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
desktop.ini
4/14/2020 10:46 PM
Configuration sett...
1 KB
languard.exe
6/16/2020 5:48 AM
Application
445,995 KB
GFI LanGuard
GFI LanGuard
Network secu
Version: 12.5 Bu
GFI LanGuard Setup
Welcome to the GFI LanGuard Setup Wizard
The Setup Wizard will install GFI LanGuard on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
< Back
Next >
Cancel
Installed
Next
Cancel

14. ☐ The **End-User License Agreement** wizard appears; accept the terms and click **Next**.
15. ☐ 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**.

> The Name field might differ in your lab environment.


Downloads
File
Home
Share
View
This PC › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
desktop.ini
4/14/2020 10:46 PM
Configuration sett...
1 KB
languard.exe
6/16/2020 5:48 AM
Application
445,995 KB
GFI LanGuard Setup
Attendant service credentials
Specify the credentials needed to run scheduled GFI LanGuard operations
GFI
Administrator user account (in format 'DOMAIN\administrator'):
Name:
SERVER2019\Administrator
Password:
NOTE: Specify the administrator account under which the scheduled operations such as scans, product update and auto-remediation will operate.
To Successfully run these operations, the specified account must have administrator privileges over target computers.
< Back
Next >
Cancel

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

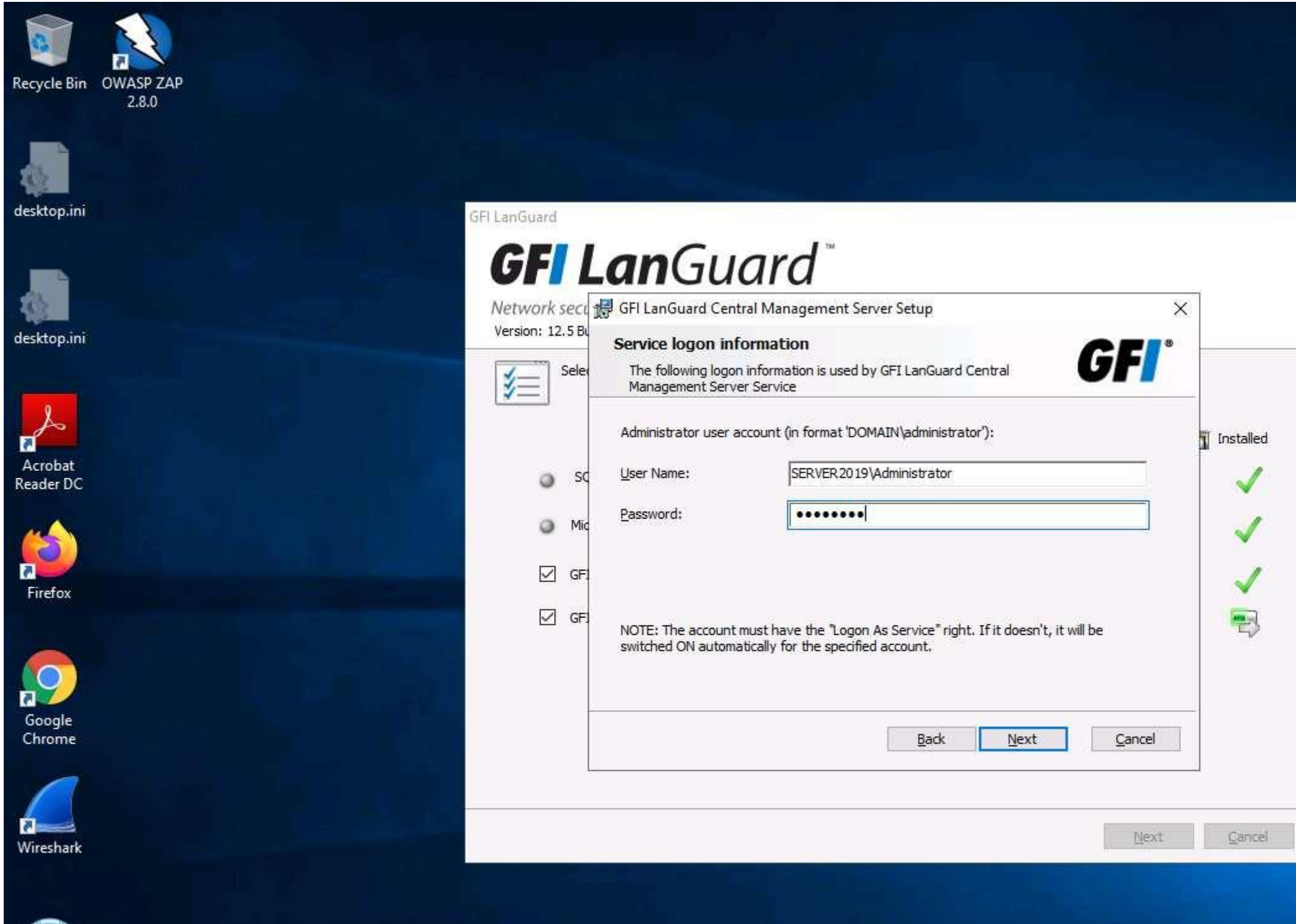

Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
GFI LanGuard
GFI LanGuard
Network secu
Version: 12.5 Bu
GFI LanGuard Setup
Choose Destination Location
Select the folder where setup will install files.
Setup will install GFI LanGuard in the following folder.
To install in this folder, click "Install". To install to a different folder, click "Browse" and select another folder.
Folder:
C:\Program Files (x86)\GFI\LanGuard 12\
Browse...
< Back
Install
Cancel
Installed
Next
Cancel

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


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
GFI LanGuard
GFI LanGuard
Network secu
Version: 12.5 Bu
GFI LanGuard Central Management Server Setup
Welcome to the GFI LanGuard Central Management Server Setup Wizard
The Setup Wizard will install GFI LanGuard Central Management Server on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel
Installed
Next
Cancel

18. 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**.

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


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
GFI LanGuard
GFI LanGuard
Network secu
Version: 12.5 Bu
GFI LanGuard Central Management Server Setup
Service logon information
The following logon information is used by GFI LanGuard Central Management Server Service
GFI
Administrator user account (in format 'DOMAIN\administrator'):
User Name:
SERVER2019\Administrator
Password:
NOTE: The account must have the "Logon As Service" right. If it doesn't, it will be switched ON automatically for the specified account.
Back
Next
Cancel
Installed
Next
Cancel

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

> The name field might differ in your lab environment.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
GFI LanGuard
GFI LanGuard
Network secu
Version: 12.5 Bu
GFI LanGuard Central Management Server HTTPS Settings
HTTPS Settings
Use this address when connecting to GFI LanGuard Central Management Server.
GFI
Name of the HTTPS server:
server2019
Installed
Back
Next
Cancel
Next
Cancel

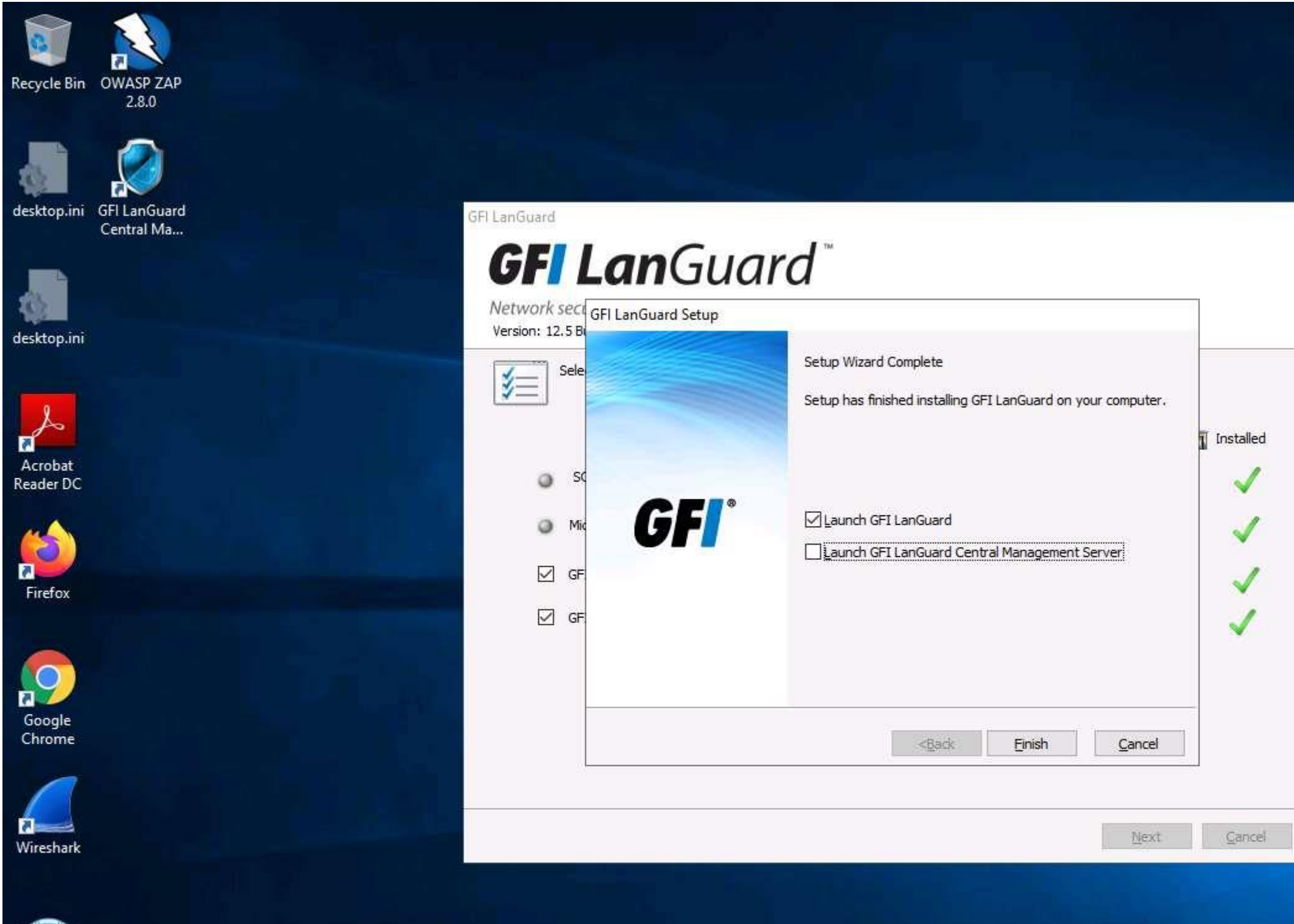
20. In the **Destination Folder** wizard, choose the location where you want to install the application (here, the default location is selected) and click **Next**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
GFI LanGuard
GFI LanGuard
Network secu
Version: 12.5 Bu
GFI LanGuard Central Management Server Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install GFI LanGuard Central Management Server to:
C:\Program Files (x86)\GFI\LanGuard 12 Server\
Change...
Back
Next
Cancel
Installed
Next
Cancel

21. In the **Ready to install** wizard, click **Install** to proceed.
22. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
GFI LanGuard Central Ma...
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
GFI LanGuard
GFI LanGuard
Version: 12.5 Bu
GFI LanGuard Central Management Server Setup
Completed the GFI LanGuard Central Management Server Setup Wizard
Click the Finish button to exit the Setup Wizard.
In order to connect to GFI LanGuard Central Management Server use address: https://server2019:1077
Back
Finish
Cancel
Installed
Next
Cancel

23. 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**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
GFI LanGuard Central Ma...
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
GFI LanGuard
GFI LanGuard
Network sec
Version: 12.5 B
GFI LanGuard Setup
Setup Wizard Complete
Setup has finished installing GFI LanGuard on your computer.
Launch GFI LanGuard
Launch GFI LanGuard Central Management Server
Installed
<Back
Finish
Cancel
Next
Cancel

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

GFI LanGuard

Dashboard Scan Remediate Activity Monitor Reports Configuration Utilities

Welcome to GFI LanGuard

GFI LanGuard is ready to audit your network for vulnerabilities

Network Vulnerability Level

View security status of the network. Click on it for details.

Current Vulnerability Level is: Not Available

View Dashboard

Investigate network vulnerability status and audit results.

GFI LanGuard

Trial period will expire in 30 days!
On expiry network vulnerability auditing & remediation features will no longer work.

License limitations	:	**Auditing restricted to 25 nodes + 25 nodes exclusively for mobile devices.***
License key	:	xtQwBRzik-MSR-nffNFbX9FtRQhxnWQBeHH-10001 (Edit...)
License type	:	30-day trial license (expires on 7/16/2020)
License usage	:	0 nodes (50 free)
Patches/Updates deployed	:	0 updates (0 target computers)
Vulnerabilities discovered	:	0 vulnerabilities (0 Critical / High)

*Contact your preferred reseller to request additional nodes/evaluation days or to buy now.

Locate reseller | Continue evaluation

LATEST NEWS

16-Jun-2020 - Vulnerability Database - List of supported OVAL checks - Read more

16-Jun-2020 - Patch Management Database - List of supported Microsoft security updates - Read more

25. ☐ The **GFI LanGuard** main window appears, and it begins to inspect the security status of the local computer.
26. ☐ Click **Launch a Scan** or **View details**.

GFI LanGuard

Dashboard Scan Remediate Activity Monitor Reports Configuration Utilities

Welcome to GFI LanGuard

GFI LanGuard is ready to audit your network for vulnerabilities

Local Computer Vulnerability Level

GFI LanGuard is inspecting security status of the local computer .

View details

View Dashboard

Investigate network vulnerability status and audit results.

Remediate Security Issues

Deploy missing patches, uninstall unauthorized software, turn on antivirus and more.

Manage Agents

Enable agents to automate network security audit and to distribute scanning load across client machin

Launch a Scan

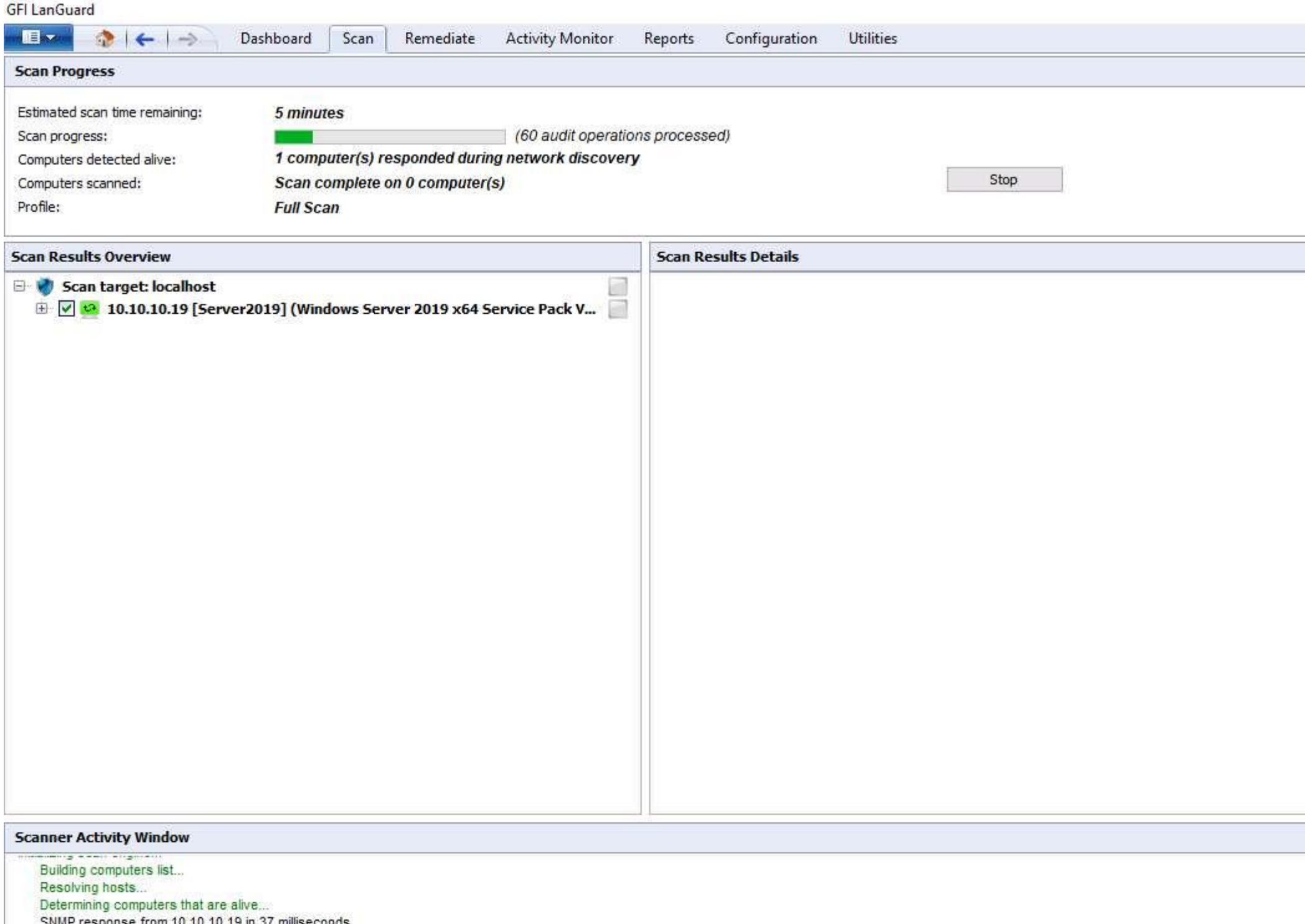
Manually set-up and trigger an agentless network security audit.

LATEST NEWS

16-Jun-2020 - Vulnerability Database - List of supported OVAL checks - Read more

16-Jun-2020 - Patch Management Database - List of supported Microsoft security updates - Read more

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


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Scan Progress
Estimated scan time remaining:
5 minutes
Scan progress:
(60 audit operations processed)
Computers detected alive:
1 computer(s) responded during network discovery
Computers scanned:
Scan complete on 0 computer(s)
Profile:
Full Scan
Stop
Scan Results Overview
Scan target: localhost
10.10.10.19 [Server2019] (Windows Server 2019 x64 Service Pack V...
Scan Results Details
Scanner Activity Window
Building computers list...
Resolving hosts...
Determining computers that are alive...
SNMP response from 10.10.10.19 in 37 milliseconds

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

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

The scan might take time to stop.

29. The **Launch a New Scan** page appears: specify the details required to scan a target/machine as follows:
    - Enter the IP address of the 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**.

GFI LanGuard

Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities

Launch a New Scan

Scan Target: 10.10.10.16 ...

Profile: Full Scan

Credentials: Currently logged on user

Username: Password: Key file: ... Scan

Scan Options...

Scan Results Overview

- **Scan target: localhost**
  - 10.10.10.19 [Server2019] (Windows Server 2019 x64 Service Pack V...

Scan Results Details

Scan was stopped by the user!

Summary of scan results generated during this network audit.

Vulnerability level:

This computer does not have a Vulnerability Level assigned.

Possible reasons:

Results statistics:

Audit operations processed:
Open ports:
Open shares:
Services:

Times:

Computers scanned:
Total scan time:
Average scan time per machine:
Minimum scan time:
Maximum scan time:

Vulnerability level listing:

High:

This may vary in your lab environment.

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

GFI LanGuard

Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities

Scan Progress

Estimated scan time remaining:	*5 minutes*
Scan progress:	*(12 audit operations processed)*
Computers detected alive:	*1 computer(s) responded during network discovery*
Computers scanned:	*Scan complete on 0 computer(s)*
Profile:	*Full Scan*

Stop

Scan Results Overview

- **Scan target: 10.10.10.16**
  - **10.10.10.16**

Scan Results Details

Scanner Activity Window

Building computers list...
Resolving hosts...
Determining computers that are alive...
NetBIOS reply from 10.10.10.16 (SERVER2016) in 93 milliseconds

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

The scanning takes approximately 20–30 minutes to complete.

GFI LanGuard

Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities

Launch a New Scan

Scan Target: 10.10.10.16 ...

Profile: Full Scan

Credentials: Currently logged on user

Username: Password: Key file: ... Scan

Scan Options...

Scan Results Overview

Scan target: 10.10.10.16

10.10.10.16 [SERVER2016] (Windows Server 2016 x64 Version 1607)

Scan Results Details

Scan completed!

Summary of scan results generated during this network audit.

Vulnerability level:

The average vulnerability level for this scanning session is: **High**

Results statistics:

Audit operations processed:
Other vulnerabilities:
Potential vulnerabilities:
Installed applications:
Open ports:

Errors:

Errors encountered during scan:

Times:

Computers scanned:

Scanner Activity Window

Time	Computer	Operation	Error Message
6/16/2020 6:50:16 AM	SERVER2016	UDP ports scanning	UDP scan is not reliable on this machine
6/16/2020 7:01:41 AM	SERVER2016	Missing patches scan	The patch management database is unavailable

32. 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.

The results might differ in your lab environment.

GFI LanGuard

Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities

Launch a New Scan

Scan Target: 10.10.10.16 ...

Profile: Full Scan

Credentials: Currently logged on user

Username: Password: Key file: ... Scan

Scan Options...

Scan Results Overview

- Scan target: 10.10.10.16
  - 10.10.10.16 [SERVER2016] (Windows Server 2016 x64 Version 1607)
    - Vulnerability Assessment
    - Network & Software Audit

Scan Results Details

10.10.10.16 [SERVER2016] (Windows Server 2016 x64)

Microsoft Hyper-V

Vulnerability level:

The average vulnerability level for this scanning session is: **High**

Top 5 issues to address:

- SNMP service is enabled on this host
- AutoRun is enabled
- OVAL:22538: A router or firewall allows source routed packets from arbitrary hosts (CVE-199
- No supported antivirus product found on this machine!
- No supported antispyware product found on this machine!

Show all vulnerabilities...

Results statistics:

Other vulnerabilities:

Potential vulnerabilities:

Scanner Activity Window

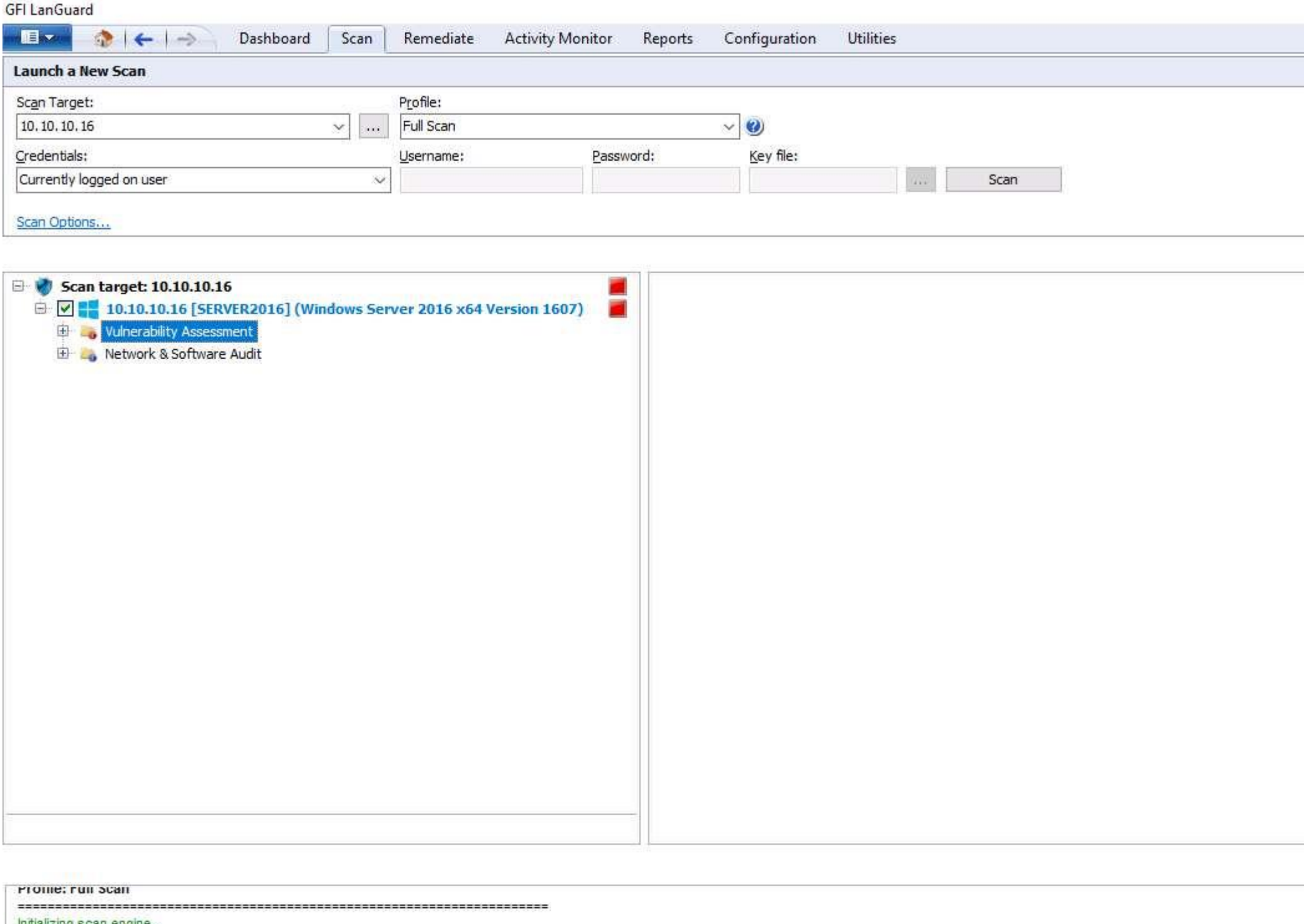
Profile: Full Scan

==========

Initializing scan engine...

==========

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


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Launch a New Scan
Scan Target:
10.10.10.16
Profile:
Full Scan
Credentials:
Currently logged on user
Username:
Password:
Key file:
Scan
Scan Options...
Scan target: 10.10.10.16
10.10.10.16 [SERVER2016] (Windows Server 2016 x64 Version 1607)
Vulnerability Assessment
Network & Software Audit
Profile: Full Scan
Initializing scan engine...

34. ☐ 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.

GFI LanGuard

Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities

Launch a New Scan

Scan Target: 10.10.10.16 ...

Profile: Full Scan

Credentials: Currently logged on user

Username: Password: Key file: ... Scan

Scan Options...

Scan Results Overview

- Scan target: 10.10.10.16
  - 10.10.10.16 [SERVER2016] (Windows Server 2016 x64 Version 1607)
    - Vulnerability Assessment
      - High Security Vulnerabilities (6)
      - Medium Security Vulnerabilities (1)
      - Low Security Vulnerabilities (23)
      - Potential Vulnerabilities (2)
    - Network & Software Audit
      - Ports
        - Open TCP Ports (17)
      - Hardware
      - Software
      - System Information

Scan Results Details

- 53 [Description: Domain Name System (DNS) / Service: Unknown]
- 80 [Description: Hypertext Transfer Protocol (HTTP) / Service: HTTP (Hyper Text Transfer Protocol)]
- 88 [Description: Kerberos - authentication system / Service: Unknown]
- 135 [Description: DCE endpoint resolution / Service: Unknown]
- 139 [Description: NetBIOS Session Service / Service: Unknown]
- 389 [Description: Lightweight Directory Access Protocol (LDAP) / Service: Unknown]
- 445 [Description: Microsoft-DS Active Directory, Windows shares / Service: Unknown]
- 464 [Description: Kerberos Change/Set password / Service: Unknown]
- 593 [Description: HTTP RPC Ep Map, Remote procedure call over Hypertext Transfer Protocol / Serv
- 636 [Description: Lightweight Directory Access Protocol over TLS/SSL (LDAPS) / Service: Unknown]
- 2103 [Description: zephyr-clt Project Athena Zephyr Notification Service serv-hm connection / Servic
- 2105 [Description: IBM MiniPay / Service: Unknown]
- 3268 [Description: msft-gc, Microsoft Global Catalog (LDAP service which contains data from Active
- 3269 [Description: msft-gc-ssl, Microsoft Global Catalog over SSL (similar to port 3268, LDAP over SS
- 3306 [Description: MySQL database system / Service: Unknown]
- 3389 [Description: Terminal Services / Service: Unknown]
- 8080 [Description: HTTP alternate (http_alt) / Service: HTTP (Hyper Text Transfer Protocol)]

Scanner Activity Window

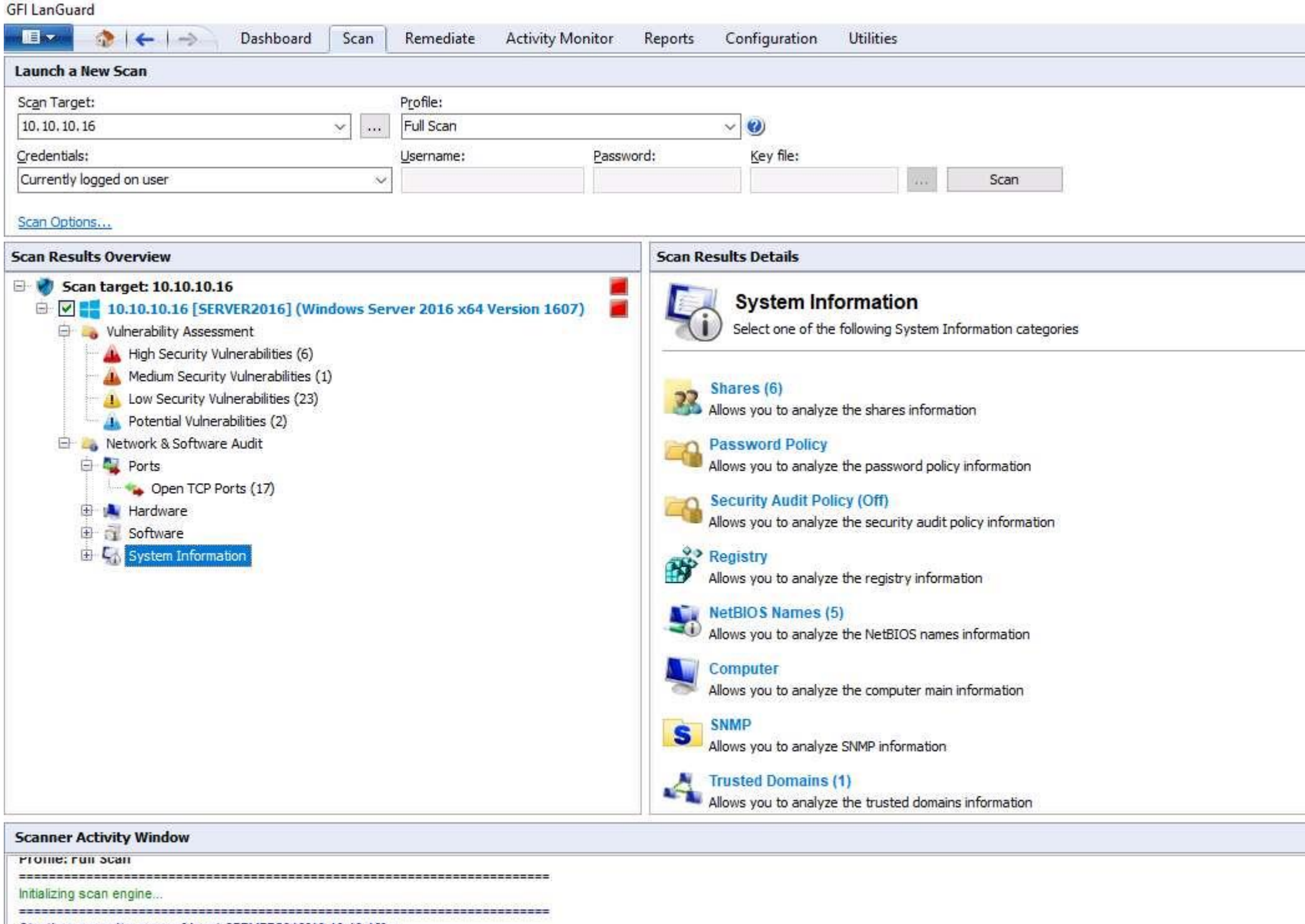
Profile: Full Scan

==========

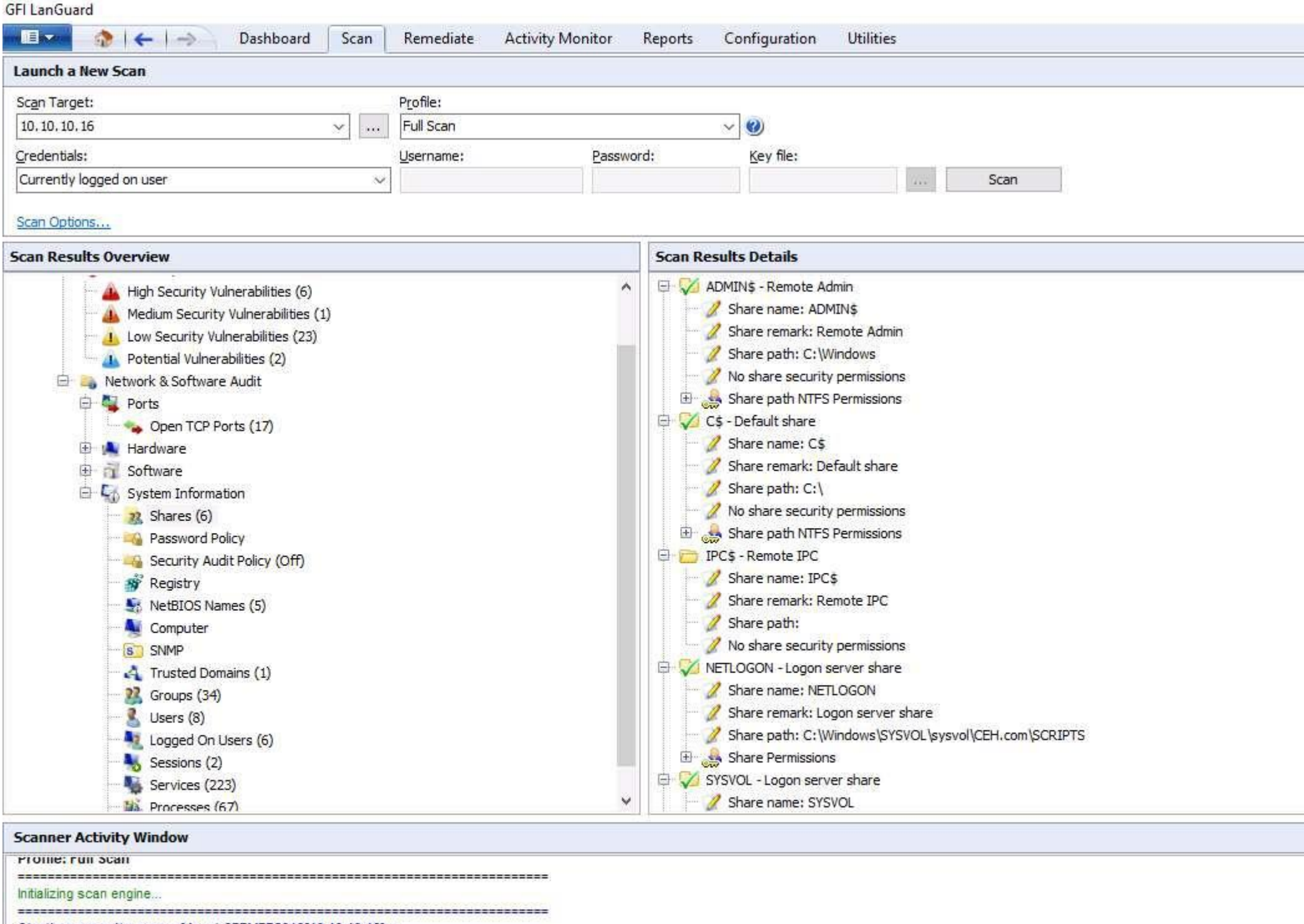
Initializing scan engine...

==========

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

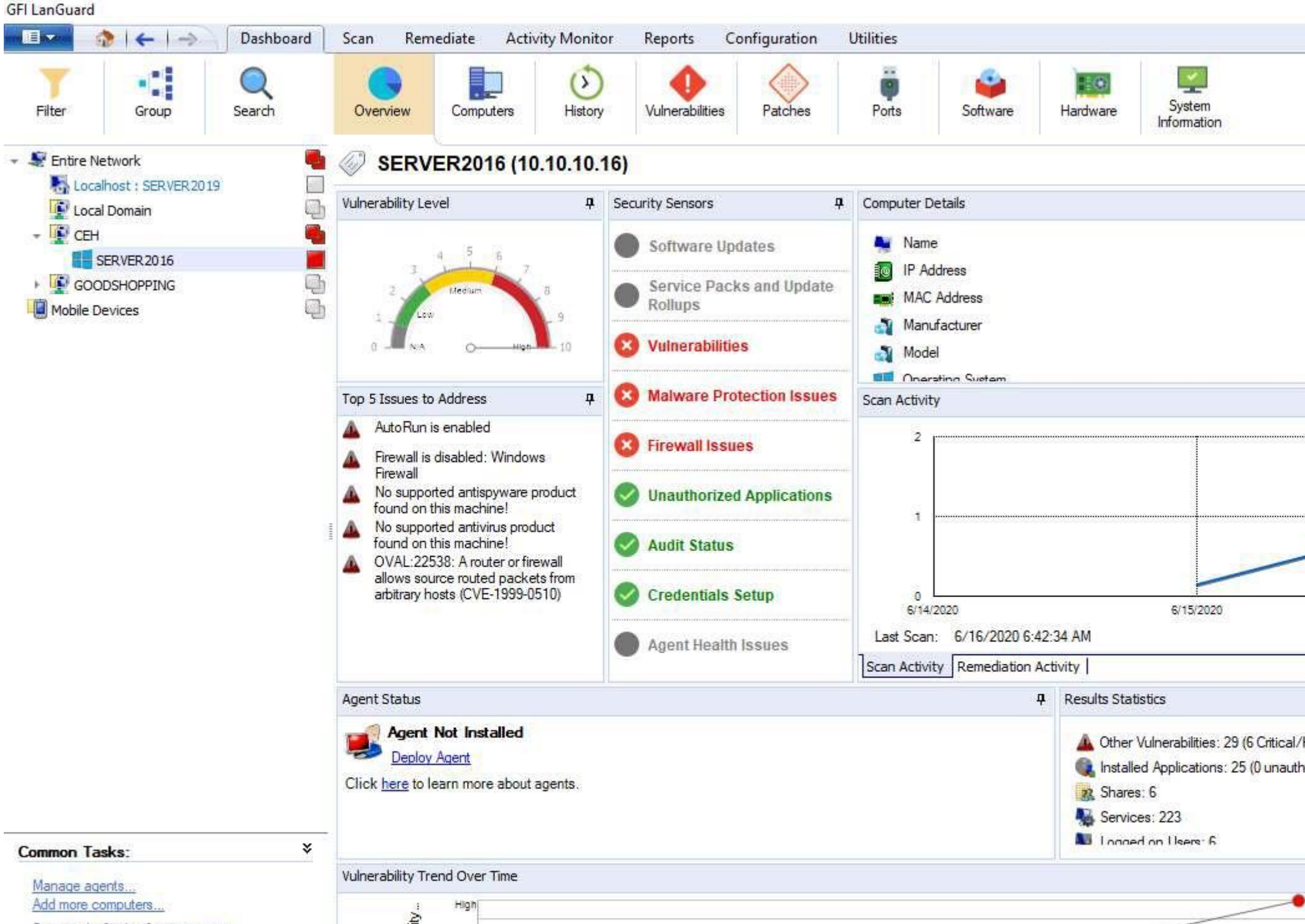

GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Launch a New Scan
Scan Target:
10.10.10.16
Profile:
Full Scan
Credentials:
Currently logged on user
Username:
Password:
Key file:
Scan
Scan Options...
Scan Results Overview
Scan target: 10.10.10.16
10.10.10.16 [SERVER2016] (Windows Server 2016 x64 Version 1607)
Vulnerability Assessment
High Security Vulnerabilities (6)
Medium Security Vulnerabilities (1)
Low Security Vulnerabilities (23)
Potential Vulnerabilities (2)
Network & Software Audit
Ports
Open TCP Ports (17)
Hardware
Software
System Information
Scan Results Details
System Information
Select one of the following System Information categories
Shares (6)
Allows you to analyze the shares information
Password Policy
Allows you to analyze the password policy information
Security Audit Policy (Off)
Allows you to analyze the security audit policy information
Registry
Allows you to analyze the registry information
NetBIOS Names (5)
Allows you to analyze the NetBIOS names information
Computer
Allows you to analyze the computer main information
SNMP
Allows you to analyze SNMP information
Trusted Domains (1)
Allows you to analyze the trusted domains information
Scanner Activity Window
Profile: Full Scan
Initializing scan engine...

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

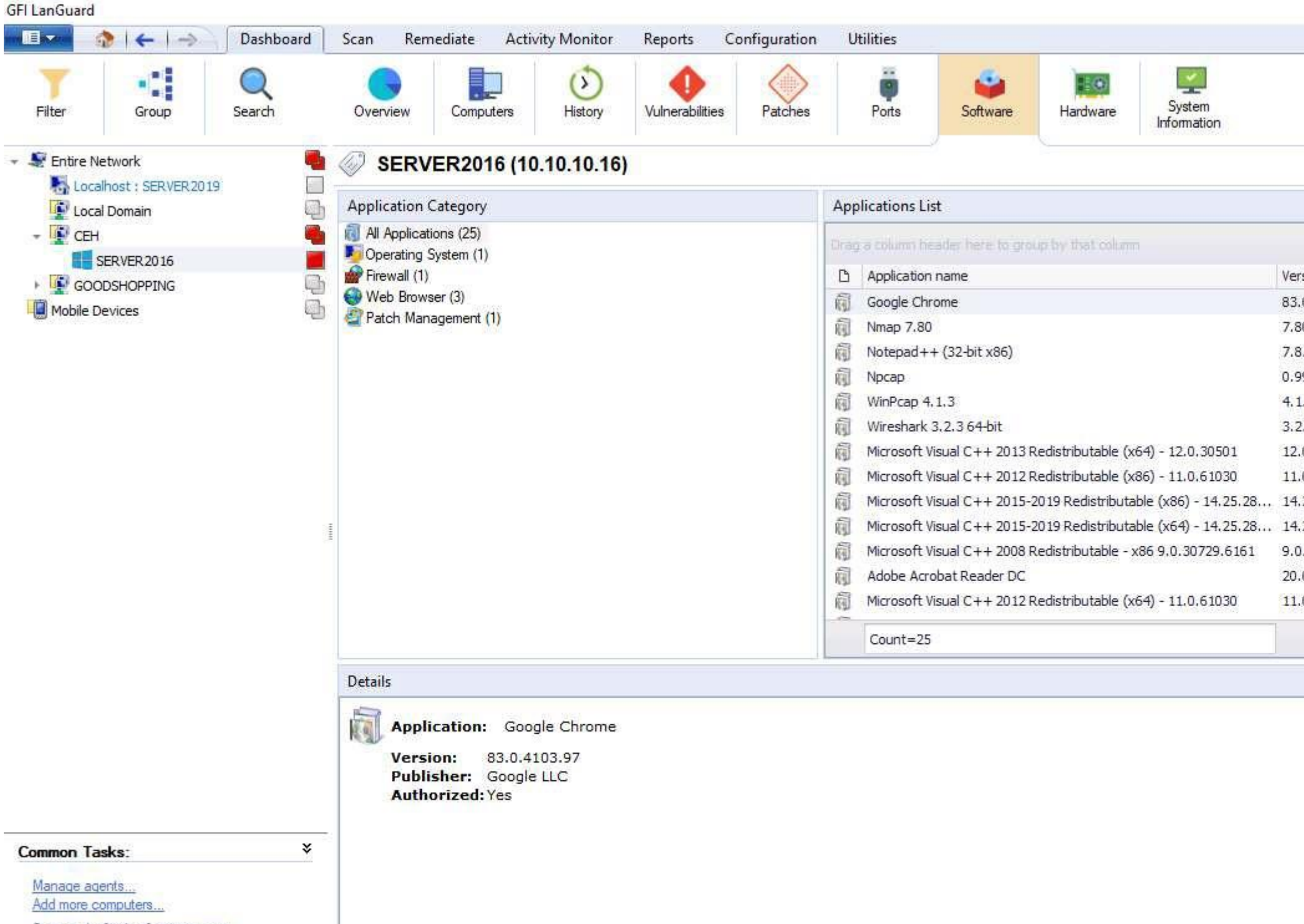

GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Launch a New Scan
Scan Target:
10.10.10.16
Profile:
Full Scan
Credentials:
Currently logged on user
Username:
Password:
Key file:
Scan
Scan Options...
Scan Results Overview
High Security Vulnerabilities (6)
Medium Security Vulnerabilities (1)
Low Security Vulnerabilities (23)
Potential Vulnerabilities (2)
Network & Software Audit
Ports
Open TCP Ports (17)
Hardware
Software
System Information
Shares (6)
Password Policy
Security Audit Policy (Off)
Registry
NetBIOS Names (5)
Computer
SNMP
Trusted Domains (1)
Groups (34)
Users (8)
Logged On Users (6)
Sessions (2)
Services (223)
Processes (67)
Scan Results Details
ADMIN$ - Remote Admin
Share name: ADMIN$
Share remark: Remote Admin
Share path: C:\Windows
No share security permissions
Share path NTFS Permissions
C$ - Default share
Share name: C$
Share remark: Default share
Share path: C:\
No share security permissions
Share path NTFS Permissions
IPC$ - Remote IPC
Share name: IPC$
Share remark: Remote IPC
Share path:
No share security permissions
NETLOGON - Logon server share
Share name: NETLOGON
Share remark: Logon server share
Share path: C:\Windows\SYSVOL\sysvol\CEH.com\SCRIPTS
Share Permissions
SYSVOL - Logon server share
Share name: SYSVOL
Scanner Activity Window
Profile: Full Scan
Initializing scan engine...

37. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.
38. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **CEH**; then, click **SERVER2016**.
39. 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

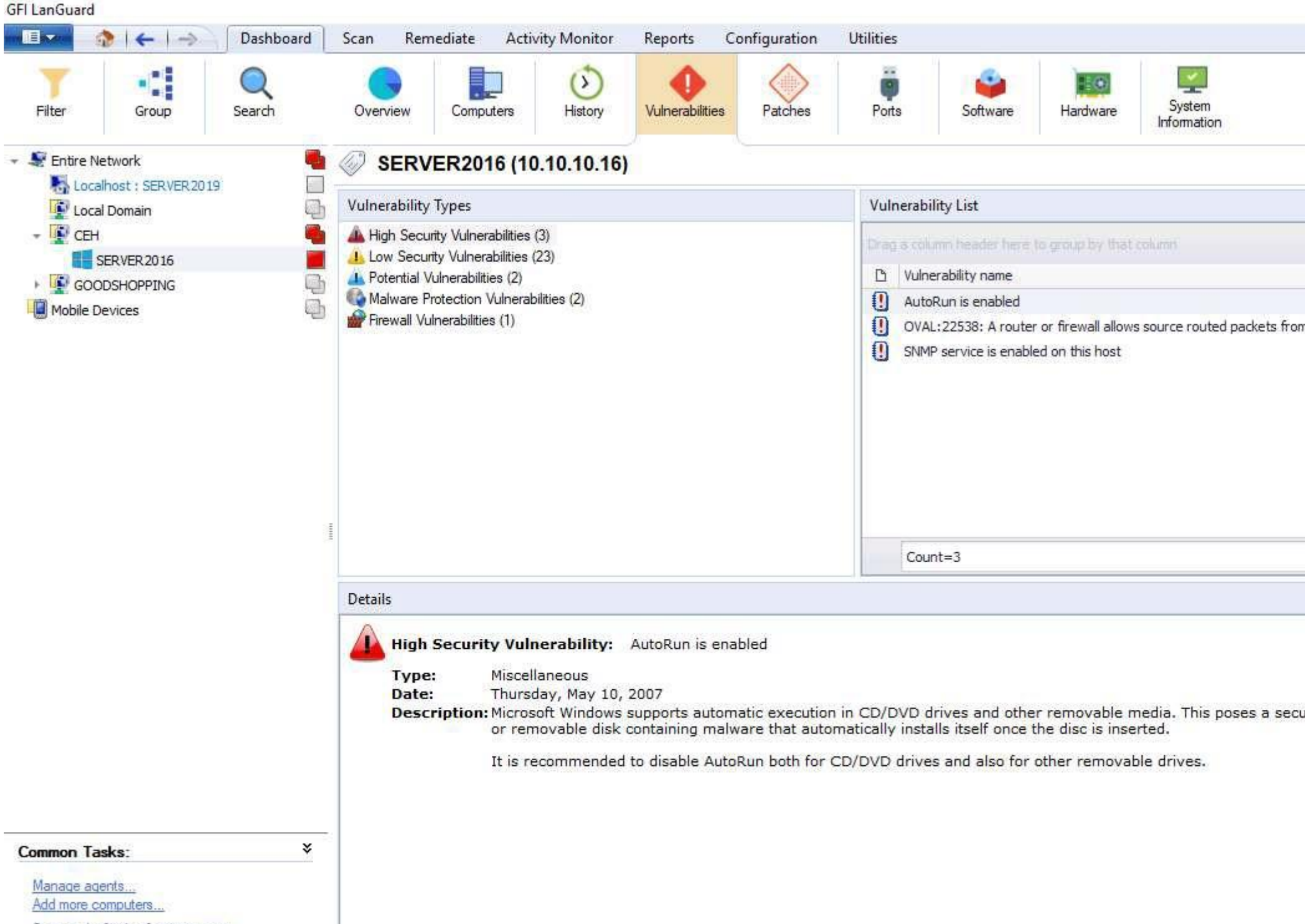
In real-time, using this vulnerability information about the target systems can be used to develop and design exploits suitable to break into a network or a single target.


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : SERVER2019
Local Domain
CEH
SERVER2016
GOODSHOPPING
Mobile Devices
SERVER2016 (10.10.10.16)
Vulnerability Level
Low
Medium
High
N/A
Security Sensors
Software Updates
Service Packs and Update Rollups
Vulnerabilities
Malware Protection Issues
Firewall Issues
Unauthorized Applications
Audit Status
Credentials Setup
Agent Health Issues
Computer Details
Name
IP Address
MAC Address
Manufacturer
Model
Top 5 Issues to Address
AutoRun is enabled
Firewall is disabled: Windows Firewall
No supported antispyware product found on this machine!
No supported antivirus product found on this machine!
OVAL:22538: A router or firewall allows source routed packets from arbitrary hosts (CVE-1999-0510)
Scan Activity
6/14/2020
6/15/2020
Last Scan: 6/16/2020 6:42:34 AM
Scan Activity
Remediation Activity
Agent Status
Agent Not Installed
Deploy Agent
Click here to learn more about agents.
Results Statistics
Other Vulnerabilities: 29 (6 Critical/
Installed Applications: 25 (0 unauth
Shares: 6
Services: 223
Logged on Users: 6
Common Tasks:
Manage agents...
Add more computers...
Vulnerability Trend Over Time
High

40. 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.


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : SERVER2019
Local Domain
CEH
SERVER2016
GOODSHOPPING
Mobile Devices
SERVER2016 (10.10.10.16)
Application Category
All Applications (25)
Operating System (1)
Firewall (1)
Web Browser (3)
Patch Management (1)
Applications List
Drag a column header here to group by that column
Application name
Google Chrome
Nmap 7.80
Notepad++ (32-bit x86)
Npcap
WinPcap 4.1.3
Wireshark 3.2.3 64-bit
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501
Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.25.28...
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.25.28...
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
Adobe Acrobat Reader DC
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030
Count=25
Details
Application: Google Chrome
Version: 83.0.4103.97
Publisher: Google LLC
Authorized: Yes
Common Tasks:
Manage agents...
Add more computers...

41. 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.


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : SERVER2019
Local Domain
CEH
SERVER2016
GOODSHOPPING
Mobile Devices
SERVER2016 (10.10.10.16)
Vulnerability Types
High Security Vulnerabilities (3)
Low Security Vulnerabilities (23)
Potential Vulnerabilities (2)
Malware Protection Vulnerabilities (2)
Firewall Vulnerabilities (1)
Vulnerability List
Drag a column header here to group by that column
Vulnerability name
AutoRun is enabled
OVAL:22538: A router or firewall allows source routed packets from
SNMP service is enabled on this host
Count=3
Details
High Security Vulnerability: AutoRun is enabled
Type: Miscellaneous
Date: Thursday, May 10, 2007
Description: Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a secu
or removable disk containing malware that automatically installs itself once the disc is inserted.
It is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives.
Common Tasks:
Manage agents...
Add more computers...

42. ☐ You can further explore scanned results by clicking various options such as **Patches**, **System Information**, **Hardware**, and **Ports**.
43. ☐ Now, click on the **Report** tab and click the **Vulnerability Status** type under **General Reports** from the right pane.

GFI LanGuard

Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities

Filter | Group | Search

SERVER2016 (10.10.10.16)

Settings | Search

- Entire Network
  - Localhost : SERVER2019
  - Local Domain
  - CEH
    - SERVER2016
  - GOODSHOPPING
- Mobile Devices

Reports:

- General Reports
  - Computer Security Overview
  - Vulnerability Status
  - Patching Status
  - Full Audit
  - Scan Based - Full Audit
  - Software Audit
  - Scan History
  - Remediation History
  - Network Security History
  - Baseline Comparison
  - Mobile Device Audit
- PCI DSS Compliance Reports
- HIPAA Compliance Reports
- SOX Compliance Reports
- GLBA Compliance Reports
- PSNCoCo Compliance Reports
- FERPA Compliance Reports
- CIPA Compliance Reports
- ISO/IEC 27001 & 27002 Complia
- FISMA Compliance Reports
- CAG Compliance Reports
- NERC CIP Compliance Reports

Scheduled Reports

Scheduled Reports List

Scheduled Reports Options

Actions:

Common Tasks:

Manage agents...

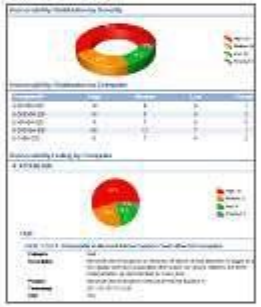
Add more computers...

General Reports

View, print, schedule, customize LanGuard reports

Computer Security Overview

An executive summary report showing computer vulnerability level, agent stat
details and summary.



Vulnerability Status

Shows statistical information related to the vulnerabilities detected on target c
vulnerability severity, timestamp and category.

Patching Status

Shows statistical information related to the missing and installed updates dete
name, severity, timestamp, vendor and category.

Full Audit

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

GFI LanGuard

Dashboard | Scan | Remediate | Activity Monitor | Reports | Configuration | Utilities

Filter | Group | Search

- Entire Network
  - Localhost : SERVER2019
  - Local Domain
  - CEH
    - SERVER2016
  - GOODSHOPPING
  - Mobile Devices

Common Tasks:

Manage agents...
Add more computers...

SERVER2016 (10.10.10.16)

Settings | Search

Reports:

- General Reports
  - Computer Security Overview
  - Vulnerability Status
  - Patching Status
  - Full Audit
  - Scan Based - Full Audit
  - Software Audit
  - Scan History
  - Remediation History
  - Network Security History
  - Baseline Comparison
  - Mobile Device Audit
- PCI DSS Compliance Reports
- HIPAA Compliance Reports
- SOX Compliance Reports
- GLBA Compliance Reports
- PSNCoCo Compliance Reports
- FERPA Compliance Reports
- CIPA Compliance Reports
- ISO/IEC 27001 & 27002 Complia
- FISMA Compliance Reports
- CAG Compliance Reports
- NERC CIP Compliance Reports

Scheduled Reports

Scheduled Reports List
Scheduled Reports Options

Actions:

Vulnerability Status

Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be
category.

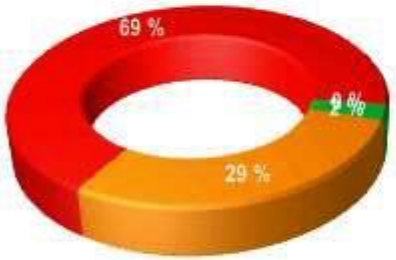
Generate Report

Use this report to get:

1. Chart displaying general vulnerabilities distribution based on selected second grouping criteria
2. Table displaying general vulnerabilities distribution based on selected grouping criteria
3. Chart displaying vulnerabilities distribution for each item from first grouping criteria
4. Vulnerabilities details for each item from first grouping criteria

Sample Report:

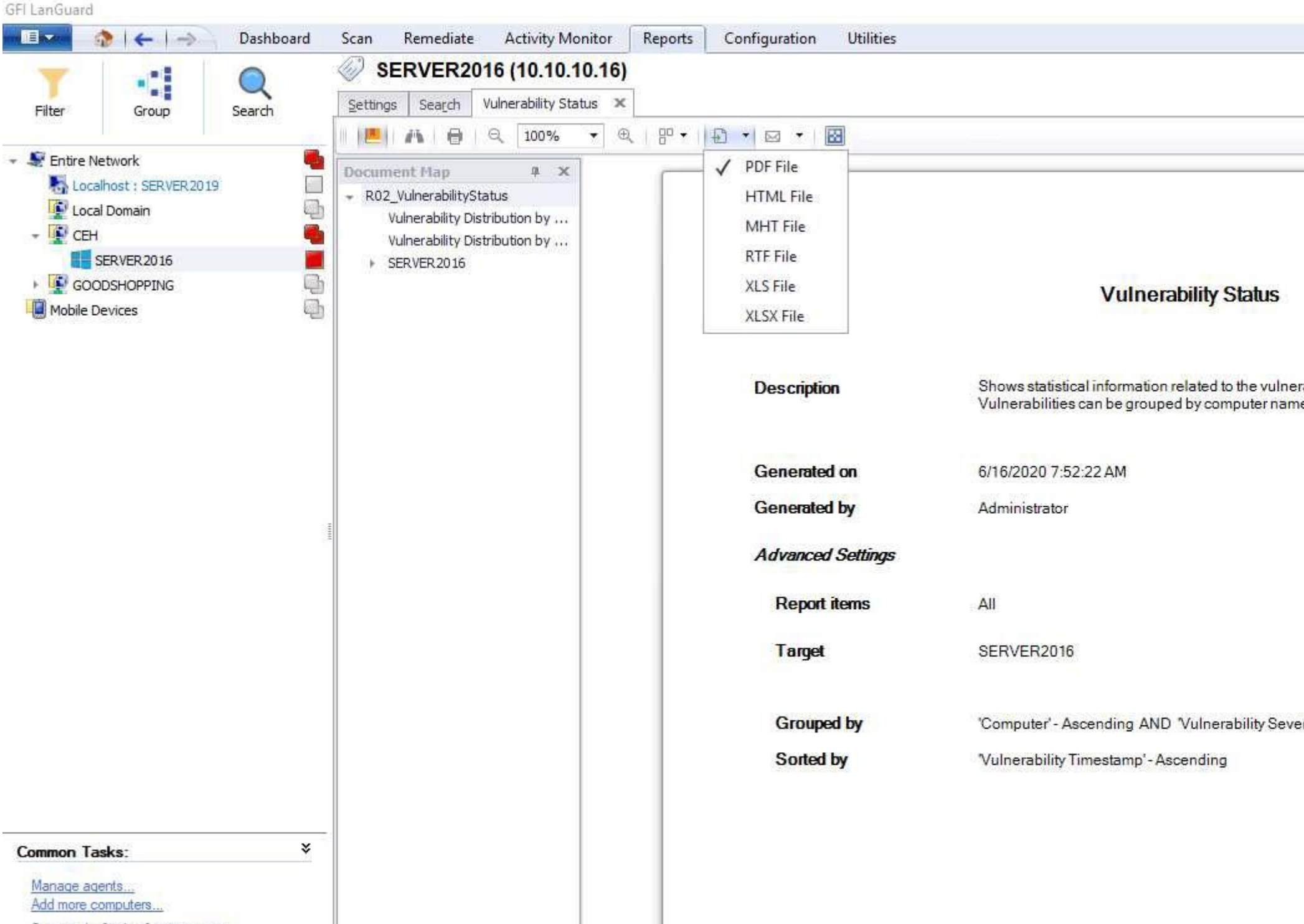
Vulnerability Distribution by Severity



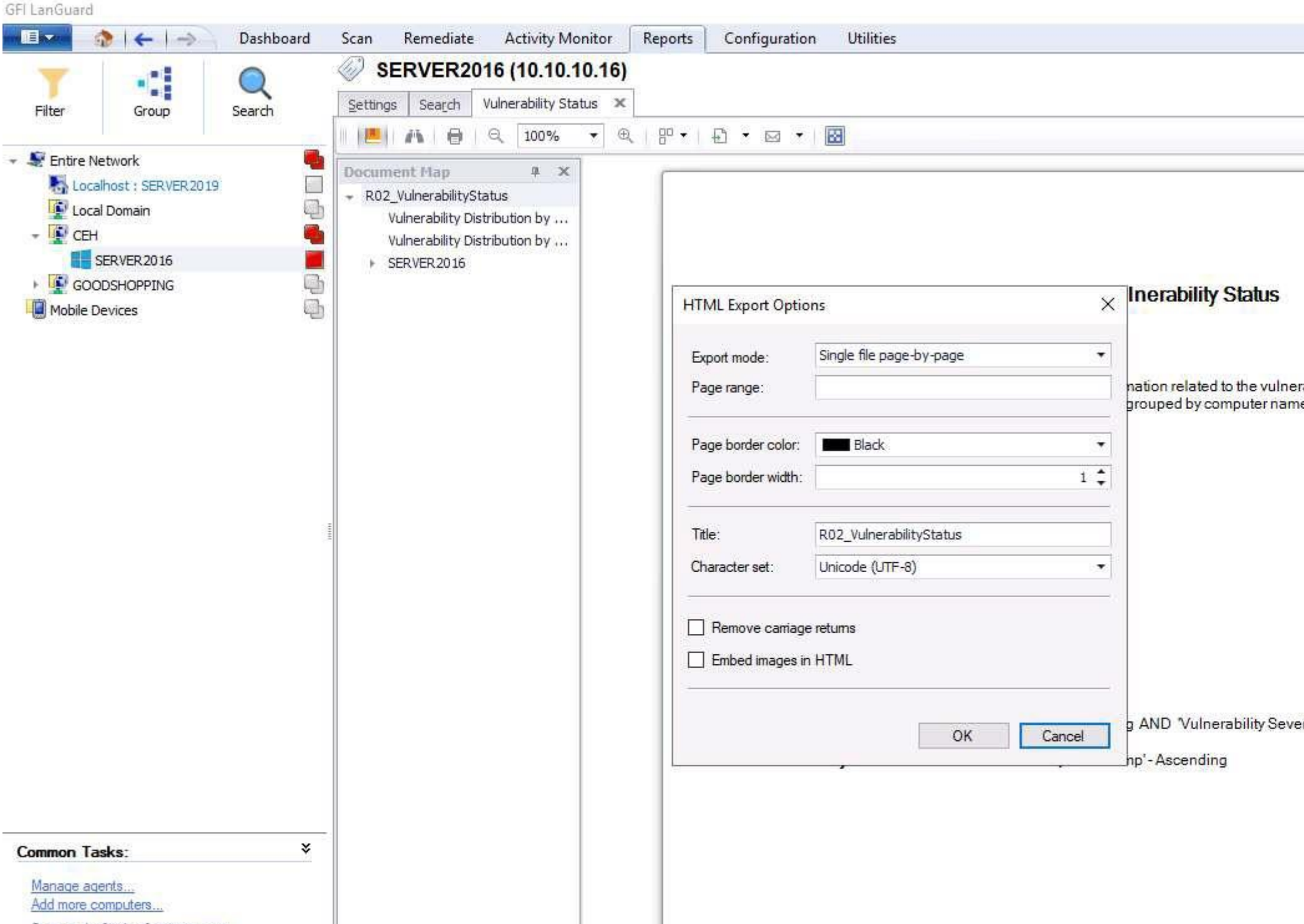
Vulnerability Distribution by Computer

Computer/IP	High	Medium
LNSSWIN7X64	448	215
LNSSWIN7X86	474	249

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

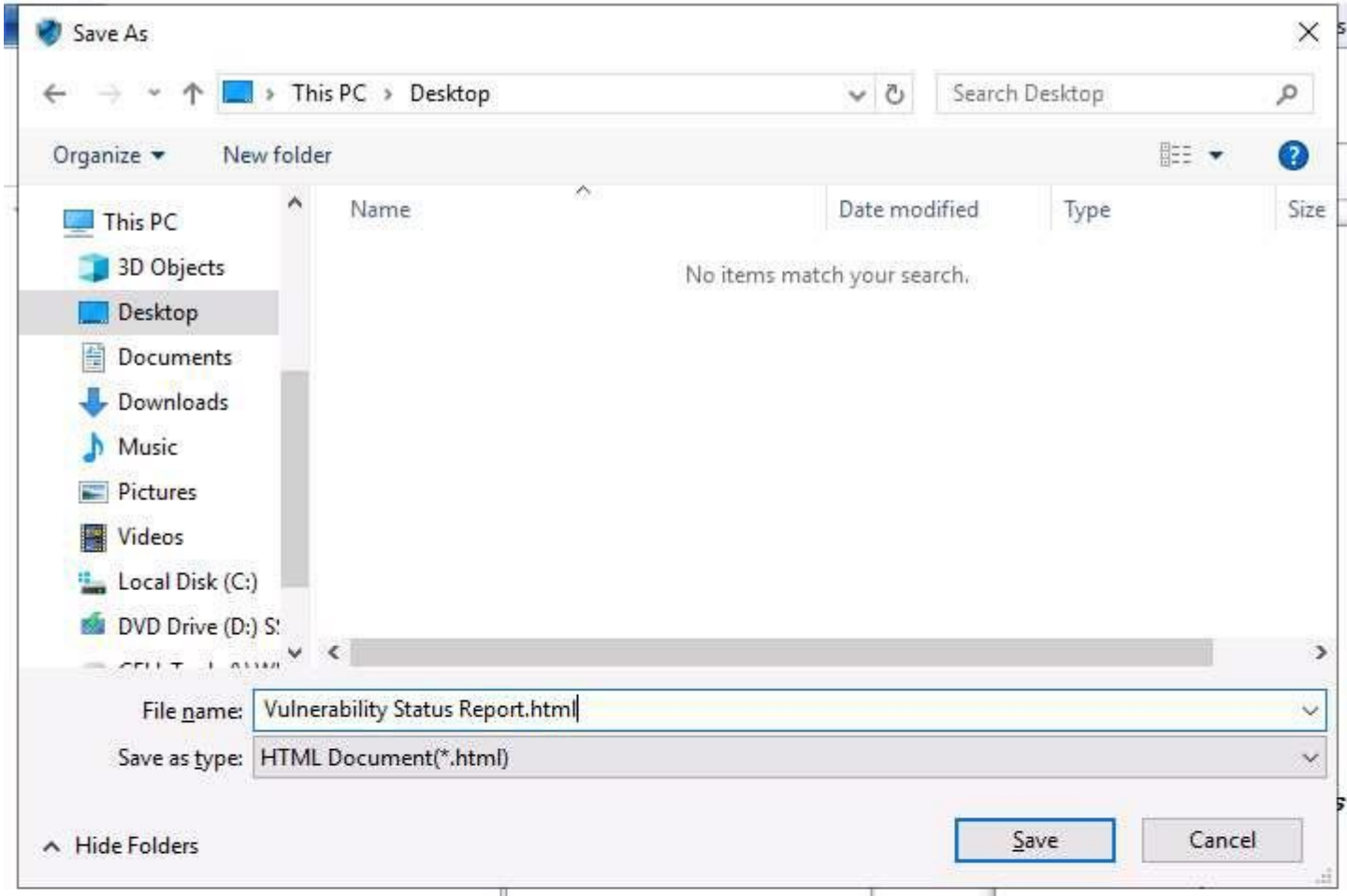

GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Filter
Group
Search
SERVER2016 (10.10.10.16)
Settings
Search
Vulnerability Status
100%
Entire Network
Localhost : SERVER2019
Local Domain
CEH
SERVER2016
GOODSHOPPING
Mobile Devices
Document Map
R02_VulnerabilityStatus
Vulnerability Distribution by ...
Vulnerability Distribution by ...
SERVER2016
PDF File
HTML File
MHT File
RTF File
XLS File
XLSX File
Vulnerability Status
Description
Shows statistical information related to the vulner
Vulnerabilities can be grouped by computer name
Generated on
6/16/2020 7:52:22 AM
Generated by
Administrator
Advanced Settings
Report items
All
Target
SERVER2016
Grouped by
'Computer' - Ascending AND 'Vulnerability Sever
Sorted by
'Vulnerability Timestamp' - Ascending
Common Tasks:
Manage agents...
Add more computers...

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


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Filter
Group
Search
SERVER2016 (10.10.10.16)
Settings
Search
Vulnerability Status
100%
Entire Network
Localhost : SERVER2019
Local Domain
CEH
SERVER2016
GOODSHOPPING
Mobile Devices
Document Map
R02_VulnerabilityStatus
Vulnerability Distribution by ...
Vulnerability Distribution by ...
SERVER2016
HTML Export Options
Export mode:
Single file page-by-page
Page range:
Page border color:
Black
Page border width:
1
Title:
R02_VulnerabilityStatus
Character set:
Unicode (UTF-8)
Remove carriage returns
Embed images in HTML
OK
Cancel
Inerability Status
nation related to the vulner
grouped by computer name
g AND 'Vulnerability Sever
hp' - Ascending
Common Tasks:
Manage agents...
Add more computers...

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

GFI LanGuard



Vulnerability Status

Shows statistical information related to the vulner
Vulnerabilities can be grouped by computer name

6/16/2020 7:52:22 AM

Administrator

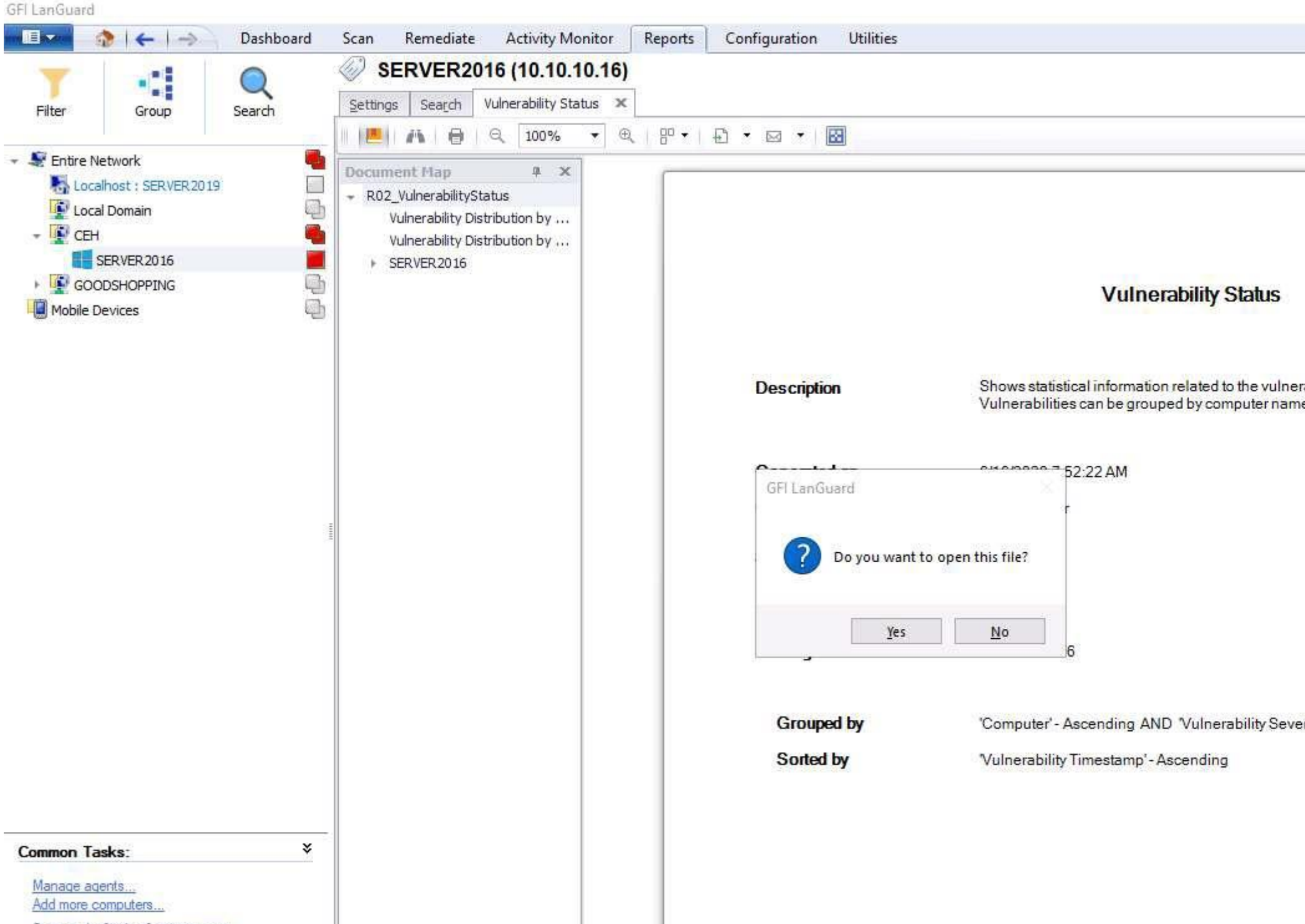
All

Target	SERVER2016
Grouped by	'Computer' - Ascending AND 'Vulnerability Seve
Sorted by	'Vulnerability Timestamp' - Ascending

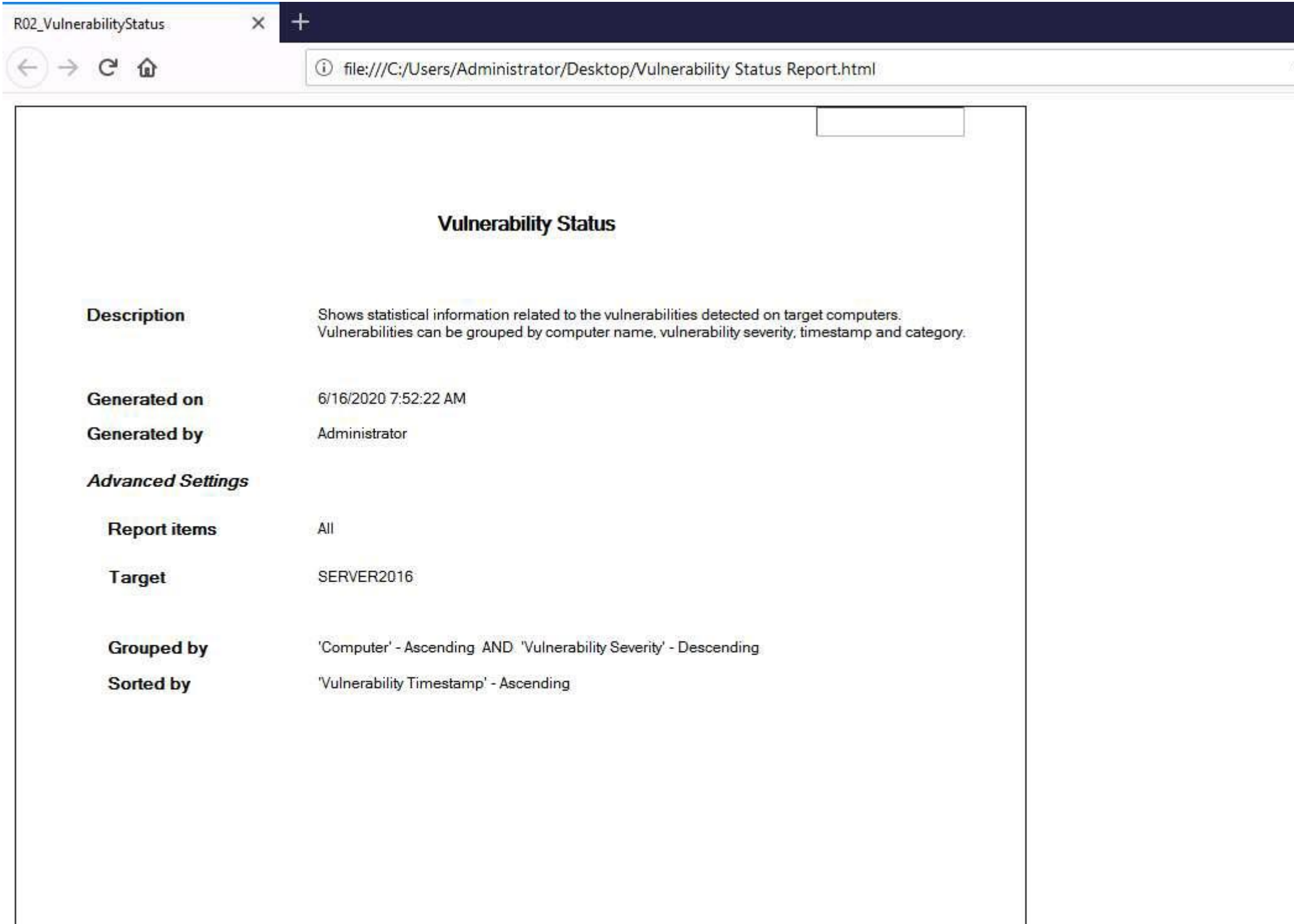
Common Tasks:

Manage agents...
Add more computers...

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


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Filter
Group
Search
SERVER2016 (10.10.10.16)
Settings
Search
Vulnerability Status
100%
Entire Network
Localhost : SERVER2019
Local Domain
CEH
SERVER2016
GOODSHOPPING
Mobile Devices
Document Map
R02_VulnerabilityStatus
Vulnerability Distribution by ...
Vulnerability Distribution by ...
SERVER2016
Vulnerability Status
Description
Shows statistical information related to the vulner
Vulnerabilities can be grouped by computer name
52:22 AM
GFI LanGuard
Do you want to open this file?
Yes
No
Grouped by
'Computer' - Ascending AND 'Vulnerability Sever
Sorted by
'Vulnerability Timestamp' - Ascending
Common Tasks:
Manage agents...
Add more computers...

49. In the **How do you want to open this file?** pop-up, select any web browser (here, **Firefox**) and click **OK**.
50. The **Vulnerability Status** report appears; you can scroll down to view detailed information regarding discovered vulnerabilities.


R02_VulnerabilityStatus
file:///C:/Users/Administrator/Desktop/Vulnerability Status Report.html
Vulnerability Status
Description
Shows statistical information related to the vulnerabilities detected on target computers.
Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.
Generated on
6/16/2020 7:52:22 AM
Generated by
Administrator
Advanced Settings
Report items
All
Target
SERVER2016
Grouped by
'Computer' - Ascending AND 'Vulnerability Severity' - Descending
Sorted by
'Vulnerability Timestamp' - Ascending

Vulnerability Status

Vulnerability Distribution by Severity

Vulnerability Distribution by Computer

Computer/IP	High	Medium	Low	Potential
SERVER2016	6	0	23	2

Vulnerability Listing by Computer

SERVER2016

High

Vulnerability Name	Product	Severity	CVSS Score	Timestamp
AutoRun is enabled	N/A	High	-	2007-05-10
Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a security risk in the case where a CD or removable disk containing malware that automatically installs itself once the disc is inserted.It is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives.				
OVAL:22538: A router or firewall allows source routed packets from arbitrary hosts (CVE-1999-0510)	N/A	High	7.5	2014-03-13
A router or firewall allows source routed packets from arbitrary hosts.				

51. ☐ This concludes the demonstration of scanning network vulnerabilities using GFI LanGuard.
52. ☐ Close all open windows and document all the acquired information.

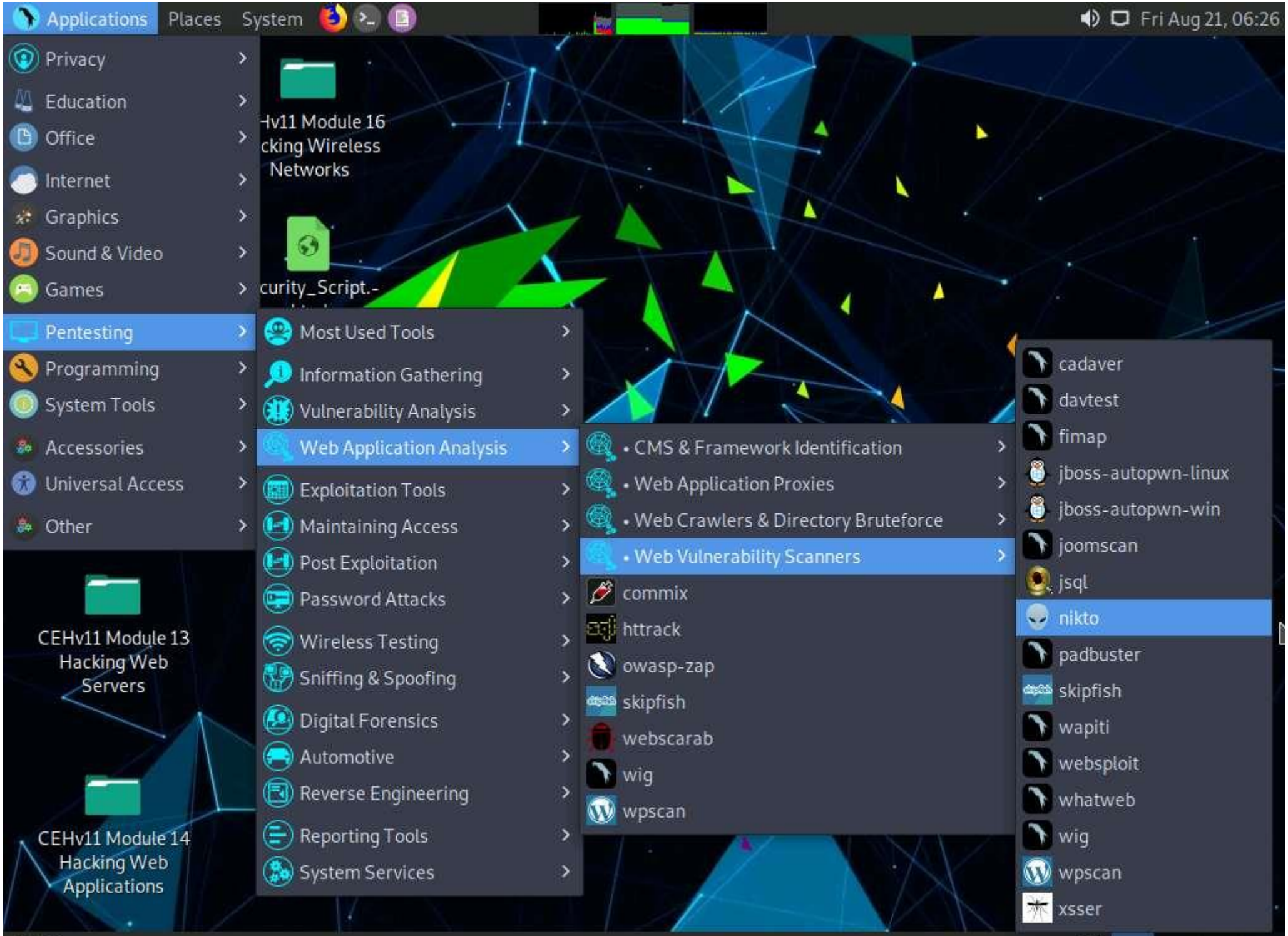
Task 4: Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

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.

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

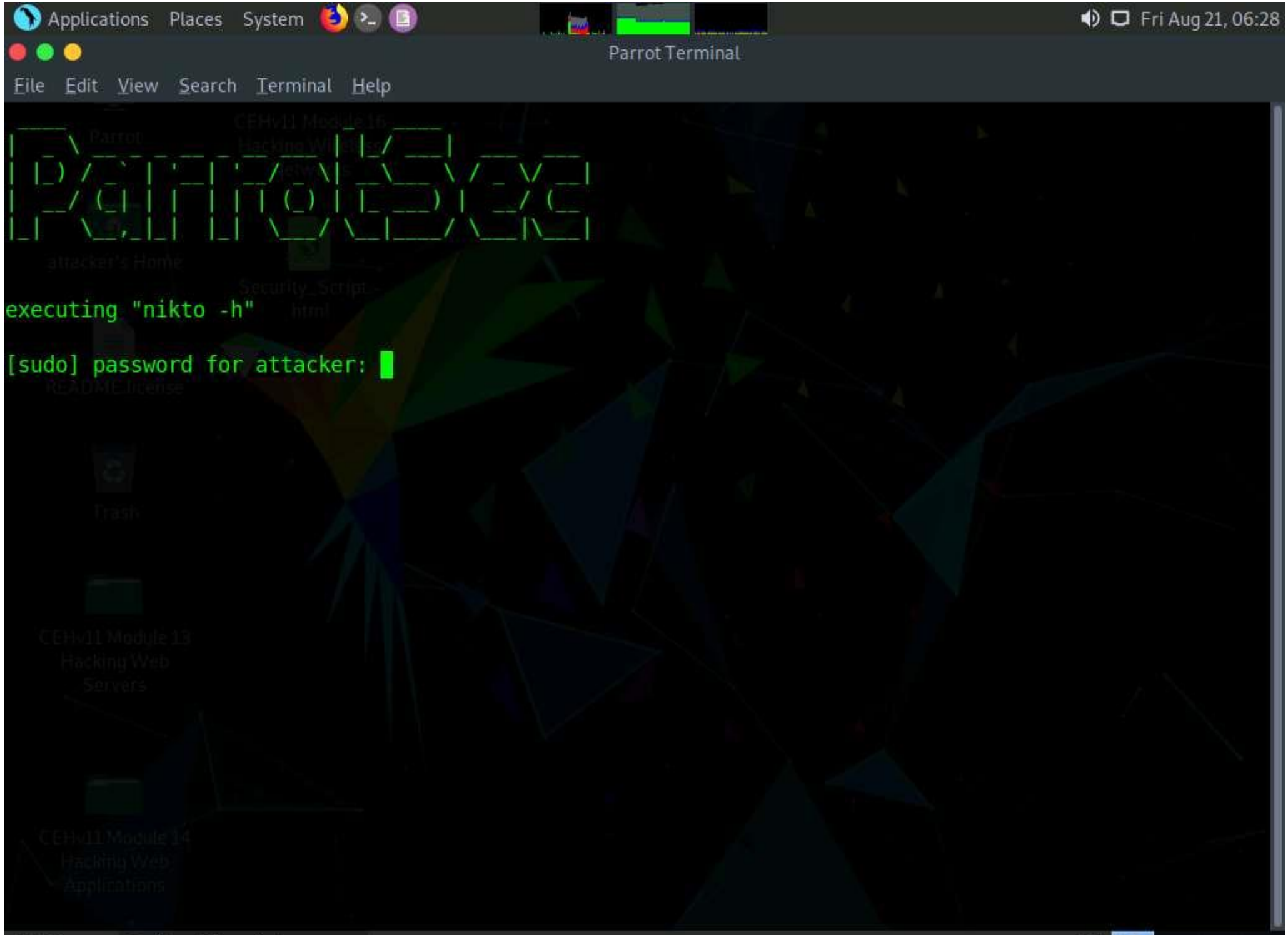
In this task, we will target the **www.certifiedhacker.com** website.

1. ☐ Click on Parrot Security to switch to **Parrot Security** machine.
2. ☐ Click the **Applications** menu in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Vulnerability Scanners** --> **nikto** to open Nikto in the **Terminal** window.

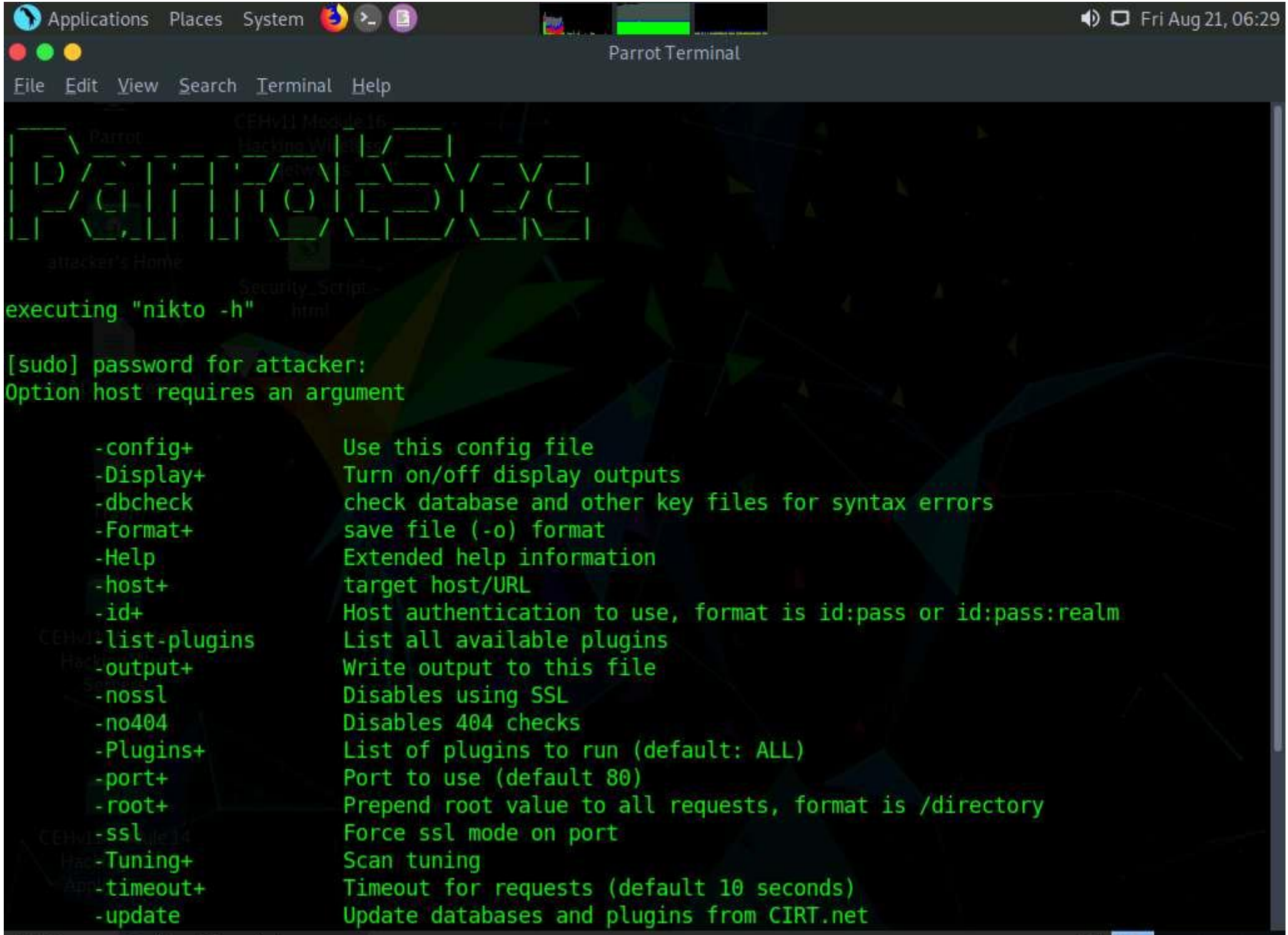

Applications
Places
System
Fri Aug 21, 06:26
Privacy
Education
Office
Internet
Graphics
Sound & Video
Games
Pentesting
Programming
System Tools
Accessories
Universal Access
Other
Most Used Tools
Information Gathering
Vulnerability Analysis
Web Application Analysis
Exploitation Tools
Maintaining Access
Post Exploitation
Password Attacks
Wireless Testing
Sniffing & Spoofing
Digital Forensics
Automotive
Reverse Engineering
Reporting Tools
System Services
• CMS & Framework Identification
• Web Application Proxies
• Web Crawlers & Directory Bruteforce
• Web Vulnerability Scanners
commix
httrack
owasp-zap
skipfish
webscarab
wig
wpscan
cadaver
davtest
fimap
jboss-autopwn-linux
jboss-autopwn-win
joomscan
jsql
nikto
padbuster
skipfish
wapiti
websploit
whatweb
wig
wpscan
xsser
-lv11 Module 16
cking Wireless
Networks
curity_Script.-
CEHv11 Module 13
Hacking Web
Servers
CEHv11 Module 14
Hacking Web
Applications

3. A **Parrot Terminal** window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Nikto initializes.

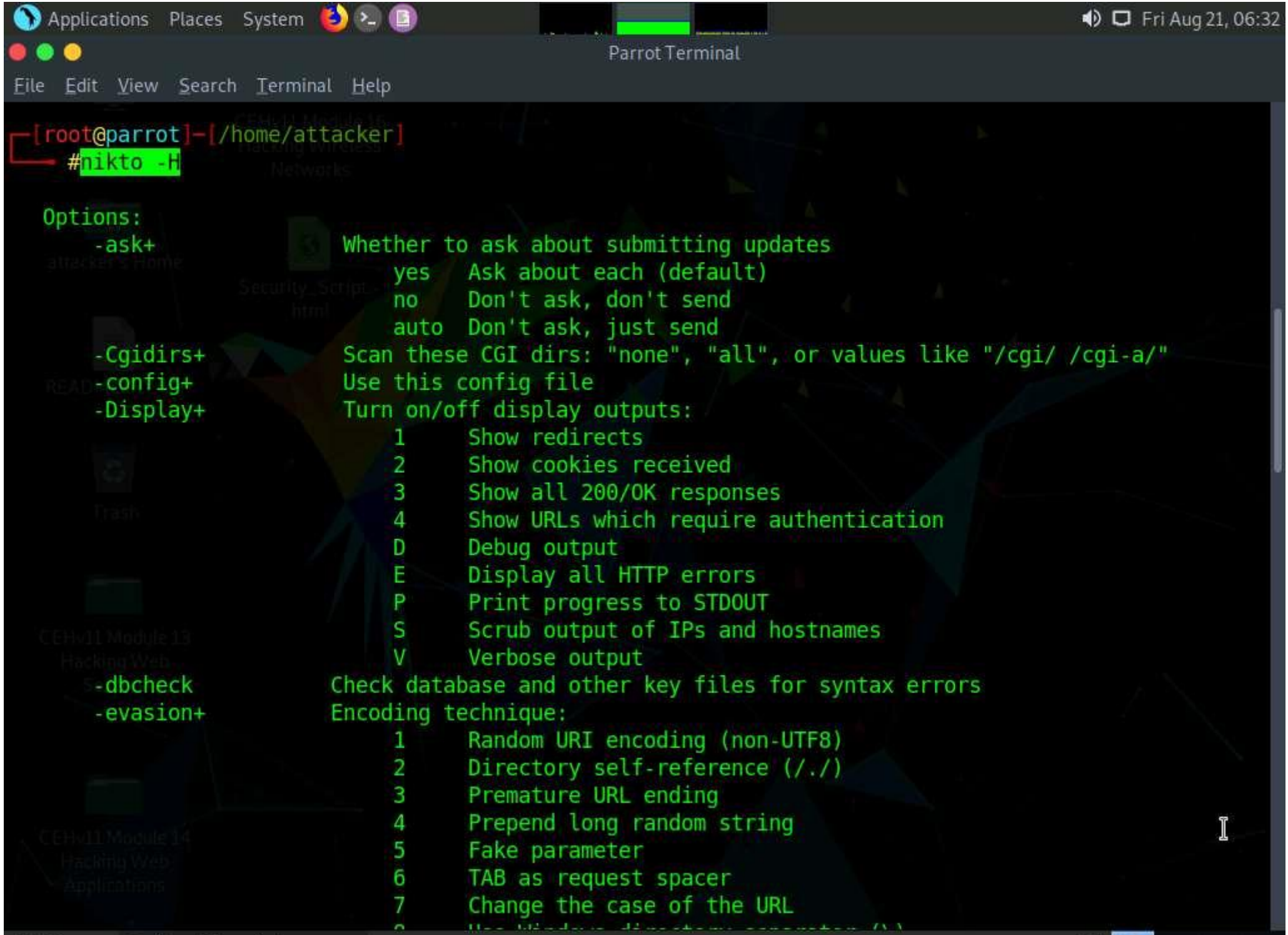
The password that you type will not be visible.


Applications
Places
System
Fri Aug 21, 06:28
Parrot Terminal
File
Edit
View
Search
Terminal
Help
executing "nikto -h"
[sudo] password for attacker:

4. Nikto scanning options will be displayed to scan the target website.

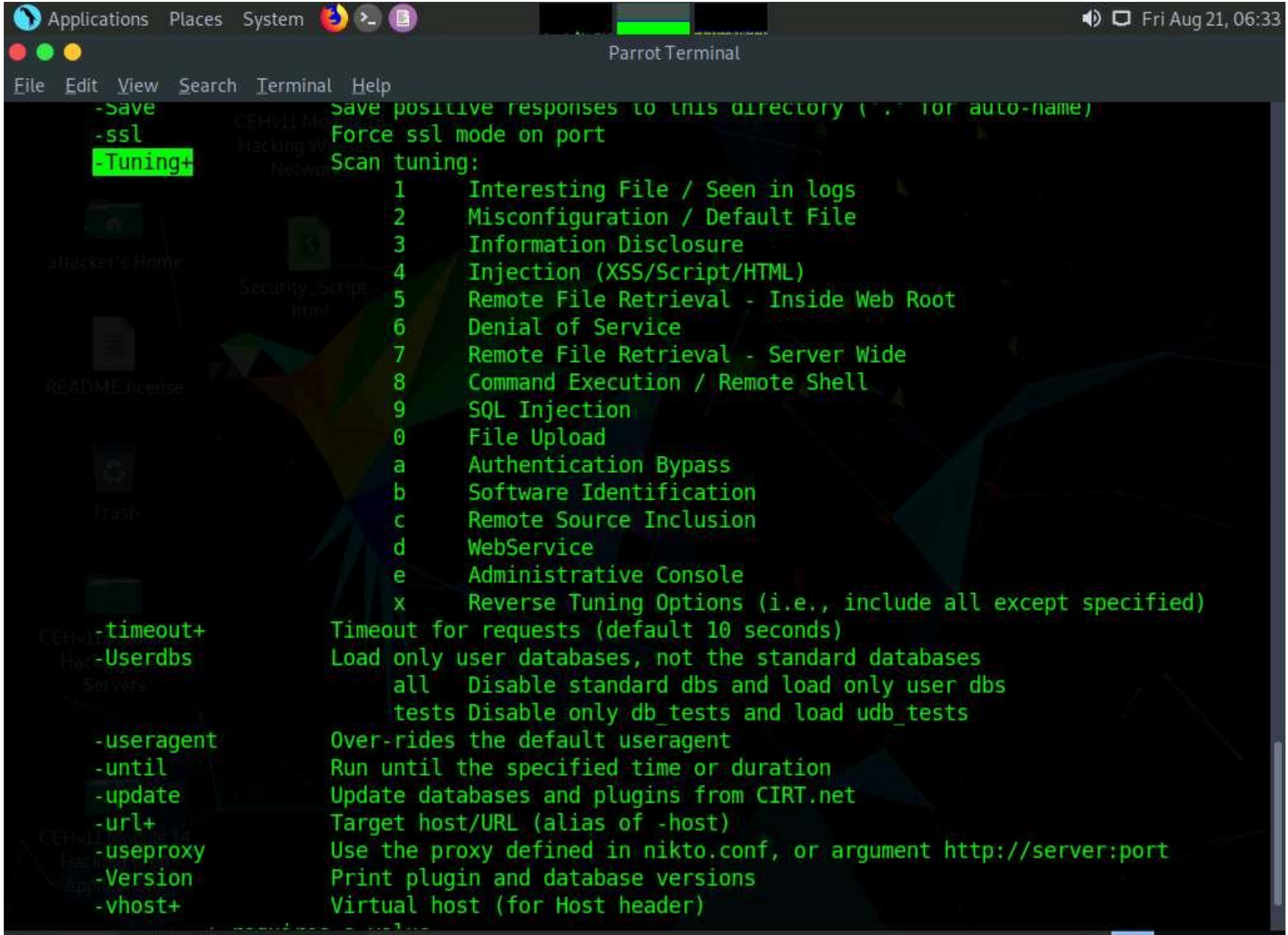

Applications Places System
Fri Aug 21, 06:29
Parrot Terminal
File Edit View Search Terminal Help
executing "nikto -h"
[sudo] password for attacker:
Option host requires an argument
-config+ Use this config file
-Display+ Turn on/off display outputs
-dbcheck check database and other key files for syntax errors
-Format+ save file (-o) format
-Help Extended help information
-host+ target host/URL
-id+ Host authentication to use, format is id:pass or id:pass:realm
-list-plugins List all available plugins
-output+ Write output to this file
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /directory
-ssl Force ssl mode on port
-Tuning+ Scan tuning
-timeout+ Timeout for requests (default 10 seconds)
-update Update databases and plugins from CIRT.net

5. You can further type **nikto -H** and press **Enter** to view various available commands with full help text


Applications Places System
Fri Aug 21, 06:32
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nikto -H
Options:
-ask+ Whether to ask about submitting updates
yes Ask about each (default)
no Don't ask, don't send
auto Don't ask, just send
-Cgidirs+ Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
-config+ Use this config file
-Display+ Turn on/off display outputs:
1 Show redirects
2 Show cookies received
3 Show all 200/OK responses
4 Show URLs which require authentication
D Debug output
E Display all HTTP errors
P Print progress to STDOUT
S Scrub output of IPs and hostnames
V Verbose output
-dbcheck Check database and other key files for syntax errors
-evasion+ Encoding technique:
1 Random URI encoding (non-UTF8)
2 Directory self-reference (/./)
3 Premature URL ending
4 Prepend long random string
5 Fake parameter
6 TAB as request spacer
7 Change the case of the URL

6. 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.

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.


Applications Places System
Fri Aug 21, 06:33
Parrot Terminal
File Edit View Search Terminal Help
-Save Save positive responses to this directory ('.' for auto-name)
-ssl Force ssl mode on port
-Tuning+ Scan tuning:
1 Interesting File / Seen in logs
2 Misconfiguration / Default File
3 Information Disclosure
4 Injection (XSS/Script/HTML)
5 Remote File Retrieval - Inside Web Root
6 Denial of Service
7 Remote File Retrieval - Server Wide
8 Command Execution / Remote Shell
9 SQL Injection
0 File Upload
a Authentication Bypass
b Software Identification
c Remote Source Inclusion
d WebService
e Administrative Console
x Reverse Tuning Options (i.e., include all except specified)
-timeout+ Timeout for requests (default 10 seconds)
-Userdbs Load only user databases, not the standard databases
all Disable standard dbs and load only user dbs
tests Disable only db_tests and load udb_tests
-useragent Over-rides the default useragent
-until Run until the specified time or duration
-update Update databases and plugins from CIRT.net
-url+ Target host/URL (alias of -host)
-useproxy Use the proxy defined in nikto.conf, or argument http://server:port
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)

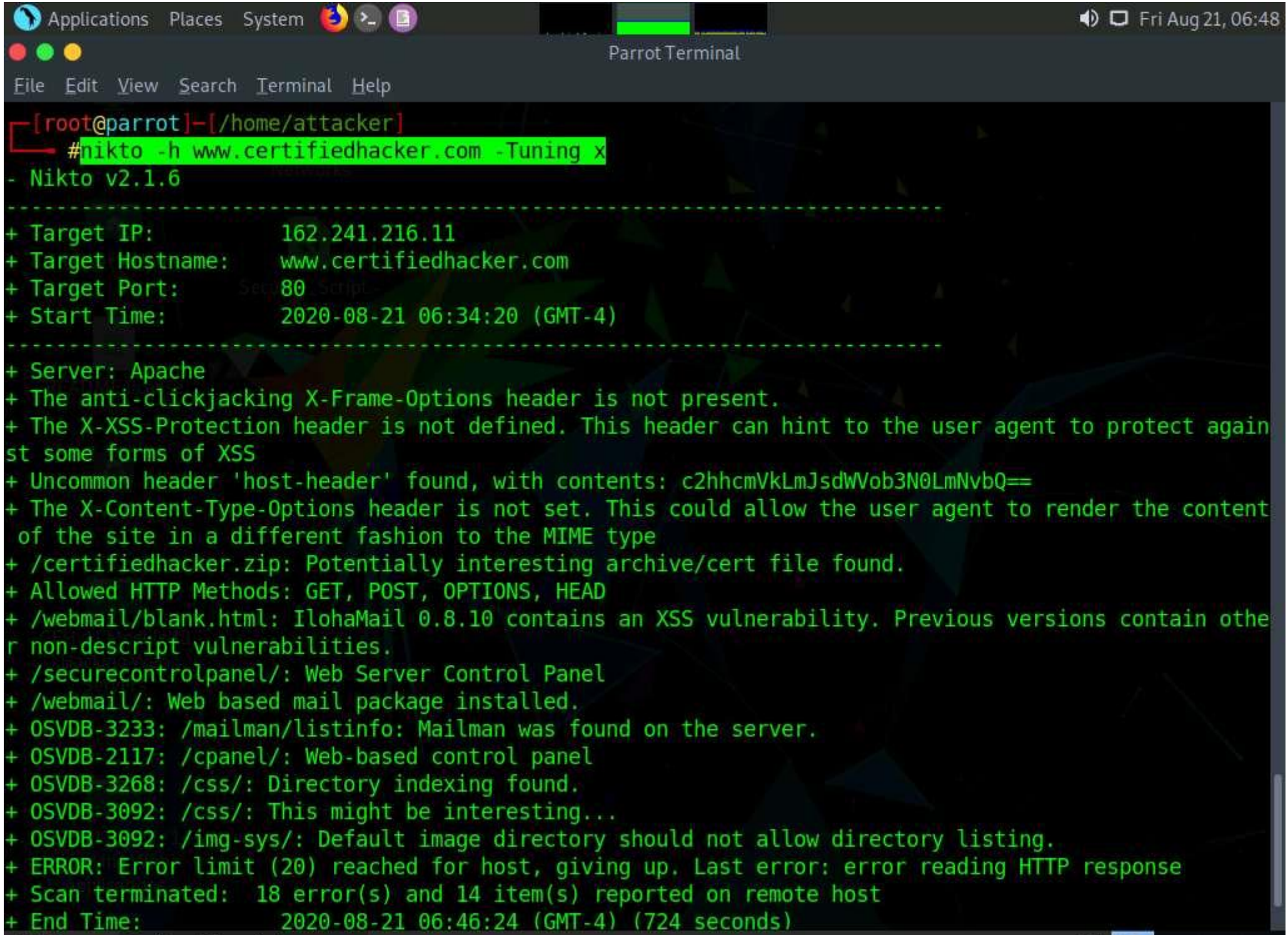
7. In the terminal window, type **nikto -h (Target Website) -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

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

The scan takes approximately 10 minutes to complete.

8. 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.

The result might vary in your lab environment.


Applications Places System
Fri Aug 21, 06:48
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nikto -h www.certifiedhacker.com -Tuning x
- Nikto v2.1.6

+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2020-08-21 06:34:20 (GMT-4)

+ 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
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3092: /img-sys/: Default image directory should not allow directory listing.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 18 error(s) and 14 item(s) reported on remote host
+ End Time: 2020-08-21 06:46:24 (GMT-4) (724 seconds)

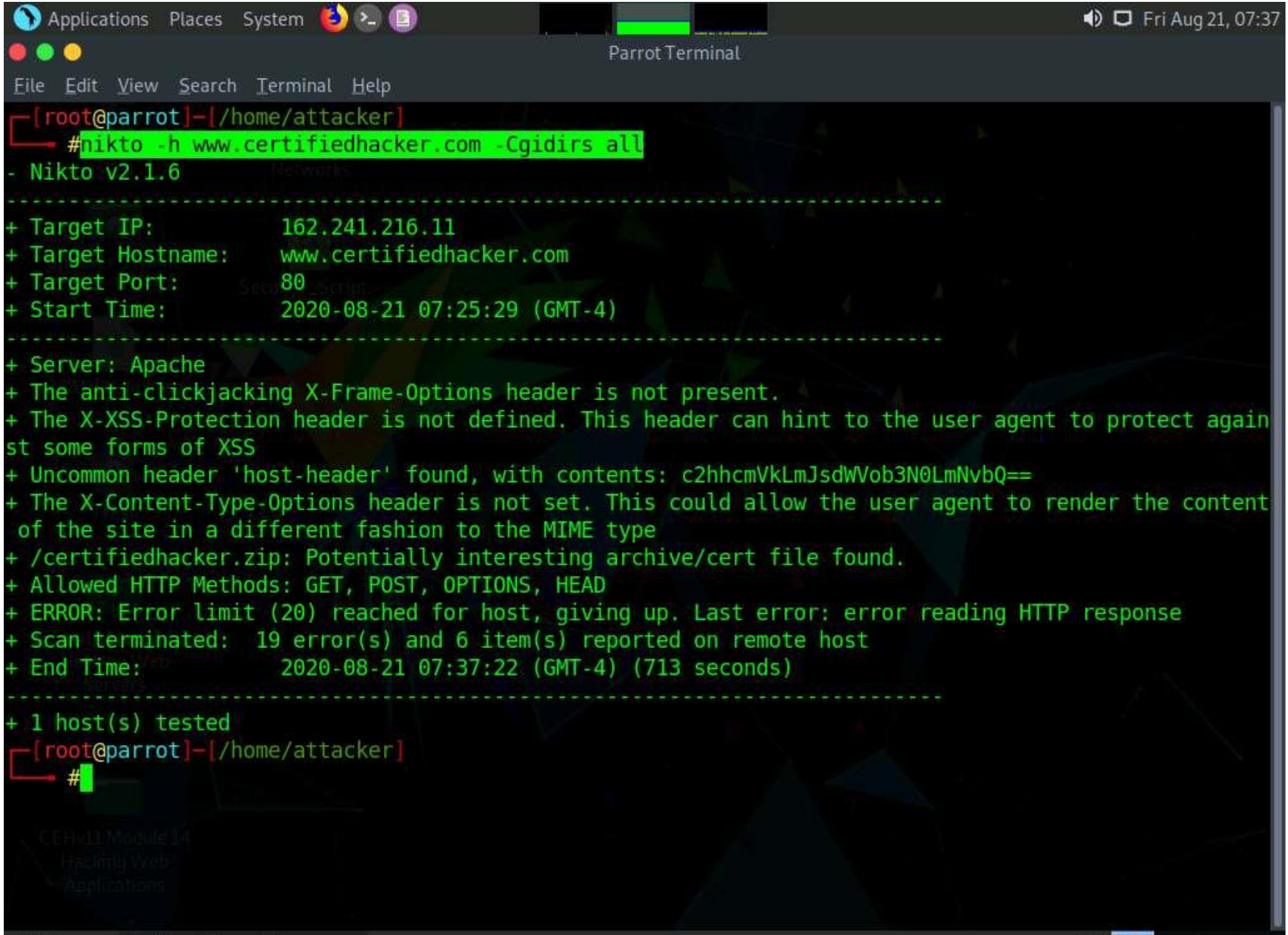
9. Here, we will check for cgi directories with the -**Cgidirs** option. In this option, search for specific directories or use **all** options to search for all the available directories.
10. In the terminal window, type **nikto -h (Target Website) -Cgidirs all**, (here, the target website is **www.certifiedhacker.com**) and hit **Enter**.

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

The scan takes approximately 10 minutes to complete.

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

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

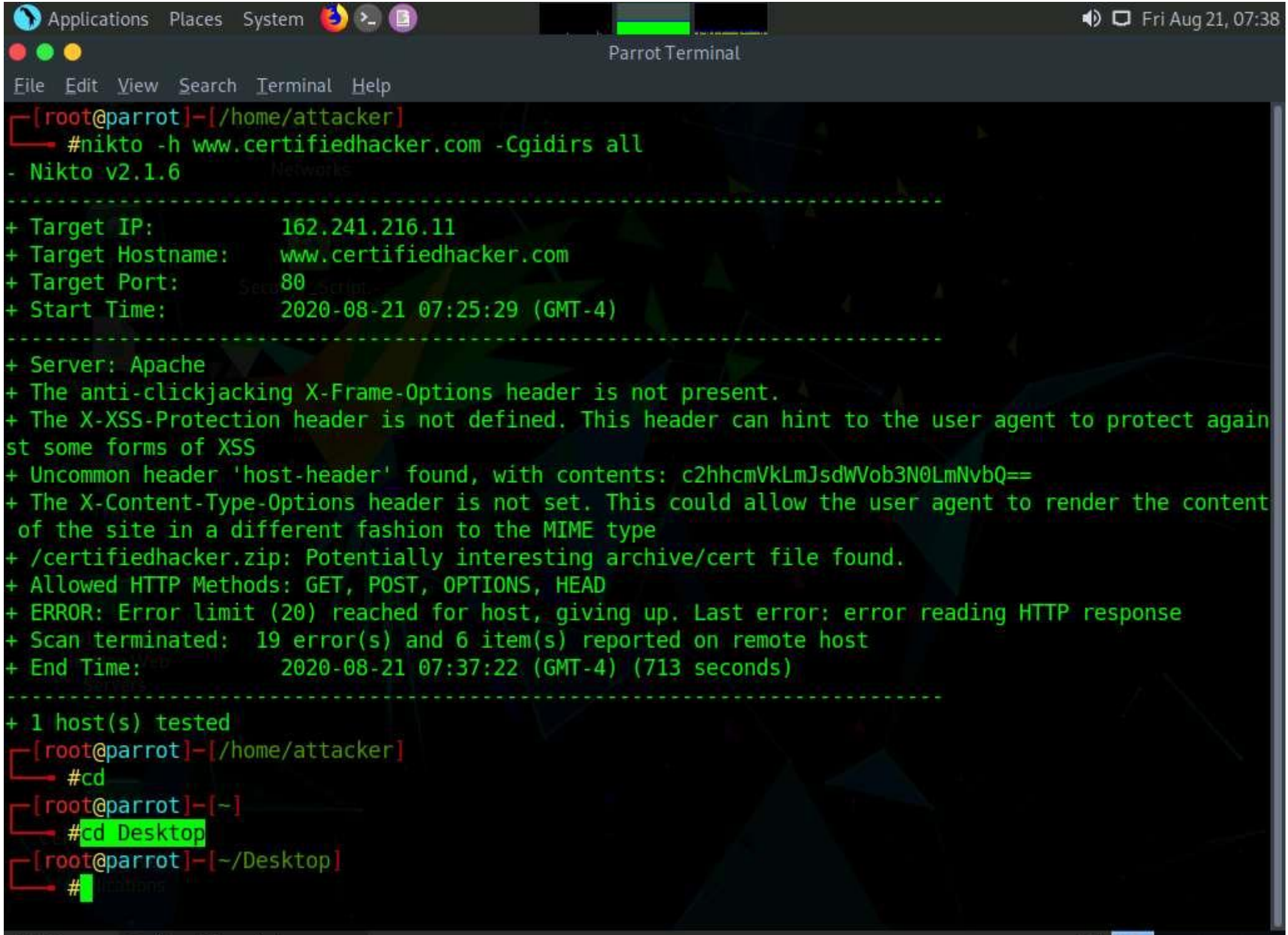

Applications Places System
Fri Aug 21, 07:37
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6

+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2020-08-21 07:25:29 (GMT-4)

+ 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
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 19 error(s) and 6 item(s) reported on remote host
+ End Time: 2020-08-21 07:37:22 (GMT-4) (713 seconds)

+ 1 host(s) tested
[root@parrot]-[/home/attacker]
#

12. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd** and press **Enter** to jump to the root directory.
13. Type **cd Desktop** and press **Enter** to navigate to the **Desktop** folder.


Applications Places System
Fri Aug 21, 07:38
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#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: 2020-08-21 07:25:29 (GMT-4)

+ 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
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 19 error(s) and 6 item(s) reported on remote host
+ End Time: 2020-08-21 07:37:22 (GMT-4) (713 seconds)

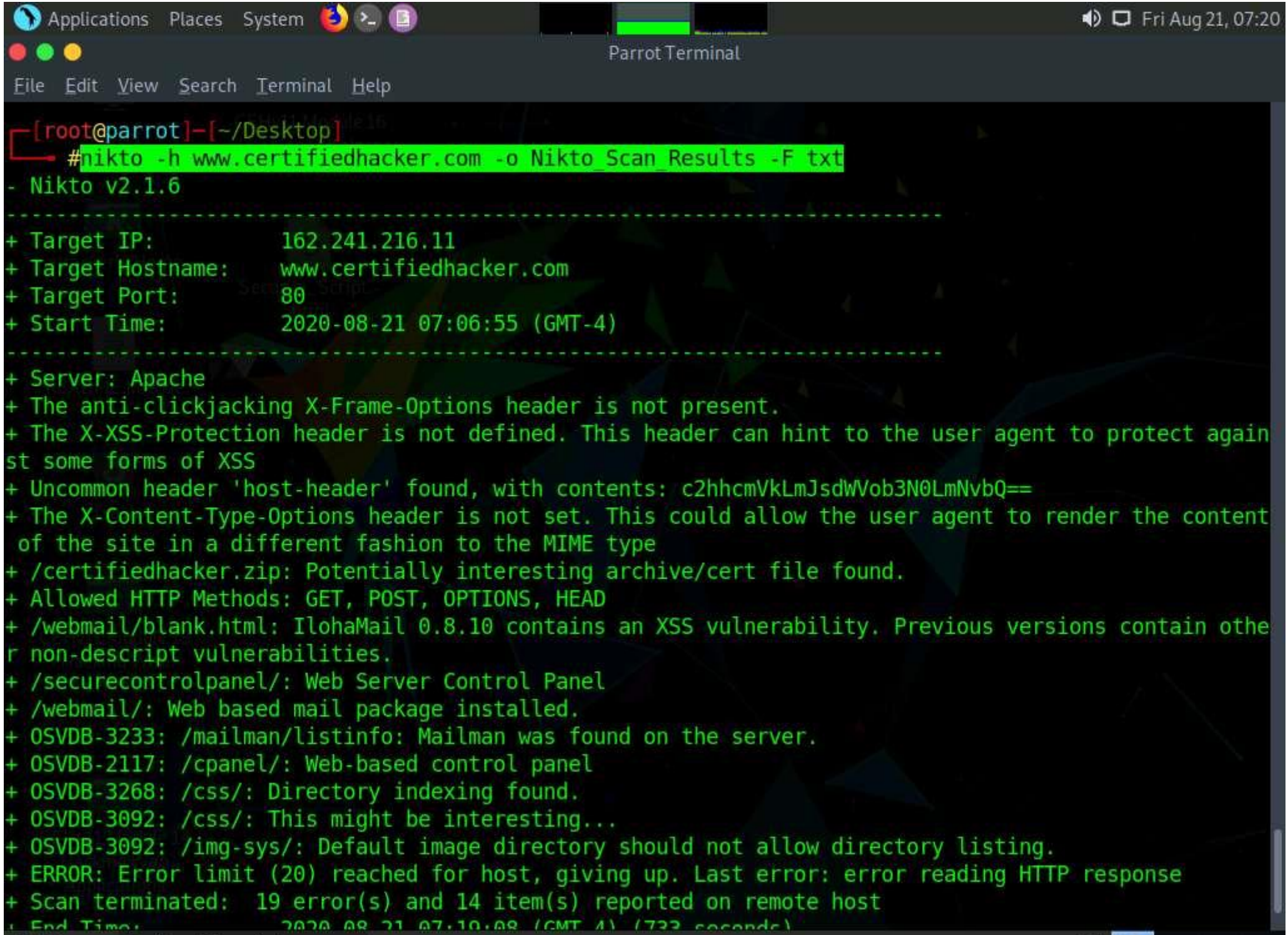
+ 1 host(s) tested
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#cd Desktop
[root@parrot]-[~/Desktop]
#

14. Type **nikto -h (Target Website) -o (File_Name) -F txt**, (here, the target website is **www.certifiedhacker.com**) and press **Enter**.

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

Name the file **Nikto_Scan_Results**

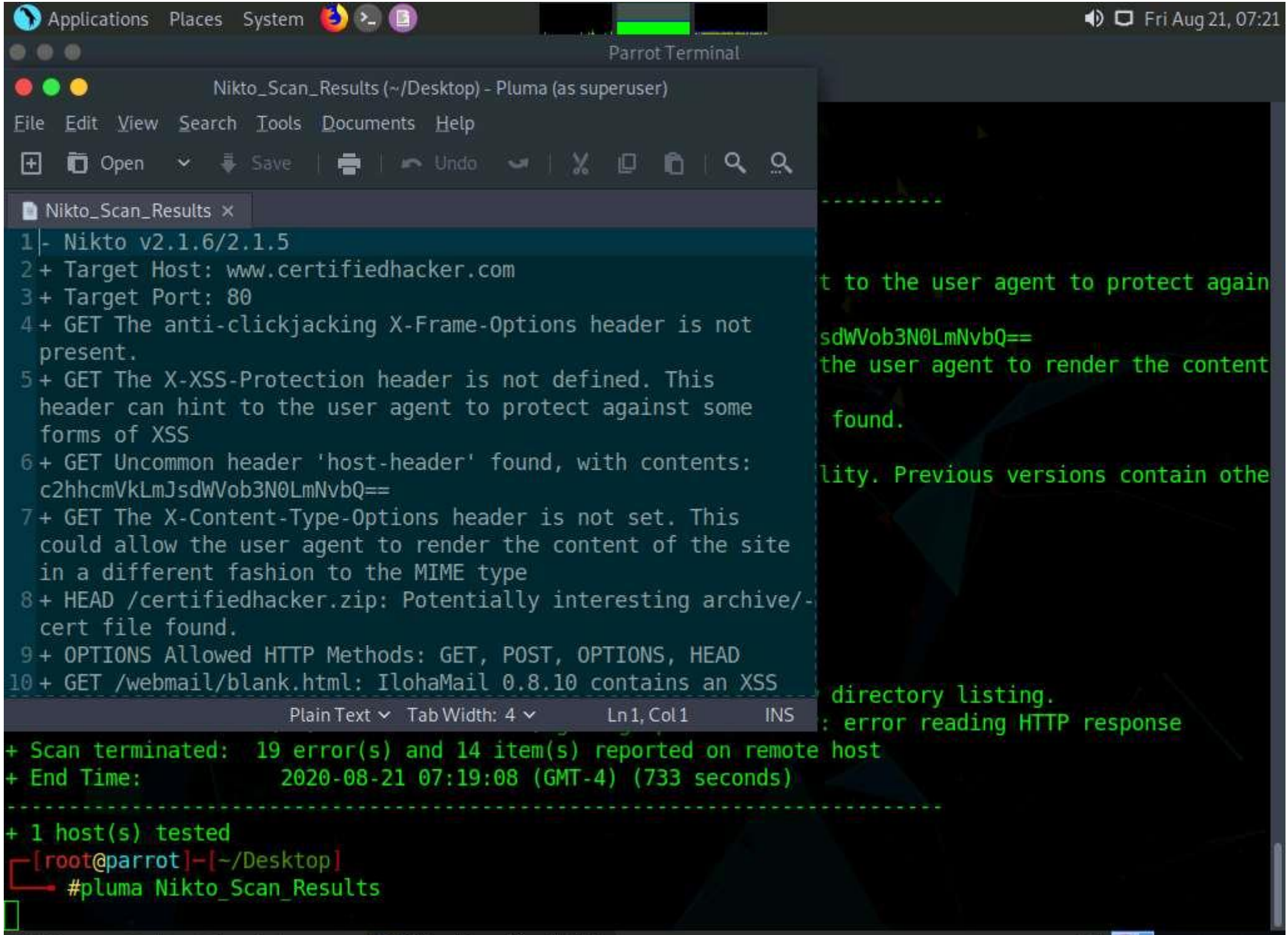
The scan takes approximately 10 minutes to complete.


Applications Places System
Fri Aug 21, 07:20
Parrot Terminal
File Edit View Search Terminal Help
[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: 2020-08-21 07:06:55 (GMT-4)

+ 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
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3092: /img-sys/: Default image directory should not allow directory listing.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 19 error(s) and 14 item(s) reported on remote host

15. Now, type **pluma Nikto_Scan_Results** and press **Enter** to open the created file in a text editor window. The file appears displaying the scanned results, as shown in the screenshot.


Applications Places System
Fri Aug 21, 07:21
Parrot Terminal
Nikto_Scan_Results (~/Desktop) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open Save Undo
Nikto_Scan_Results
1 - Nikto v2.1.6/2.1.5
2 + Target Host: www.certifiedhacker.com
3 + Target Port: 80
4 + GET The anti-clickjacking X-Frame-Options header is not present.
5 + GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
6 + GET Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
7 + GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
8 + HEAD /certifiedhacker.zip: Potentially interesting archive/cert file found.
9 + OPTIONS Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
10 + GET /webmail/blank.html: IlohaMail 0.8.10 contains an XSS
Plain Text Tab Width: 4 Ln 1, Col 1 INS
t to the user agent to protect again
sdWVob3N0LmNvbQ==
the user agent to render the content
found.
lity. Previous versions contain othe
directory listing.
: error reading HTTP response
+ Scan terminated: 19 error(s) and 14 item(s) reported on remote host
+ End Time: 2020-08-21 07:19:08 (GMT-4) (733 seconds)
+ 1 host(s) tested
[root@parrot]-[~/Desktop]
#pluma Nikto_Scan_Results

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.