B. With IP Address, displays the NetBIOS name table and MAC address information
C. NetBIOS name cache information
D. Displays the names registered locally by NetBIOS applications

6. Which one of the following is not an example of SNMP Manager software? A. PRTG
B. SolarWinds
C. OPManager
D. Wireshark

7. Which of the following is correct about SNMP? A. SNMP v 1 does not support encryption B. SNMP v 1 & v2c do not support encryption C. SNMP does not support encryption D. All SNMP versions support encryption

8. SNMPv3 supports:
A. DES
B. Both DES and hashing (MD5 or SHA) C. Hashing
D. SNMP does not support encryption

9. Which port does not belong to NetBIOS over TCP (NetBT)? A. TCP port 136
B. UDP port 137
C. UDP port 138
D. TCP port 139

10. Which of the following statement is true about NTP authentication?
A. NTPv 1 does not support authentication
B. NTPv 1 & NTPv2 do not support authentication
C. NTPv 1, NTPv2 & NTPv3 do not support authentication D. Only NTPv4 supports authentication

Chapter 5: Vulnerability Analysis

Technology Brief

Vulnerability analysis is a part of the scanning phase. It is a major and highly important part of the Hacking cycle. In this chapter, we will discuss the concept of vulnerability assessment, the phases of vulnerability assessment, the types of assessment, the tools, and some other important aspects.

The Concept of Vulnerability Assessment

A fundamental task for a penetration tester is to discover vulnerabilities in an environment. Vulnerability assessment includes discovering weaknesses in an environment, any design flaws, and other security concerns that can cause an Operating System, application, or website to be misused. These vulnerabilities include misconfigurations, default configurations, buffer overflows, Operating System flaws, Open Services, etc. There are different tools available for network administrators and pentesters to scan for vulnerabilities in a network. Any vulnerabilities that are discovered are classified into three different categories based on their threat level, i.e., low, medium, or high. Furthermore, they can also be categorized as an exploit range such as local or remote.

Vulnerability Assessment

Vulnerability Assessment can be defined as a process of examining, discovering, and identifying weaknesses in systems and applications and evaluating the implemented security measures. The security measures deployed in systems and applications are evaluated to identify the effectiveness of the security layer to withstand attacks and exploitations. Vulnerability assessment also helps to recognize the vulnerabilities that could be exploited, any need for additional security layers, and information that can be revealed using scanners.

Types of Vulnerability Assessment

■ *Active Assessment:* Active Assessment includes actively sending requests to the live network and examining the responses. In short, it is a process of assessment that requires probing the targeted host

■ *Passive Assessment:* Passive Assessment usually includes packet sniffing to discover vulnerabilities, running services, open ports, and other information. However, this process of assessment does not involve the targeted host

■ *External Assessment:* External Assessment is a process of assessment that is carried out from a hacker's point of view in order to discover vulnerabilities and exploit them from the outside. Outside of the network refers to how a potential attacker could cause a threat to a resource. External network vulnerability assessment identifies how someone could cause a threat to your network or systems from outside of your network

■ *Internal Assessment:* This is another technique for finding vulnerabilities. Internal assessment includes discovering vulnerabilities by scanning the internal network and infrastructure. Internal network vulnerability assessment is usually based on IT industry best practices and Department of Defense (DoD) technical implementation guides (STIGs). Internal assessment identifies misconfigurations, weaknesses, policy non-compliance vulnerabilities, patching issues, etc. Internal network assessment focuses on network infrastructure in order to secure it.

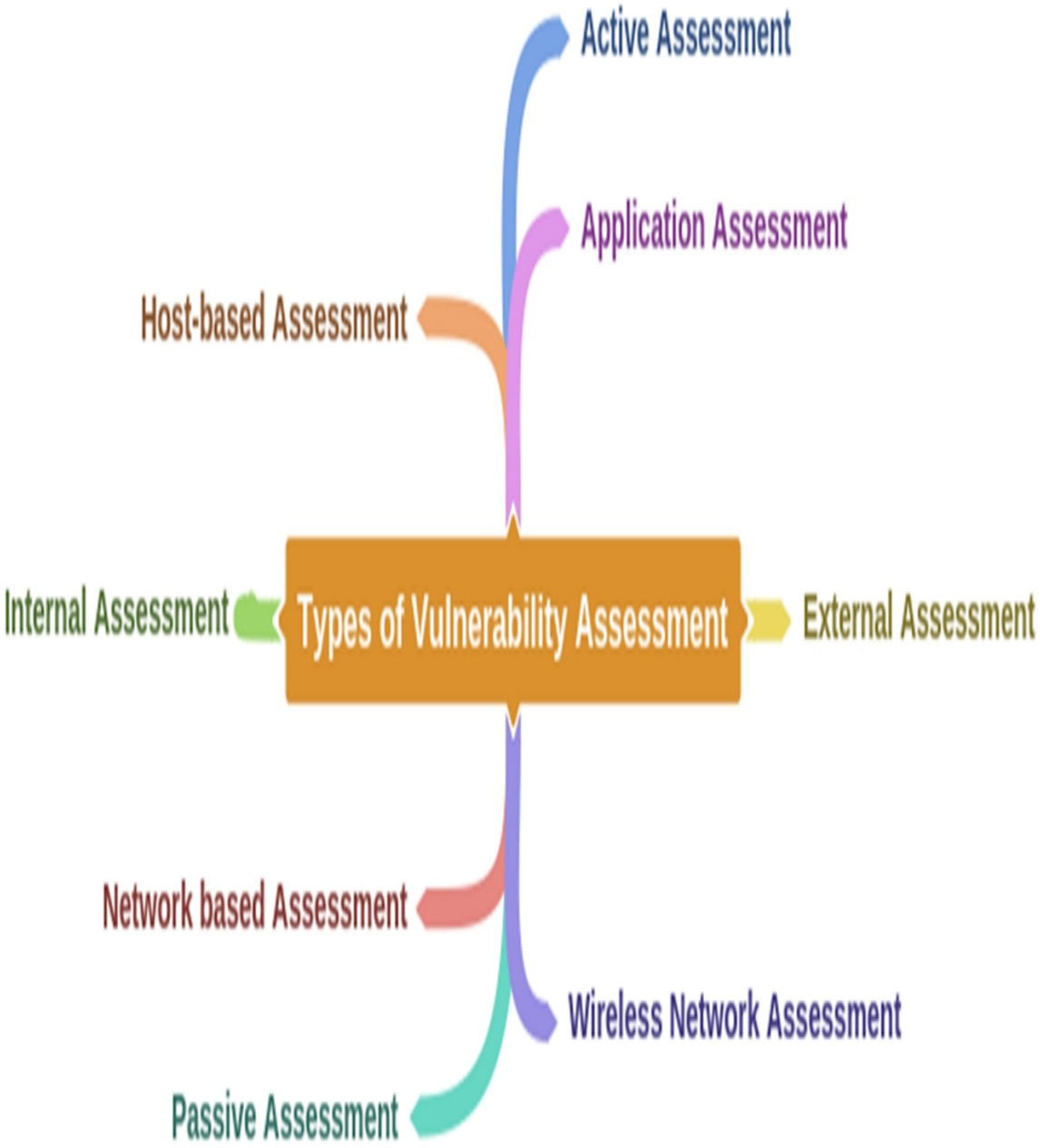


Figure 5-01: Types of Vulnerability Assessment

Vulnerability Assessment Life Cycle

The Vulnerability Assessment life cycle consists of the following phases:

Creating a Baseline

Creating a Baseline is a pre-assessment phase of the vulnerability assessment life cycle. In this phase, a pentester, or network administrator who is performing assessment, identifies the nature of the corporate network, applications, and services. He/she creates an inventory of all resources and assets, which helps to manage and prioritize the assessment. Furthermore, the pentester maps the infrastructure and learns about the security controls, policies, and standards implemented by the organization. Additionally, the baseline helps in planning the process effectively, scheduling tasks, and managing them according to their priority levels.

Vulnerability Assessment

The Vulnerability Assessment phase focuses on assessment of the target. This phase includes the examination and inspection of security measures such as physical security, security policies, and controls. In this phase, the target is evaluated for misconfigurations, default configurations, faults, and other vulnerabilities either by probing each component individually or by using assessment tools. Once the scanning is complete, the findings are ranked in terms of their priority level. At the end of this phase, the vulnerability assessment report shows all detected vulnerabilities, their scope, and priority.

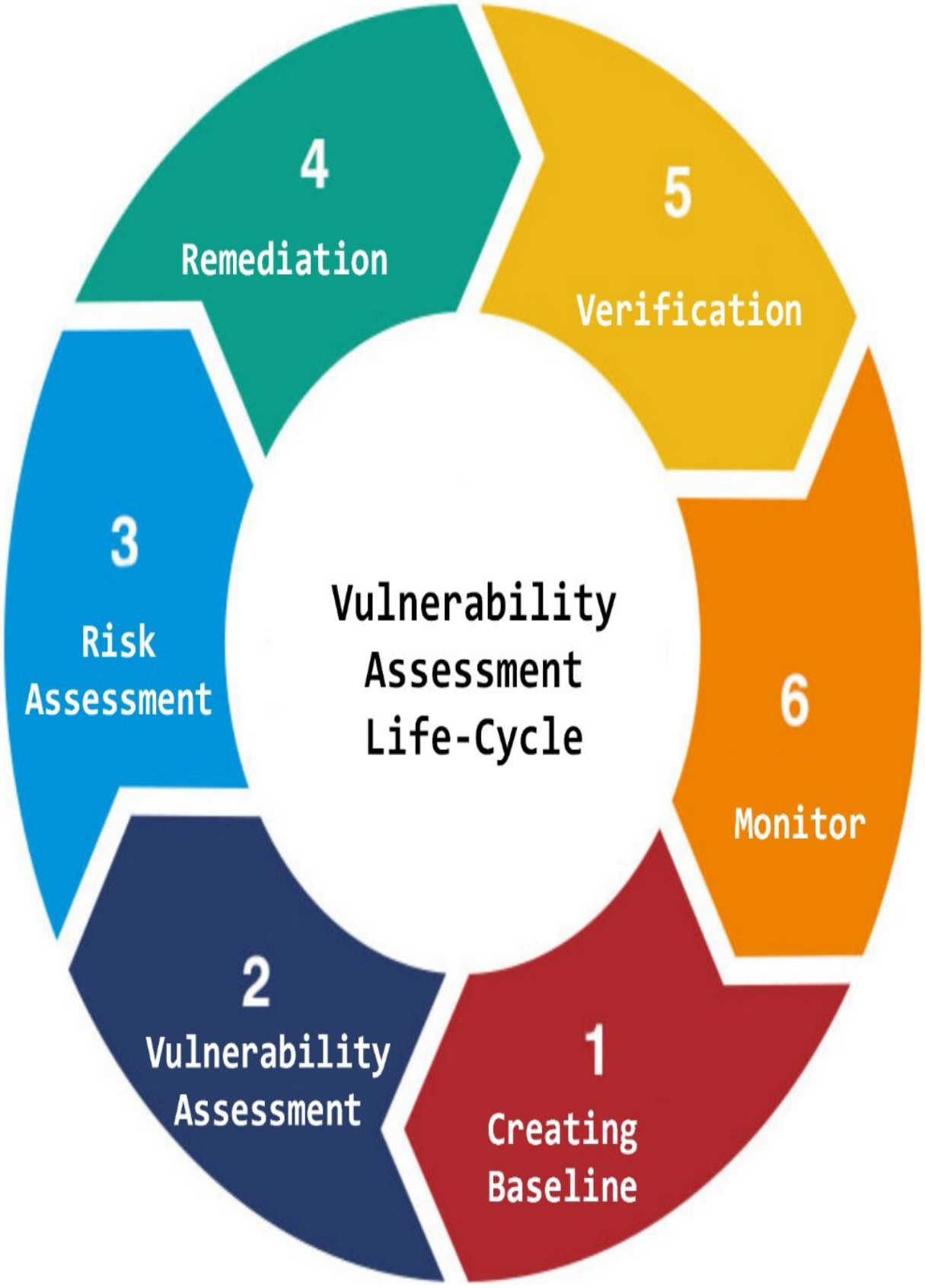


Figure 5 - 03: Vulnerability Assessment Life Cycle

Figure 5-02: Vulnerability Assessment Life Cycle

Risk Assessment

Risk Assessment includes scoping identified vulnerabilities and their impact on the corporate network or on an organization.

Remediation

The Remediation phase includes remedial action in response to the detected vulnerabilities. High priority vulnerabilities are addressed first because they can cause a huge impact.

Verification

The Verification phase ensures that all vulnerabilities in an environment are eliminated. *Monitor*

The Monitoring phase includes monitoring the network traffic and system behaviors for any further intrusion.

Note:

Annualized Loss Expectancy (ALE) is the product of Annual Rate of Occurrence (ARO) and Single Loss Expectancy (SLE) i.e. mathematically expressed as:

ALE = ARO * SLE

While performing quantitative risk assessment, ALE estimation defines the cost of any protection or countermeasure to protect an asset. SLE defines the loss value of a single incident whereas ARO estimates the frequency – how often a threat is successful in exploiting a vulnerability. Exposure Factor (EF) is the subjective, potential percentage of loss to a specific asset if a specific threat is realized.

SLE = EF * AV

Real-World Scenario: An organization is approximating the cost of replacement and recovery operations. The maintenance team reported that the hardware costs $300, which needs to be replaced once in every three years. A technician charges $ 10 per hour for the maintenance; it takes 14 hours to completly replace the hardware and install the software. The Exposure Factor (EF) is 1 (100%). The requirement for quantitative risk analysis is to calculate the Single Loss

Expectancy (SLE), the Annual Rate of Occurrence (ARO) and the Annualized Loss Expectancy (ALE).

Calculation :
Asset Value (AV) = $300 + (14 * $ 10) = $440 Single Loss Expectancy (SLE) = EF * AV = 1 * $440 = $440 Annual Rate of Occurrence (ARO) = 1/3 (Once in every three year) Annual Loss Expectancy (ALE) = SLE * ARO = 1/3 * $440 = $ 146.6

Vulnerability Assessment Solutions

Product-based Solution Vs Service-based Solution

Product-based Solutions are deployed within the corporate network of an organization or a private network. These solutions are usually dedicated for internal (private) networks.

Service-based Solutions are third-party solutions, which offer security and auditing services to a network. These solutions can be hosted either inside or outside the network. As these third-party solutions are allowed to access and monitor the internal network, they too carry a security risk.

Tree-based Assessment Vs. Inference-based Assessment

Tree-based Assessment is an assessment approach in which an auditor follows different strategies for each component of an environment. For example, consider a scenario of an organization's network on which different machines are live—the auditor may use a different approach for Windows-based machines and a different approach for Linuxbased servers.

Inference-based Assessment is another approach to assessing vulnerabilities depending on the inventory of protocols in an environment. For example, if an auditor finds a protocol, using inference-based assessment approach, he will look for ports and services related to that protocol.

Best Practice for Vulnerability Assessment

Following are some recommended steps for vulnerability assessment to achieve effective results. A network administrator or auditor must follow these best practices for vulnerability assessment.

■ Before starting any vulnerability assessment tool on a network, the auditor must understand the complete functionality of that assessment tool. This will help in selecting the appropriate tool for extracting the desired information

■ Make sure that the assessment tool will not cause any sort of damage or render services unavailable while running on a network ■ Be specific about the scan's source location to reduce the focus area ■ Run a scan frequently for identifying vulnerabilities

Vulnerability Scoring Systems

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) helps in diagnosing the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (i.e., low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Security Base Score Rating None 0.0 Low 0. 1 3.9 Medium 4.0 6.9 High 7.0 8.9 Critical 9.0 10.0 *Table 5-01: CVSSv3 Scoring*

To learn more about CVSS-SIG, go to the website https://www.first.org . *Common Vulnerabilities and Exposure (CVE)*

Common Vulnerabilities and Exposure (CVE) is another platform where you can find information about vulnerabilities. CVE maintains a list of known vulnerabilities including an identification number and description of cybersecurity vulnerabilities.

The U.S. National Vulnerability Database (NVD) was launched by the National Institute of Standards and Technology (NIST). The CVE entities are input to the NVD, which automates vulnerability management,

security and compliance management using CVE entries to provide enhanced information for each entity, for example fixing information, severity scores, and impact ratings. Apart from its enhanced information, the NVD also provides advanced search features such as using an Operating System, vendor's name, product name, version number, and by vulnerability type, severity, related exploit range, and impact.

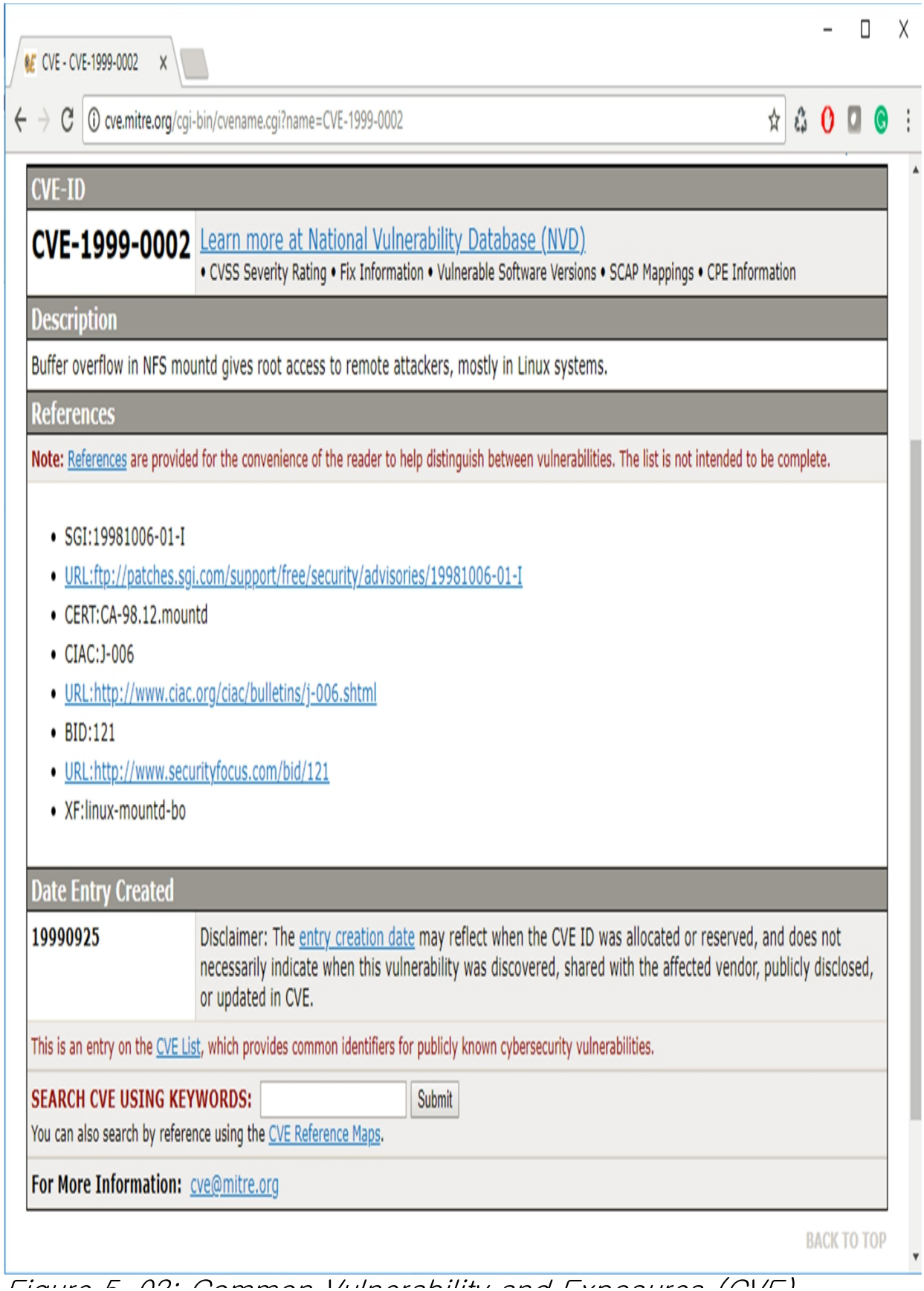


Figure 5- 03: Common Vulnerability and Exposures (CVE)

Figure 5-03: Common Vulnerability and Exposures (CVE)

To learn more about CVE, go to the website http://cve.mitre.org .

Vulnerability Scanning

In this era of modern technology and advancement, various tools have made finding vulnerabilities in an existing environment very easy. Different tools, automated as well as manual, are available to help you find vulnerabilities. Vulnerability Scanners are automated utilities that are specially developed to detect vulnerabilities, weaknesses, problems, and loopholes in an Operating System, network, software, and applications. These scanning tools perform deep inspection of scripts, open ports, banners, running services, configuration errors, and other areas.

These vulnerability scanning tools include:

- Nessus
- OpenVAS
- Nexpose
- Retina
- GFI LanGuard
- Qualys FreeScan, etc.

These tools are not only used by security experts to find any risks and vulnerabilities in running software and applications but are also used by attackers to find any loopholes in an organization's operating environment.

Vulnerability Scanning Tool

1. Nessus

Nessus Professional Vulnerability Scanner is the most comprehensive vulnerability scanner software powered by Tenable Network Security. This scanning product focuses on vulnerabilities and configuration assessment. By using this tool, you can customize and schedule scans and extract reports.

2. GFI LanGuard

GFI LanGuard is a network security and patch management software

that performs virtual security consultancy. This product offers:

- Patch Management for Windows®, Mac OS® and Linux®
- Path Management for third-party applications
- Vulnerability scanning for computers and mobile devices
- Smart network and software auditing
- Web reporting console
- Tracking latest vulnerabilities and missing updates

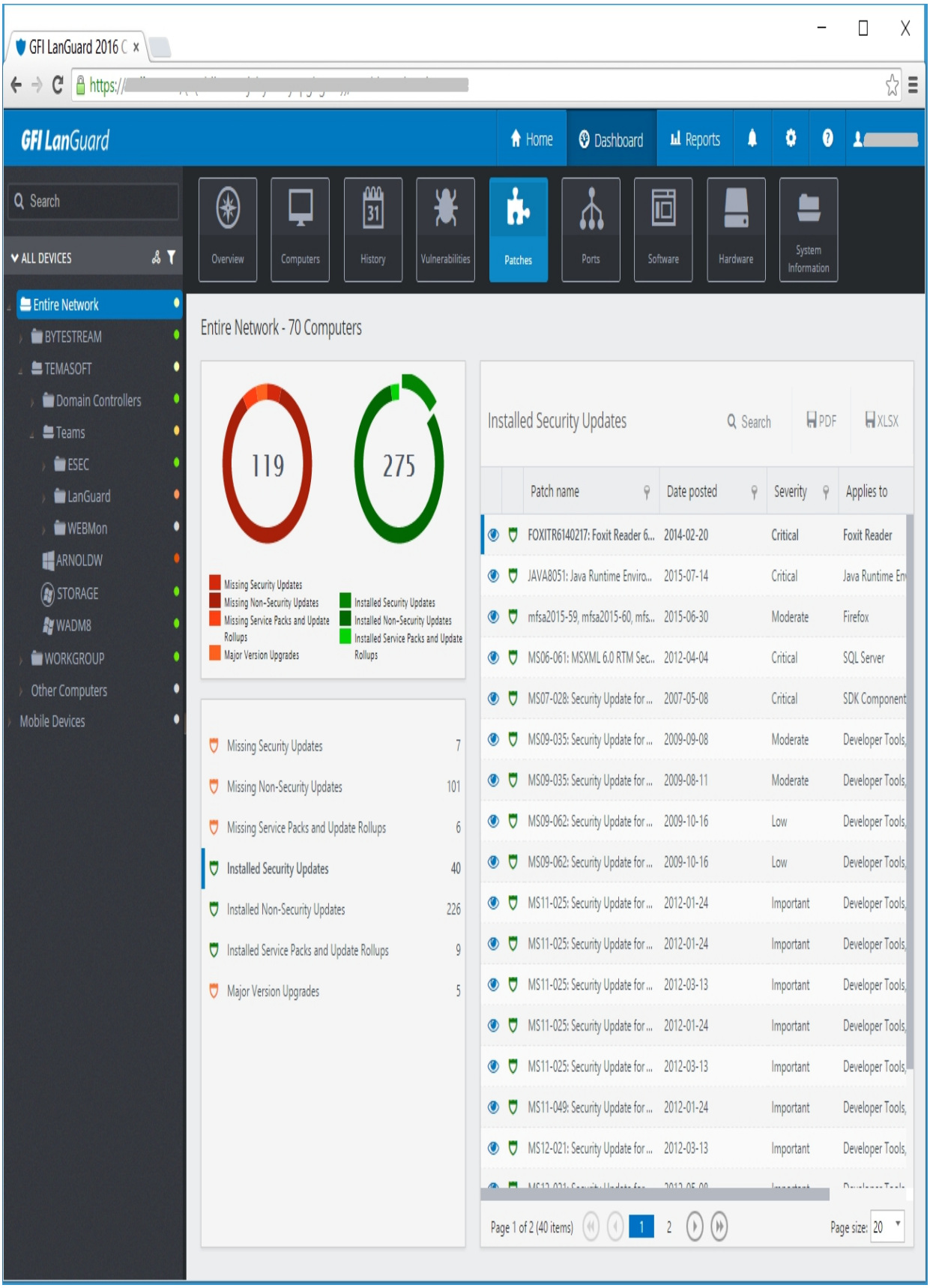


Figure 5 .04: GFI LanGuard Vulnerability Scanning Tool

Figure 5-04: GFI LanGuard Vulnerability Scanning Tool

3. Qualys FreeScan

Qualys FreeScan tool offers Online Vulnerability scanning. It provides a quick snapshot of the security and compliances posture of a network and web along with recommendations. Qualys FreeScan tool is effective for:

- Network Vulnerability scans for server and App
- Patches
- OWA SP Web Application Audits
- SCAP Compliance Audits

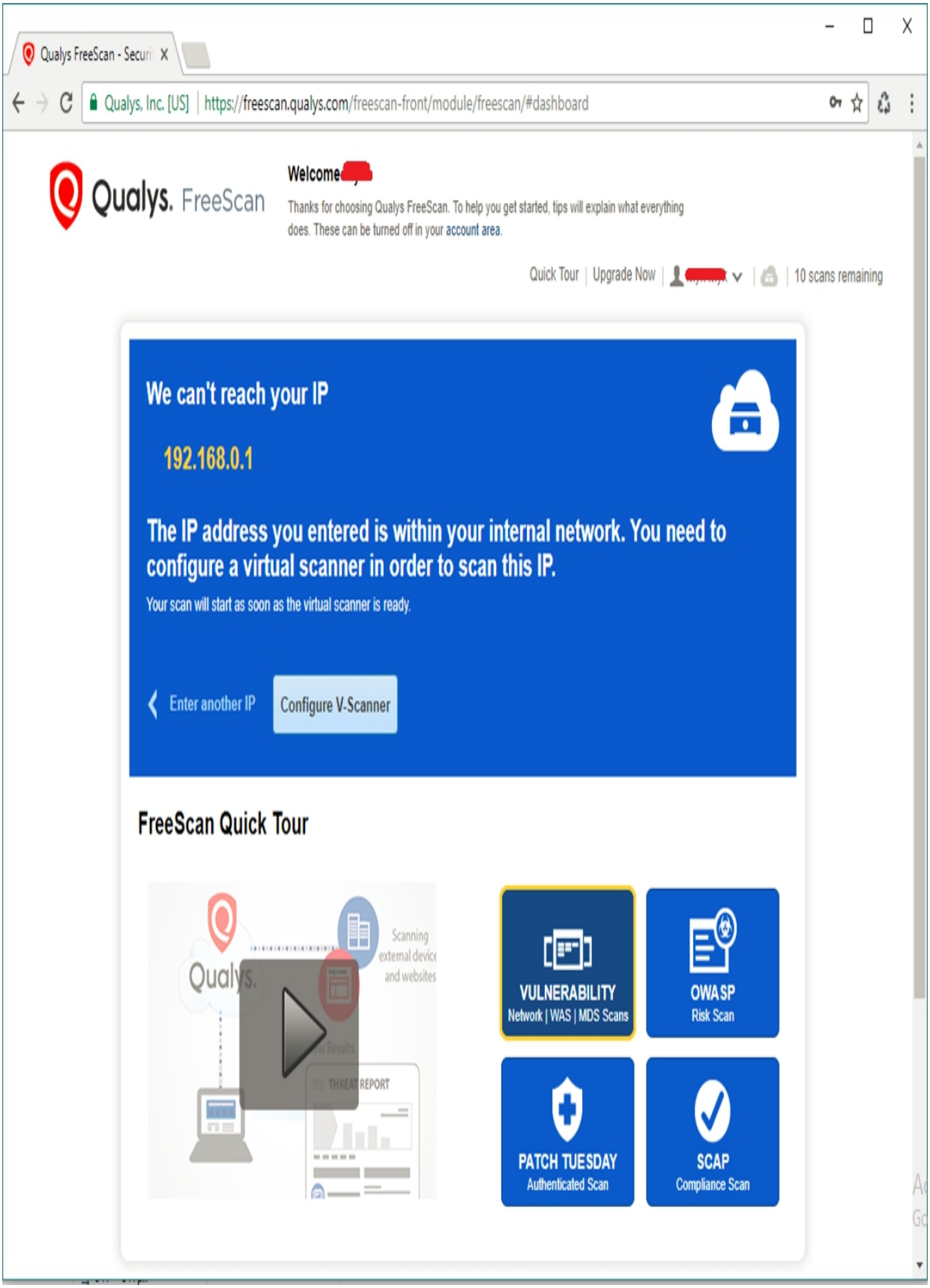


Figure 5-05: Qualys FreeScan Vulnerability Scanning Tool

Figure 5-05: Qualys FreeScan Vulnerability Scanning Tool

Go to http://www.qualys.com to purchase this vulnerability scanning tool or register for the trial version and try to perform a scan. To scan the local network, Qualys offers a Virtual Scanner, which can be virtualized on any virtualization hosting environment. Figure 5-06 shows the results of a vulnerability scan performed on a targeted network.

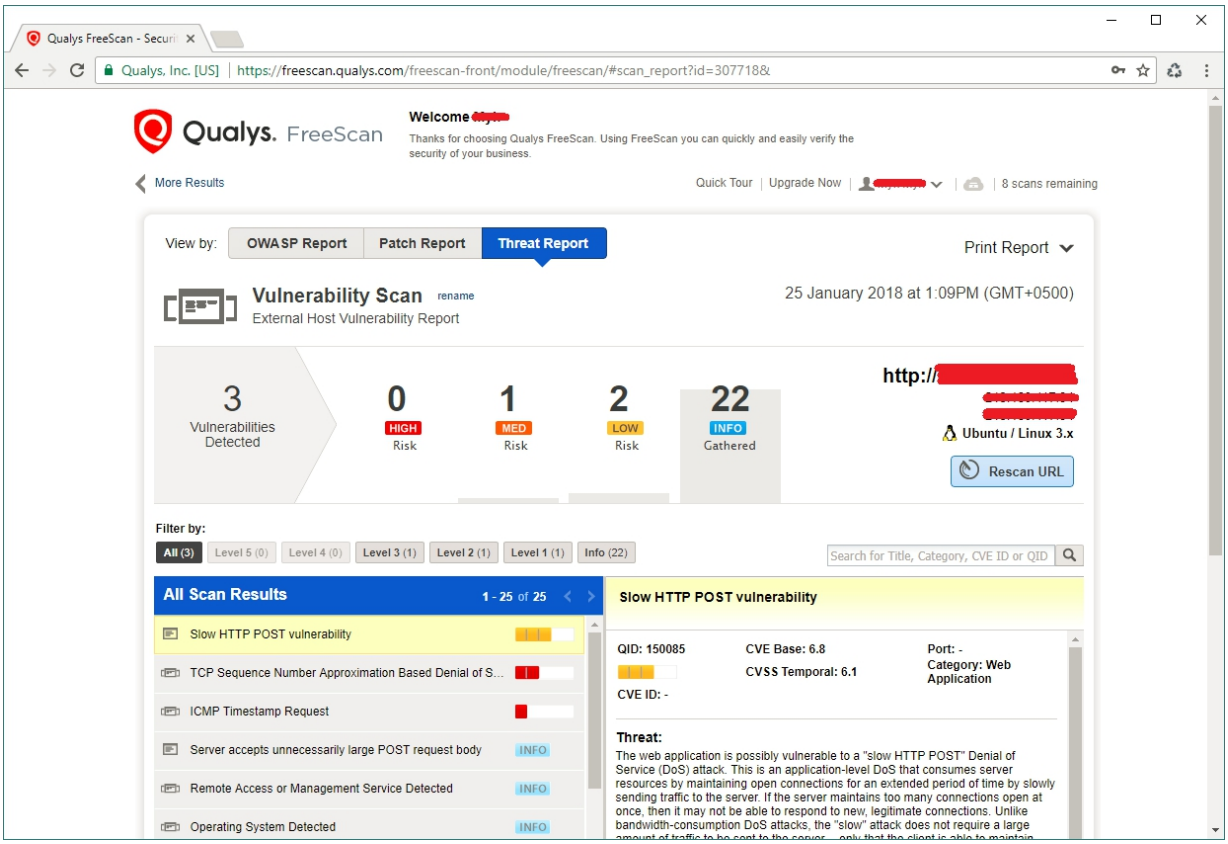


Figure 5-06: Qualys FreeScan Vulnerability Scanning Tool

Vulnerability Scanning Tools for Mobiles

Following is a list of vulnerability scanning tools for mobiles:

Application	Website
Retina CS for Mobile	http://www.byondtrust.com
Security Metrics Mobile Scan	http://www.securitymetrics.com
Nessus Vulnerability Scanner	http://www.tenable.com

Table 5-02: Vulnerability Scanning Tools for Mobiles

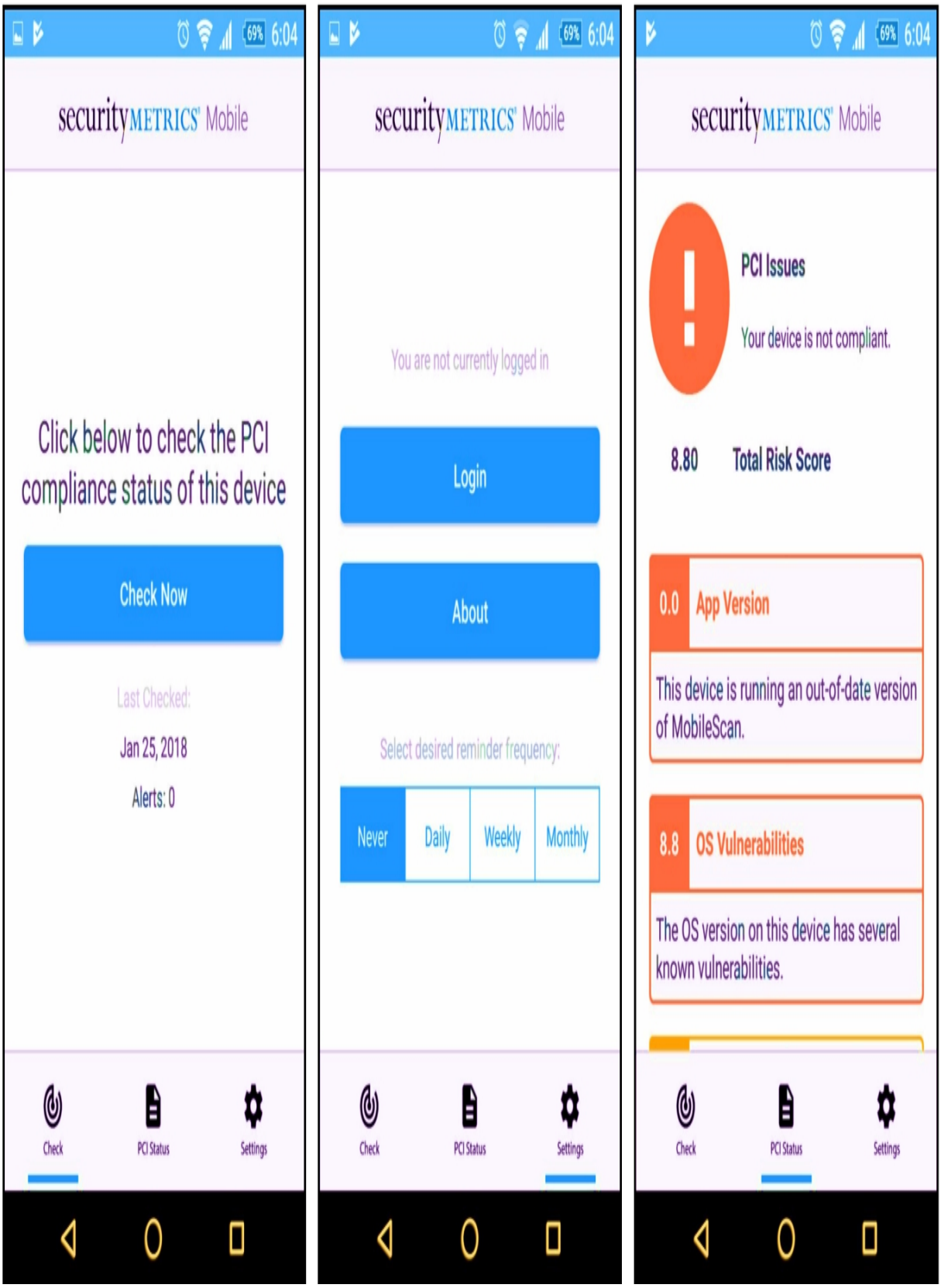
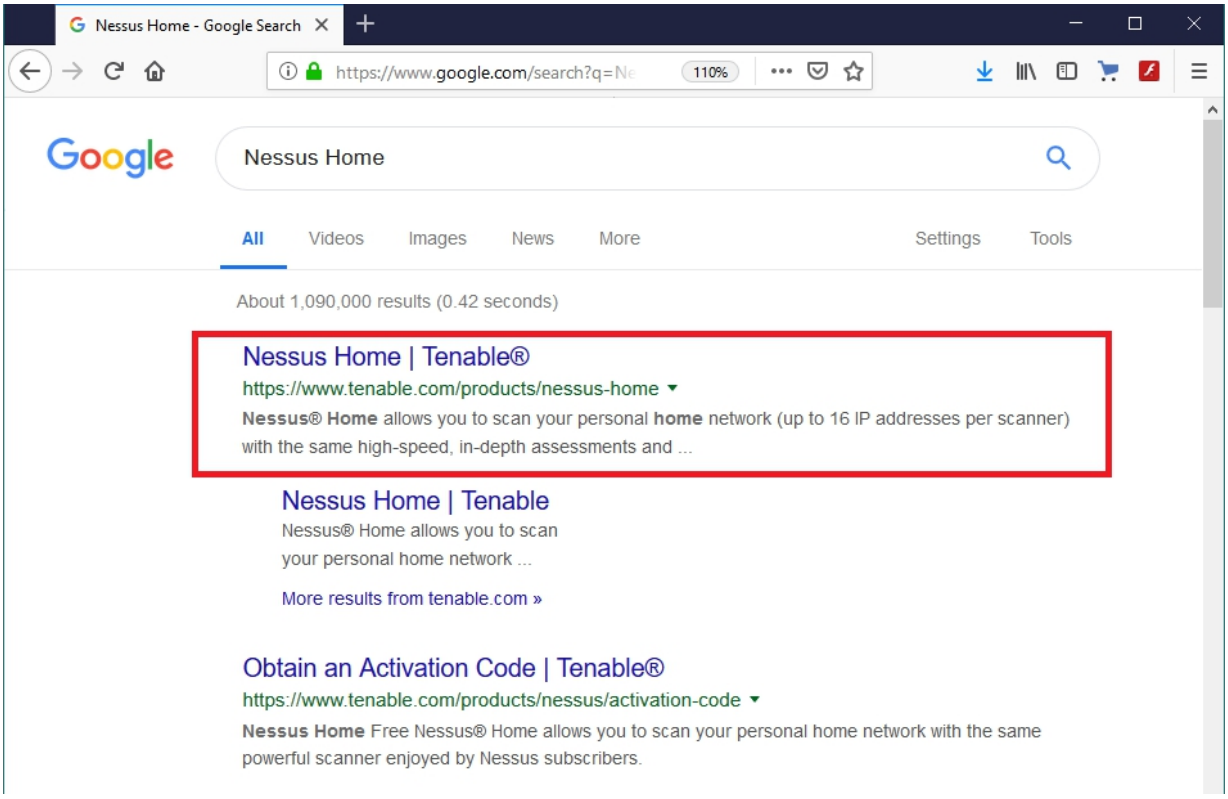


Figure 5-07: Security Metrics Mobile Scan

LAB 5- 1: Installing and Using a Vulnerability Assessment Tool

Main Objective: In this lab, you will learn how to install and use a vulnerability assessment tool. There are many tools available for vulnerability scanning. The one we will be installing and using is Nessus.

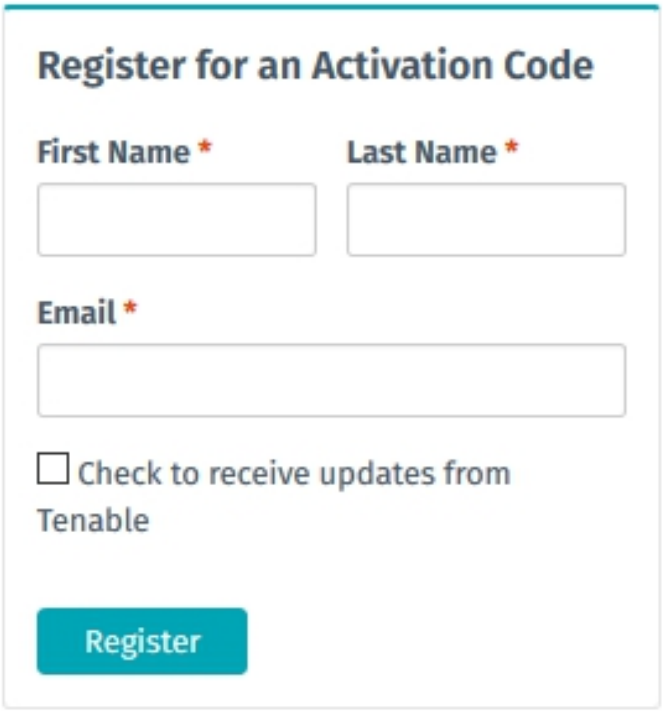
Go to the browser and type "Nessus Home". Click on the Nessus home link, as marked below.



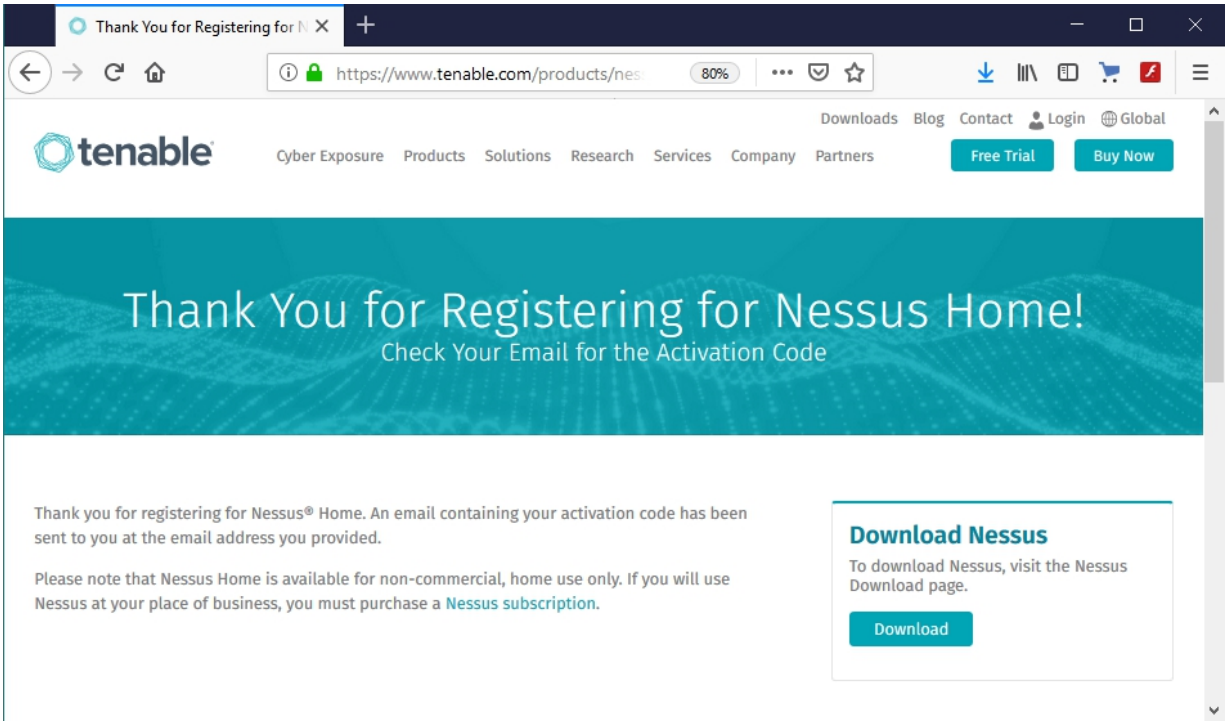
This will take you to the Nessus registration page. You need to register in order to get the activation code, which you are going to need to activate Nessus.

For registration, you need to put in your first name, last name, and email

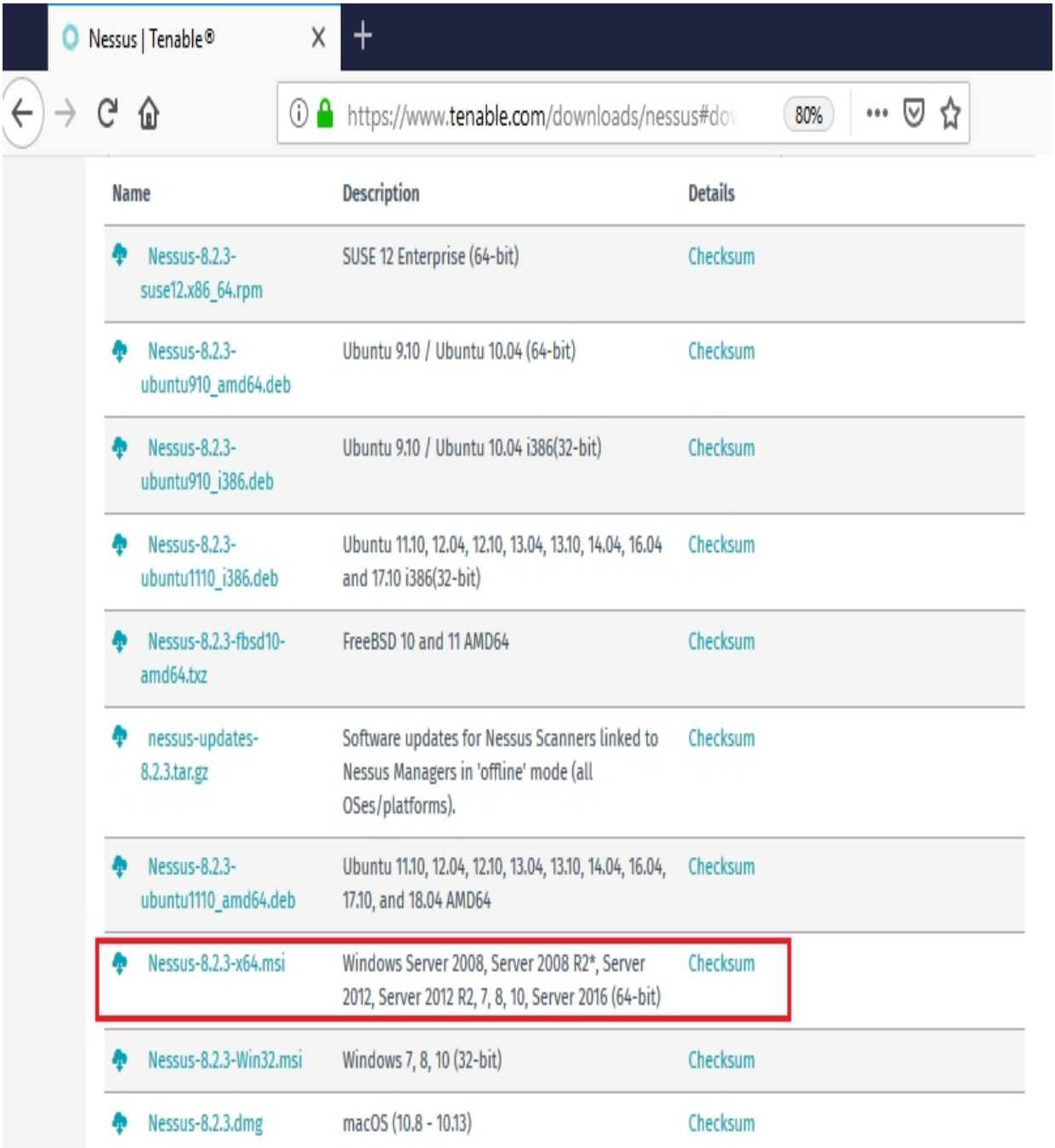
address. Check the checkbox and click on “Register”.



Now to download Nessus, click on the download link.

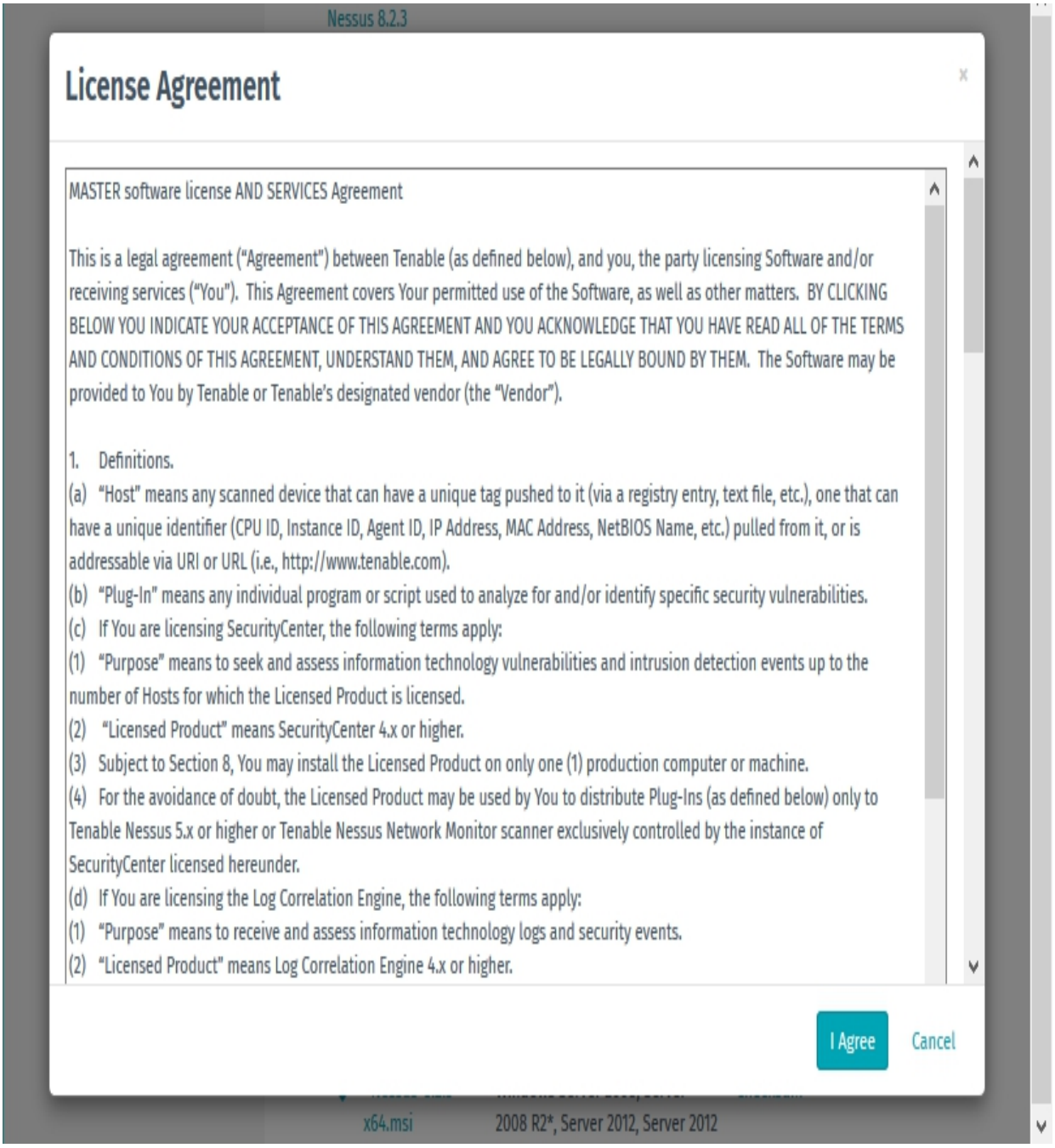


Select the Operating System on which you are going to install Nessus. Here, we are going to install it on Windows 8 machine (64 bit), therefore we will download the first link, which is for the 64-bit version of Windows.

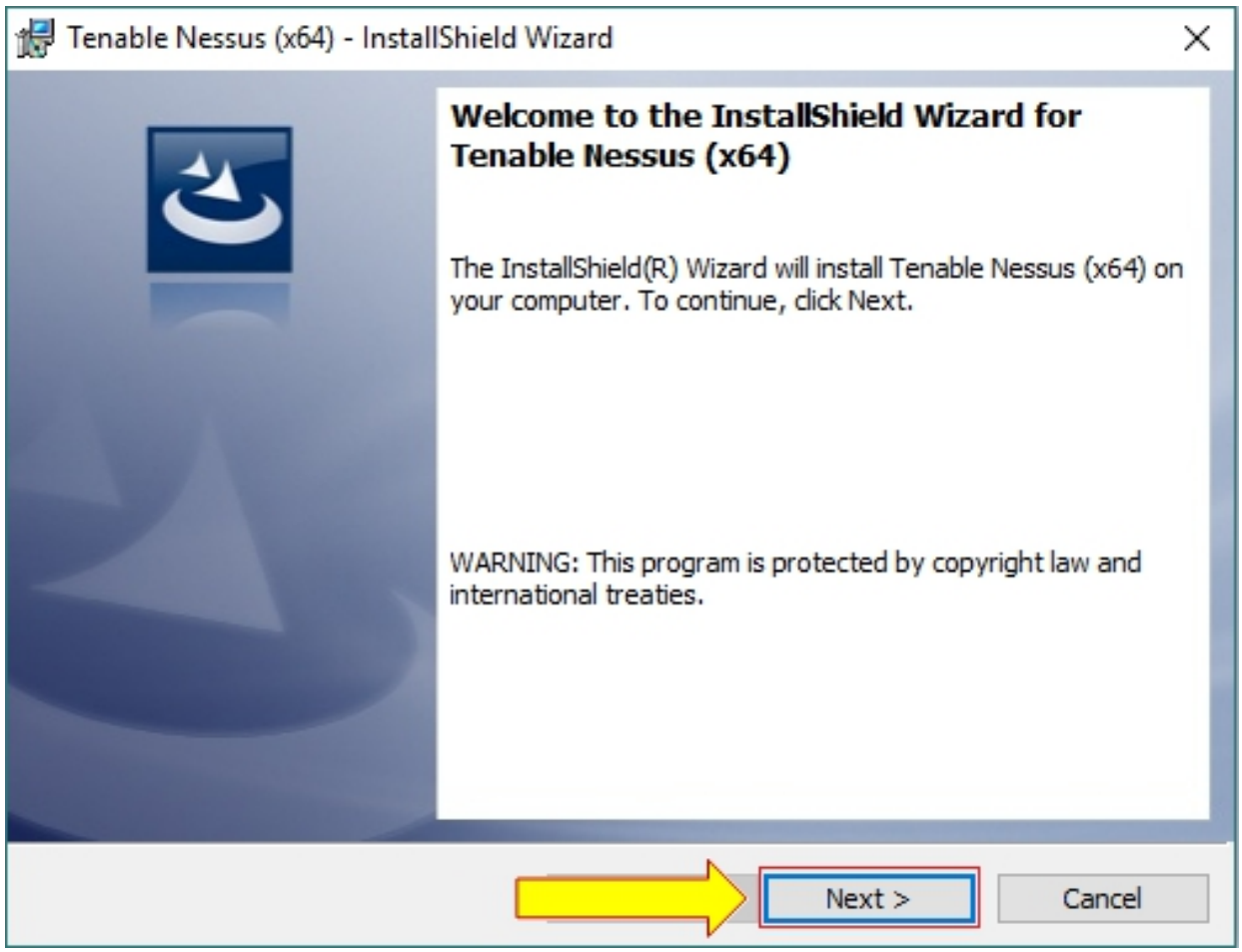


Name	Description	Details
Nessus-8.2.3-suse12.x86_64.rpm	SUSE 12 Enterprise (64-bit)	Checksum
Nessus-8.2.3-ubuntu910_amd64.deb	Ubuntu 9.10 / Ubuntu 10.04 (64-bit)	Checksum
Nessus-8.2.3-ubuntu910_i386.deb	Ubuntu 9.10 / Ubuntu 10.04 i386(32-bit)	Checksum
Nessus-8.2.3-ubuntu1110_i386.deb	Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 i386(32-bit)	Checksum
Nessus-8.2.3-fbsd10-amd64.txz	FreeBSD 10 and 11 AMD64	Checksum
nessus-updates-8.2.3.tar.gz	Software updates for Nessus Scanners linked to Nessus Managers in 'offline' mode (all OSes/platforms).	Checksum
Nessus-8.2.3-ubuntu1110_amd64.deb	Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04, 17.10, and 18.04 AMD64	Checksum
Nessus-8.2.3-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	Checksum
Nessus-8.2.3-Win32.msi	Windows 7, 8, 10 (32-bit)	Checksum
Nessus-8.2.3.dmg	macOS (10.8 - 10.13)	Checksum

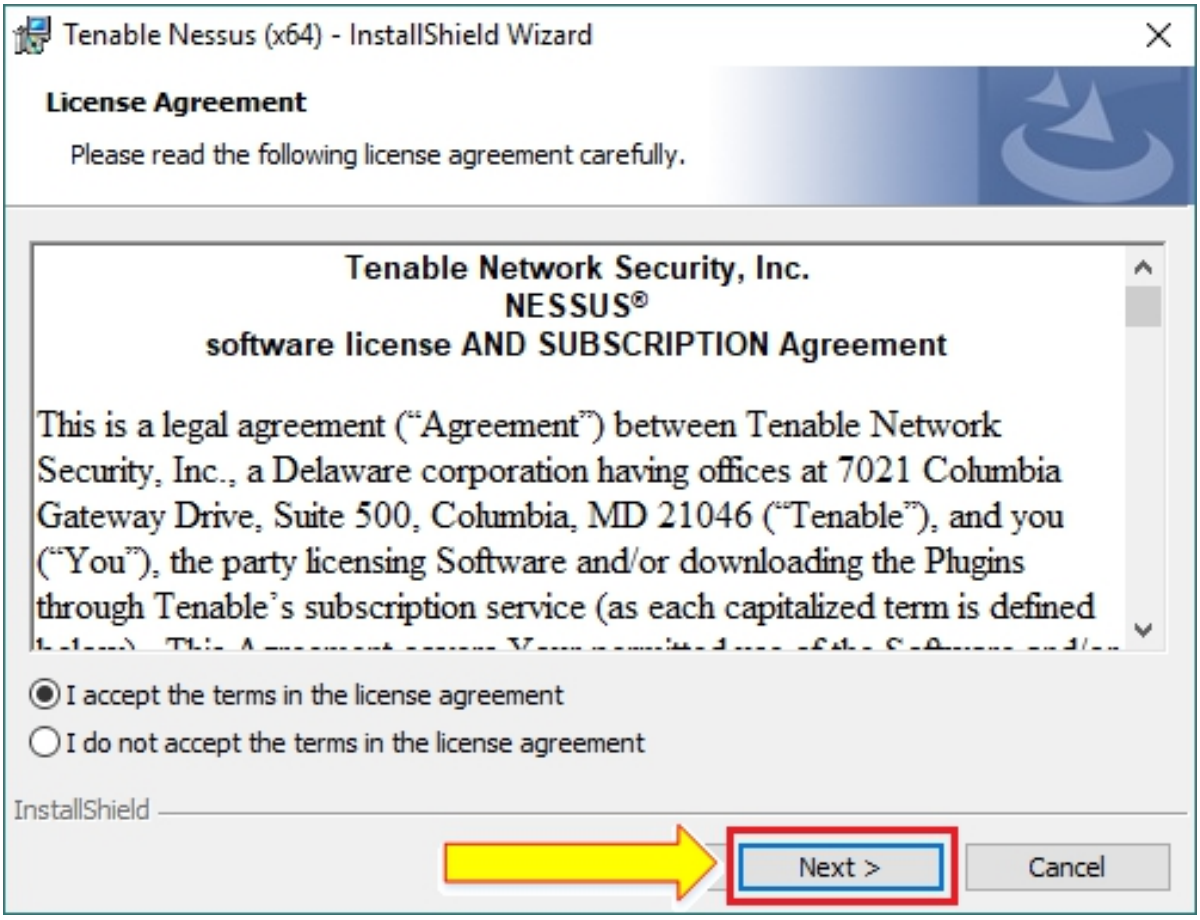
Now read the agreement, click on "I Agree", and save the file to your computer.



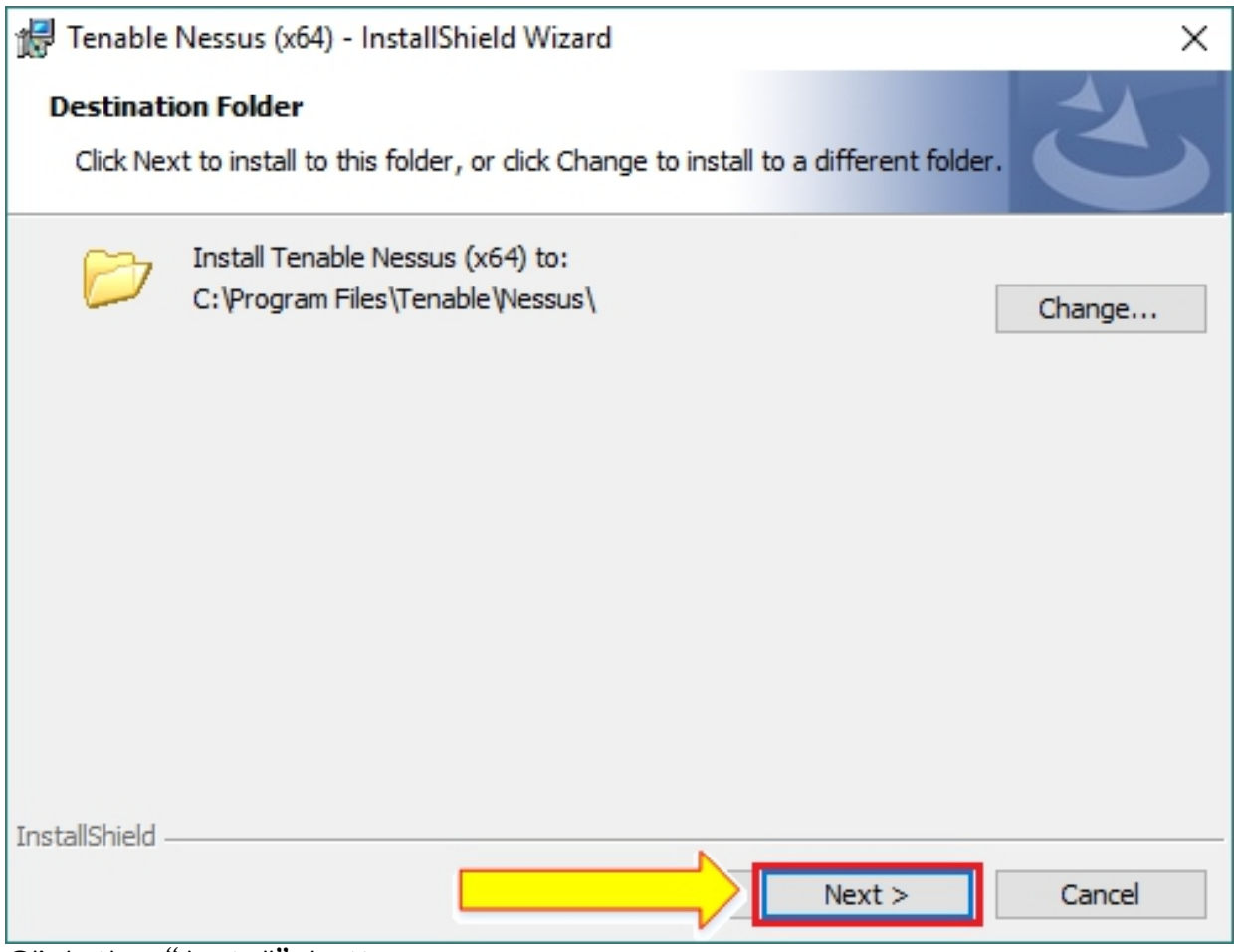
Download and install the software.



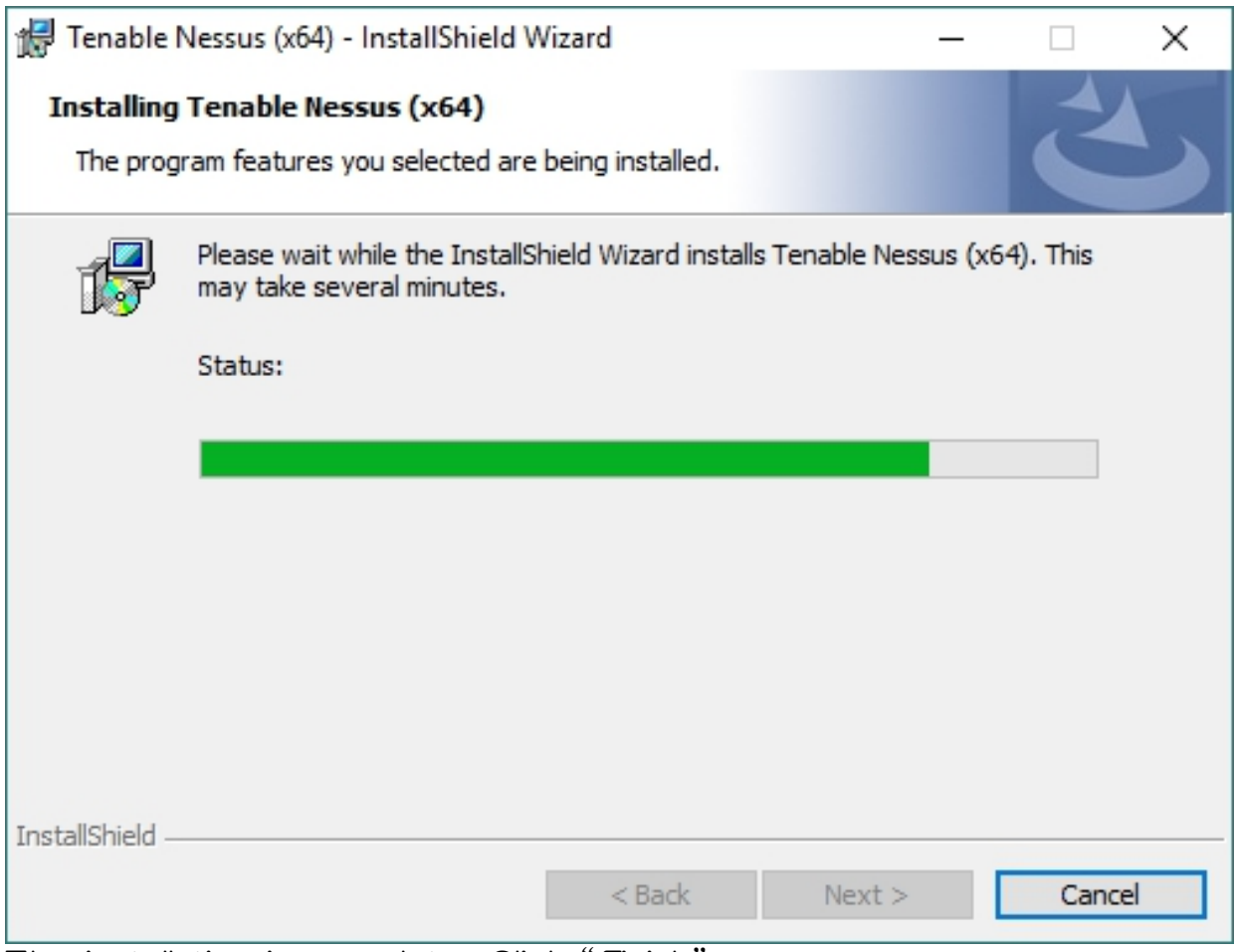
Select “I agree” and click “Next”.



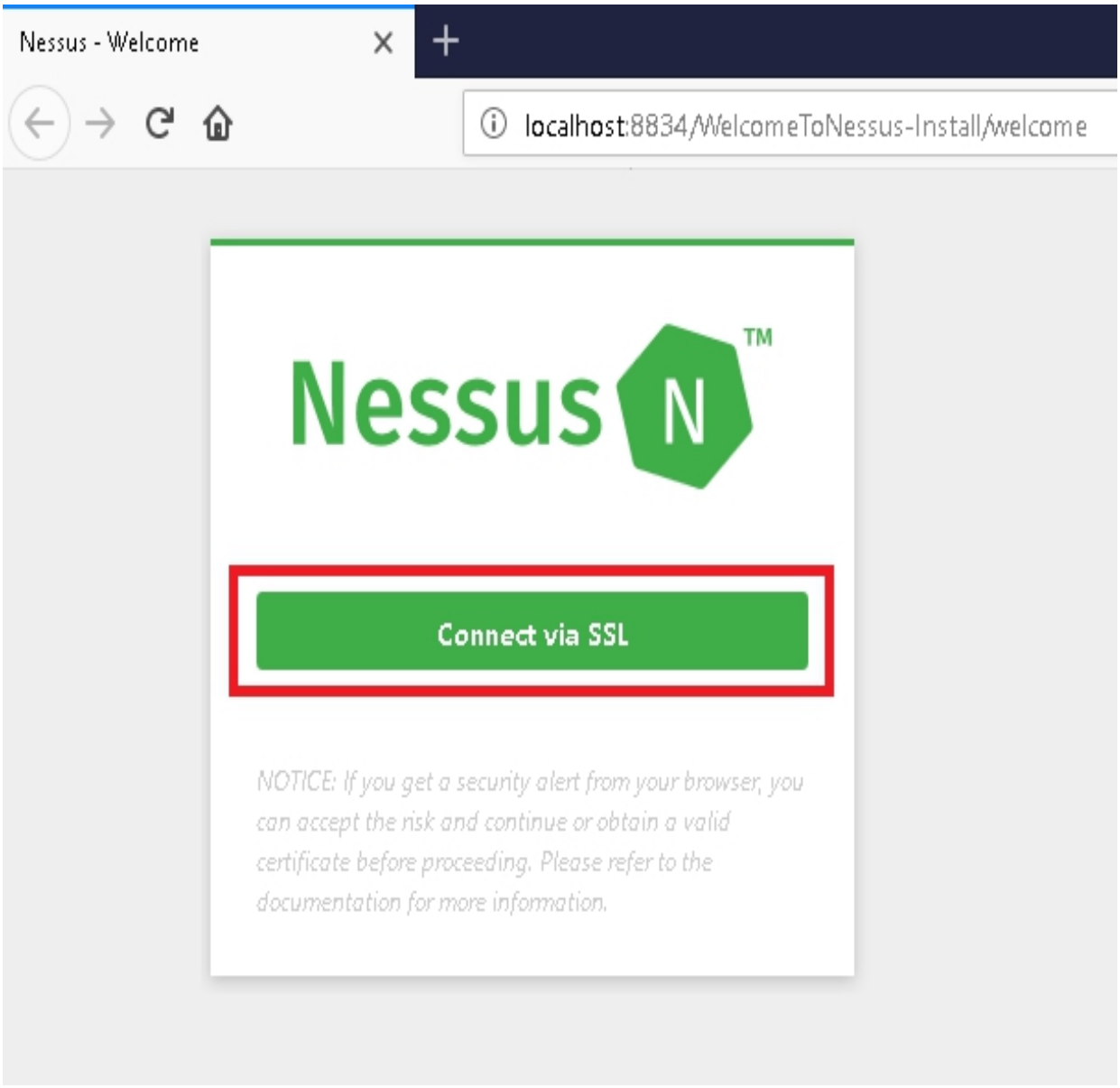
Now, if you want to change the file destination, click on the "Change" button, or else just click "Next".



Click the “Install” button.
The installation process will now start.

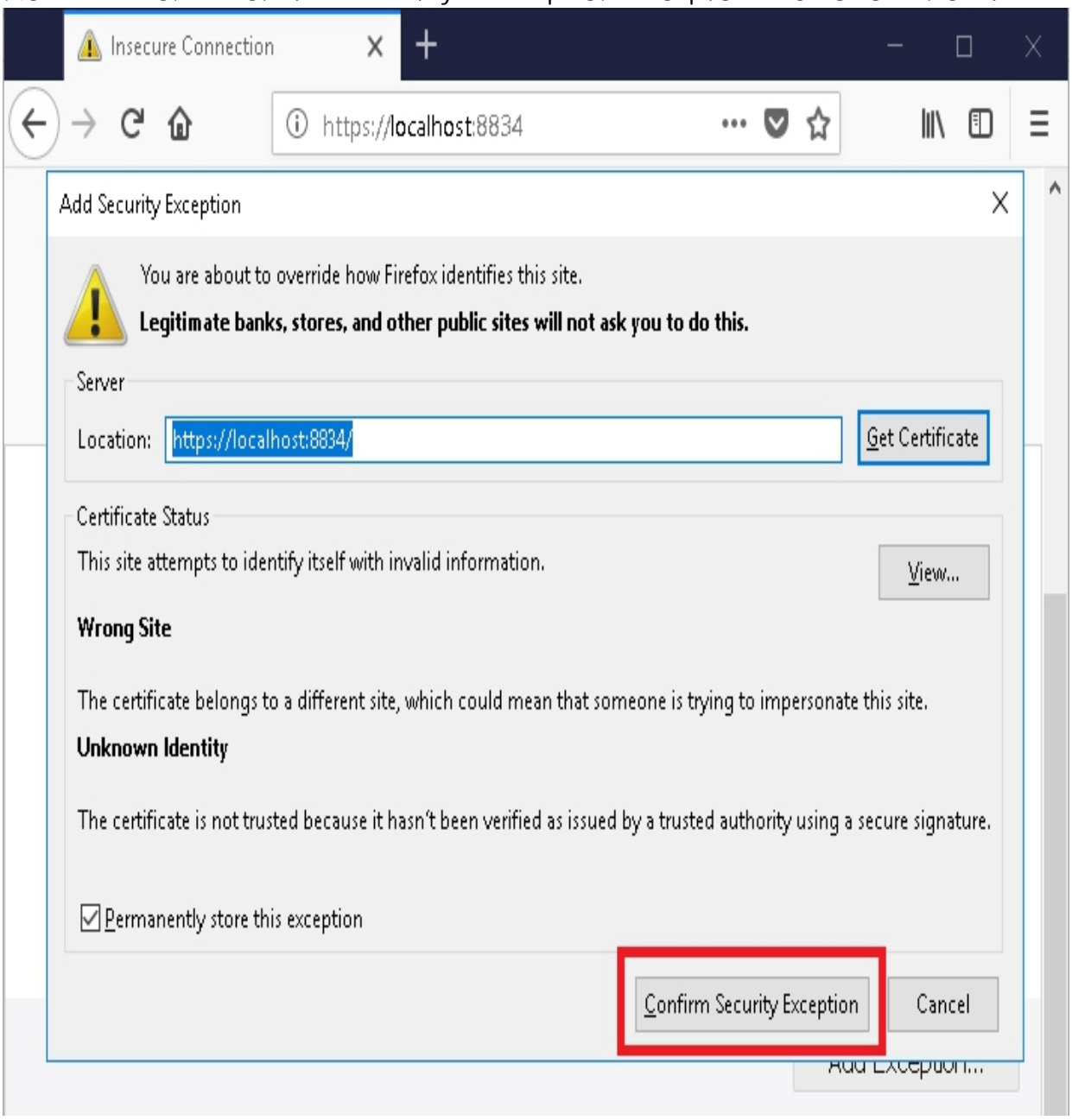


The installation is complete. Click “Finish”.
When you see this window, click on “Connect via SSL”.

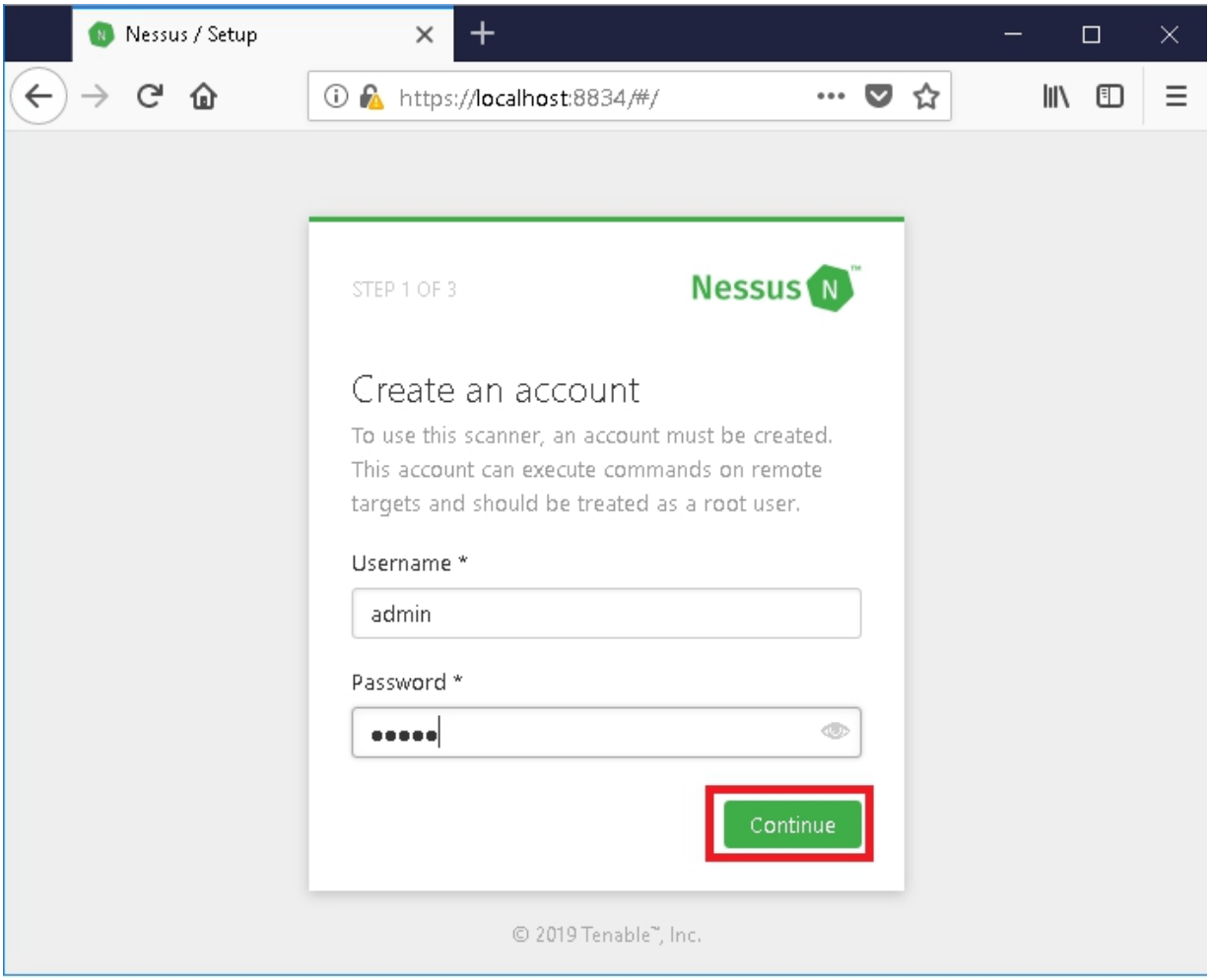


Click on the “Advanced” option.

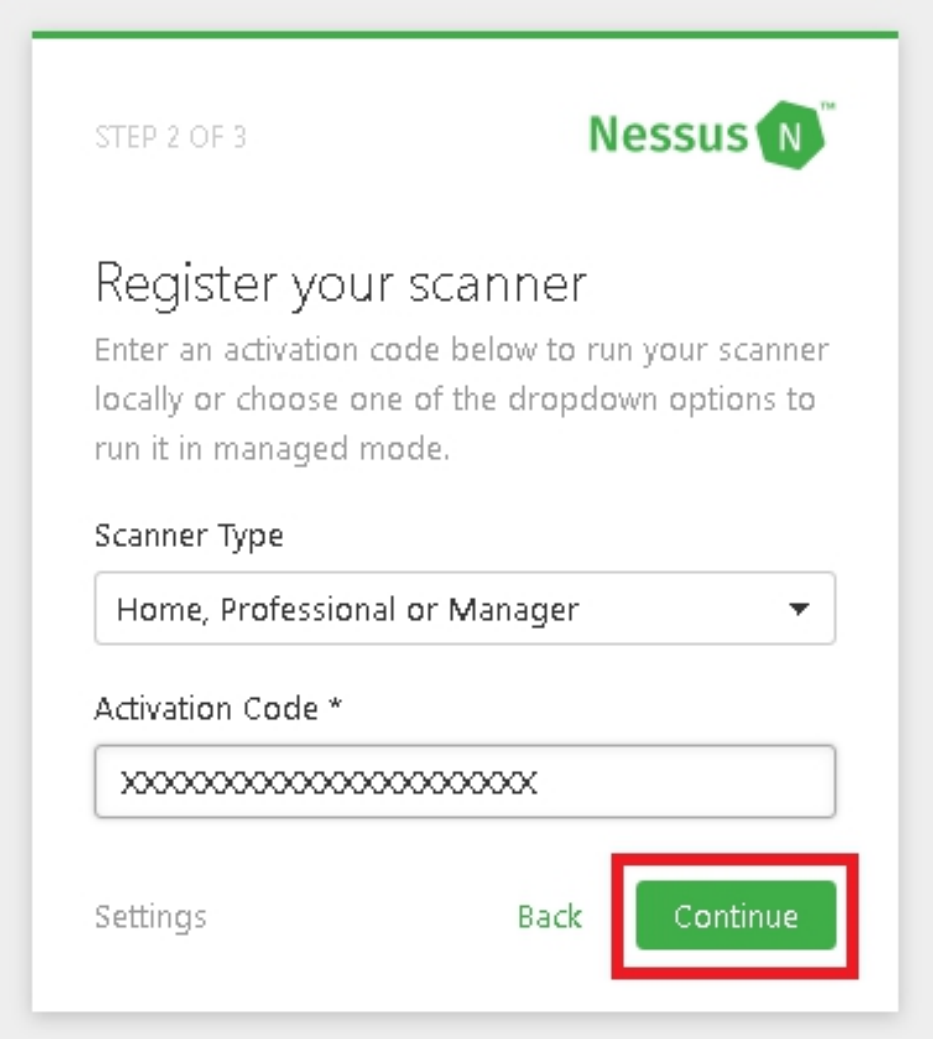
Now click on “Confirm Security Exception” to proceed to localhost.



Now you have to create an account for the Nessus server. Here, you are going to choose a login name and password – make sure you remember it because this is what you going to use to log in to Nessus from now on. After inserting username and password, click the “Continue” button.

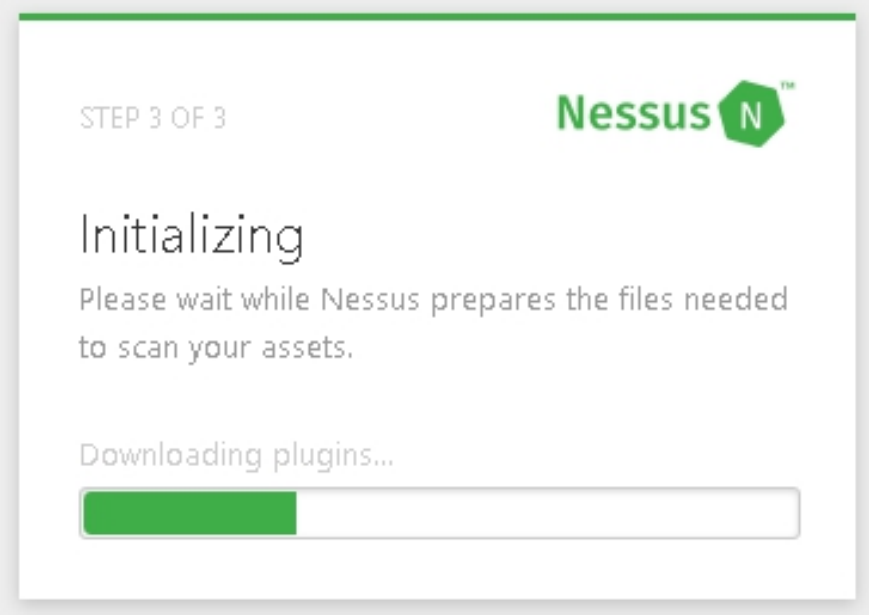


Now choose the scanner type that you want. Here, we have selected the first one which is "Home, Professional or Manager".



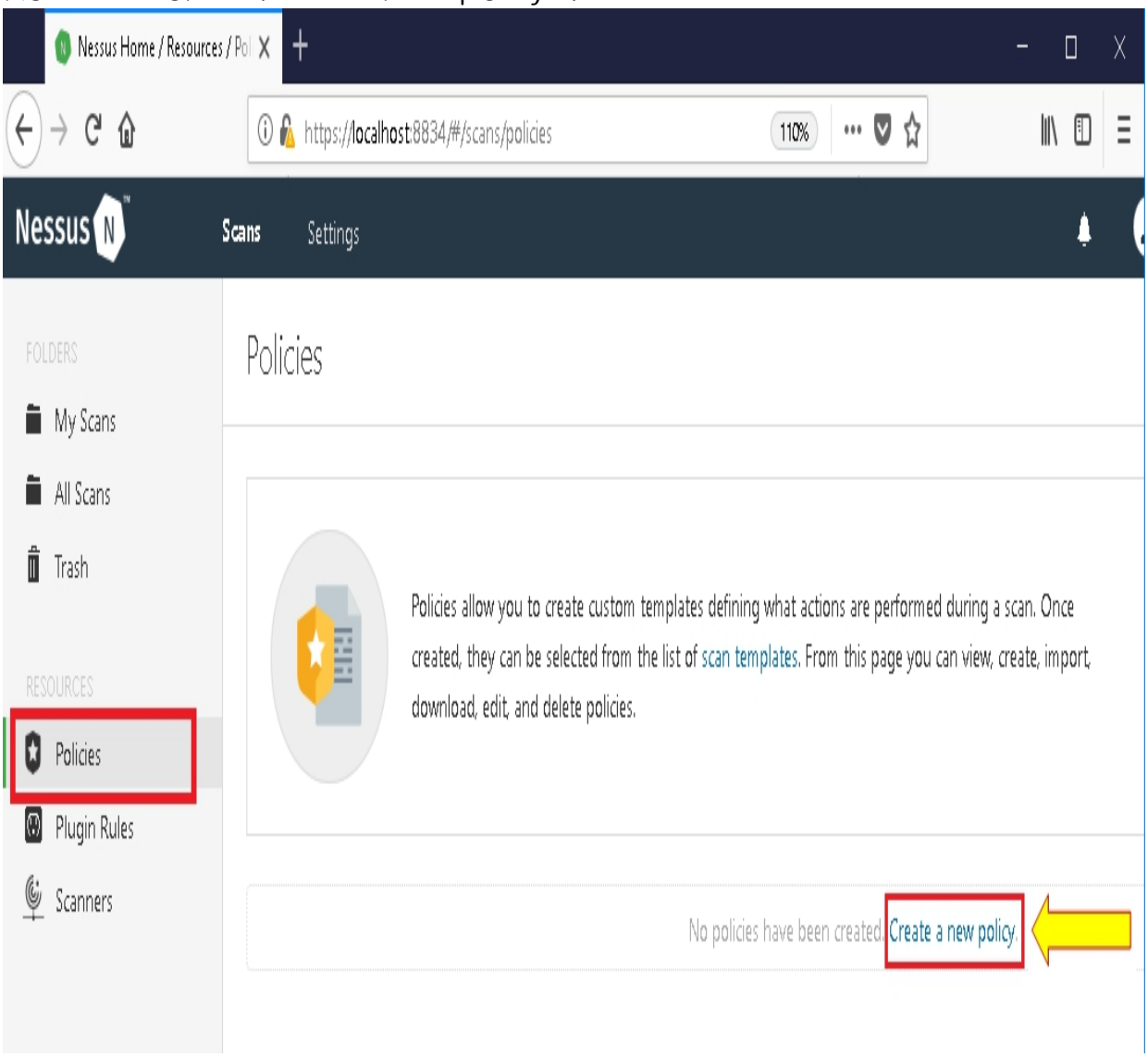
Now go to the email and copy the activation code that was forwarded to you and paste it here, then click “Continue”.

After that, you are going to see the “Initializing” window. It basically fetches all the plugins for Nessus, which can take about 15 to 20 minutes.

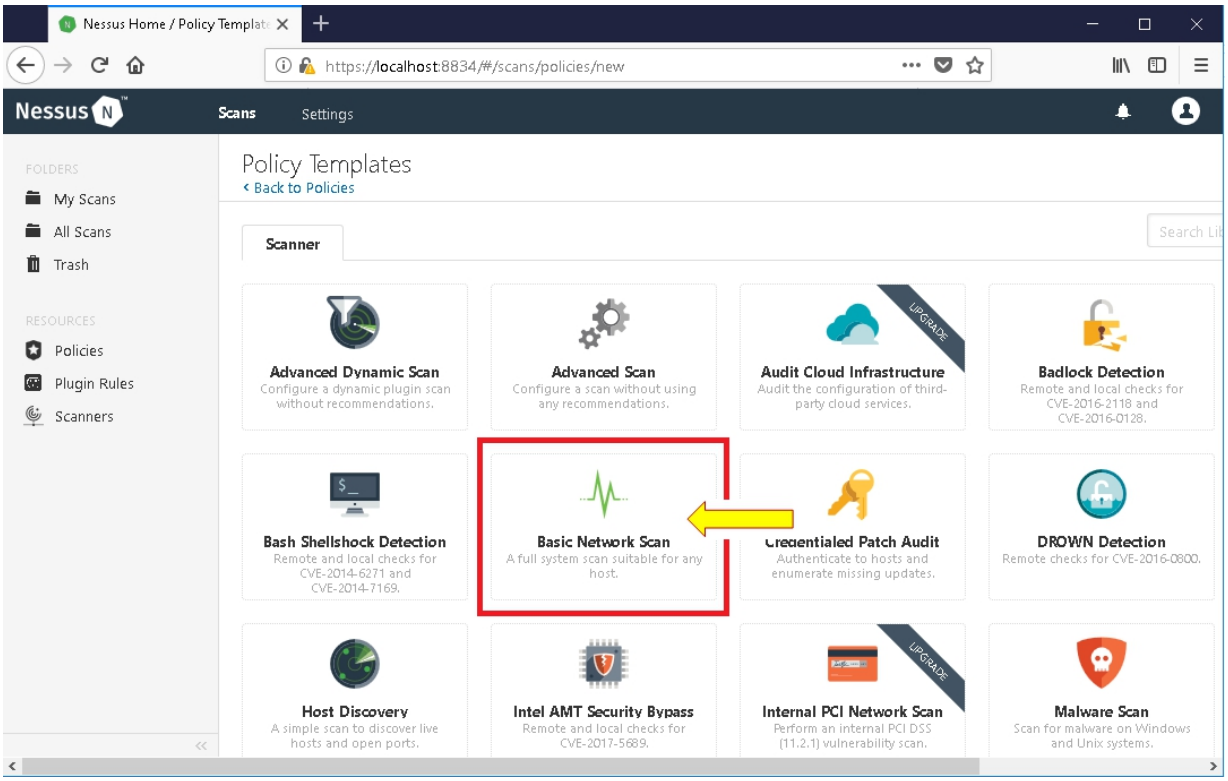


Once all the plugins are installed, this window will appear and this is what Nessus looks like. Now, the first thing you have to do is create a policy. Click on “Policies”.

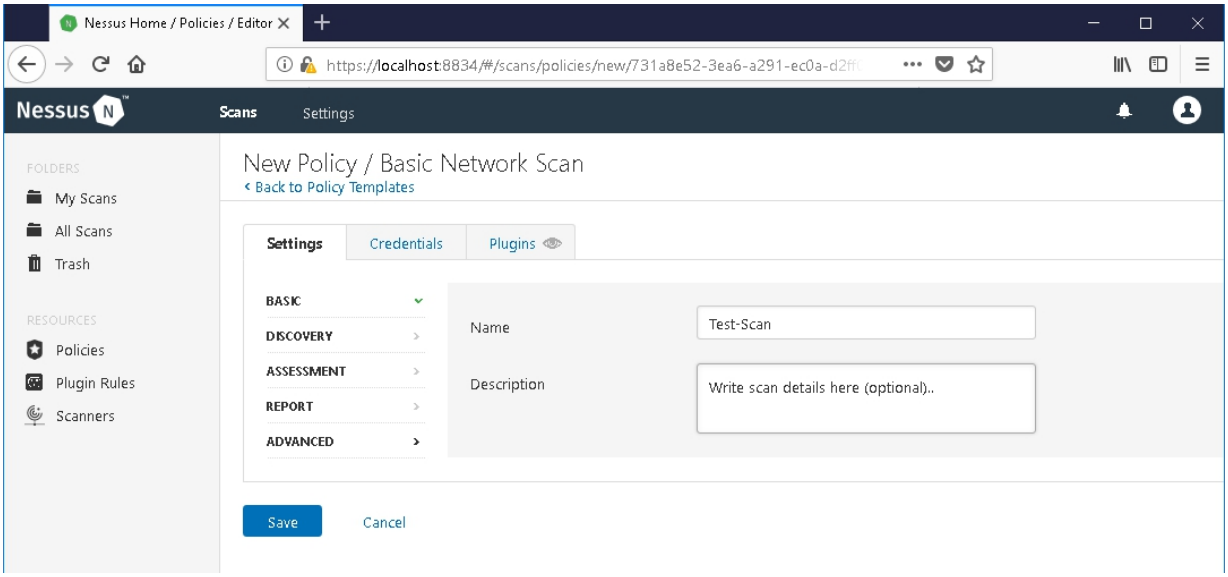
Now click on “Create a new policy”.



Here, you have multiple scanner options available. What we are going to do now is “Basic Network Scan”. So for this, click on the “Basic Network Scan” option.

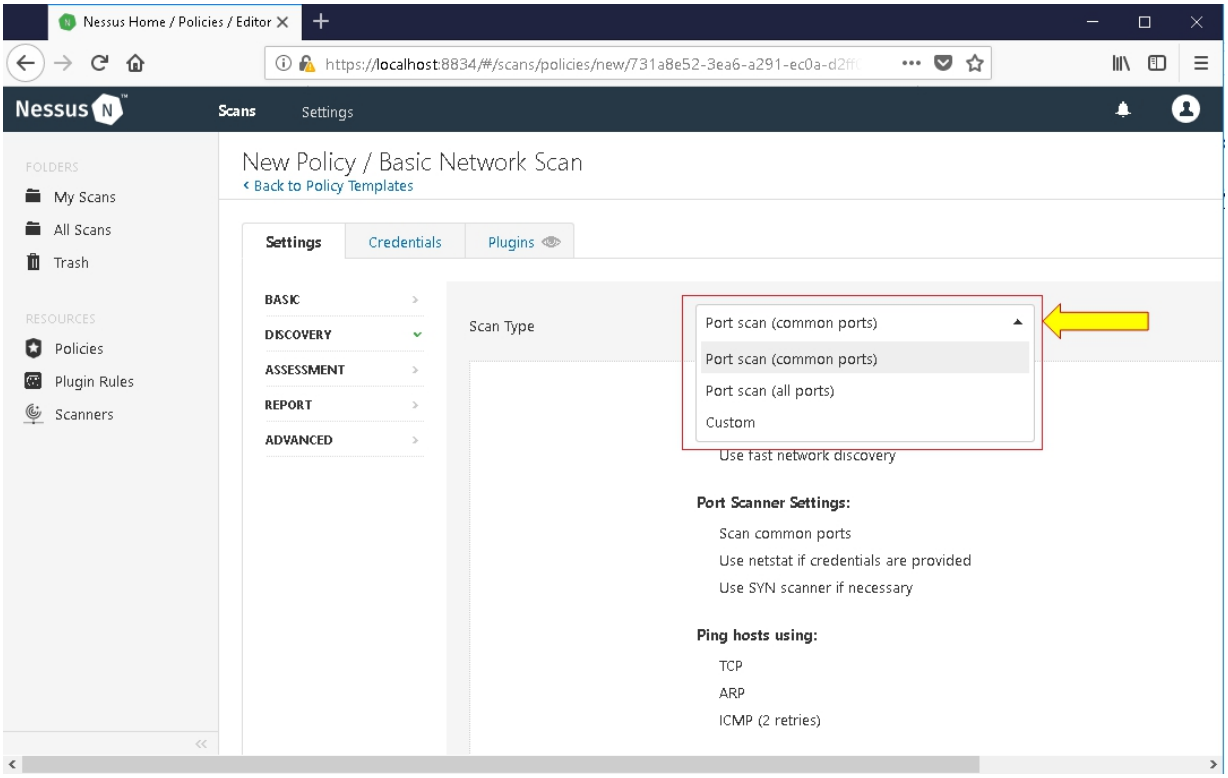


When you see this window, you have to name the policy. You may name it anything you want; for now, we are going to name it "Basic Scan".

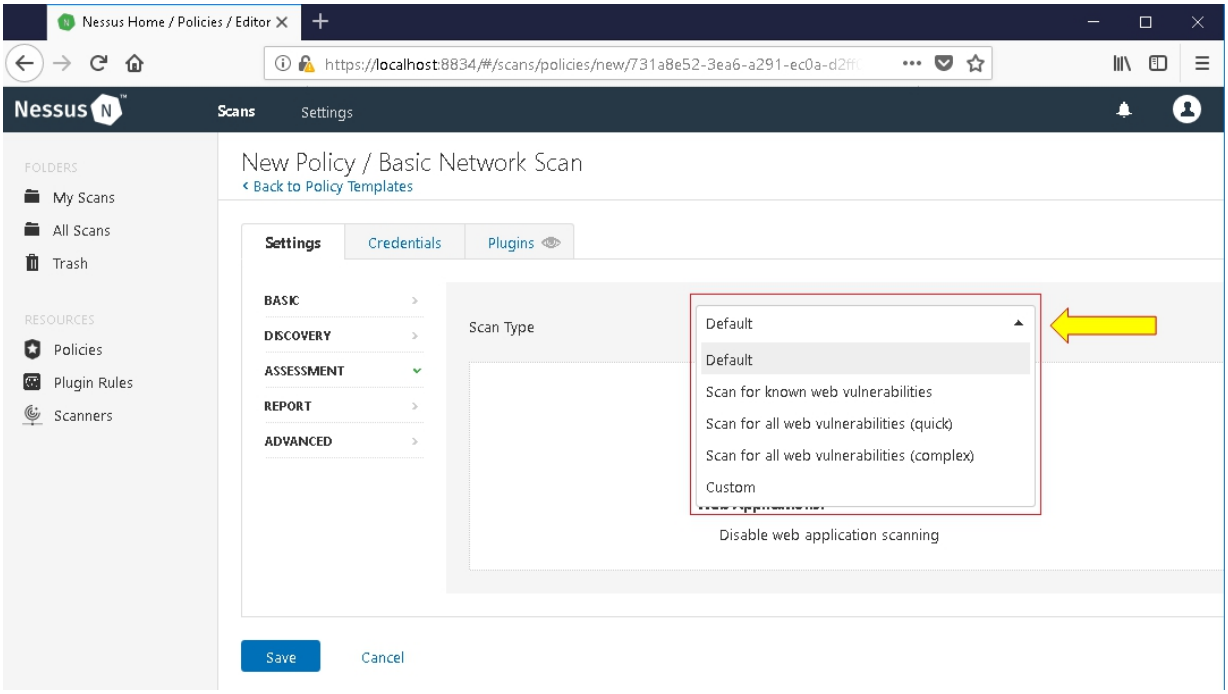


In basic settings, you have another setting option that is the "Permission" setting. In this, you have two options: one is "No

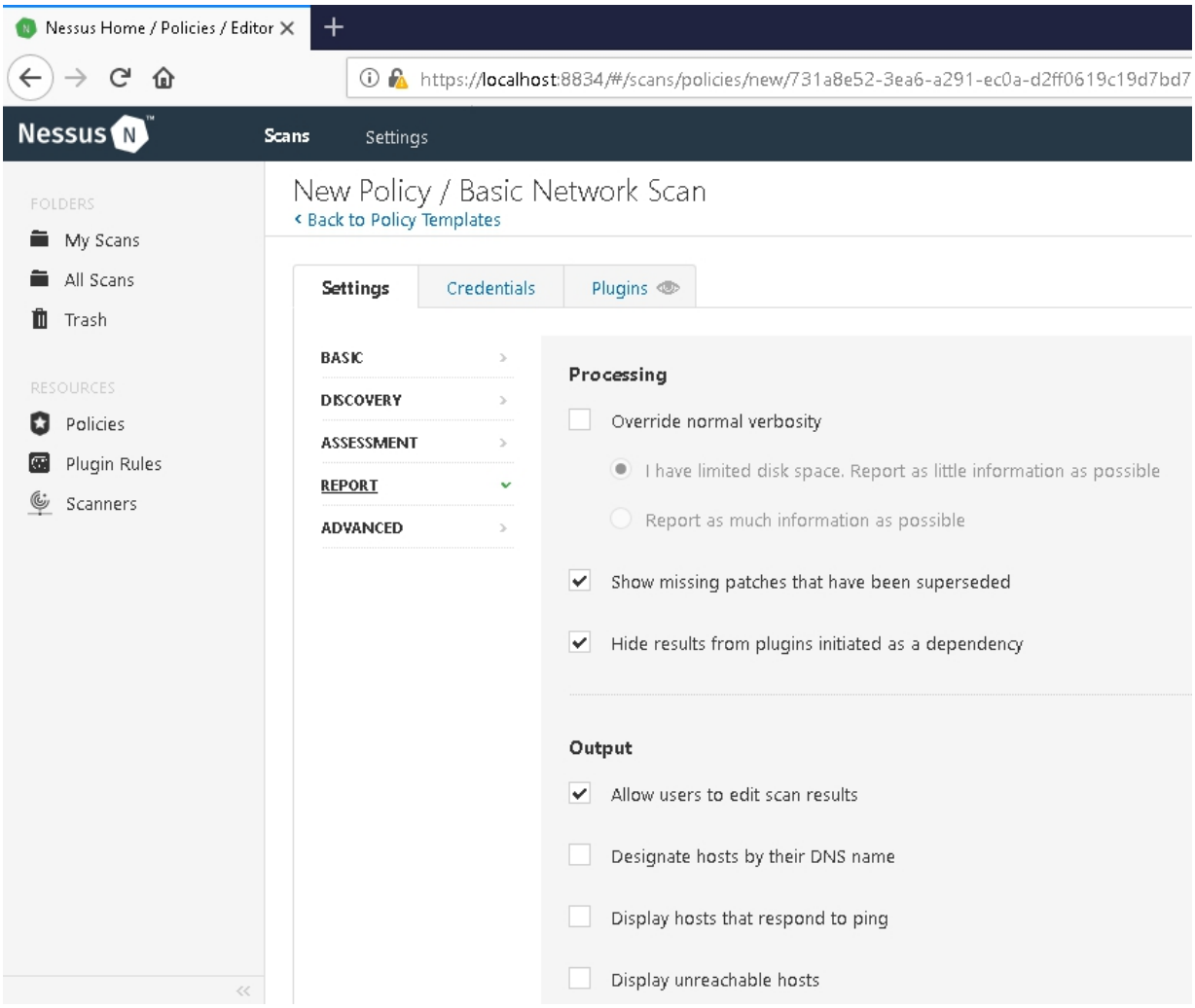
Access" and the other is "Can Use". Here, we are going to leave it as default. Now click the "Discovery" option.



Here, you have to choose the Scan Type. You can either choose to scan common ports, all ports, or customize it. After selecting your desired option, click on "Assessment".

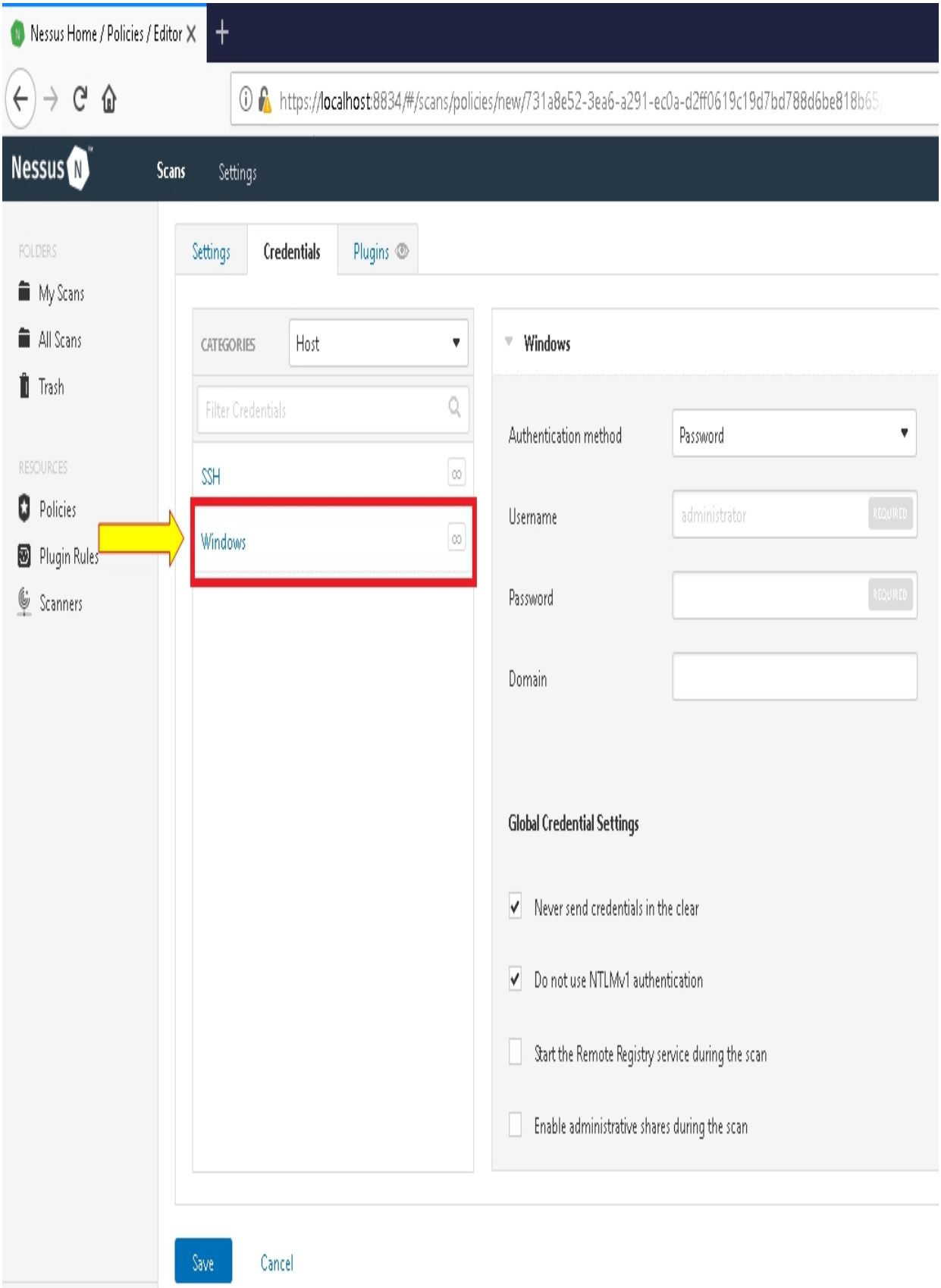


Here, you will see three scanning options. Choose whichever you want and then click on “Report”.



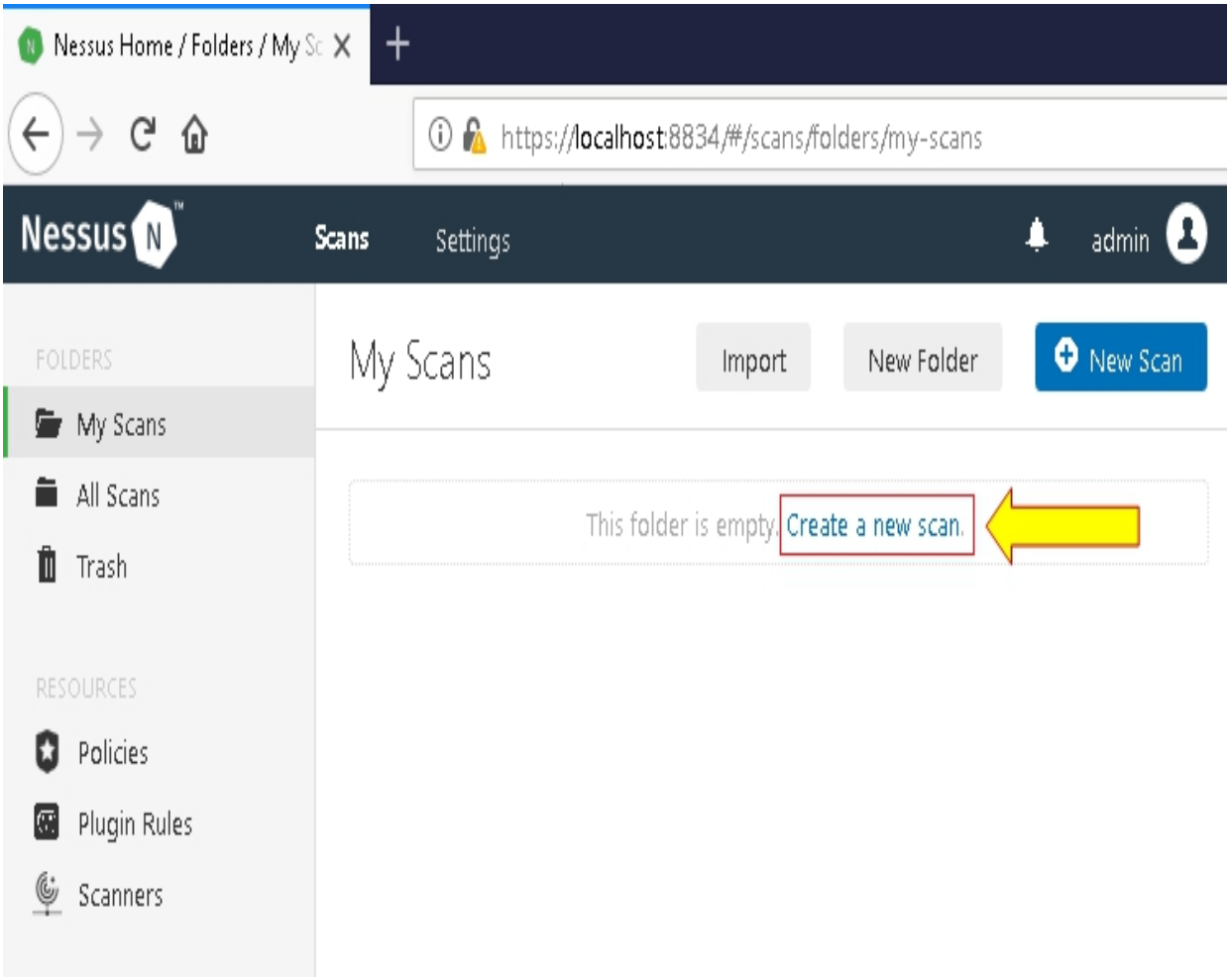
In this window, you have multiple options and you can see that some of them are 'checked' by default. We are going to leave it as default, but if you want to change some settings, you may change them according to your needs.

Here in the "Advanced" setting option, you have three options to choose from. Select any of them and click on the "Credentials" button.
Here, we are going to select "Windows" as we are using Windows OS. However, if you have Mac or Linux, then you have to select SSH.



Go ahead and insert your credentials and authentication method. If you

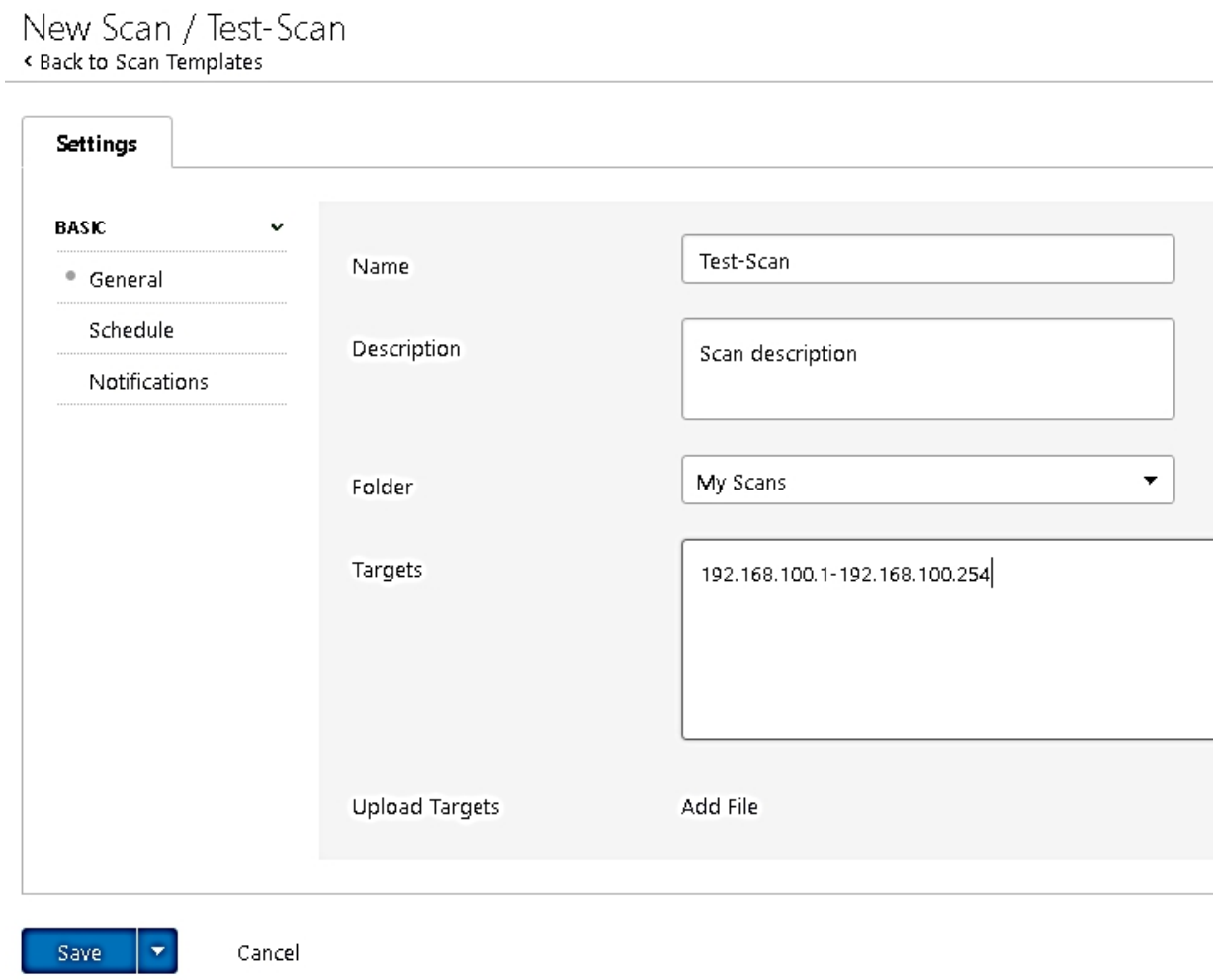
Go ahead and insert your credentials and authentication method. If you have a domain, you may insert that (optional). Check the boxes and click the "Save" button. And that is it, the policy has been created.
Now in order to scan, you have to click on the "Scan" button at the top of the page.
Click on the "Create a new scan" option.



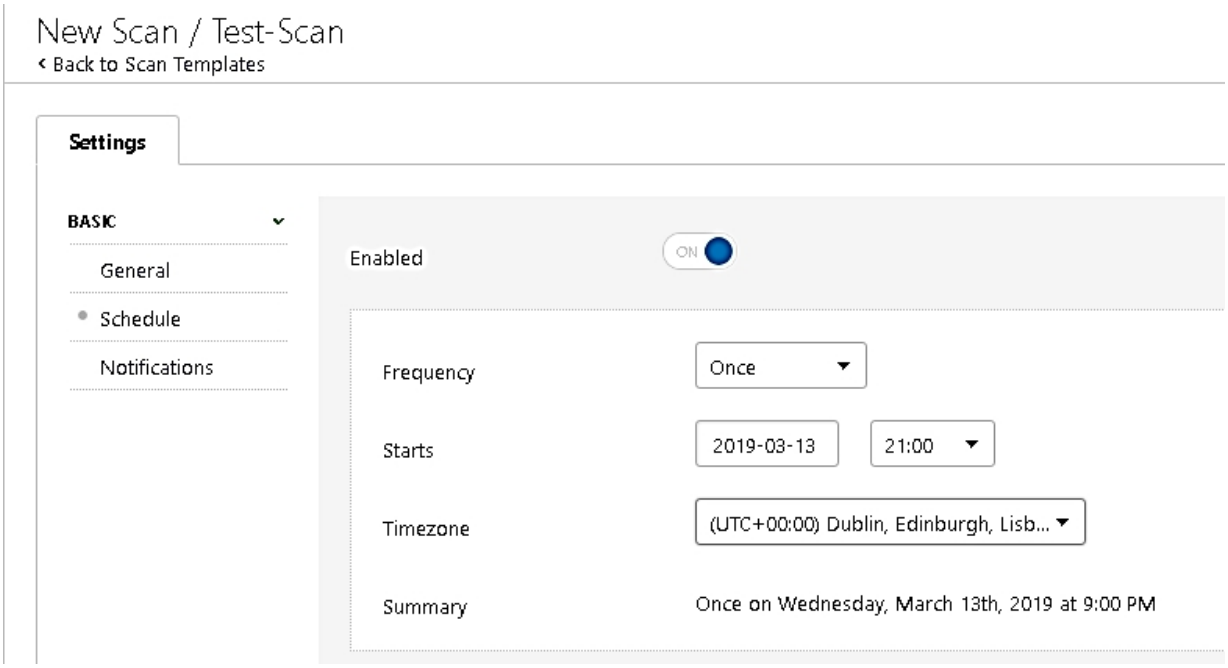
Go to the "User Defined" option. Click on "Basic Scan".
Now, name this Scan. We are going to name it "Basic Scan" – the same as the policy name. You can also add a description if you want.

Select the folder where you want to save a scan and, finally, insert the IP address of the target.

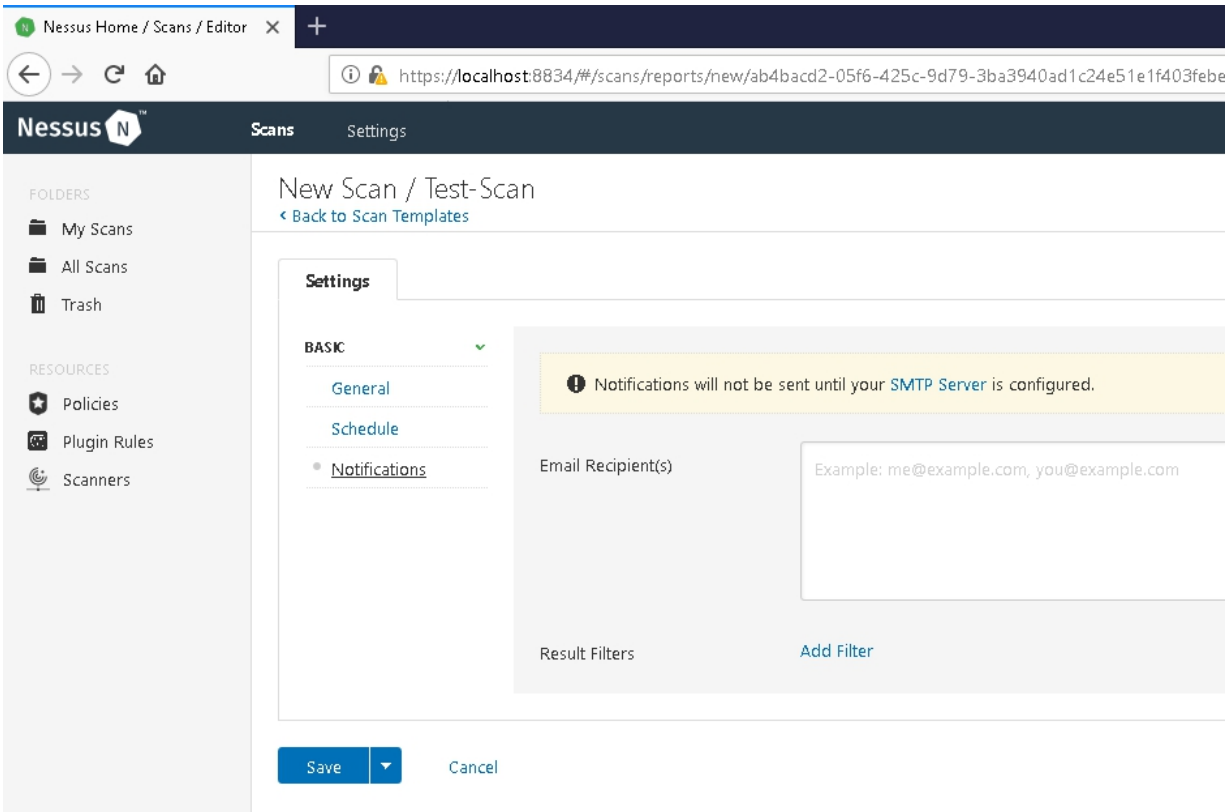
You may insert the target in different ways. For example: 192. 168. 1. 1, 192. 168. 1. 1/24, and test.com.



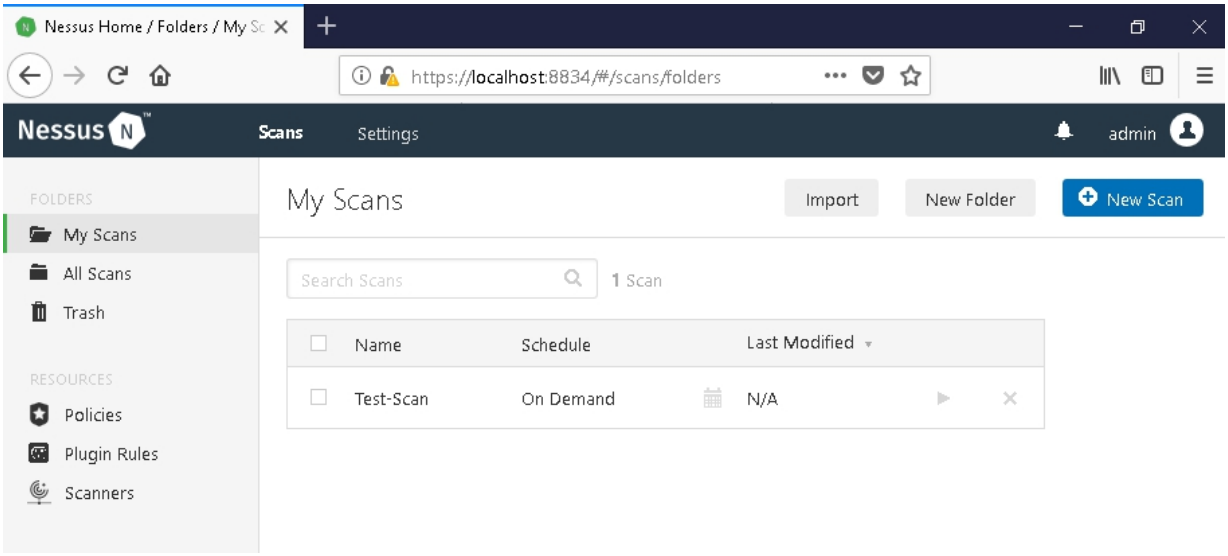
You can also schedule your scan. For this, click on “Enabled”, now select the frequency, start time, and Time zone.



If you want to get a notification, you can add your email address. After configuring all the settings, click on the "Save" button.



Here you can see that the scanning process has started. Once the scanning process is complete, you can see the results by clicking on the section that is marked below.



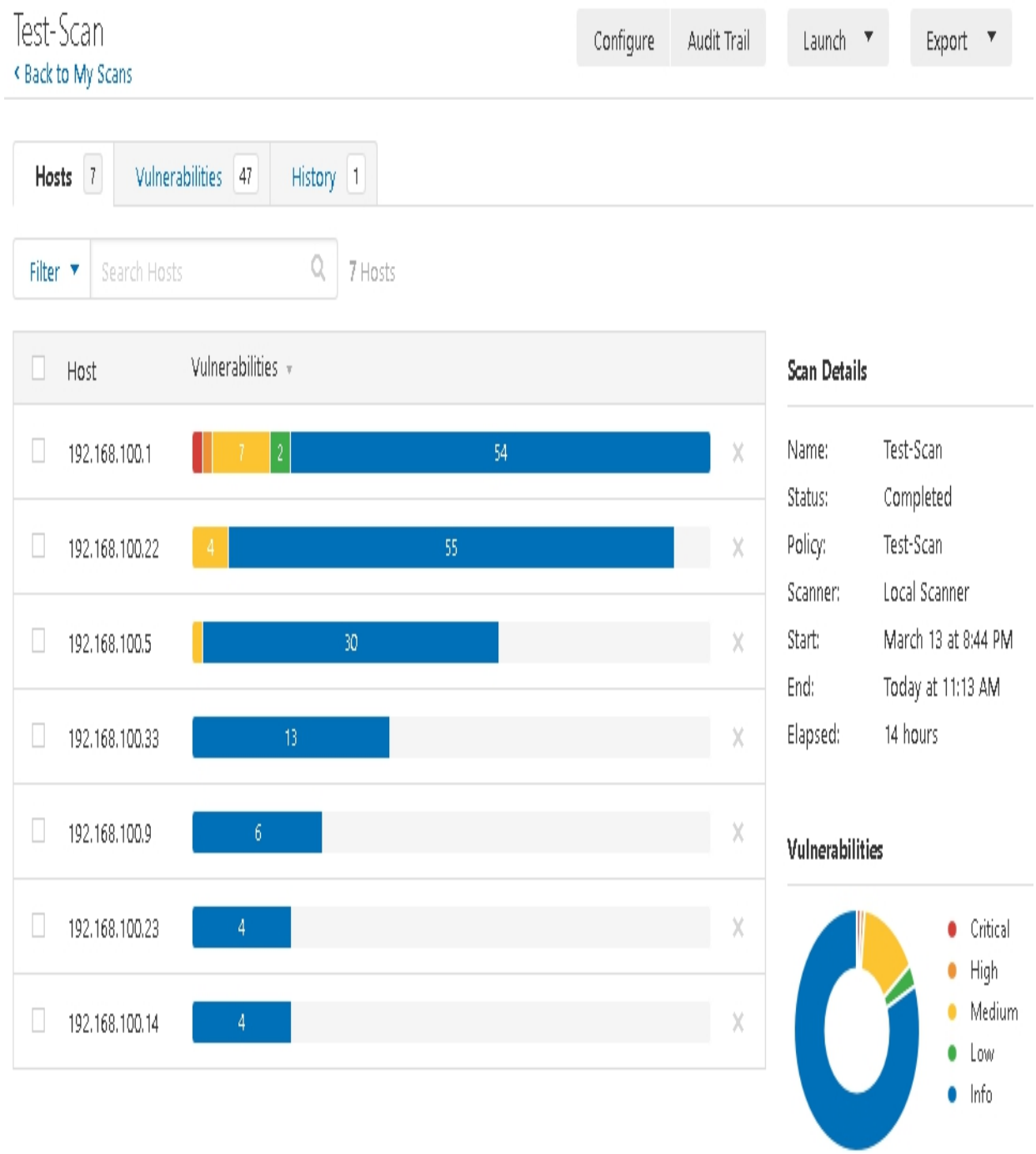
Here is the scan result. The result is shown in multiple colors. The red represents the Critical Vulnerability, the orange is for High, Yellow is for Medium, Green is for Low and Blue is for Info.

Scan Details

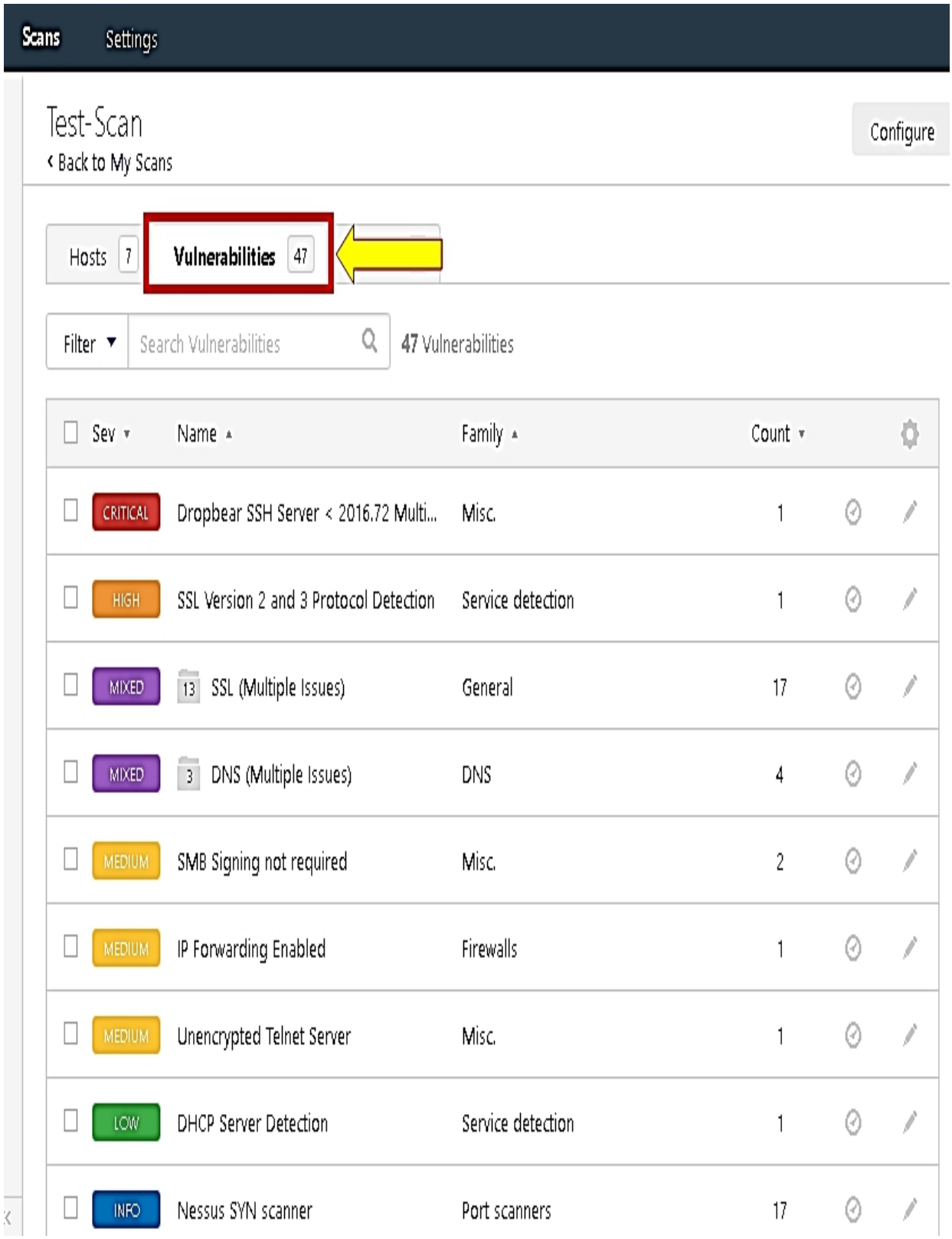
Name:	Test-Scan
Status:	Completed
Policy:	Test-Scan
Scanner:	Local Scanner
Start:	March 13 at 8:44 PM
End:	Today at 11:13 AM
Elapsed:	14 hours

Vulnerabilities

Now, click on the “Vulnerability” next to the “Host” option. Here you will see the vulnerabilities that have been found. Click on any one of them.



You can see the description of a particular vulnerability as well as a solution for it.


Scans
Settings
Test-Scan
‹ Back to My Scans
Configure
Hosts 7
Vulnerabilities 47
Filter
Search Vulnerabilities
47 Vulnerabilities
Sev
Name
Family
Count
CRITICAL
Dropbear SSH Server < 2016.72 Multi...
Misc.
1
HIGH
SSL Version 2 and 3 Protocol Detection
Service detection
1
MIXED
13
SSL (Multiple Issues)
General
17
MIXED
3
DNS (Multiple Issues)
DNS
4
MEDIUM
SMB Signing not required
Misc.
2
MEDIUM
IP Forwarding Enabled
Firewalls
1
MEDIUM
Unencrypted Telnet Server
Misc.
1
LOW
DHCP Server Detection
Service detection
1
INFO
Nessus SYN scanner
Port scanners
17

Test-Scan / Plugin #93650

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Export

Hosts 7 | Vulnerabilities 47 | History 1

CRITICAL Dropbear SSH Server < 2016.72 Multiple Vulnerabilities

Description

According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities :

- A format string flaw exists due to improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges. (CVE-2016-7406)

- A flaw exists in dropbearconvert due to improper handling of specially crafted OpenSSH key files. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-7407)

- A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code. (CVE-2016-7408)

- A flaw exists in dbclient or dropbear server if they are compiled with the DEBUG_TRACE option and then run using the -v switch. A local attacker can exploit this to disclose process memory. (CVE-2016-7409)

Solution

Upgrade to Dropbear SSH version 2016.74 or later.

See Also

Plugin Details

Severity:	Critical
ID:	93650
Version:	1.4
Type:	remote
Family:	Misc.
Published:	September 22, 2016
Modified:	July 10, 2018

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

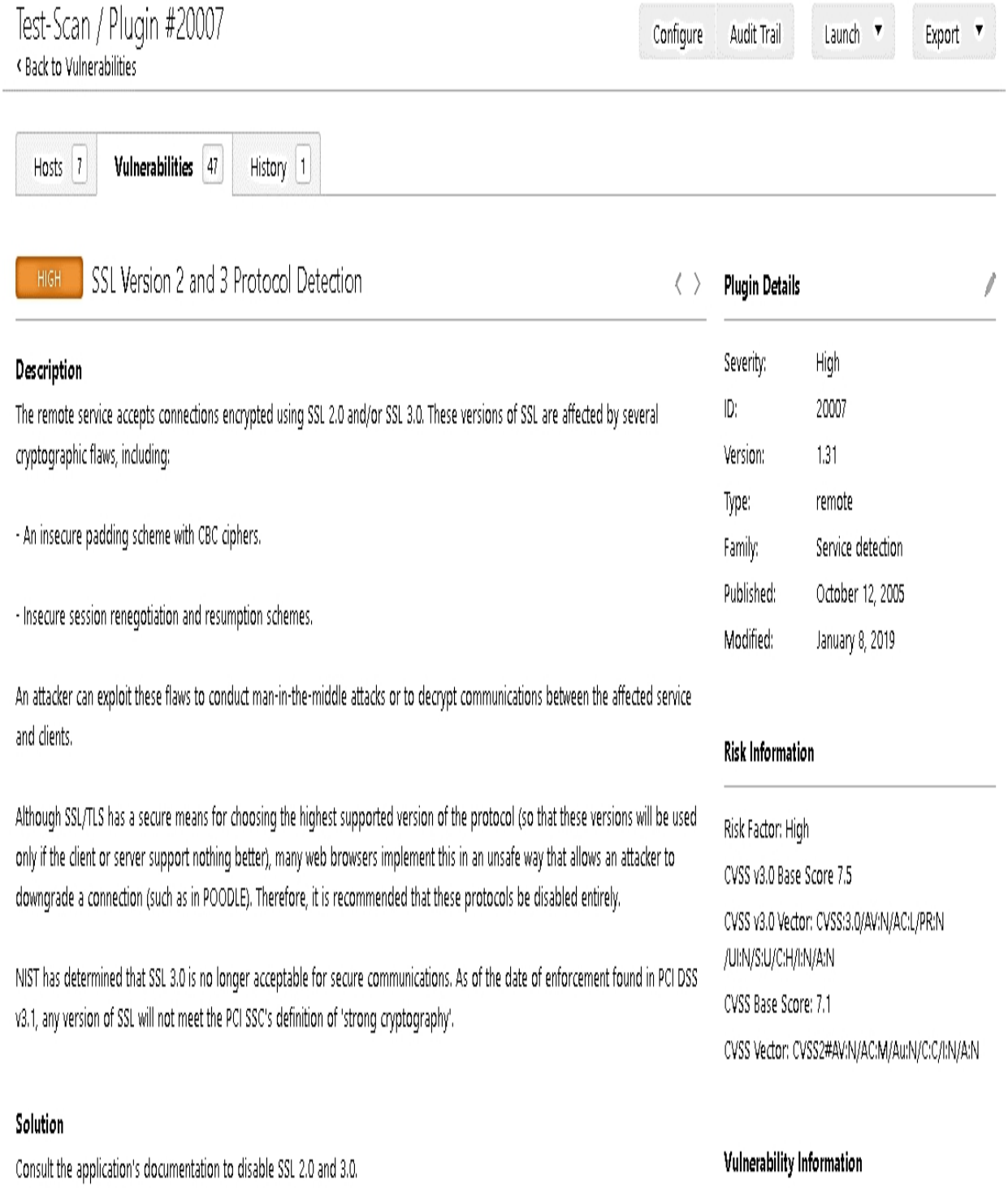
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 8.7

CVSS Base Score: 10.0

CVSS Temporal Score: 7.4

Here are some other vulnerabilities that were found.



Lab 5.2: Vulnerability Scanning using the Nessus Vulnerability Scanning Tool

Case Study: In this case, we are going to scan a private network of 10. 10. 10.0/24 for vulnerabilities using a vulnerability scanning tool.

This lab is performed on a Windows 10 virtual machine using the Nessus vulnerability scanning tool. You can download this tool from Tenable's website: https://www.tenable.com/products/nessus/nessusprofessional .

Configuration:

1. Download and install Nessus vulnerability scanning tool.
2. Open a web browser.
3. Go to the URL http://localhost:8834

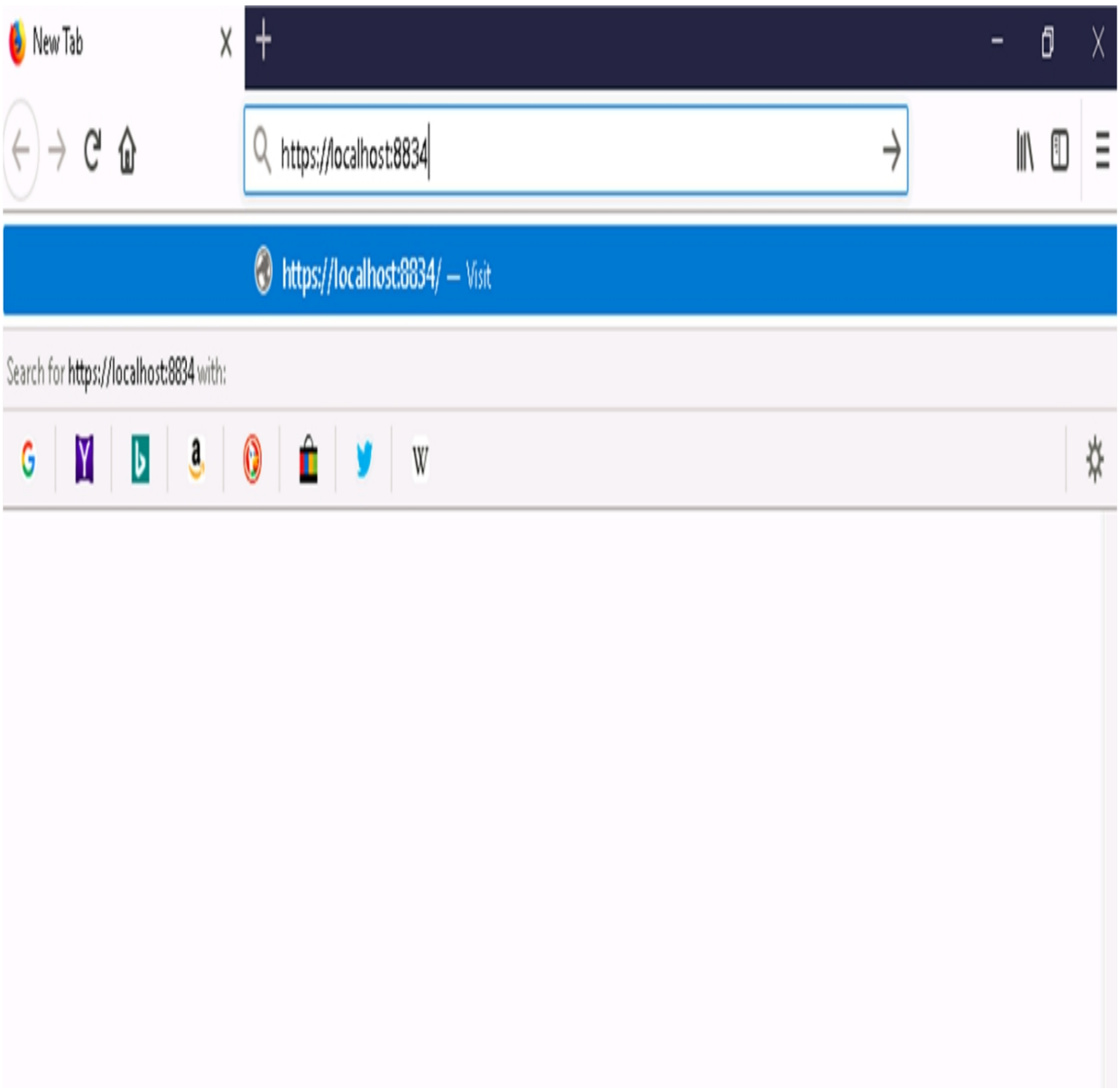


Figure 5-08: https://localhost:8834

4. Click on the "**Advanced**" button.

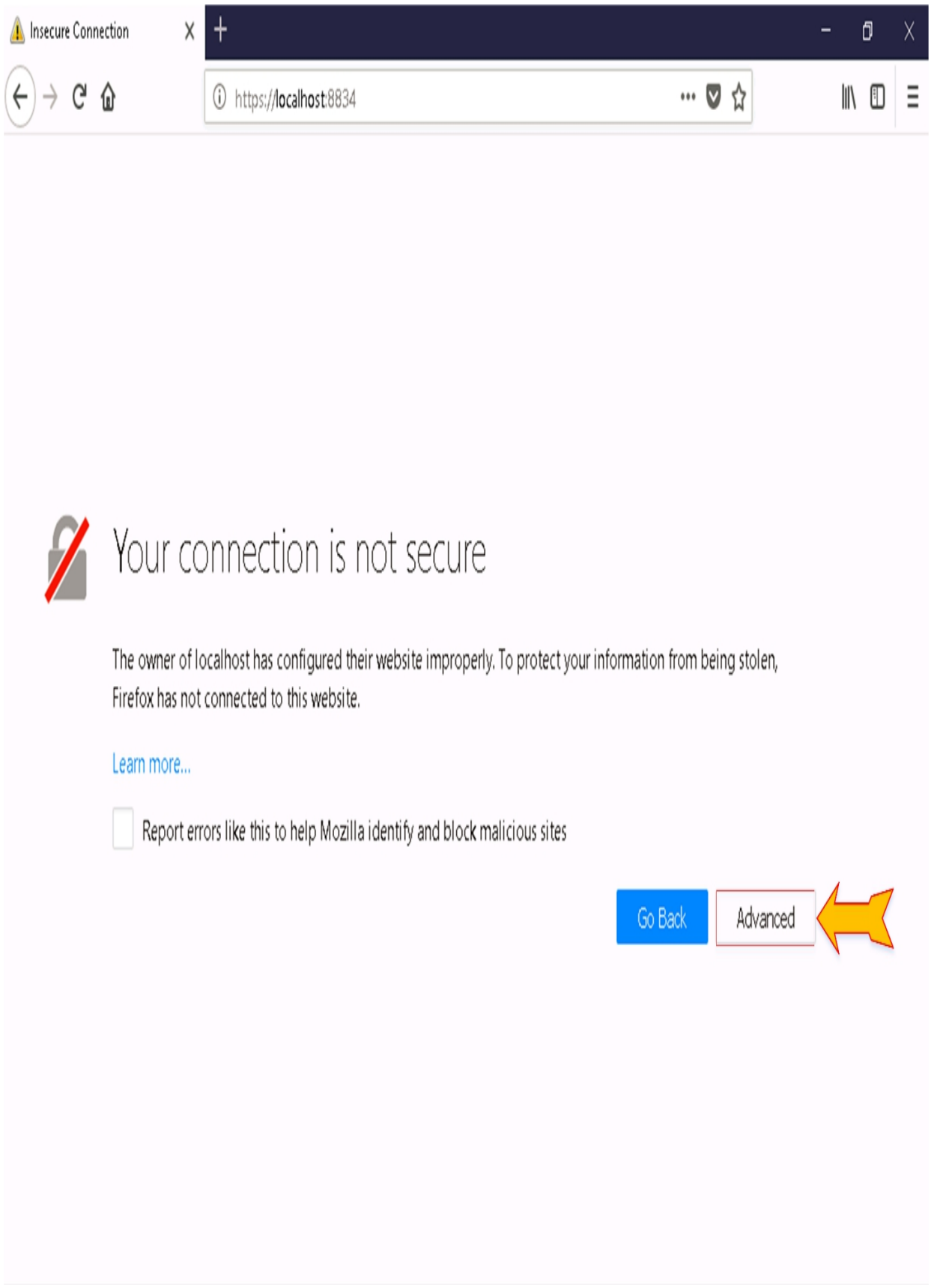

Insecure Connection
https://localhost:8834
Your connection is not secure
The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced

Figure 5-09: Security Exception Required Window

5. Proceed to Add Security Exception.

Figure 5-10: Add Security Exception Window

6. Confirm Security Exception.

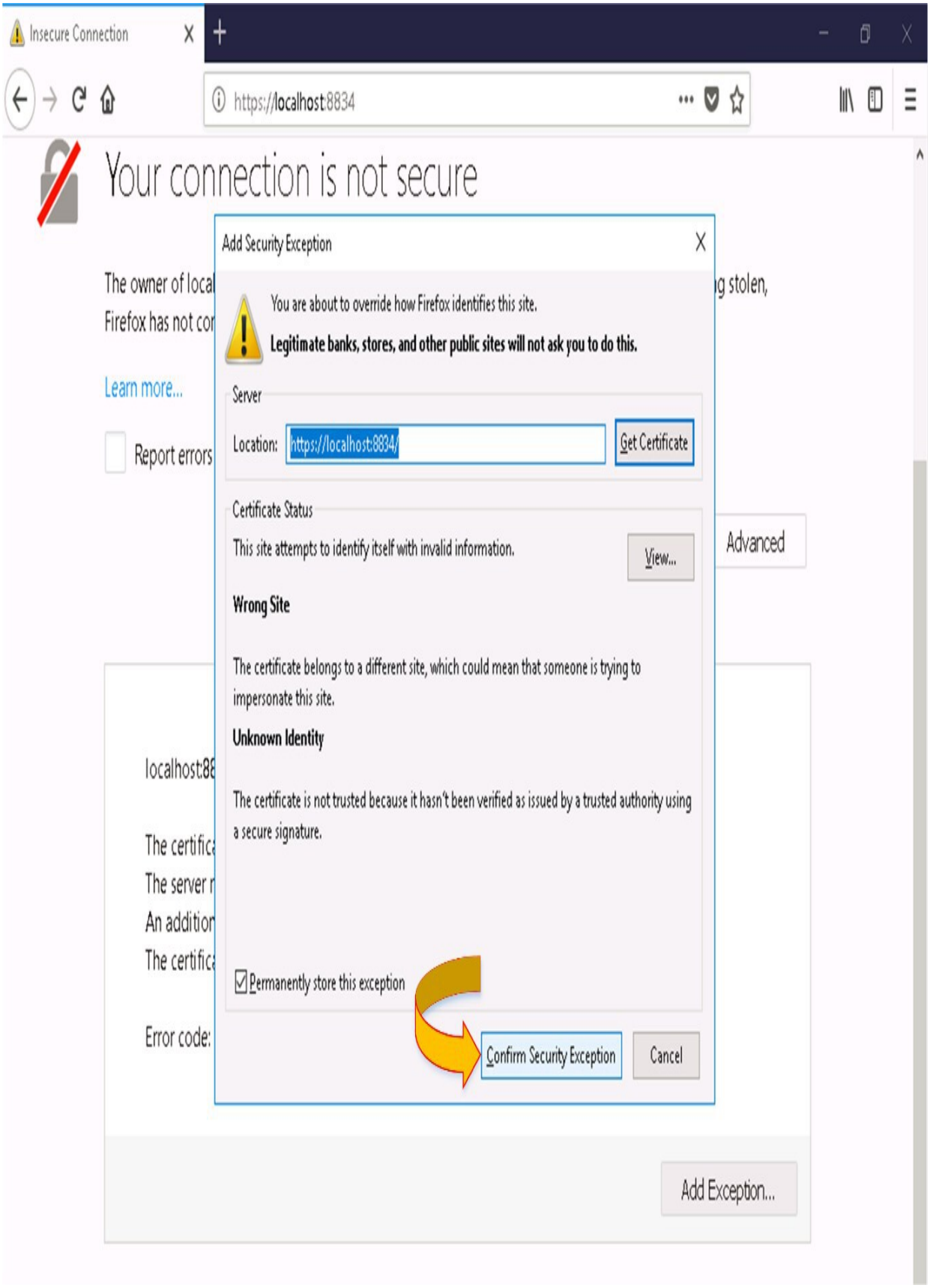

Insecure Connection
https://localhost:8834
Your connection is not secure
The owner of local
Firefox has not cor
g stolen,
Learn more...
Report errors
Advanced
localhost:88
The certifica
The server r
An additior
The certifica
Error code:
Add Exception...
Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://localhost:8834/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.
Unknown Identity
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
Permanently store this exception
Confirm Security Exception
Cancel

Figure 5-11: Confirm Security Exception Window

7. Enter Username and Password of your Nessus Account (You have to register in order to create an account to download the tool from website).

Figure 5-12: Nessus Login Page

8. Following dashboard will appear.

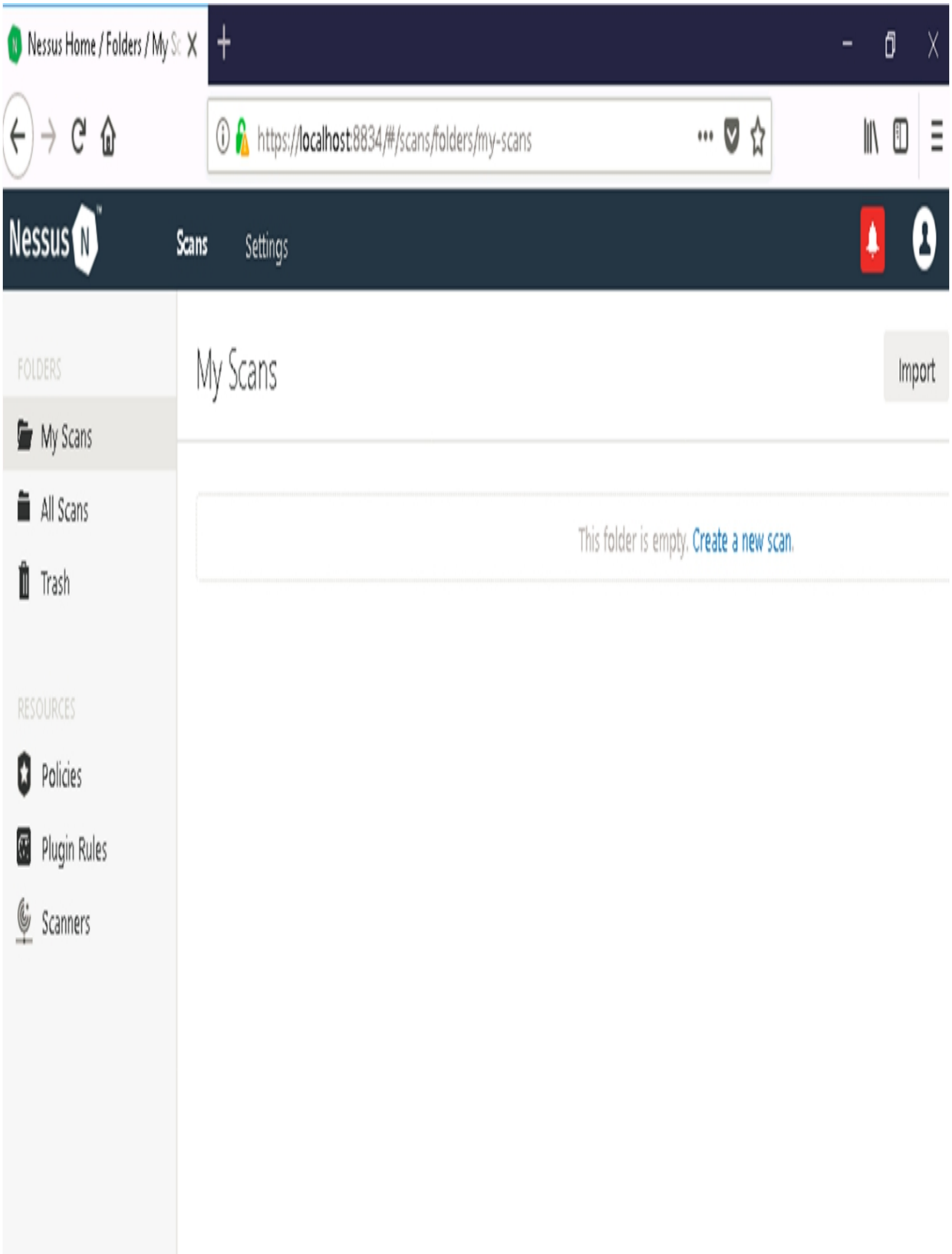


Figure 5-13: Nessus Dashboard

9. Go to the "Policies" tab and click "Create New Policy".

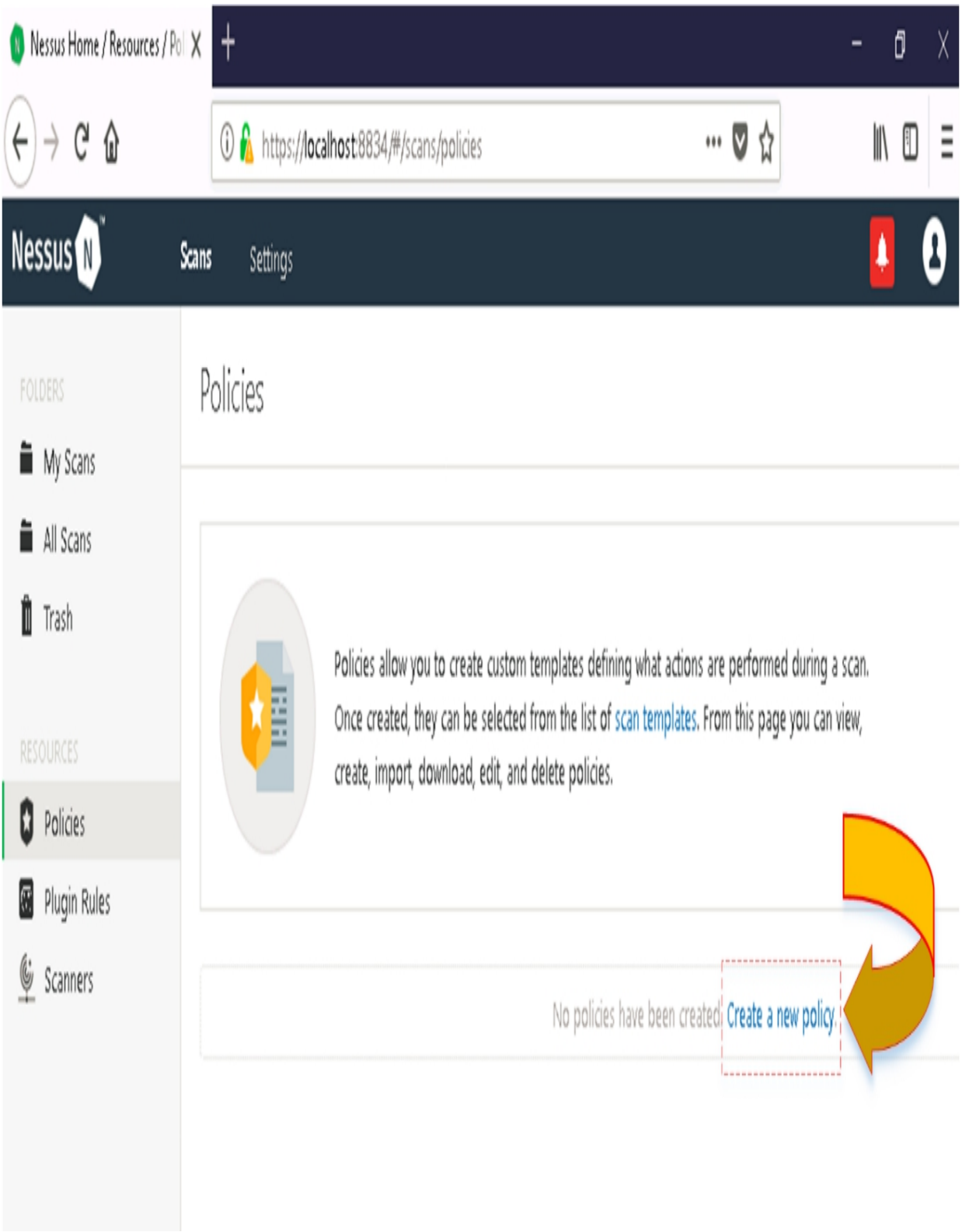


Figure 5-14: Create New Policy

10. In Basic Settings, set a name of the policy.

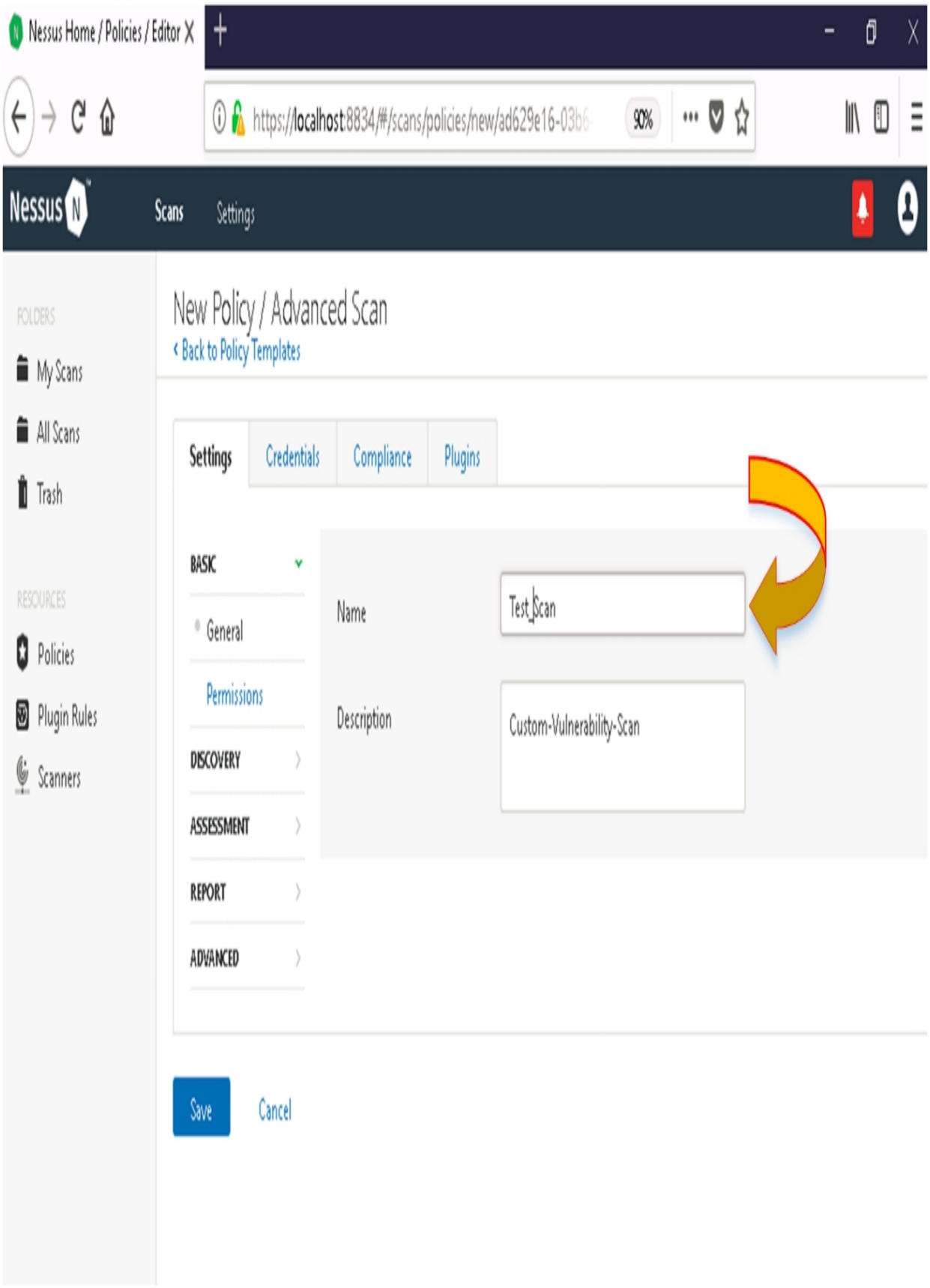

Nessus Home / Policies / Editor
https://localhost:8834/#/scans/policies/new/ad629e16-03b6
90%
Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Advanced Scan
‹ Back to Policy Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Permissions
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Test Scan
Description
Custom-Vulnerability-Scan
Save
Cancel

Figure 5-15: Configuring Policy

11. Go to **Settings > Basics > Discovery** to configure discovery settings.

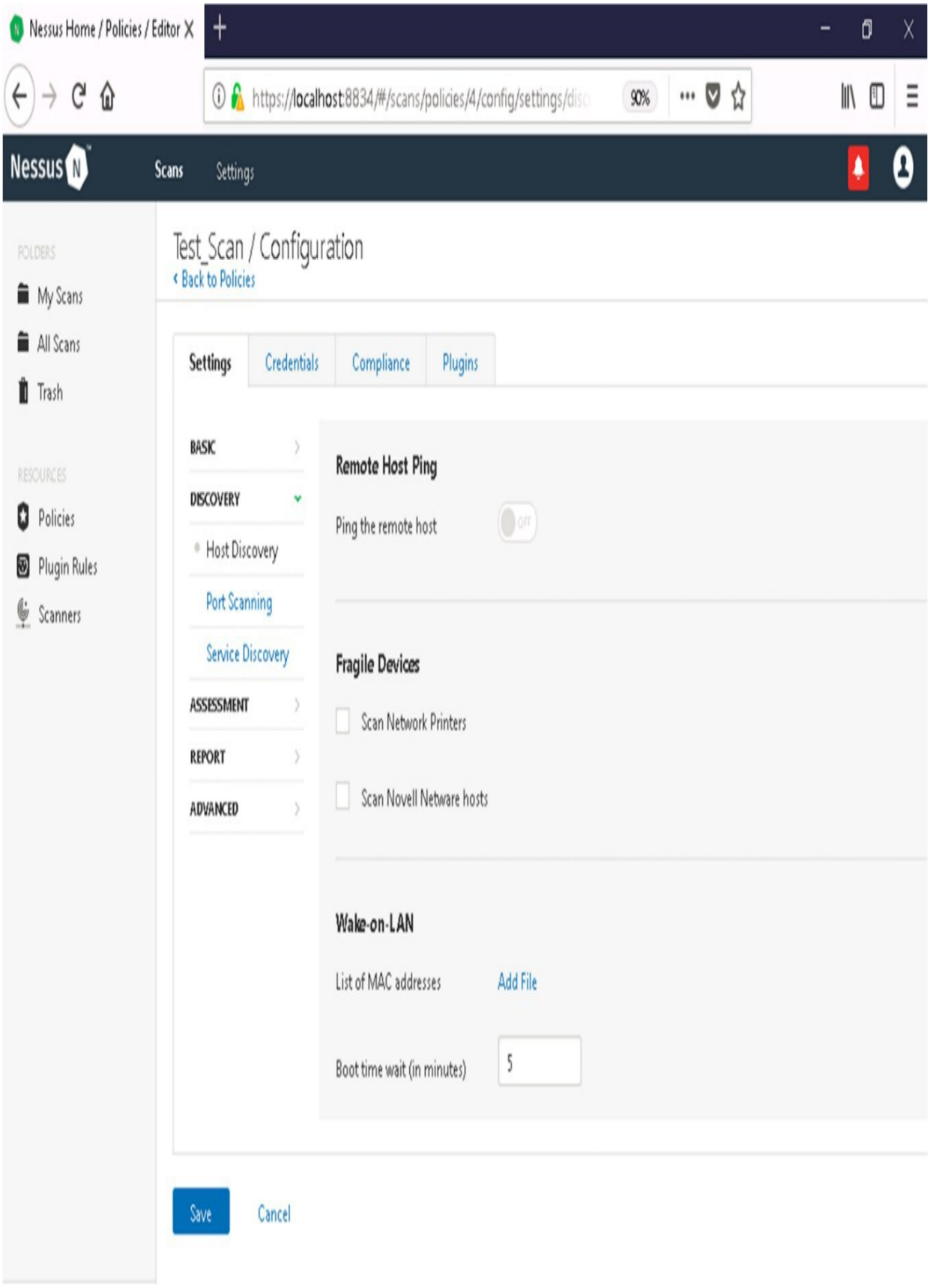

Nessus Home / Policies / Editor
https://localhost:8834/#/scans/policies/4/config/settings/disc
90%
Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Test_Scan / Configuration
‹ Back to Policies
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
Host 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
Wake-on-LAN
List of MAC addresses
Add File
Boot time wait (in minutes)
5
Save
Cancel

Figure 5-16: Configuring Policy

12. Configure port scanning settings under the “Port Scanning” tab.

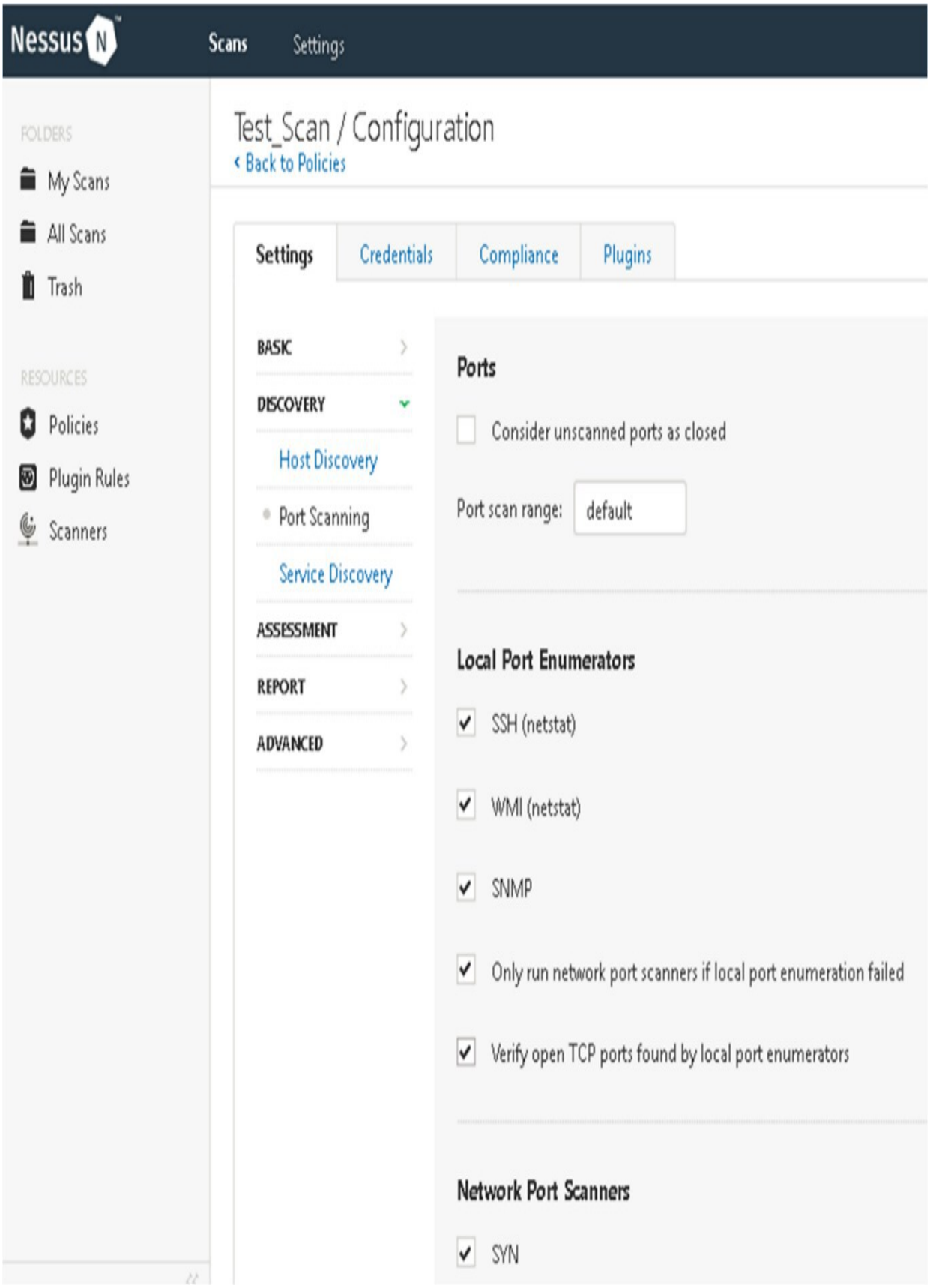

Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Test_Scan / Configuration
‹ Back to Policies
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Ports
Consider unscanned ports 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

Figure 5-17: Configuring Policy

13. Under the “Report” tab, configure settings as per your requirements.

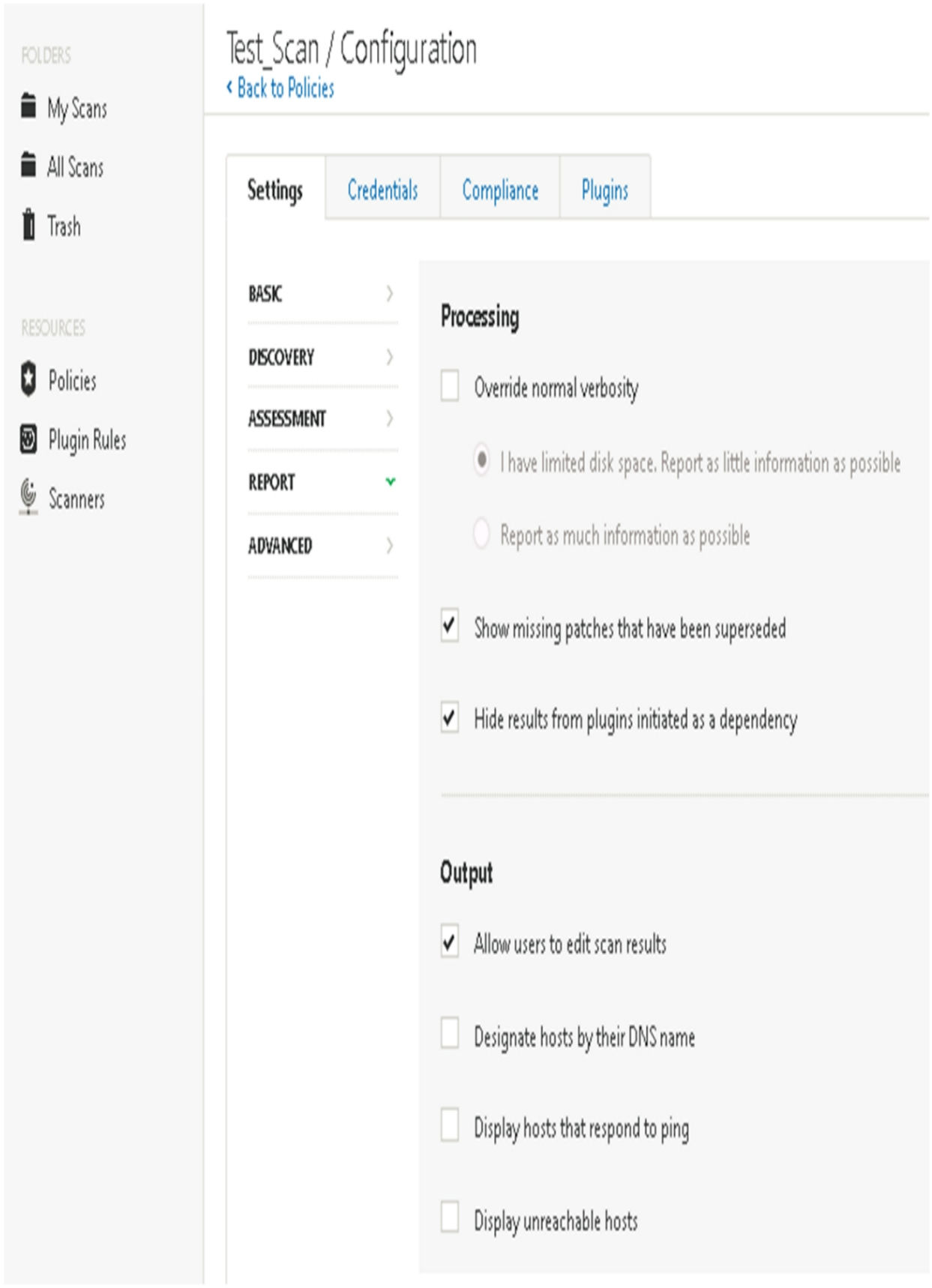

FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Test_Scan / Configuration
‹ Back to Policies
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Processing
Override normal verbosity
I have limited disk space. Report as little information as possible
Report as much information as possible
Show missing patches that have been superseded
Hide results from plugins initiated as a dependency
Output
Allow users to edit scan results
Designate hosts by their DNS name
Display hosts that respond to ping
Display unreachable hosts

Figure 5-18: Configuring Policy

14. Under the "Advanced" tab, configure parameters.

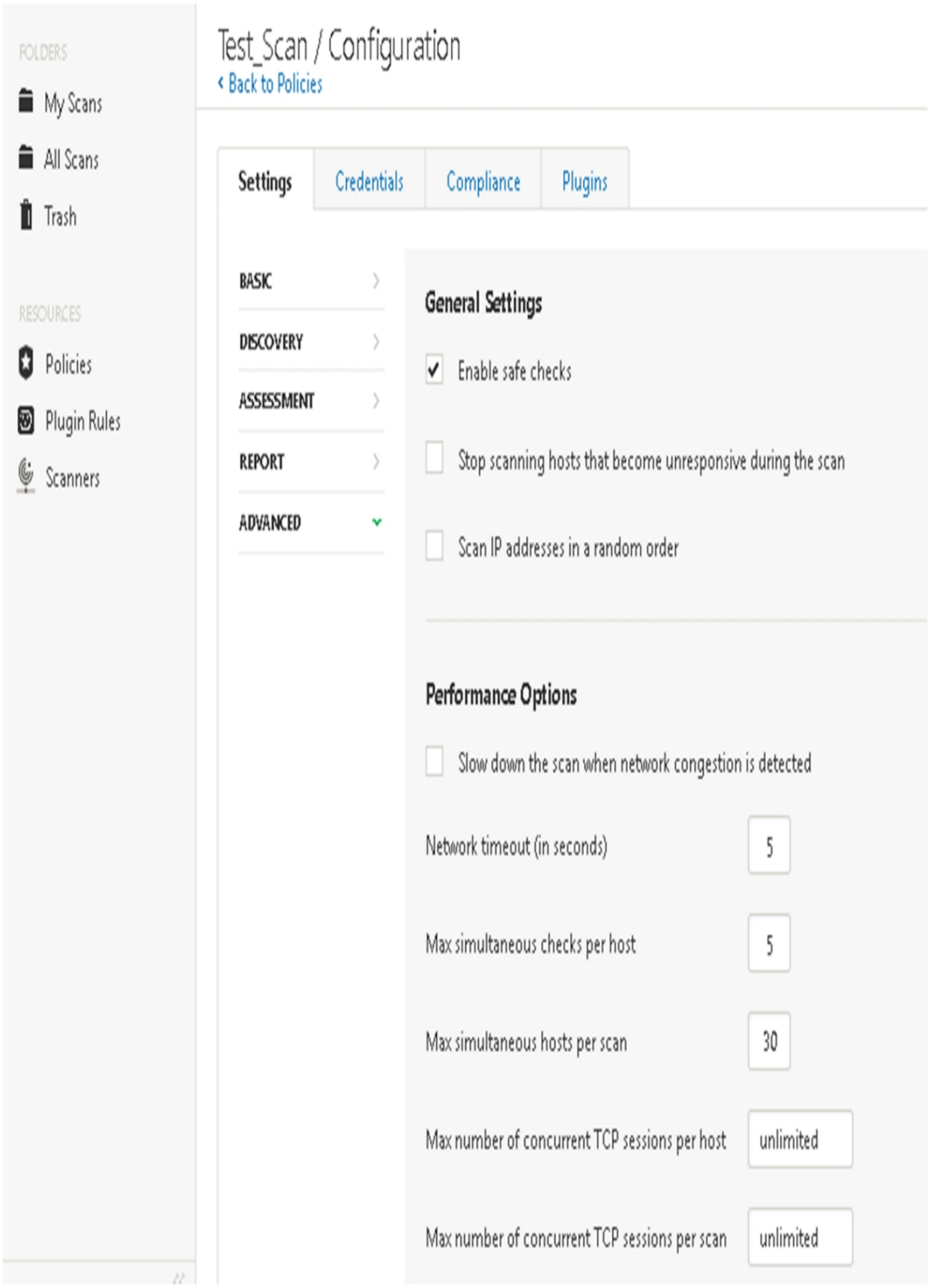

FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Test_Scan / Configuration
‹ Back to Policies
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
General Settings
Enable safe checks
Stop scanning hosts that become unresponsive during the scan
Scan 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
30
Max number of concurrent TCP sessions per host
unlimited
Max number of concurrent TCP sessions per scan
unlimited

Figure 5-19: Configuring Policy

15. Now go to the “Credentials” tab to set credentials.

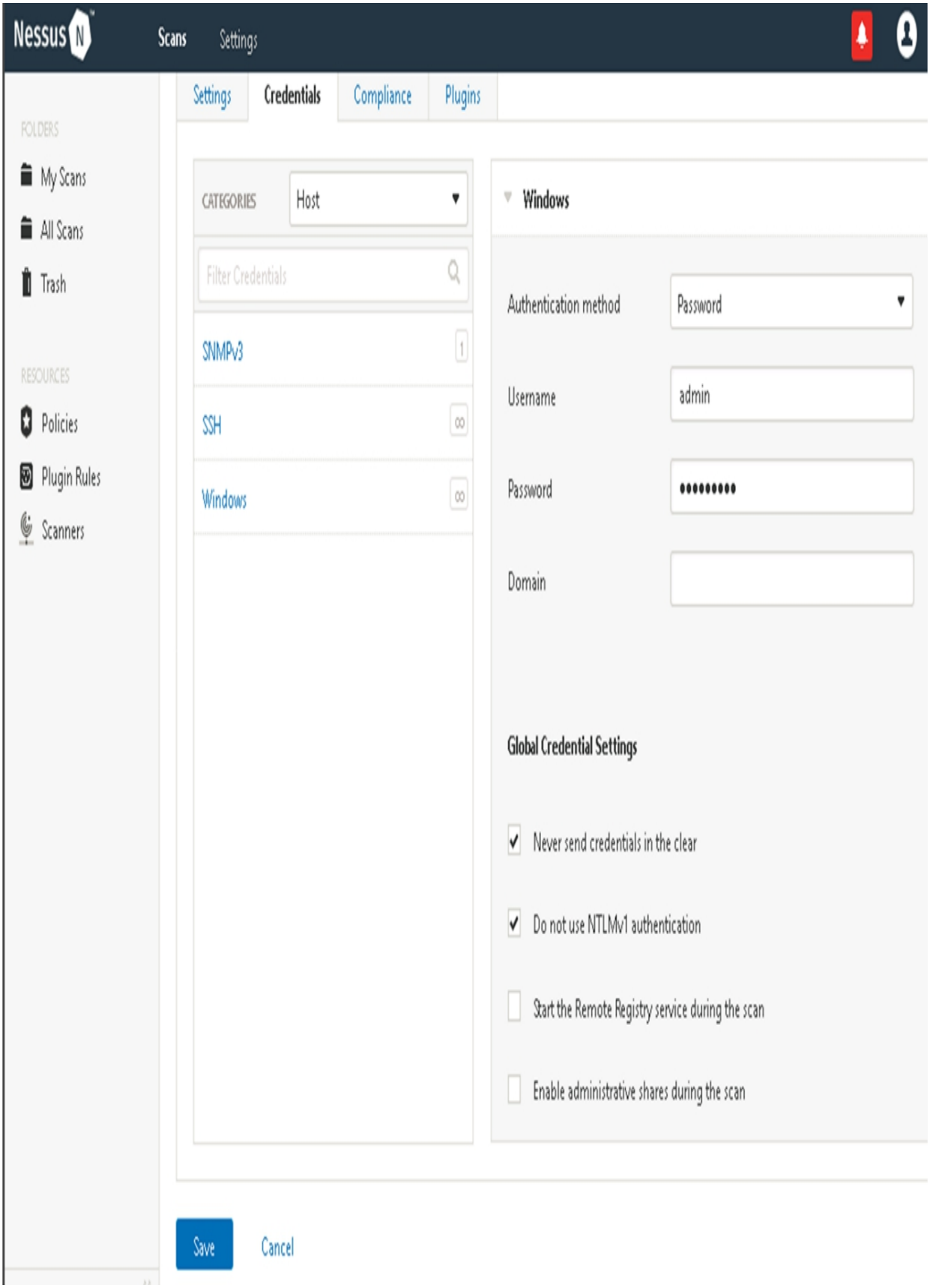

Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Settings
Credentials
Compliance
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
Windows
Authentication method
Password
Username
admin
Password
Domain
Global Credential Settings
Never send credentials in the clear
Do not use NTLMv1 authentication
Start the Remote Registry service during the scan
Enable administrative shares during the scan
Save
Cancel

Figure 5-20: Configuring Policy

16. Enable/disable desired plugins.

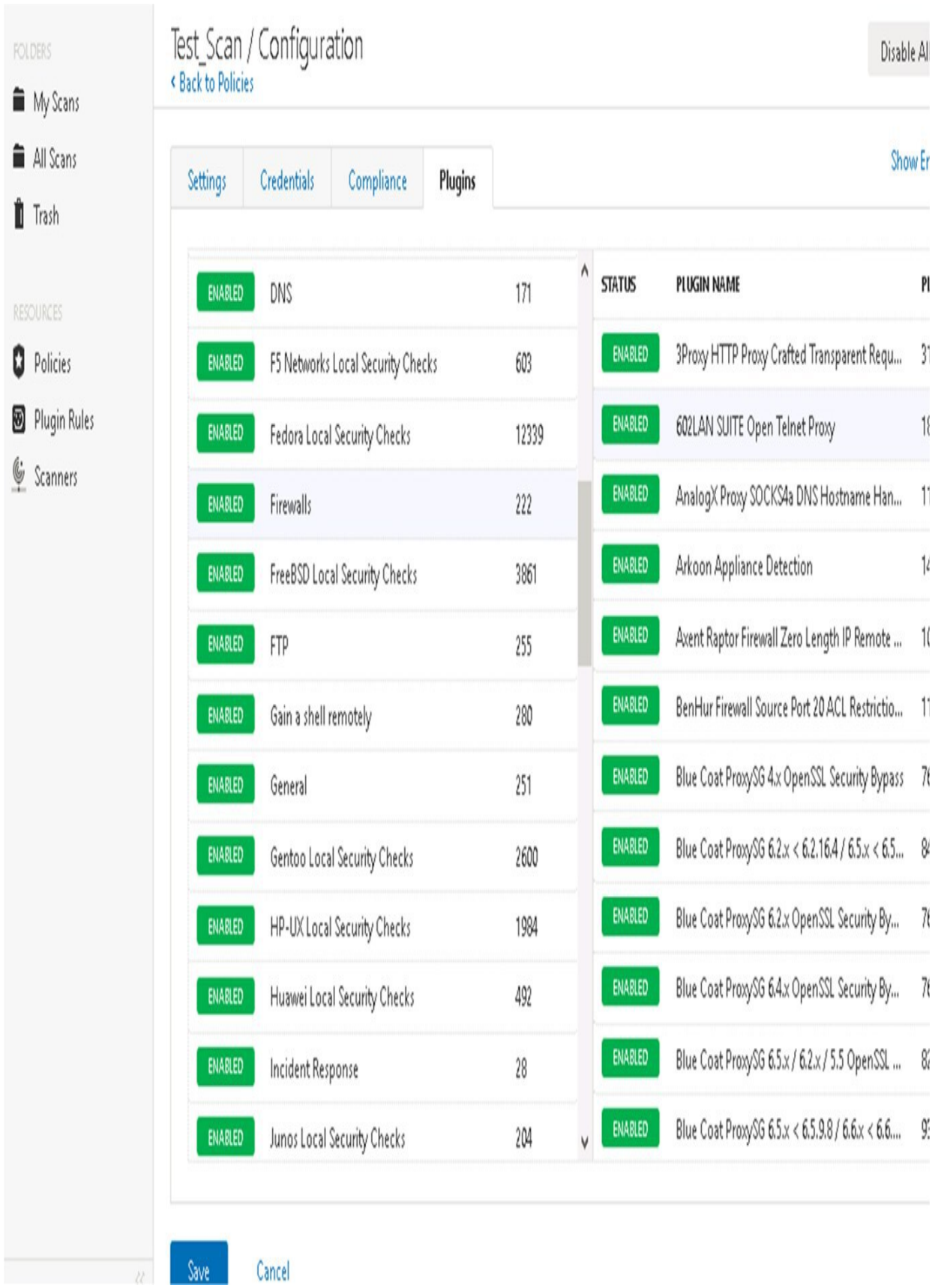

FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Test_Scan / Configuration
‹ Back to Policies
Disable Al
Settings
Credentials
Compliance
Plugins
Show Er
ENABLED DNS 171
ENABLED F5 Networks Local Security Checks 603
ENABLED Fedora Local Security Checks 12339
ENABLED Firewalls 222
ENABLED FreeBSD Local Security Checks 3861
ENABLED FTP 255
ENABLED Gain a shell remotely 280
ENABLED General 251
ENABLED Gentoo Local Security Checks 2600
ENABLED HP-UX Local Security Checks 1984
ENABLED Huawei Local Security Checks 492
ENABLED Incident Response 28
ENABLED Junos Local Security Checks 204
STATUS
PLUGIN NAME
ENABLED 3Proxy HTTP Proxy Crafted Transparent Requ...
ENABLED 602LAN SUITE Open Telnet Proxy
ENABLED AnalogX Proxy SOCKS4a DNS Hostname Han...
ENABLED Arkoon Appliance Detection
ENABLED Axent Raptor Firewall Zero Length IP Remote ...
ENABLED BenHur Firewall Source Port 20 ACL Restrictio...
ENABLED Blue Coat ProxySG 4.x OpenSSL Security Bypass
ENABLED Blue Coat ProxySG 6.2.x < 6.2.16.4 / 6.5.x < 6.5...
ENABLED Blue Coat ProxySG 6.2.x OpenSSL Security By...
ENABLED Blue Coat ProxySG 6.4.x OpenSSL Security By...
ENABLED Blue Coat ProxySG 6.5.x / 6.2.x / 5.5 OpenSSL ...
ENABLED Blue Coat ProxySG 6.5.x < 6.5.9.8 / 6.6.x < 6.6....
Save
Cancel

Figure 5-21: Configuring Policy

17. Check whether the policy is successfully configured or not.

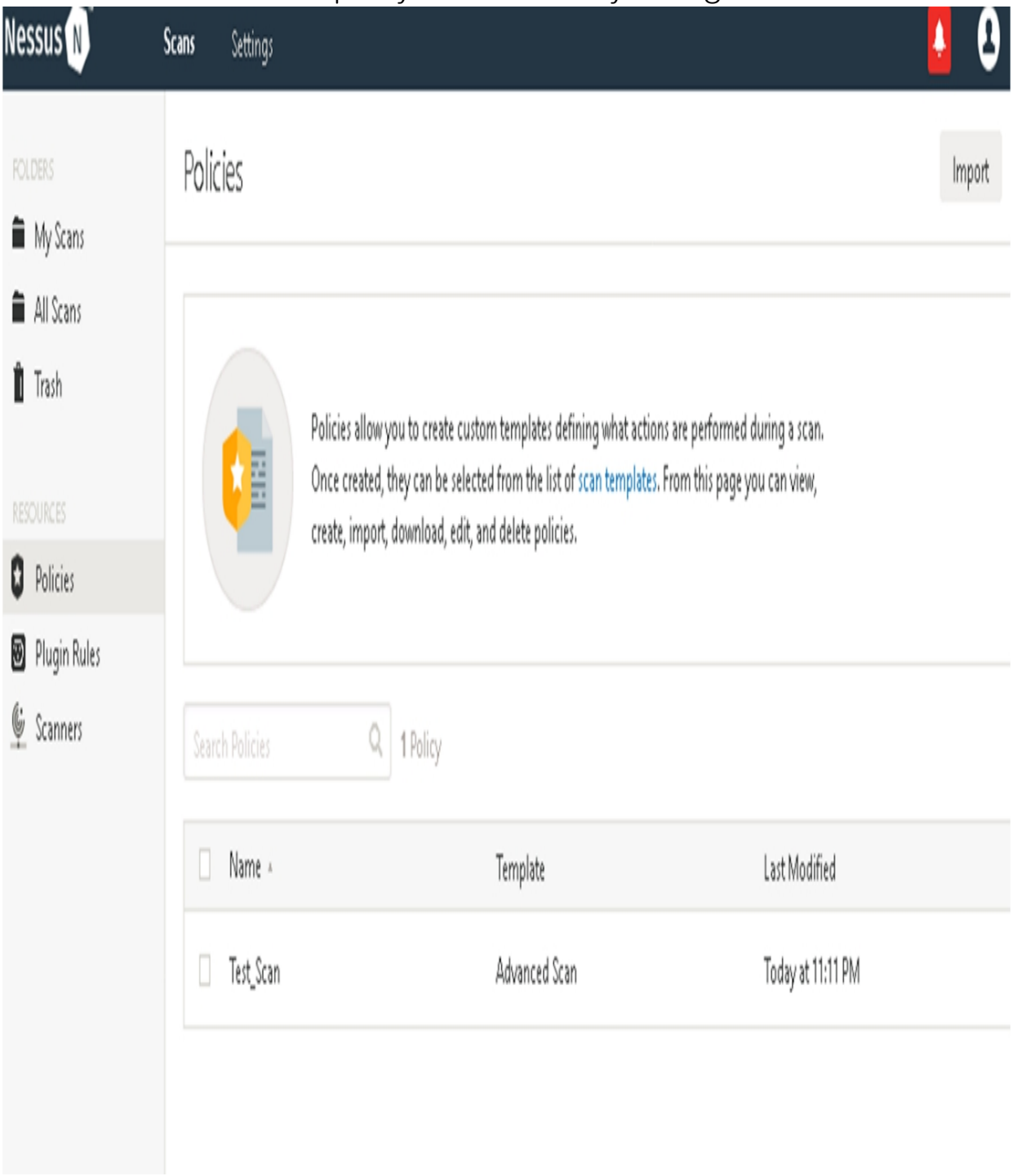


Figure 5-22: Verify Policy

18. Go to “Scan” > “Create New Scan”.

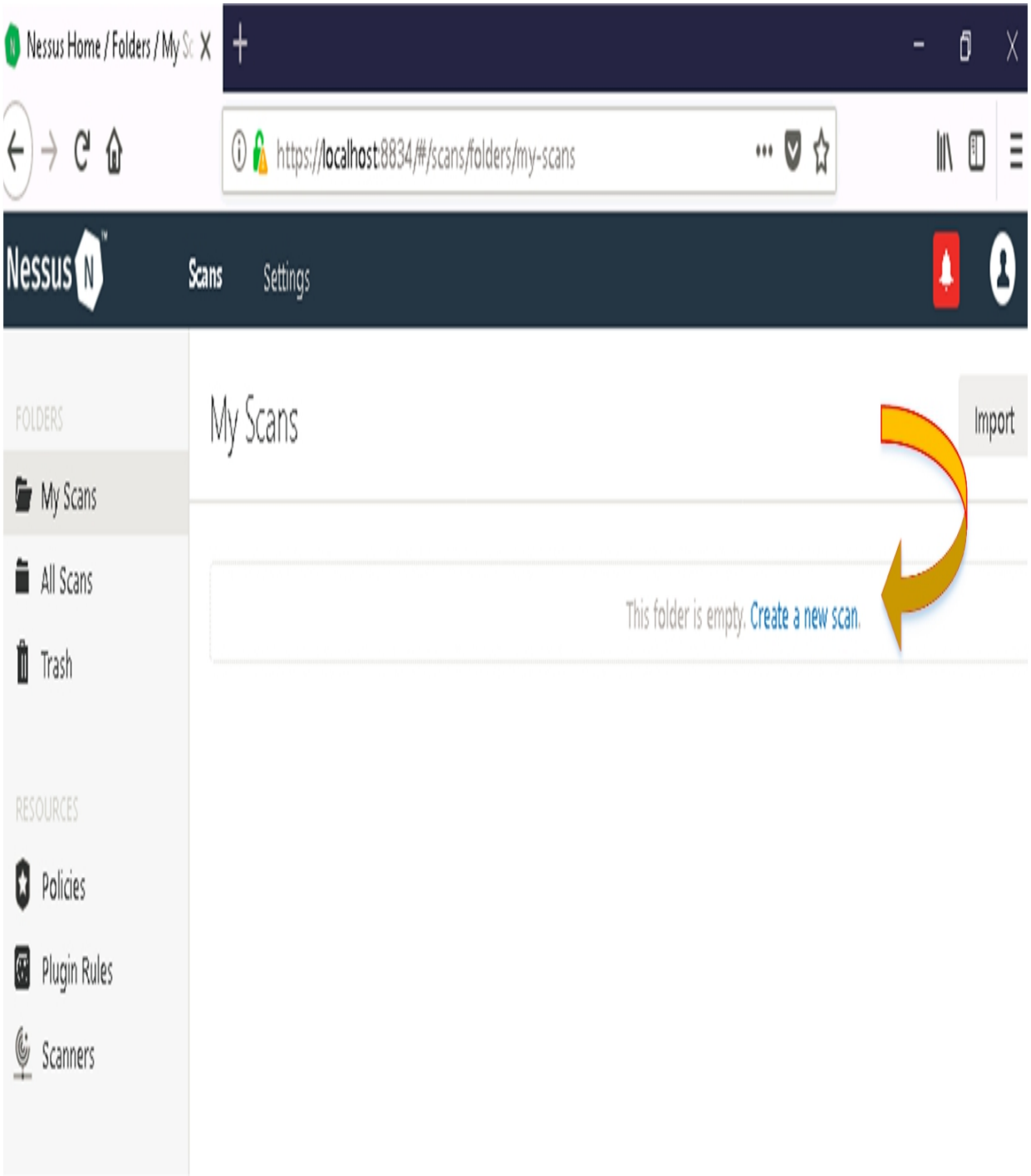


Figure 5-23: Configuring Scan

19. Enter the name for a new scan.

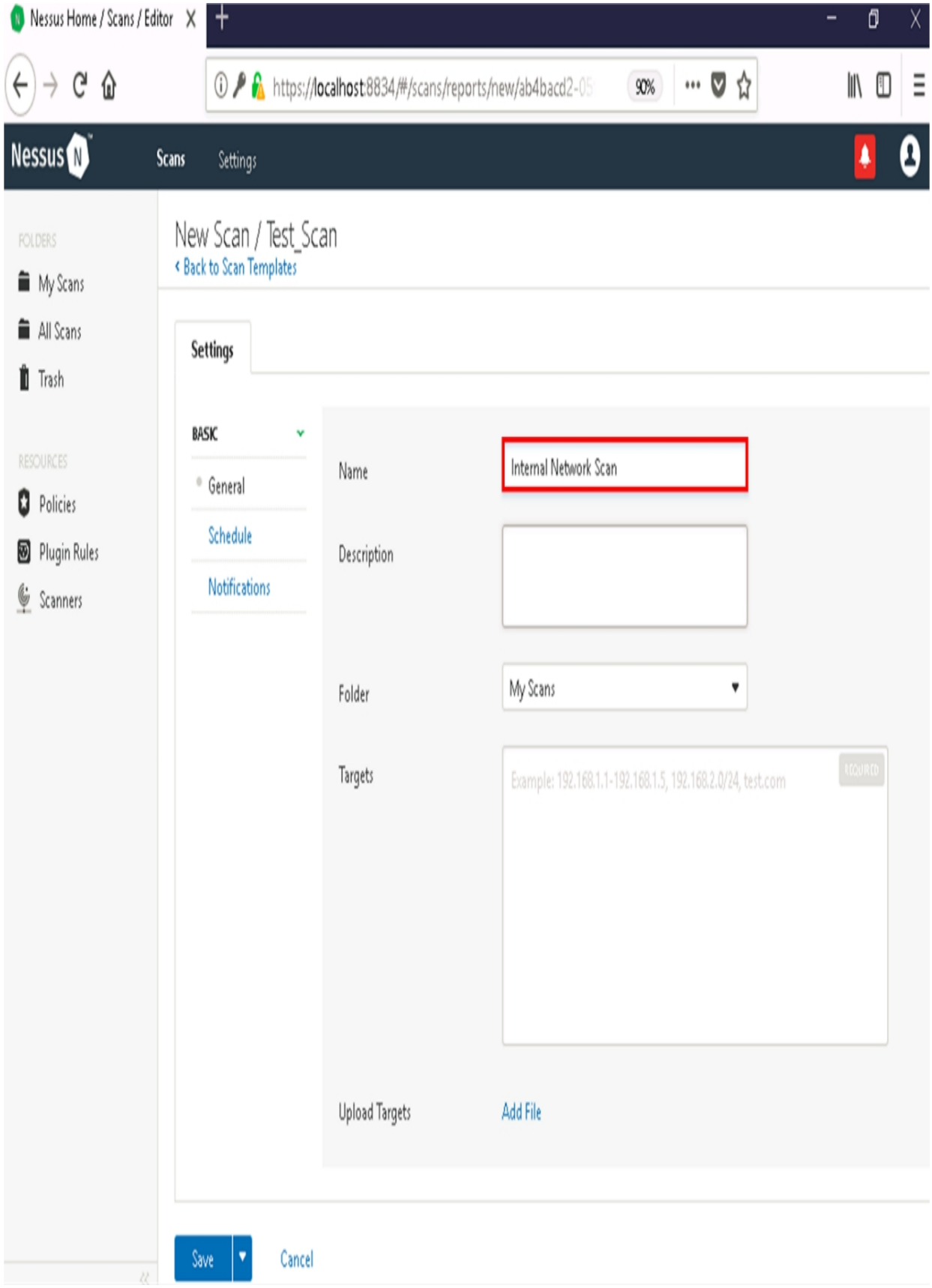

Nessus Home / Scans / Editor
https://localhost:8834/#/scans/reports/new/ab4bacd2-05
90%
Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Scan / Test_Scan
‹ Back to Scan Templates
Settings
BASIC
General
Schedule
Notifications
Name
Internal Network Scan
Description
Folder
My Scans
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED
Upload Targets
Add File
Save
Cancel

Figure 5-24: Configuring Scan

20. Enter target address.

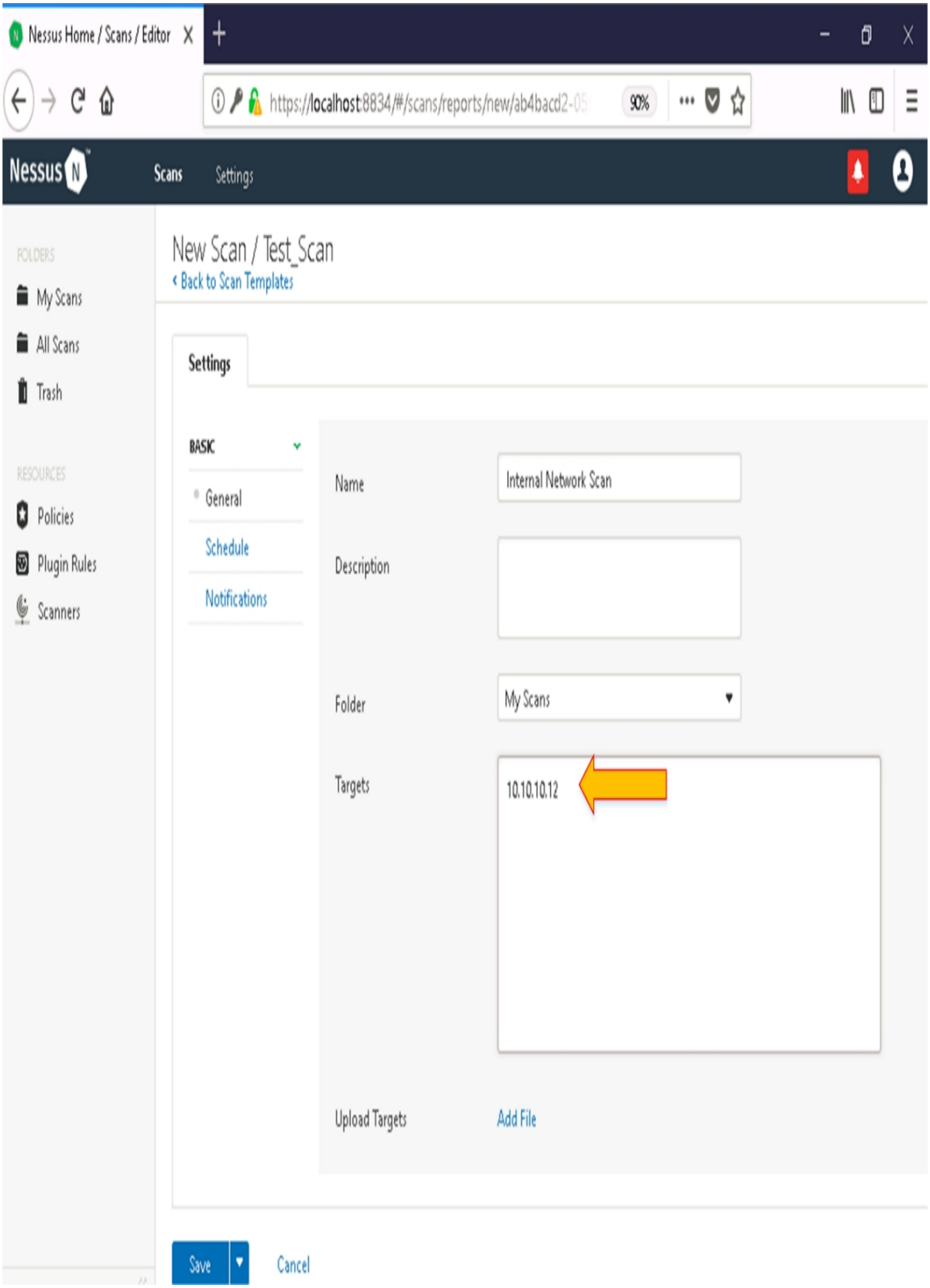

Nessus Home / Scans / Editor
https://localhost:8834/#/scans/reports/new/ab4bacd2-05
90%
Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Scan / Test_Scan
‹ Back to Scan Templates
Settings
BASIC
General
Schedule
Notifications
Name
Internal Network Scan
Description
Folder
My Scans
Targets
10.10.10.12
Upload Targets
Add File
Save
Cancel

Figure 5-25: Configuring Scan

21. Go to "My Scan", select your created scan and launch it.

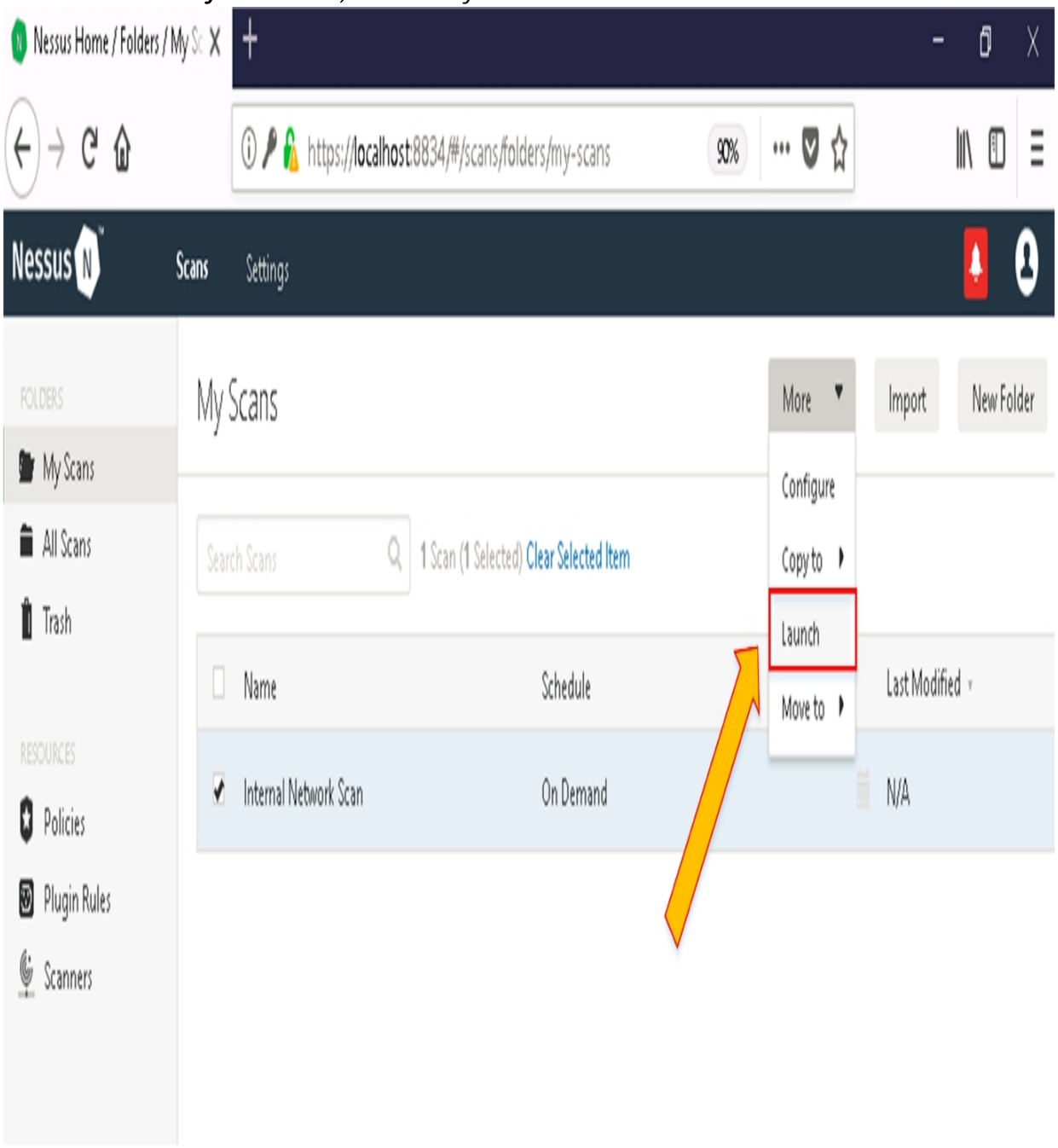


Figure 5-26: Launching Scan

22. Observe the status to check if scan has successfully started or not.

Figure 5-27: Scanning

23. Upon completion, observe the result.

Internal Network Scan

Configure | Audit Trail | Launch | Export

‹ Back to My Scans

Hosts 1 | Vulnerabilities 76 | Remediations 2 | Notes 1 | History 1

Filter | Search Hosts | 1 Host

Host	Vulnerabilities
10.10.10.12	3 13 3 83

Scan Details

Name:	Internal Network Scan
Status:	Completed
Policy:	Test_Scan
Scanner:	Local Scanner
Start:	Today at 11:16 PM
End:	Today at 11:20 PM
Elapsed:	4 minutes

Vulnerabilities

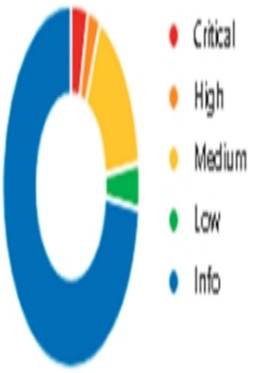


Figure 5-28: Scan Results

24. Click on the “Vulnerabilities Tab” to observe the detected vulnerabilities. You can also check other tabs like “Remediation”, “Notes”, and “History” to get more details about history, issues, and remediation actions.

Figure 5-29: Scan Results

25. Go to “Export” tab to export the report and select the required format.

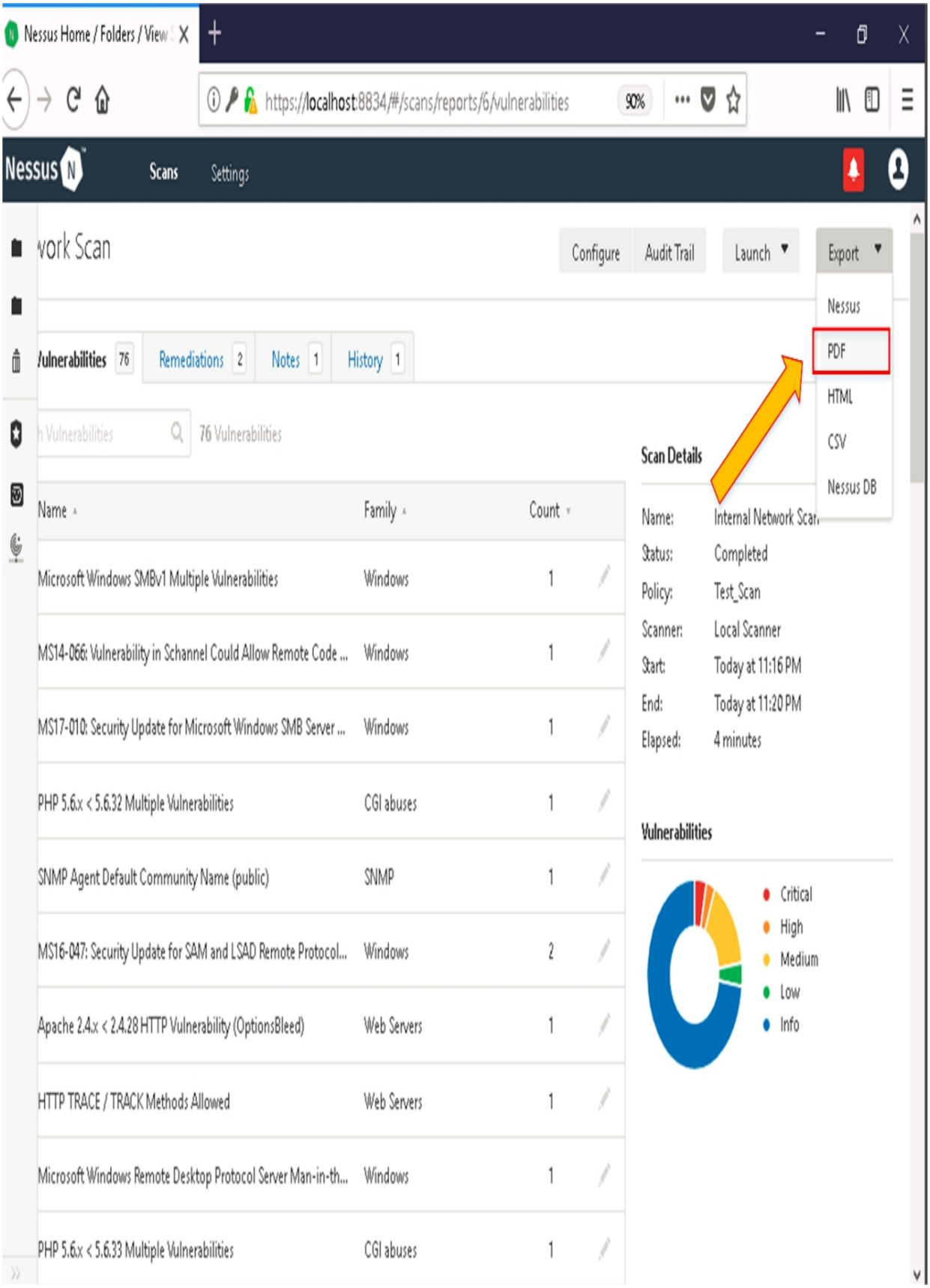

Nessus Home / Folders / View
https://localhost:8834/#/scans/reports/6/vulnerabilities
90%
Nessus
Scans
Settings
work Scan
Configure
Audit Trail
Launch
Export
Nessus
PDF
HTML
CSV
Nessus DB
Vulnerabilities 76
Remediations 2
Notes 1
History 1
Vulnerabilities
76 Vulnerabilities
Name
Family
Count
Microsoft Windows SMBv1 Multiple Vulnerabilities
Windows
1
MS14-066: Vulnerability in Schannel Could Allow Remote Code ...
Windows
1
MS17-010: Security Update for Microsoft Windows SMB Server ...
Windows
1
PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CGI abuses
1
SNMP Agent Default Community Name (public)
SNMP
1
MS16-047: Security Update for SAM and LSAD Remote Protocol...
Windows
2
Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)
Web Servers
1
HTTP TRACE / TRACK Methods Allowed
Web Servers
1
Microsoft Windows Remote Desktop Protocol Server Man-in-th...
Windows
1
PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
CGI abuses
1
Scan Details
Name:
Status: Completed
Policy: Test_Scan
Scanner: Local Scanner
Start: Today at 11:16 PM
End: Today at 11:20 PM
Elapsed: 4 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

Figure 5-30: Scan Results

26. Figure 5-31 is displaying a preview of the exported report in pdf format.

Vulnerabilities Total: 76

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	9.3	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted

Figure 5-31: Scan Results

Note: Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), which is a simple language that defines individual threats and potential attacks.

Practice Questions

1. The process of finding weaknesses, design flaws and security concerns in a network, Operating System, applications or website is called:
A. Enumeration
B. Vulnerability Analysis
C. Scanning Networks
D. Reconnaissance

2. Which of the following is a Pre-Assessment phase of Vulnerability Assessment Life-Cycle?
A. Creating Baseline
B. Vulnerability Assessment
C. Risk Assessment
D. Remediation

3. Vulnerability Post Assessment phase includes: A. Risk Assessment
B. Remediation
C. Monitoring
D. Verification
E. All of the above

4. Vulnerability assessment process, in which auditor follows different strategies for each network component is called:
A. Product-based Assessment
B. Service-based Assessment
C. Tree-based Assessment
D. Inference-based Assessment