

- 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.

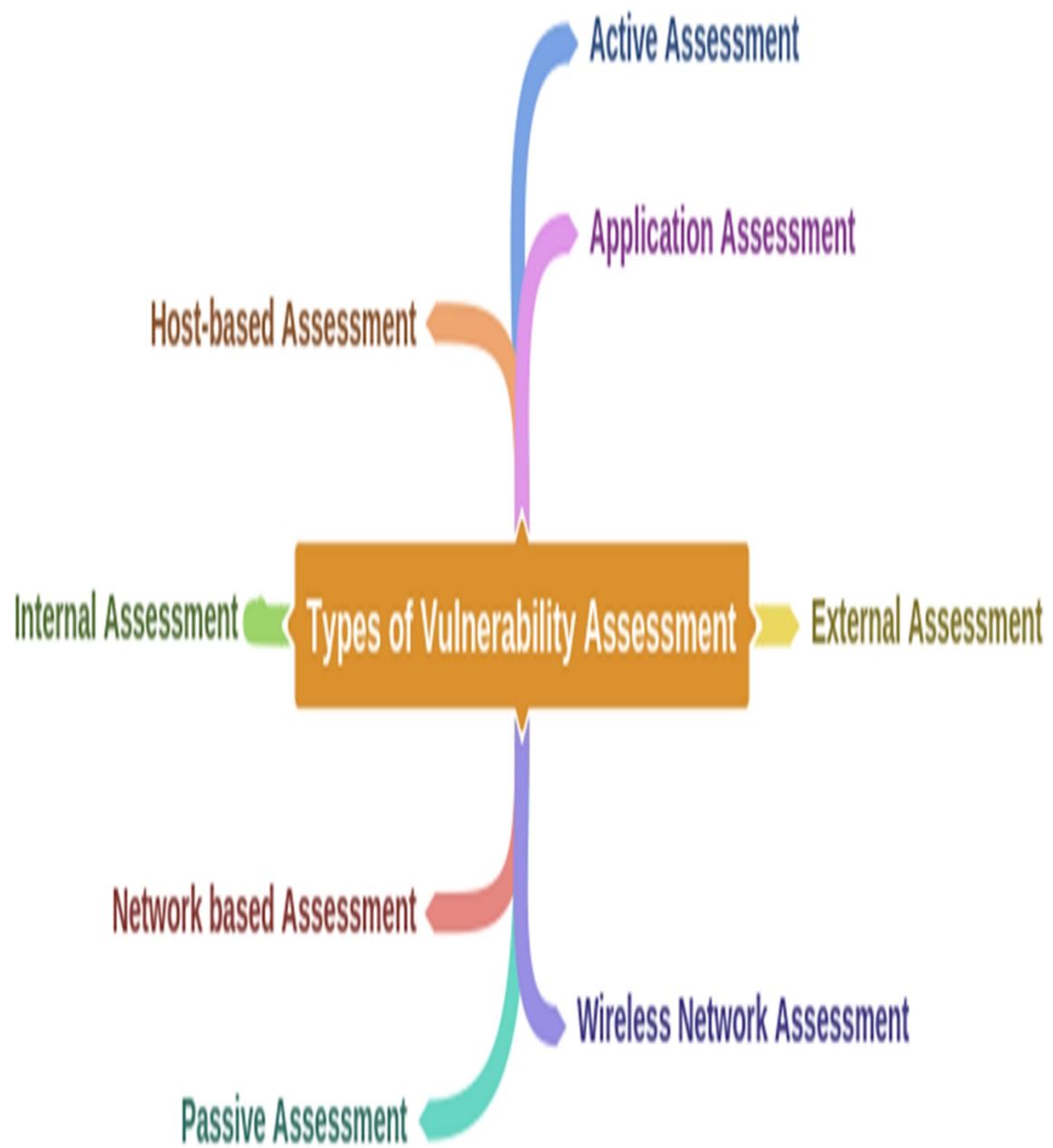


Figure 5–01: Types of Vulnerability Assessment

## 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.

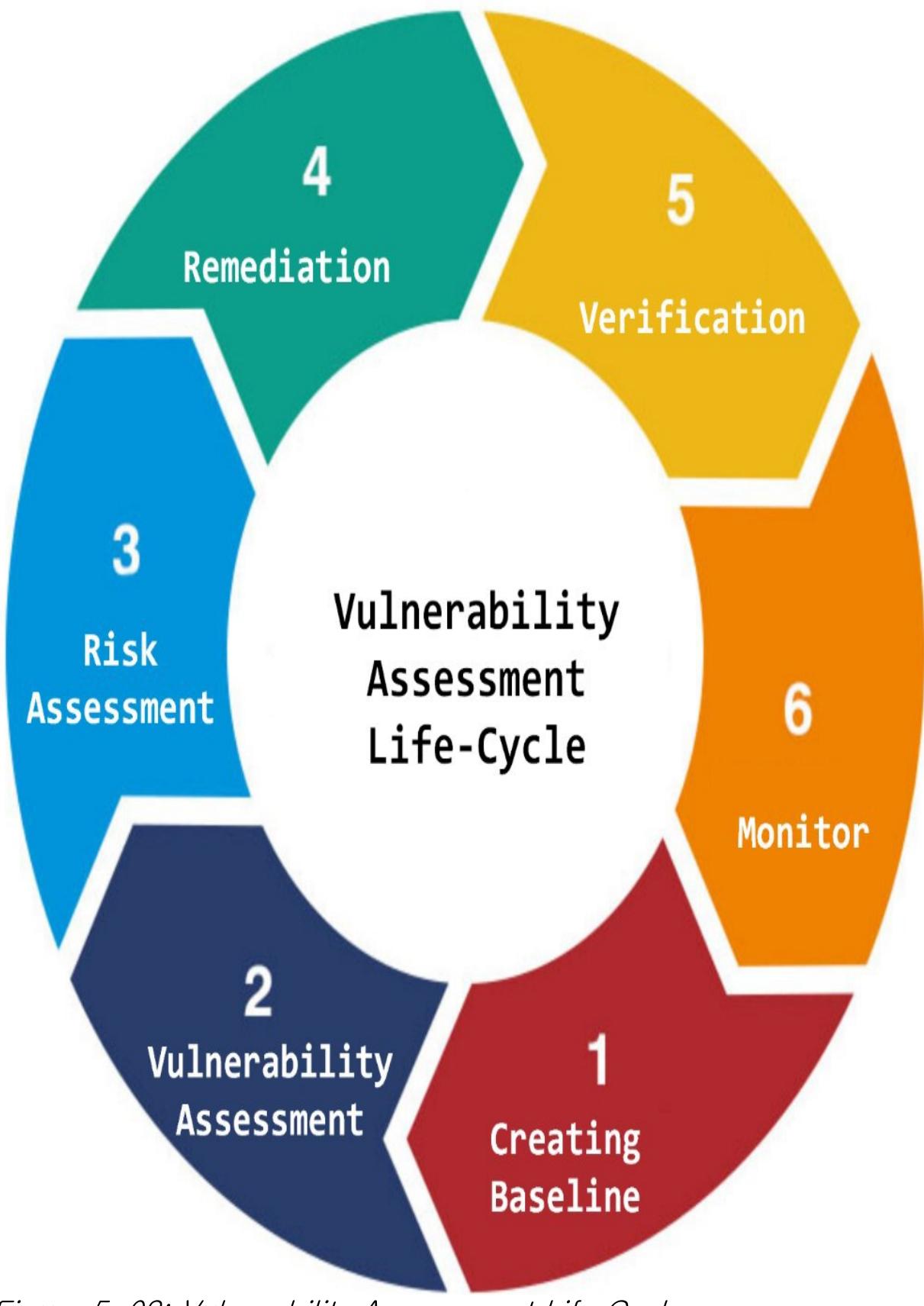


Figure 5: Vulnerability Assessment Life-Cycle

## *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:

$$\text{ALE} = \text{ARO} * \text{SLE}$$

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.

$$\text{SLE} = \text{EF} * \text{AV}$$

**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 completely 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 Linux based 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	<i>Table 5-01: CVSSv3 Scoring</i>	

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.

CVE - CVE-1999-0002 X

← → C i cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0002

**CVE-ID**

**CVE-1999-0002** [Learn more at National Vulnerability Database \(NVD\)](#)  
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

**Description**

Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems.

**References**

**Note:** [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- SGI:19981006-01-I
- [URL:ftp://patches.sgi.com/support/free/security/advisories/19981006-01-I](http://patches.sgi.com/support/free/security/advisories/19981006-01-I)
- CERT:CA-98.12.mountd
- CIAC:j-006
- [URL:http://www.ciac.org/ciac/bulletins/j-006.shtml](http://www.ciac.org/ciac/bulletins/j-006.shtml)
- BID:121
- [URL:http://www.securityfocus.com/bid/121](http://www.securityfocus.com/bid/121)
- XF:linux-mountd-bo

**Date Entry Created**

19990925	Disclaimer: The <a href="#">entry creation date</a> may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
----------	--

This is an entry on the [CVE List](#), which provides common identifiers for publicly known cybersecurity vulnerabilities.

**SEARCH CVE USING KEYWORDS:**

You can also search by reference using the [CVE Reference Maps](#).

**For More Information:** [cve@mitre.org](mailto:cve@mitre.org)

BACK TO TOP

## *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

GFI LanGuard 2016 C

https://

**GFI LanGuard**

Home Dashboard Reports Bell Gear Help User

Search ALL DEVICES Overview Computers History Vulnerabilities Patches Ports Software Hardware System Information

Entire Network - 70 Computers

Entire Network - 70 Computers

119 275

Missing Security Updates  
Missing Non-Security Updates  
Missing Service Packs and Update Rollups  
Major Version Upgrades

Installed Security Updates  
Installed Non-Security Updates  
Installed Service Packs and Update Rollups

Patch name	Date posted	Severity	Applies to
FOXITR6140217: Foxit Reader 6...	2014-02-20	Critical	Foxit Reader
JAVA8051: Java Runtime Enviro...	2015-07-14	Critical	Java Runtime Env...
mfsa2015-59, mfsa2015-60, mfs...	2015-06-30	Moderate	Firefox
MS06-061: MSXML 6.0 RTM Sec...	2012-04-04	Critical	SQL Server
MS07-028: Security Update for...	2007-05-08	Critical	SDK Component
MS09-035: Security Update for...	2009-09-08	Moderate	Developer Tools,
MS09-035: Security Update for...	2009-08-11	Moderate	Developer Tools,
MS09-062: Security Update for...	2009-10-16	Low	Developer Tools,
MS09-062: Security Update for...	2009-10-16	Low	Developer Tools,
MS11-025: Security Update for...	2012-01-24	Important	Developer Tools,
MS11-025: Security Update for...	2012-01-24	Important	Developer Tools,
MS11-025: Security Update for...	2012-03-13	Important	Developer Tools,
MS11-025: Security Update for...	2012-01-24	Important	Developer Tools,
MS11-049: Security Update for...	2012-01-24	Important	Developer Tools,
MS12-021: Security Update for...	2012-03-13	Important	Developer Tools,
MS12-021: Security Update for...	2012-05-09	Important	Developer Tools,

Page 1 of 2 (40 items) 1 2 3 Page size: 20

Figure 5. GFI LanGuard Vulnerability Scanning Tool

*Figure 5-04. GFI LAN GUARD 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

Qualys FreeScan - Security Scan

← → C Qualys, Inc. [US] | https://freescan.qualys.com/freescan-front/module/freescan/#dashboard

Welcome

Thanks for choosing Qualys FreeScan. To help you get started, tips will explain what everything does. These can be turned off in your account area.

Quick Tour | Upgrade Now | | 10 scans remaining

We can't reach your IP  
**192.168.0.1**

The IP address you entered is within your internal network. You need to configure a virtual scanner in order to scan this IP.

Your scan will start as soon as the virtual scanner is ready.

Enter another IP Configure V-Scanner

### FreeScan Quick Tour

Scanning external devices and websites

New Results

Threat Report

**VULNERABILITY**  
Network | WAS | MDS Scans

**OWASP**  
Risk Scan

**PATCH TUESDAY**  
Authenticated Scan

**SCAP**  
Compliance Scan

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.

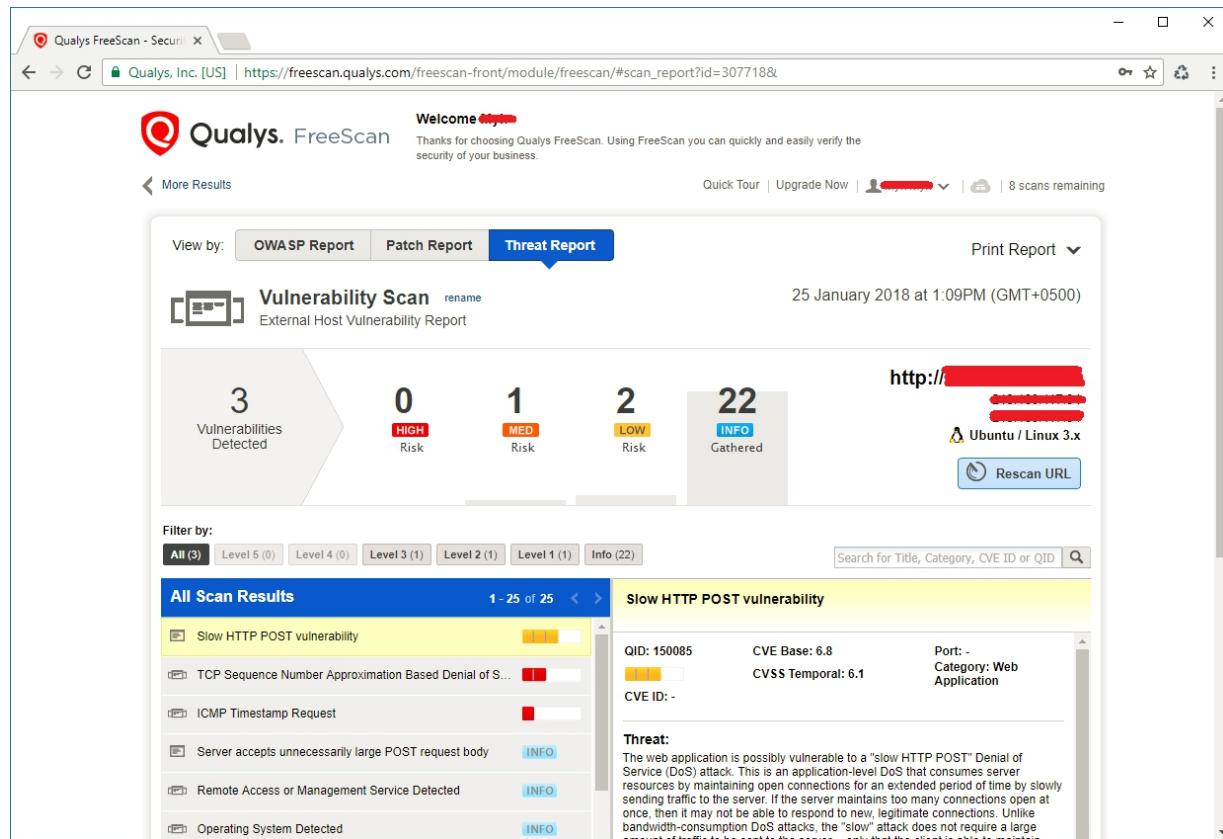


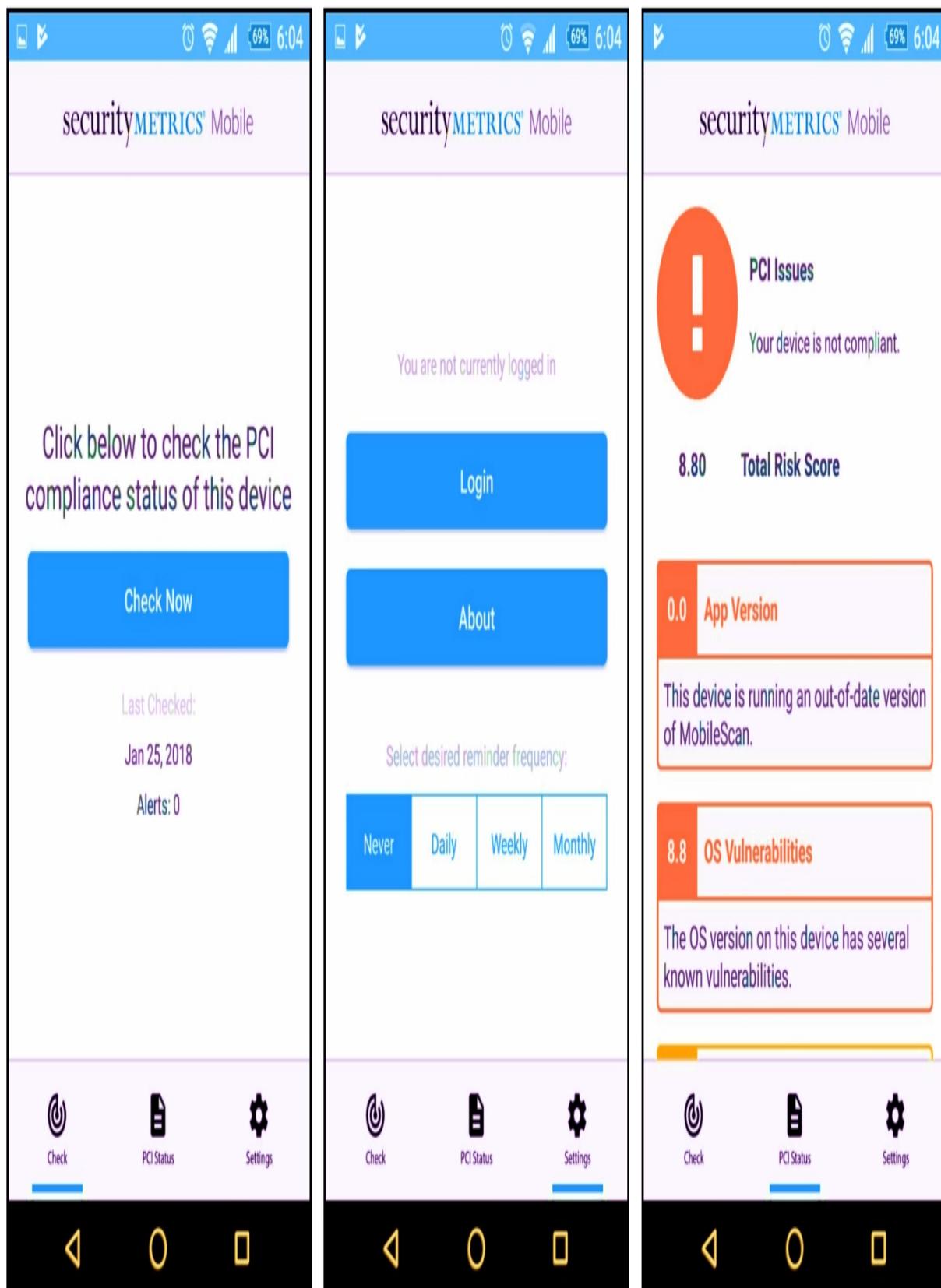
Figure 5–06: Qualys FreeScan Vulnerability Scanning Tool  
Vulnerability Scanning Tools for Mobiles

Following is a list of vulnerability scanning tools for mobiles:

### Application Website

Retina CS for Mobile <http://www.beyondtrust.com> Security Metrics  
Mobile Scan <http://www.securitymetrics.com> Nessus Vulnerability  
Scanner <http://www.tenable.com>

Table 5–02: Vulnerability Scanning Tools for Mobiles

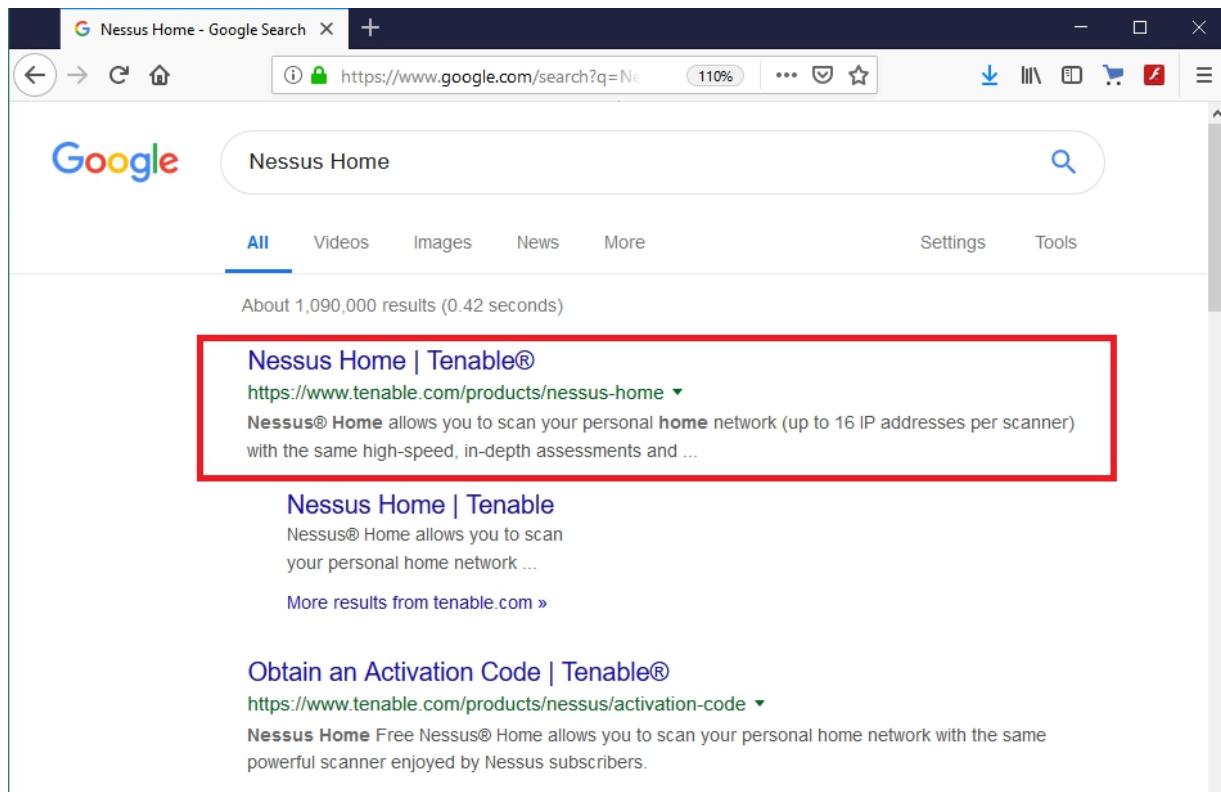


*Figure 5–07: Security Metrics Mobile Scan*

## 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.

The screenshot shows a web browser window with the following details:

- Title Bar:** Nessus Home | Tenable®
- Address Bar:** https://www.tenable.com/products/nessus-home
- Page Content:**
  - Tenable Logo:** A blue circular icon with a white 't' followed by the word "tenable".
  - Navigation Links:** Cyber Exposure, Products, Solutions, Research, Services, Company, Partners.
  - Call-to-Action Buttons:** Free Trial, Buy Now.
  - Section Header:** Nessus Home
  - Text:** Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.
  - Note:** Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these [additional features](#), please purchase a [Nessus](#) subscription.
  - Text:** Nessus Home is available for personal use in a home environment only. It is not for use by any organization.
  - Text:** Waiting for dsum-sec.casalemedia.com...
- Form:** Register for an Activation Code
  - First Name \*
  - Last Name \*
  - Email \*

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

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

### Register for an Activation Code

First Name \*      Last Name \*

Email \*

Check to receive updates from Tenable

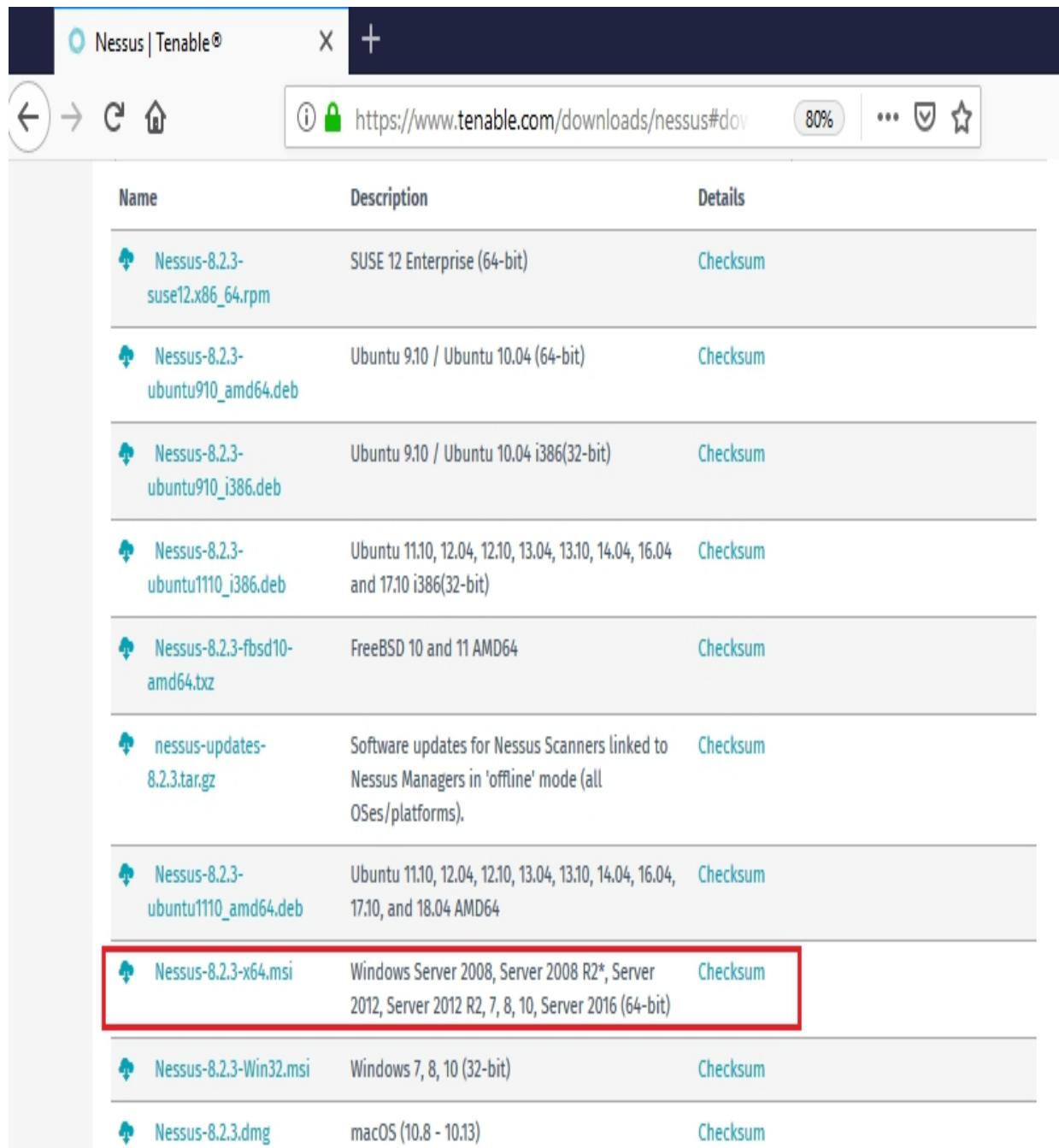
**Register**

Now to download Nessus, click on the download link.

The screenshot shows a web browser window with the following details:

- Title Bar:** "Thank You for Registering for N..."
- Address Bar:** <https://www.tenable.com/products/nessus>
- Header:** Tenable logo, navigation links: Cyber Exposure, Products, Solutions, Research, Services, Company, Partners, and buttons for Free Trial and Buy Now.
- Main Content:** A teal-colored banner with the text "Thank You for Registering for Nessus Home!" and "Check Your Email for the Activation Code".
- Left Side:** A message: "Thank you for registering for Nessus® Home. An email containing your activation code has been sent to you at the email address you provided." Another message below it: "Please note that Nessus Home is available for non-commercial, home use only. If you will use Nessus at your place of business, you must purchase a [Nessus subscription](#)".
- Right Side:** A box titled "Download Nessus" with the text "To download Nessus, visit the Nessus Download page." and a "Download" button.

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)	<a href="#">Checksum</a>
Nessus-8.2.3-ubuntu910_amd64.deb	Ubuntu 9.10 / Ubuntu 10.04 (64-bit)	<a href="#">Checksum</a>
Nessus-8.2.3-ubuntu910_i386.deb	Ubuntu 9.10 / Ubuntu 10.04 i386(32-bit)	<a href="#">Checksum</a>
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)	<a href="#">Checksum</a>
Nessus-8.2.3-fbsd10-amd64.txz	FreeBSD 10 and 11 AMD64	<a href="#">Checksum</a>
nessus-updates-8.2.3.tar.gz	Software updates for Nessus Scanners linked to Nessus Managers in 'offline' mode (all OSes/platforms).	<a href="#">Checksum</a>
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	<a href="#">Checksum</a>
Nessus-8.2.3-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	<a href="#">Checksum</a>
Nessus-8.2.3-Win32.msi	Windows 7, 8, 10 (32-bit)	<a href="#">Checksum</a>
Nessus-8.2.3.dmg	macOS (10.8 - 10.13)	<a href="#">Checksum</a>

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

## License Agreement

### MASTER software license AND SERVICES Agreement

This is a legal agreement ("Agreement") between Tenable (as defined below), and you, the party licensing Software and/or receiving services ("You"). This Agreement covers Your permitted use of the Software, as well as other matters. BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM. The Software may be provided to You by Tenable or Tenable's designated vendor (the "Vendor").

#### 1. Definitions.

- (a) "Host" means any scanned device that can have a unique tag pushed to it (via a registry entry, text file, etc.), one that can have a unique identifier (CPU ID, Instance ID, Agent ID, IP Address, MAC Address, NetBIOS Name, etc.) pulled from it, or is addressable via URI or URL (i.e., <http://www.tenable.com>).
- (b) "Plug-In" means any individual program or script used to analyze for and/or identify specific security vulnerabilities.
- (c) If You are licensing SecurityCenter, the following terms apply:
  - (1) "Purpose" means to seek and assess information technology vulnerabilities and intrusion detection events up to the number of Hosts for which the Licensed Product is licensed.
  - (2) "Licensed Product" means SecurityCenter 4.x or higher.
  - (3) Subject to Section 8, You may install the Licensed Product on only one (1) production computer or machine.
  - (4) For the avoidance of doubt, the Licensed Product may be used by You to distribute Plug-Ins (as defined below) only to Tenable Nessus 5.x or higher or Tenable Nessus Network Monitor scanner exclusively controlled by the instance of SecurityCenter licensed hereunder.
- (d) If You are licensing the Log Correlation Engine, the following terms apply:
  - (1) "Purpose" means to receive and assess information technology logs and security events.
  - (2) "Licensed Product" means Log Correlation Engine 4.x or higher.

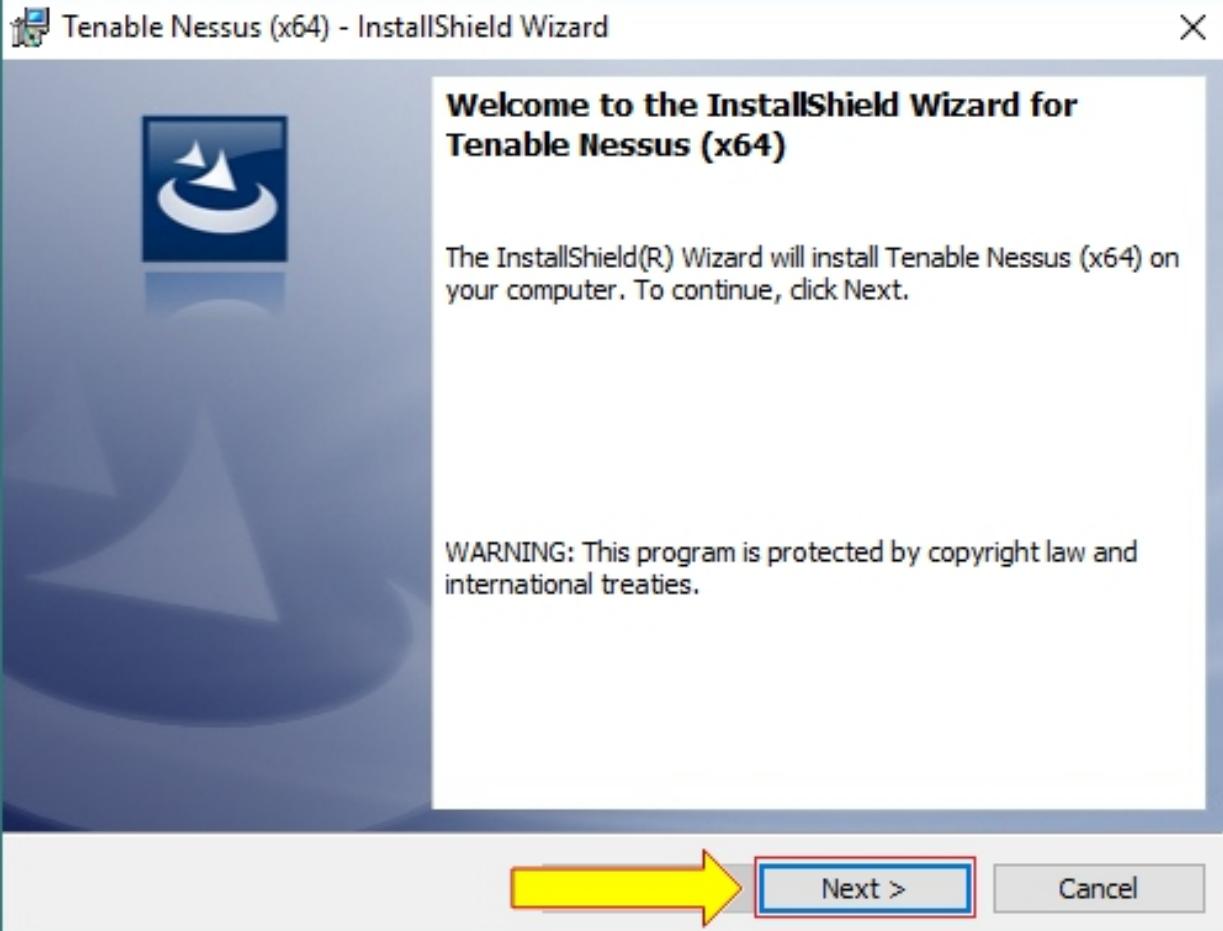
I Agree

Cancel

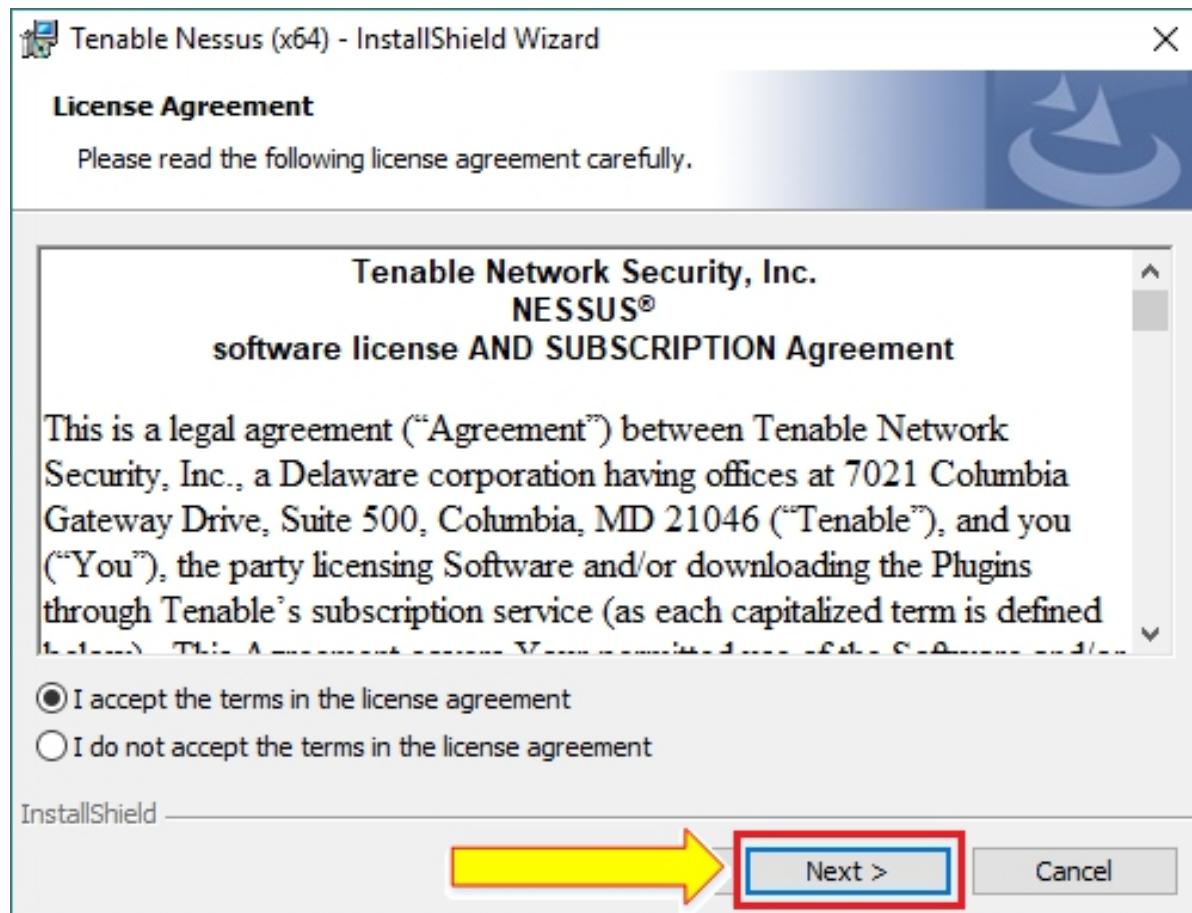
x64.msi

2008 R2\*, Server 2012, Server 2012

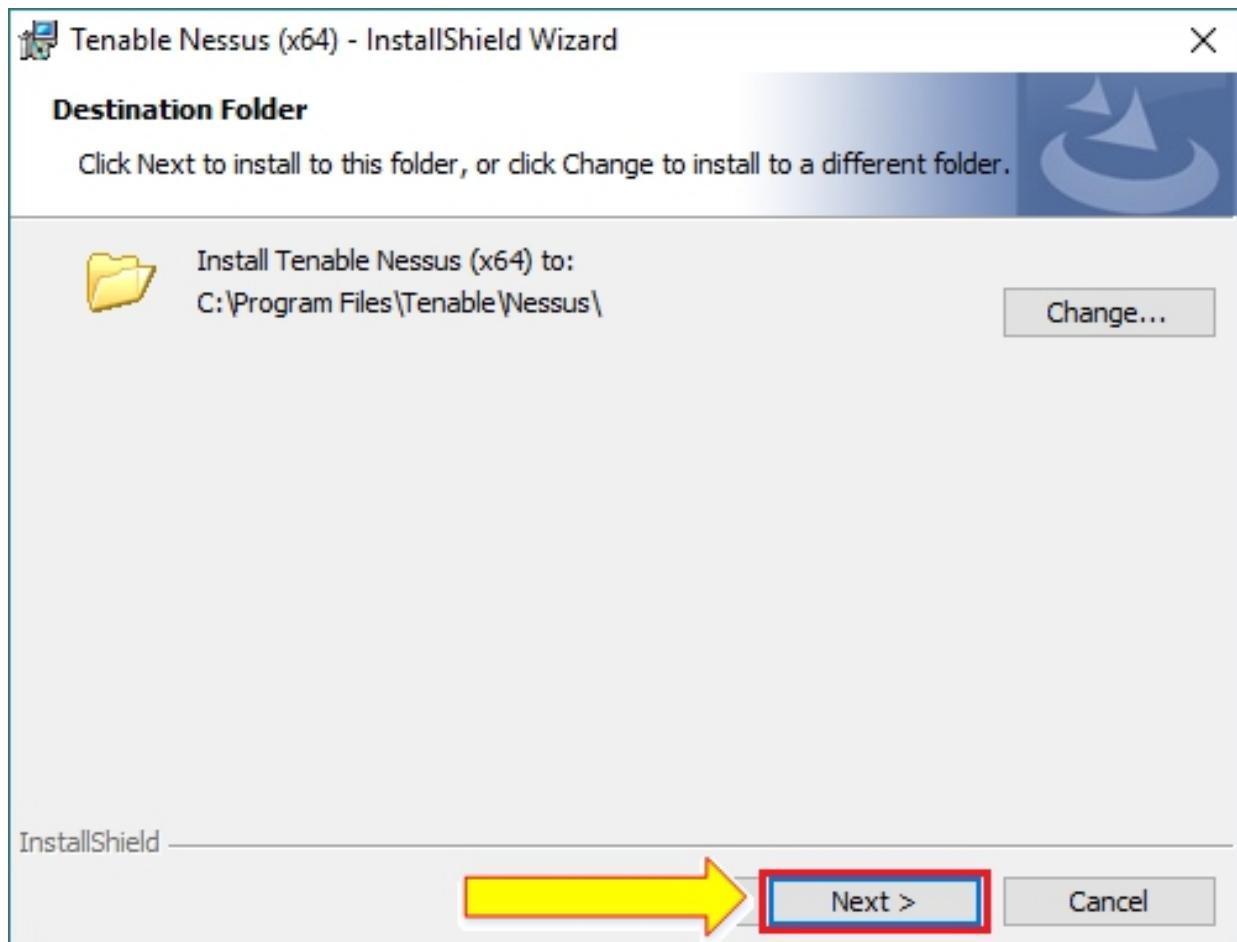
Download and install the software.



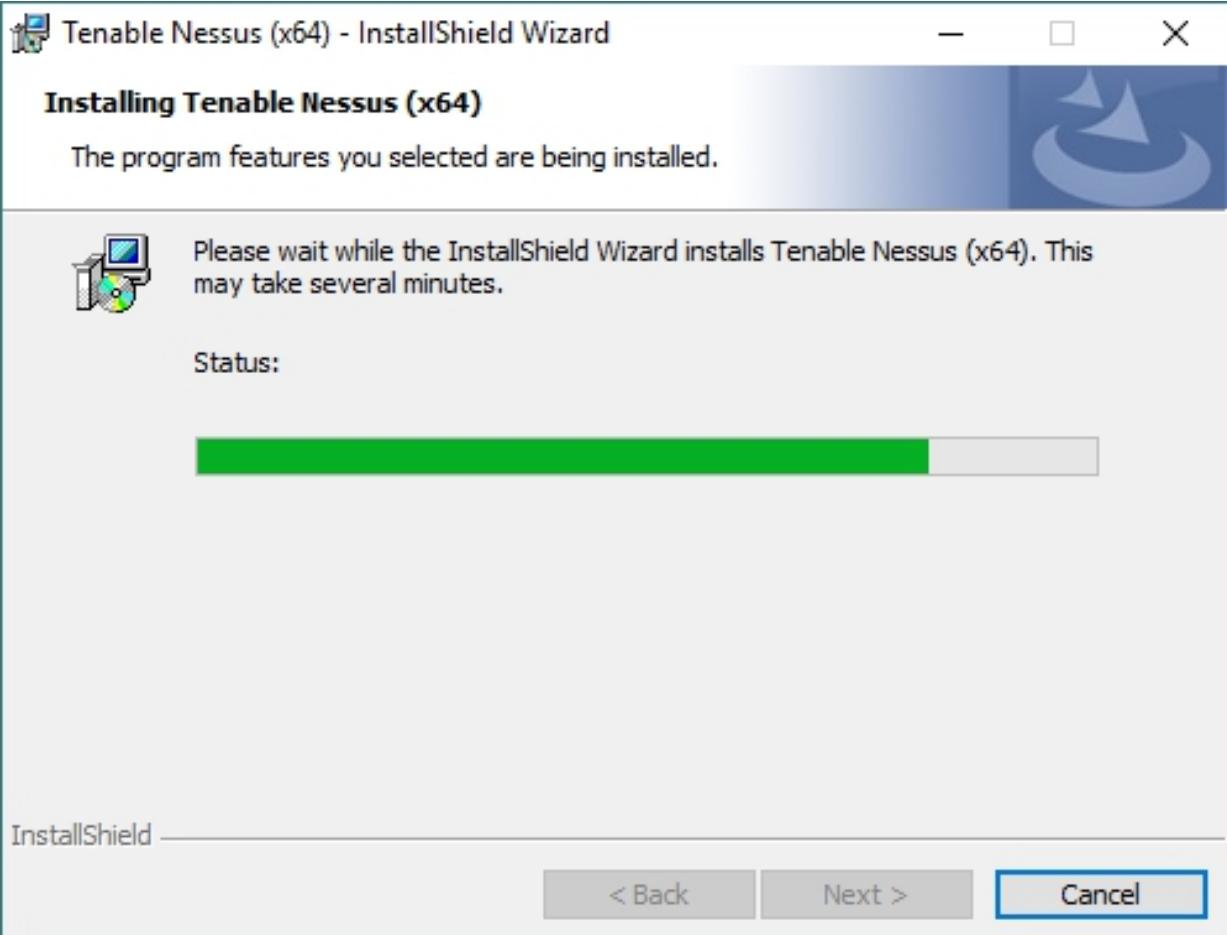
Select “I agree” and click “Next”.



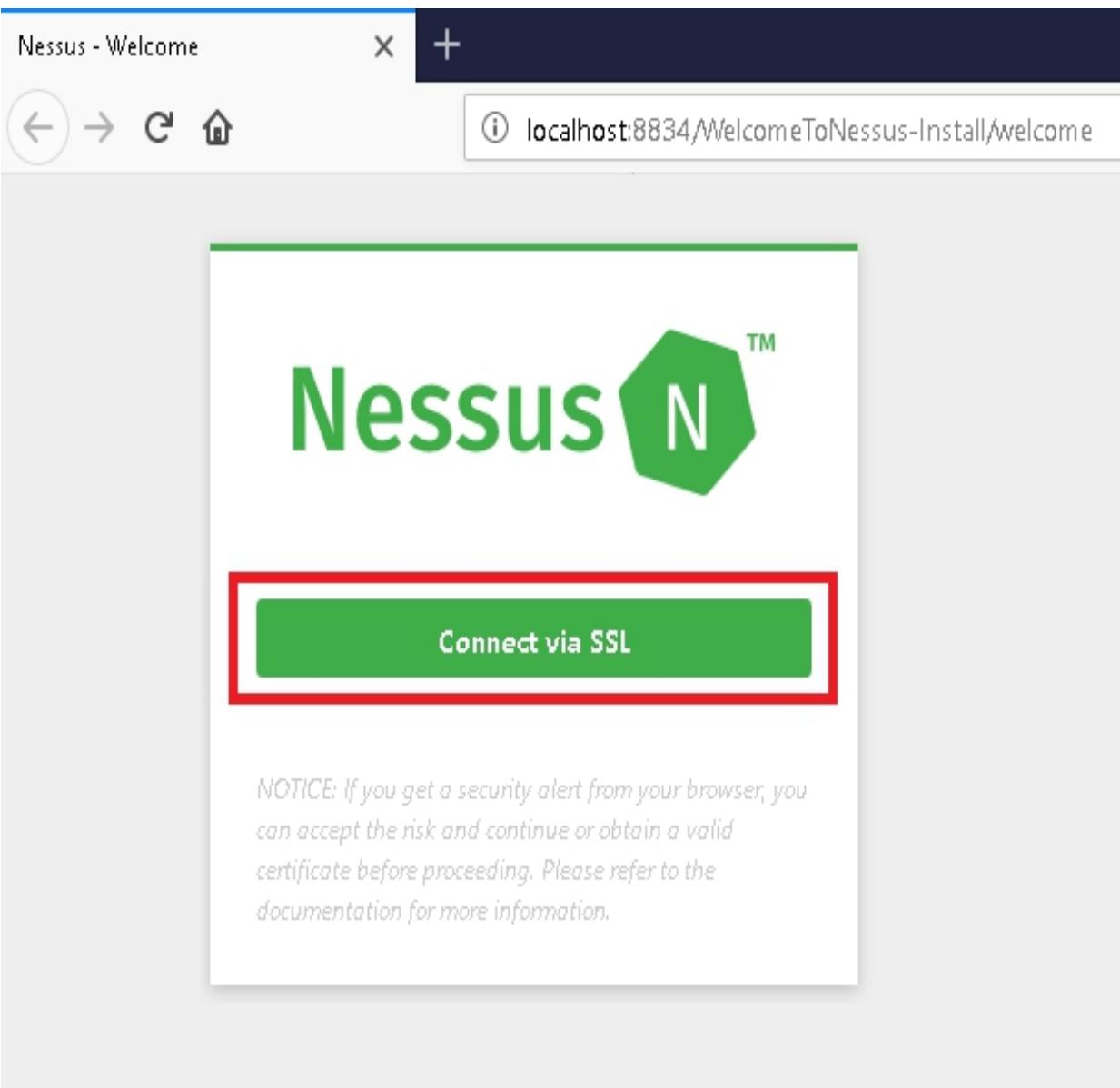
Now, if you want to change the file destination, click on the “Change” button, or else just click “Next”.



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

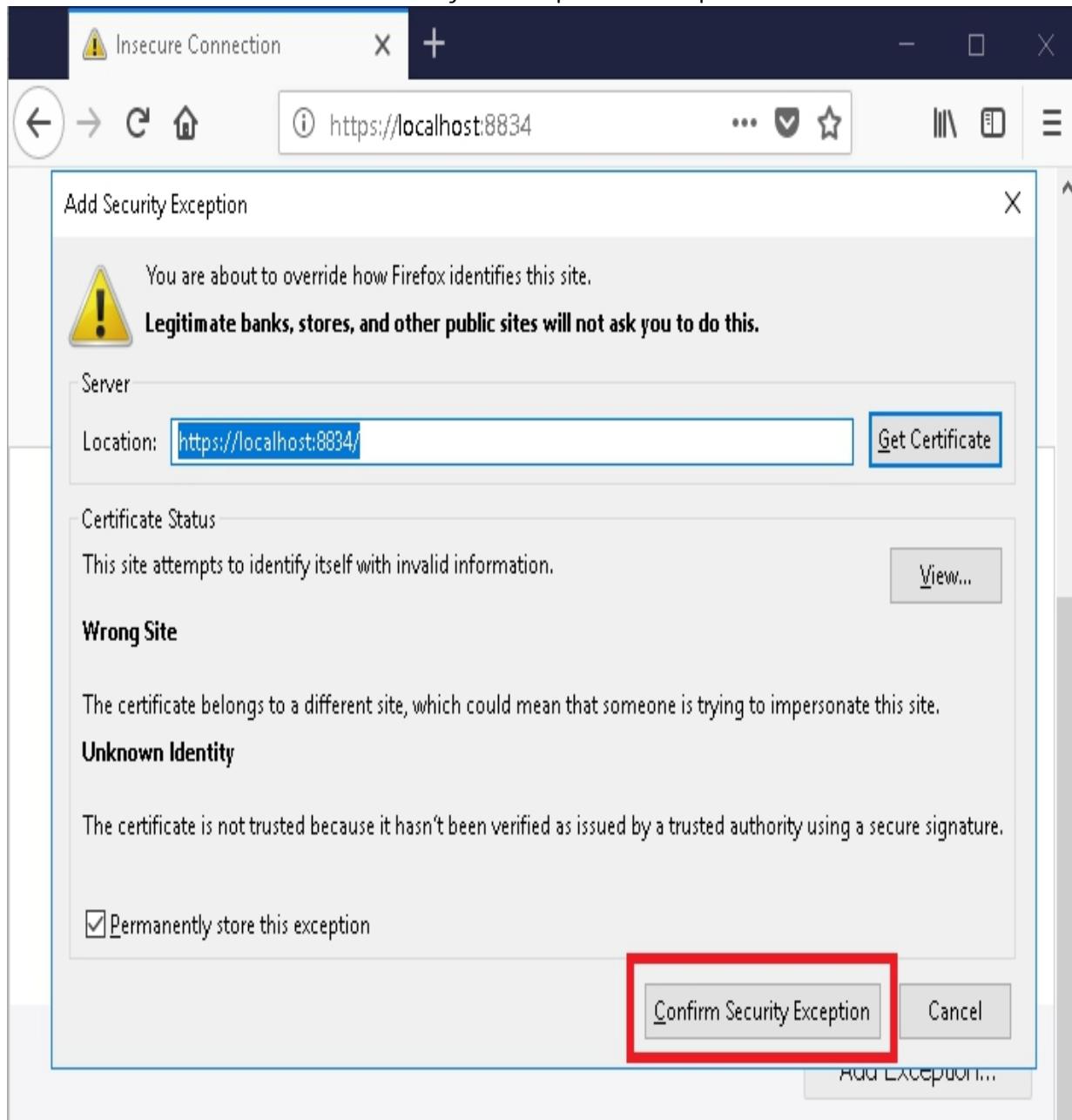


The installation is complete. Click “Finish”.  
When you see this window, click on “Connect via SSL”.

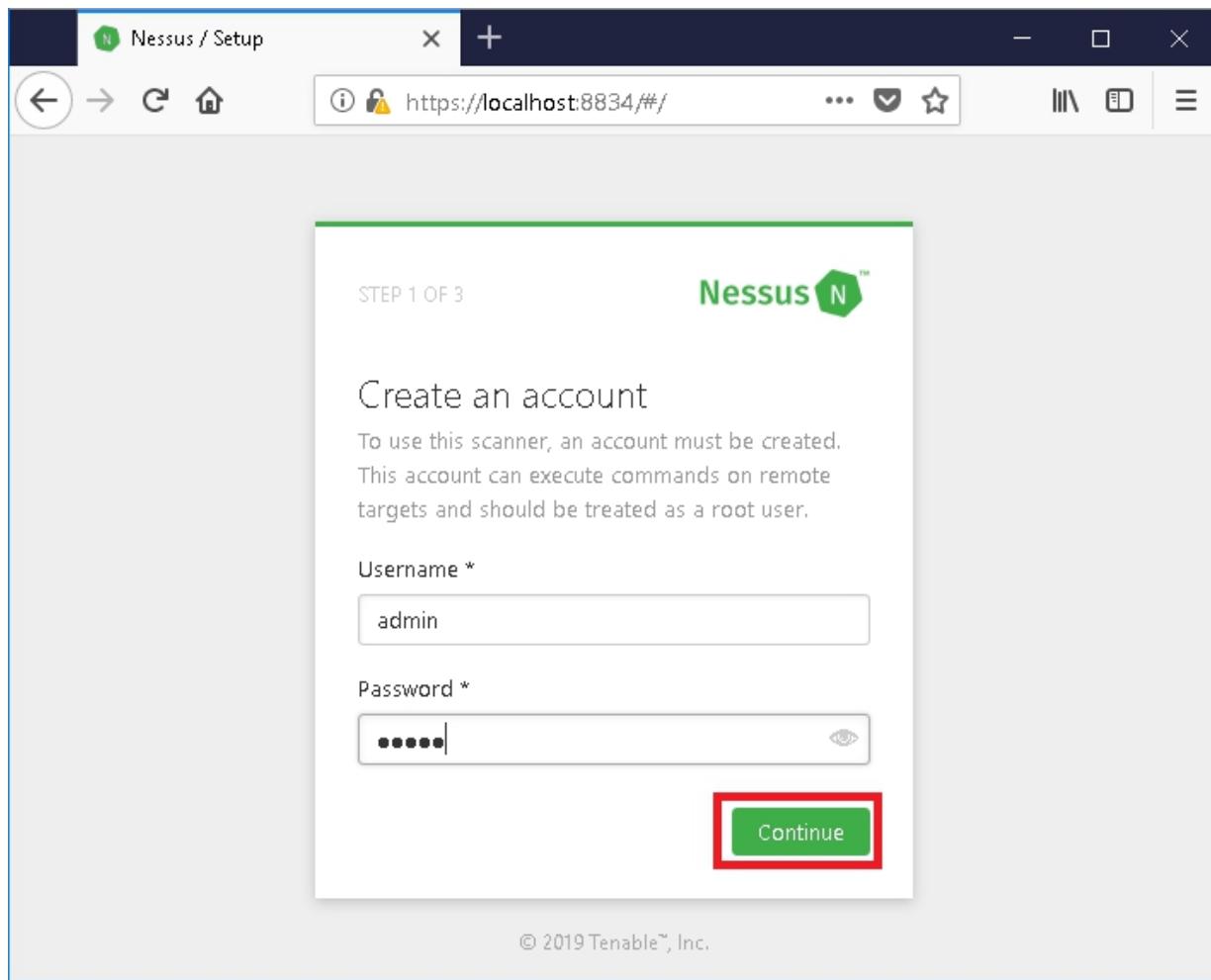


Click on the “Advanced” option.

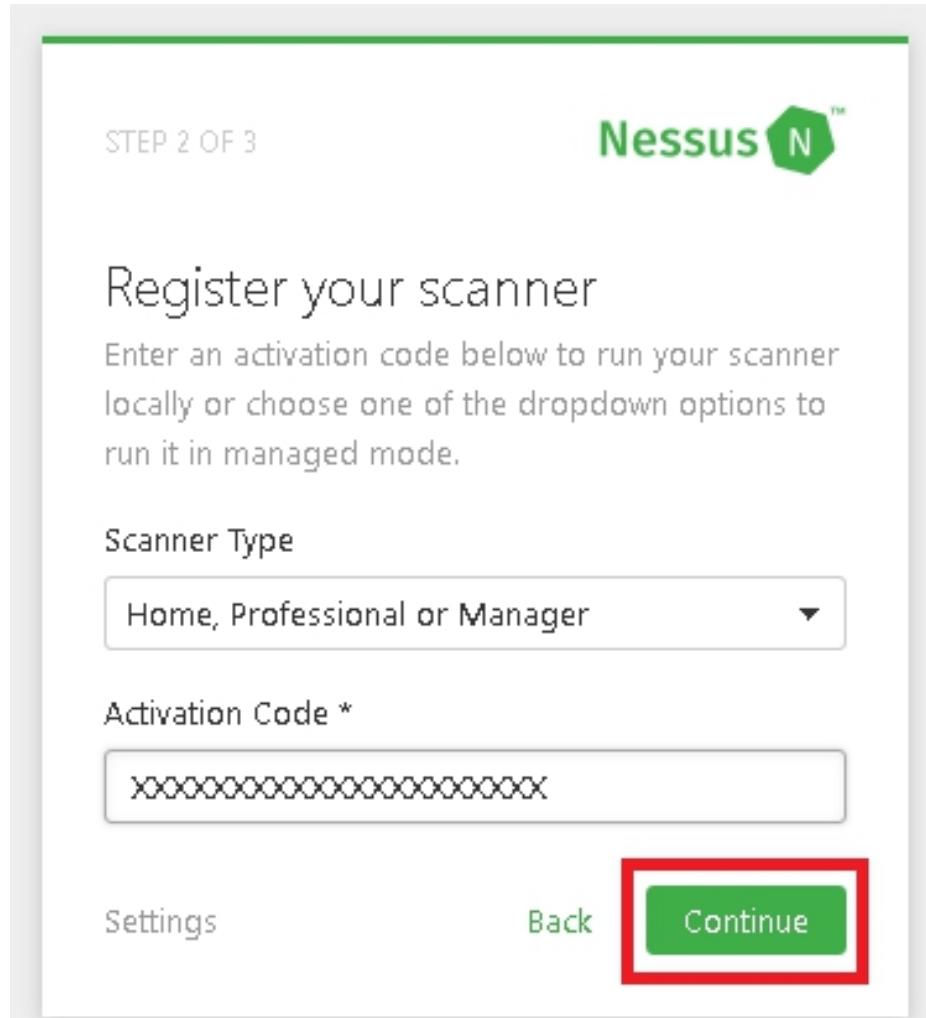
Now click on “Confirm Security Exception” to proceed to localhost.



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're going to use to log in to Nessus from now on. After inserting username and password, click the “Continue” button.

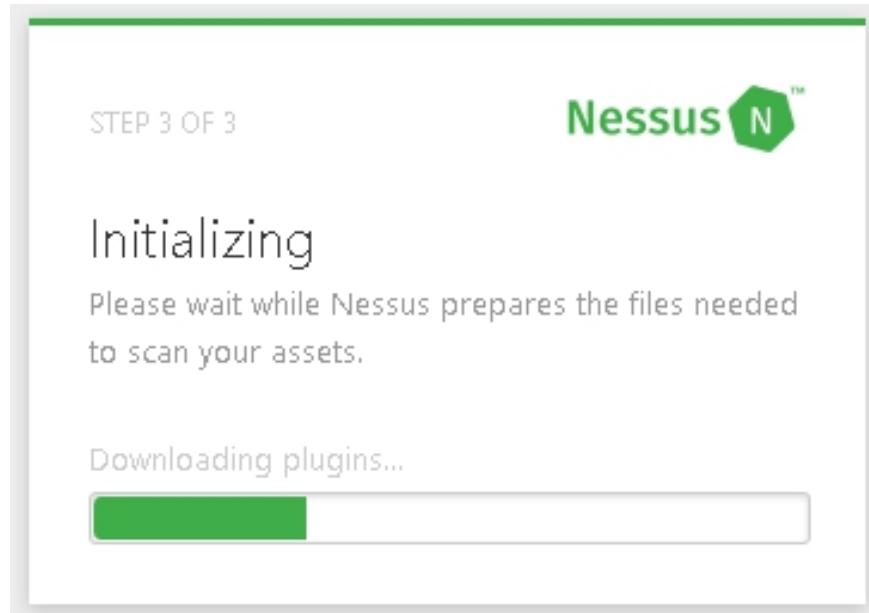


Now choose the scanner type that you want. Here, we have selected the first one which is “Home, Professional or Manager”.



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.

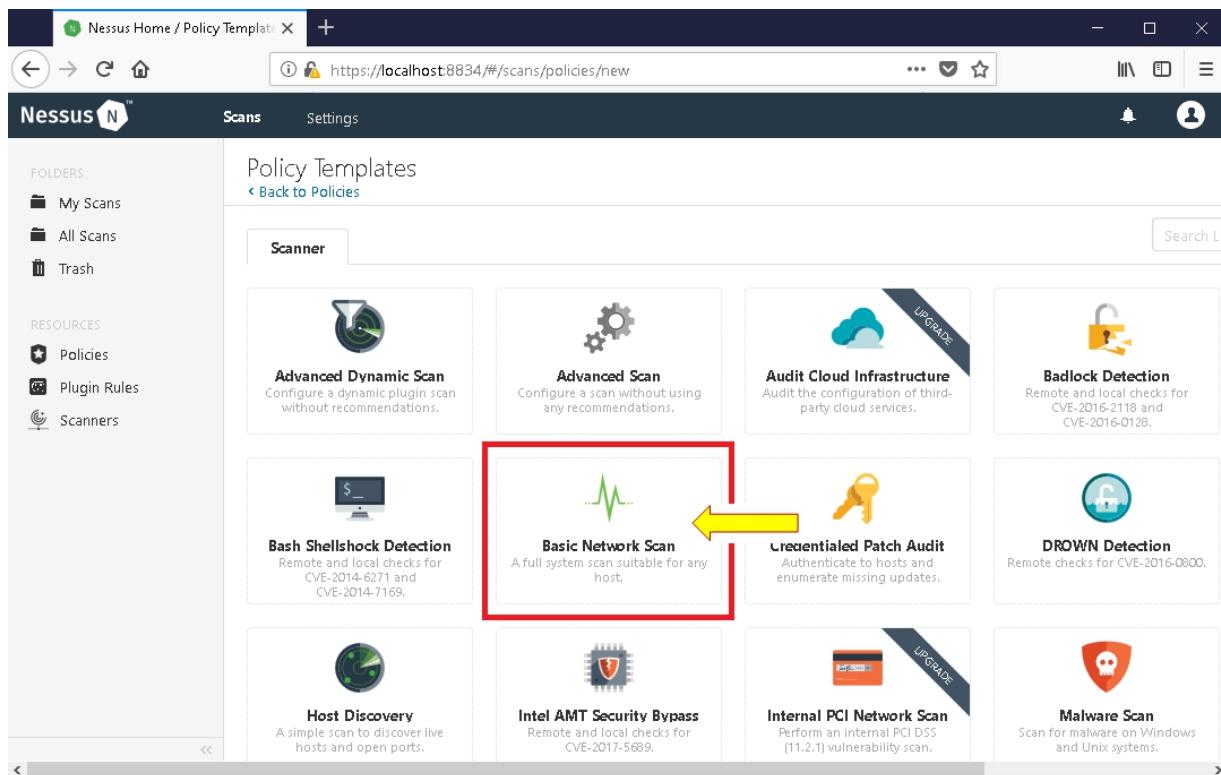


Once all the plugins are installed, this window will appear and this is what Nessus looks like. Now, the first thing you have to do is create a policy. Click on “Policies”.

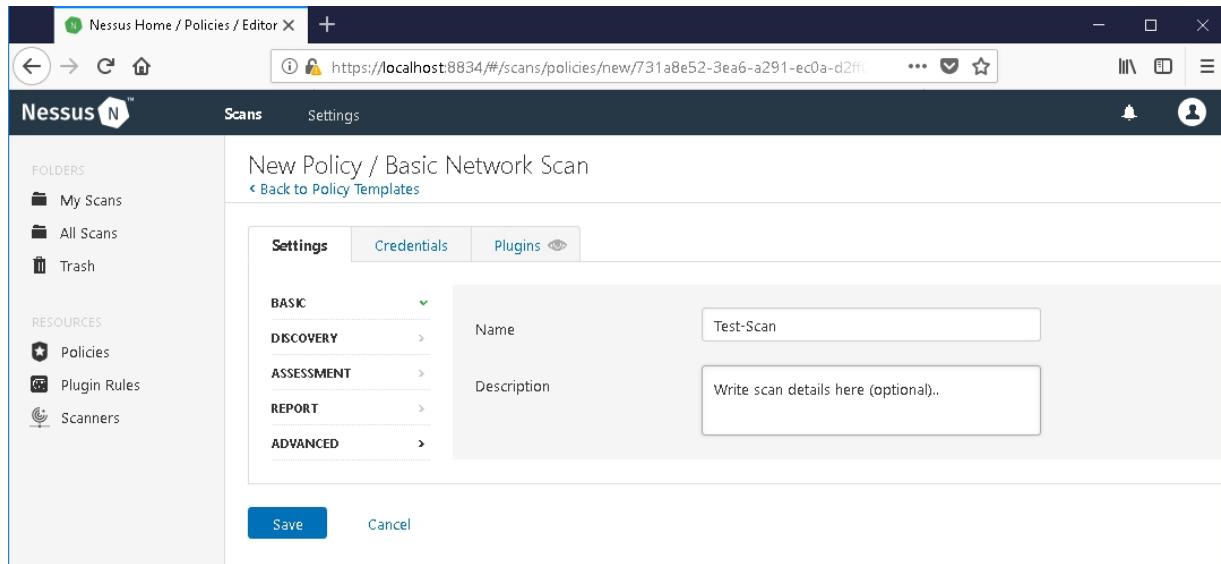
Now click on “Create a new policy”.

The screenshot shows the Nessus web interface. The top navigation bar includes a back/forward button, refresh, search, and a URL bar showing <https://localhost:8834/#/scans/policies>. Below the bar are tabs for 'Scans' and 'Settings'. The main content area is titled 'Policies'. It features a large icon of a shield with a star and text explaining what policies are. A message at the bottom states 'No policies have been created' and includes a blue 'Create a new policy' button. On the left, a sidebar under 'RESOURCES' has three items: 'Policies' (which is highlighted with a red box), 'Plugin Rules', and 'Scanners'. The 'Policies' item is also highlighted with a red box. A yellow arrow points from the text above to the 'Create a new policy' button.

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.

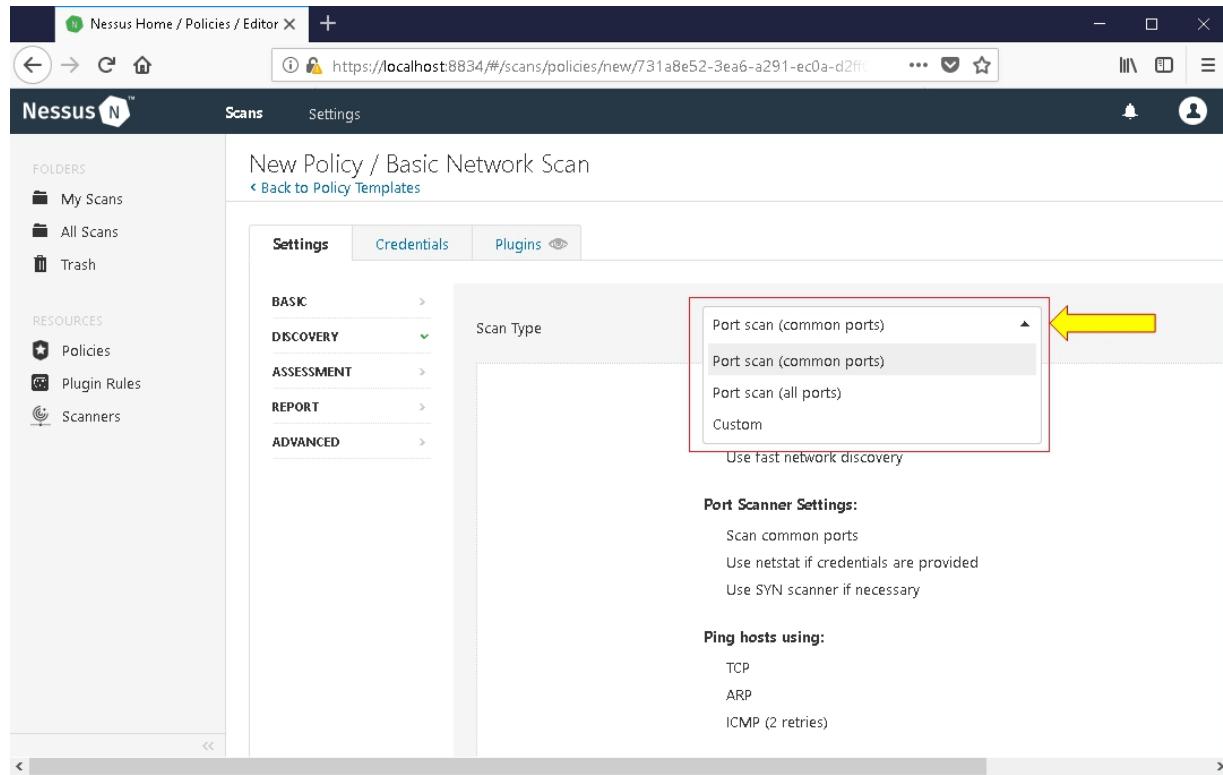


When you see this window, you have to name the policy. You may name it anything you want; for now, we are going to name it “Basic Scan”.



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.



The screenshot shows the Nessus web interface for creating a new policy. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Scanners), and navigation links (Scans, Settings). The main area is titled "New Policy / Basic Network Scan" and includes a "Back to Policy Templates" link. A horizontal tab bar at the top of the main area includes "Settings" (selected), "Credentials", and "Plugins". On the left, a vertical navigation menu lists "BASIC", "DISCOVERY" (selected), "ASSESSMENT", "REPORT", and "ADVANCED". The "DISCOVERY" section is expanded, showing "Scan Type" with four options: "Port scan (common ports)" (selected), "Port scan (common ports)", "Port scan (all ports)", and "Custom". Below this, under "Port Scanner Settings", are options for "Scan common ports", "Use netstat if credentials are provided", and "Use SYN scanner if necessary". Under "Ping hosts using:", the options are "TCP", "ARP", and "ICMP (2 retries)". A yellow arrow points to the "Port scan (common ports)" option in the dropdown menu.

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”.

The screenshot shows the Nessus web interface for creating a new policy. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Scanners). The main area is titled "New Policy / Basic Network Scan" and includes tabs for Settings, Credentials, and Plugins. Under Settings, there's a "Scan Type" dropdown menu with the following options:

- Default
- Default
- Scan for known web vulnerabilities
- Scan for all web vulnerabilities (quick)
- Scan for all web vulnerabilities (complex)
- Custom

A yellow arrow points to the "Default" option in the dropdown menu. At the bottom of the screen are "Save" and "Cancel" buttons.

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

The screenshot shows the Nessus web interface for creating a new policy. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Scanners). The main area title is "New Policy / Basic Network Scan" with a "Back to Policy Templates" link. A navigation bar at the top includes back, forward, search, and home icons, along with the URL "https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd7". The central content area has tabs for "Settings" (selected), "Credentials", and "Plugins". The "Settings" tab contains several sections: "Processing" (checkboxes for override verbosity, disk space limit, information level, superseded patches, and hiding dependency results); "Output" (checkboxes for allowing users to edit results, designating hosts by DNS name, displaying pingable hosts, and displaying unreachable hosts); and "Advanced" (which is currently expanded). The "Advanced" section includes options for "Discovery", "Assessment", and "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.

Nessus Home / Policies / Editor X

https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65

Nessus

Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

Settings Credentials Plugins

CATEGORIES Host

Filter Credentials

SSH Windows

Windows

Authentication method Password

Username administrator REQUIRED

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

On behalf of and import your credentials and authentication methods 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.

The screenshot shows the Nessus web interface. At the top, there is a navigation bar with a back arrow, forward arrow, a refresh icon, and a home icon. The URL is https://localhost:8834/#/scans/folders/my-scans. Below the navigation is a header with the Nessus logo, a 'Scans' button, a 'Settings' button, a notification bell, and a user account for 'admin'. On the left, there is a sidebar with sections for 'FOLDERS' and 'RESOURCES'. Under 'FOLDERS', 'My Scans' is selected and highlighted with a green bar. Under 'RESOURCES', there are links for 'Policies', 'Plugin Rules', and 'Scanners'. The main content area is titled 'My Scans' and contains a message 'This folder is empty'. A blue button labeled 'New Scan' is visible. A yellow arrow points from the text 'Create a new scan.' in the message box towards the 'New Scan' button.

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.

## New Scan / Test-Scan

[◀ Back to Scan Templates](#)

**Settings**

**BASIC**

General

Schedule

Notifications

Name: Test-Scan

Description: Scan description

Folder: My Scans

Targets: 192.168.100.1-192.168.100.254

Upload Targets      Add File

**Save** ▾      Cancel

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

## New Scan / Test-Scan

[◀ Back to Scan Templates](#)

**Settings**

**BASIC**

- [General](#)
- [Schedule](#)
- [Notifications](#)

Enabled

Frequency

Starts

Timezone

Summary

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

Nessus Home / Scans / Editor

[\(i\) https://localhost:8834/#/scans/reports/new/ab4bacd2-05f6-425c-9d79-3ba3940ad1c24e51e1f403febe](#)

**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](#)

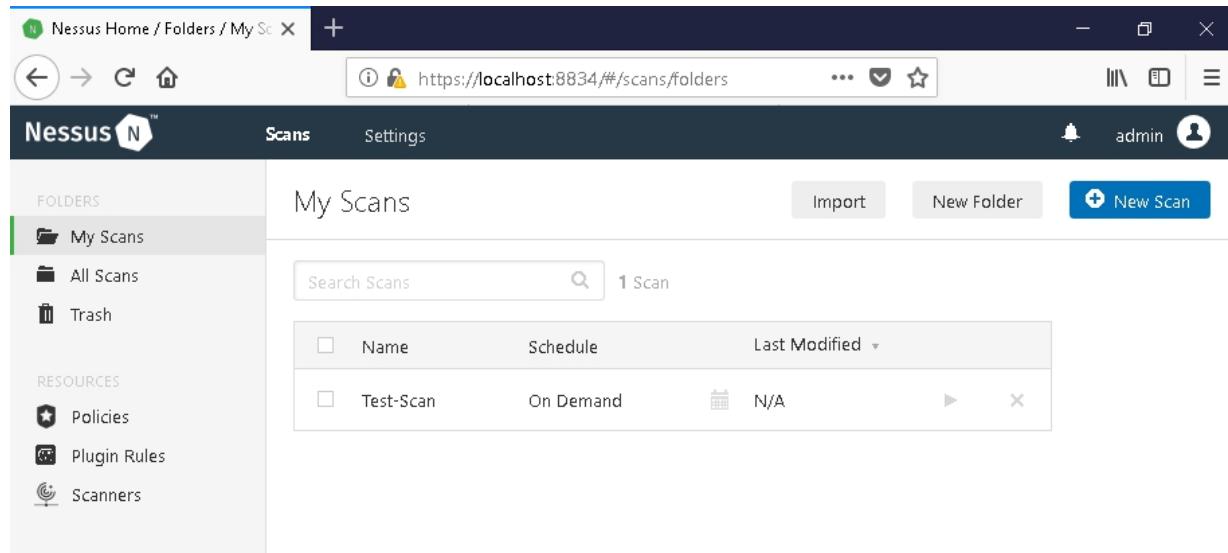
**Notifications**

Notifications will not be sent until your [SMTP Server](#) is configured.

Email Recipient(s)

Result Filters

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.



The screenshot shows the Nessus web interface. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Scanners). The main area is titled 'My Scans' and shows a table with one row:

<input type="checkbox"/>	Name	Schedule	Last Modified
<input type="checkbox"/>	Test-Scan	On Demand	N/A

Buttons at the top right include 'Import', 'New Folder', and 'New Scan'.

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.

# Test-Scan

[Back to My Scans](#)

Configure

Audit Trail

Launch ▾

Export ▾

Hosts

7

Vulnerabilities

47

History

1

Filter ▾

Search Hosts



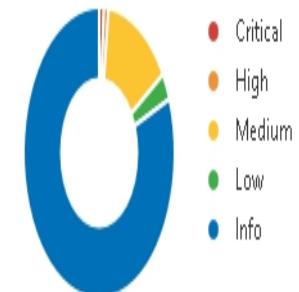
7 Hosts

Host	Vulnerabilities
192.168.100.1	<div><div style="width: 7%;">Critical</div><div style="width: 2%;">High</div><div style="width: 51%;">Medium</div><div style="width: 2%;">Low</div><div style="width: 44%;">Info</div></div> 7 2 54
192.168.100.22	<div><div style="width: 4%;">Critical</div><div style="width: 5%;">High</div><div style="width: 41%;">Medium</div><div style="width: 2%;">Low</div><div style="width: 49%;">Info</div></div> 4 55
192.168.100.5	<div><div style="width: 1%;">Critical</div><div style="width: 4%;">High</div><div style="width: 55%;">Medium</div><div style="width: 2%;">Low</div><div style="width: 36%;">Info</div></div> 30
192.168.100.33	<div><div style="width: 13%;">Critical</div><div style="width: 87%;">Info</div></div> 13
192.168.100.9	<div><div style="width: 6%;">Critical</div><div style="width: 94%;">Info</div></div> 6
192.168.100.23	<div><div style="width: 4%;">Critical</div><div style="width: 96%;">Info</div></div> 4
192.168.100.14	<div><div style="width: 4%;">Critical</div><div style="width: 96%;">Info</div></div> 4

## 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



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

[Scans](#)[Settings](#)

## Test-Scan

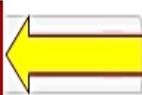
[← Back to My Scans](#)[Configure](#)

Hosts

7

Vulnerabilities

47



Filter ▾

Search Vulnerabilities



47 Vulnerabilities

<input type="checkbox"/> Sev ▾	Name ▾	Family ▾	Count ▾	
<input type="checkbox"/> <span style="background-color: red; border: 1px solid black; padding: 2px;">CRITICAL</span>	Dropbear SSH Server < 2016.72 Multi...	Misc.	1	
<input type="checkbox"/> <span style="background-color: orange; border: 1px solid black; padding: 2px;">HIGH</span>	SSL Version 2 and 3 Protocol Detection	Service detection	1	
<input type="checkbox"/> <span style="background-color: purple; border: 1px solid black; padding: 2px;">MIXED</span>	13 SSL (Multiple Issues)	General	17	
<input type="checkbox"/> <span style="background-color: purple; border: 1px solid black; padding: 2px;">MIXED</span>	3 DNS (Multiple Issues)	DNS	4	
<input type="checkbox"/> <span style="background-color: orange; border: 1px solid black; padding: 2px;">MEDIUM</span>	SMB Signing not required	Misc.	2	
<input type="checkbox"/> <span style="background-color: orange; border: 1px solid black; padding: 2px;">MEDIUM</span>	IP Forwarding Enabled	Firewalls	1	
<input type="checkbox"/> <span style="background-color: orange; border: 1px solid black; padding: 2px;">MEDIUM</span>	Unencrypted Telnet Server	Misc.	1	
<input type="checkbox"/> <span style="background-color: green; border: 1px solid black; padding: 2px;">LOW</span>	DHCP Server Detection	Service detection	1	
<input type="checkbox"/> <span style="background-color: blue; border: 1px solid black; padding: 2px;">INFO</span>	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

Plugin Details

## 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

Here are some other vulnerabilities that were found.

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/JU: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

## Test-Scan / Plugin #20007

[« Back to Vulnerabilities](#)

Configure

Audit Trail

Launch ▾

Export ▾

Hosts 7

Vulnerabilities 47

History 1

HIGH

### SSL Version 2 and 3 Protocol Detection



#### Plugin Details



#### Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Severity: High

ID: 20007

Version: 1.31

Type: remote

Family: Service detection

Published: October 12, 2005

Modified: January 8, 2019

#### Risk Information

Risk Factor: High

CVSS v3.0 Base Score 7.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N

/U:N/S:U/C:H/I:N/A:N

CVSS Base Score: 7.1

CVSS Vector: CVSS:2#AV:N/AC:M/Au:N/C:C/I:N/A:N

#### Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

#### Vulnerability Information

## 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`

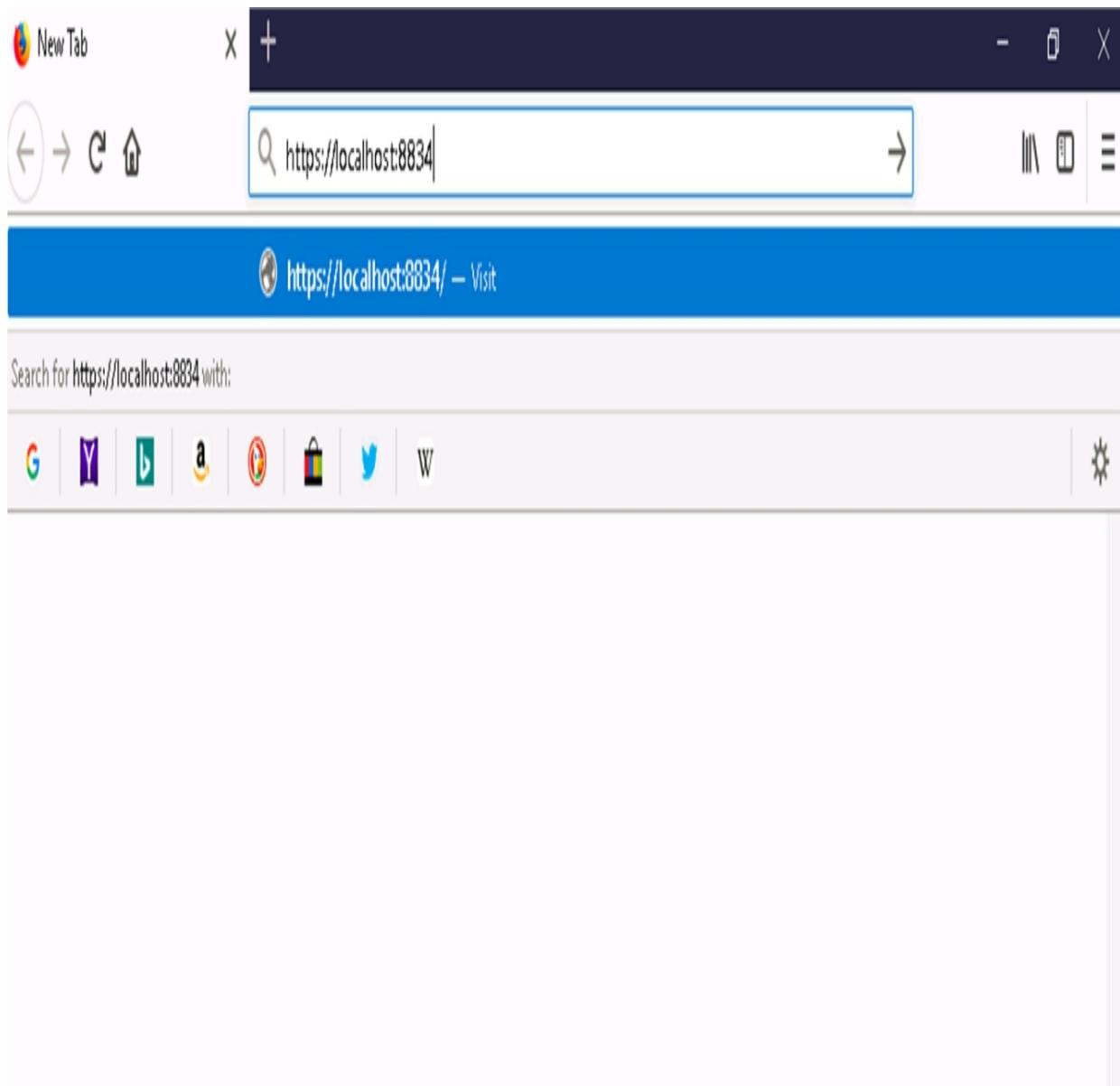
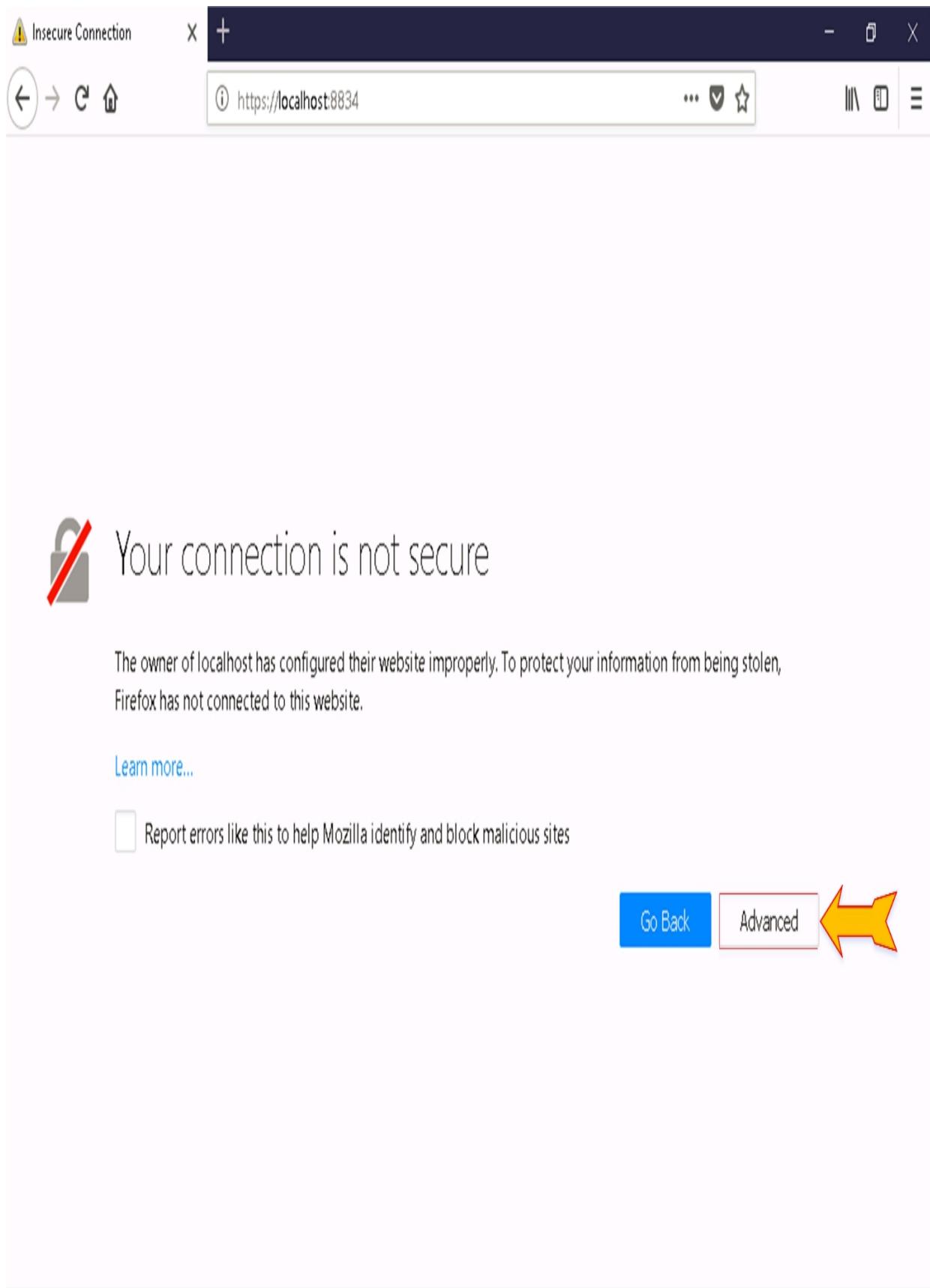


Figure 5–08: <https://localhost:8834>

4. Click on the “Advanced” button.



*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 X +

← → C ⌂

https://localhost:8834

Your connection is not secure

Add Security Exception X

The owner of local Firefox has not configured this site.

You are about to override how Firefox identifies this site.  
Legitimate banks, stores, and other public sites will not ask you to do this.

Learn more...

Report errors

Server

Location: https://localhost:8834/ Get Certificate

Certificate Status

This site attempts to identify itself with invalid information. View...

Advanced

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.

localhost:8834

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

The server is not identified by a certificate that is trusted by your operating system.

An additional security check is required to proceed.

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

Error code:

Permanently store this exception

Confirm Security Exception Cancel

Add Exception...

*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.

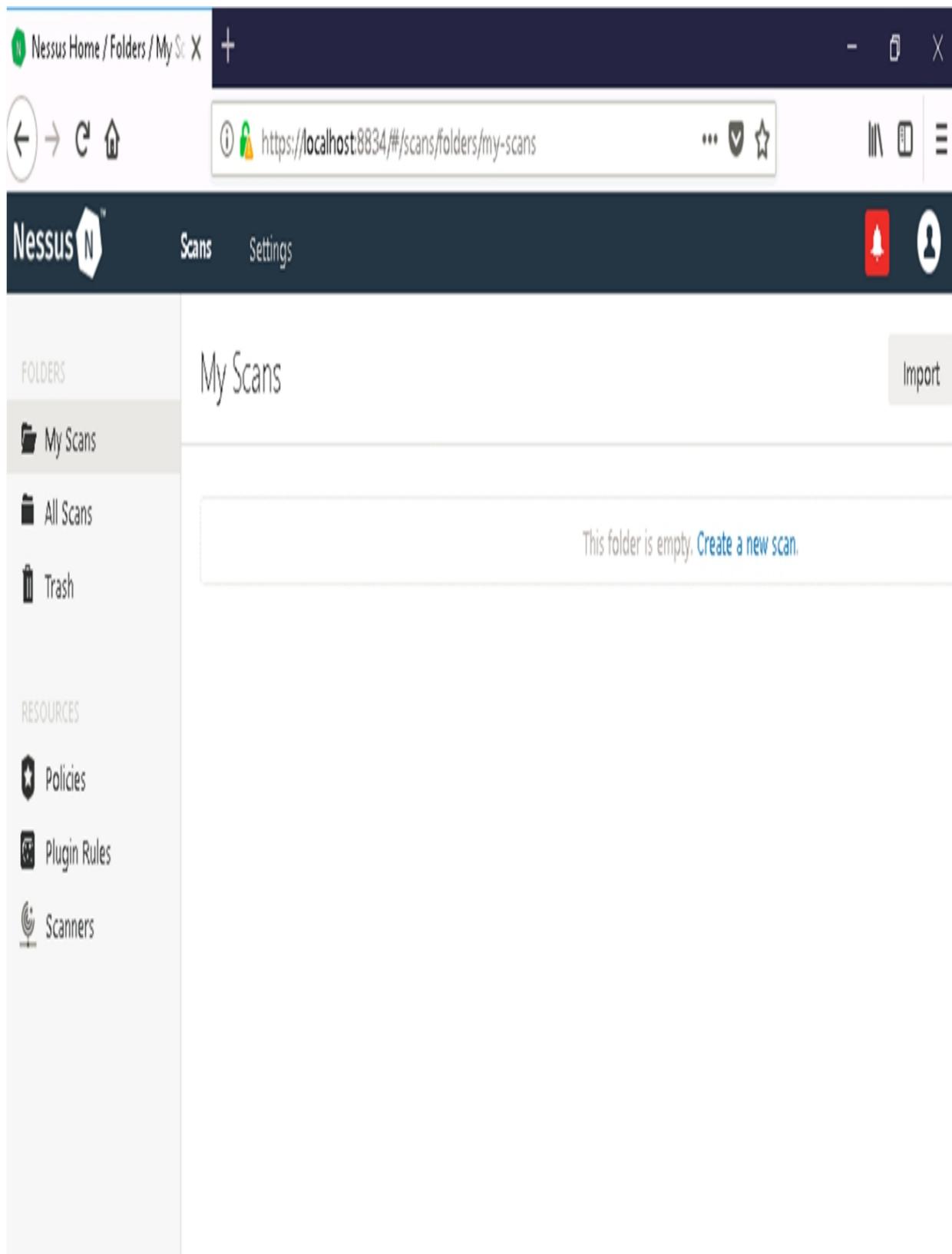


Figure 5–13: Nessus Dashboard

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

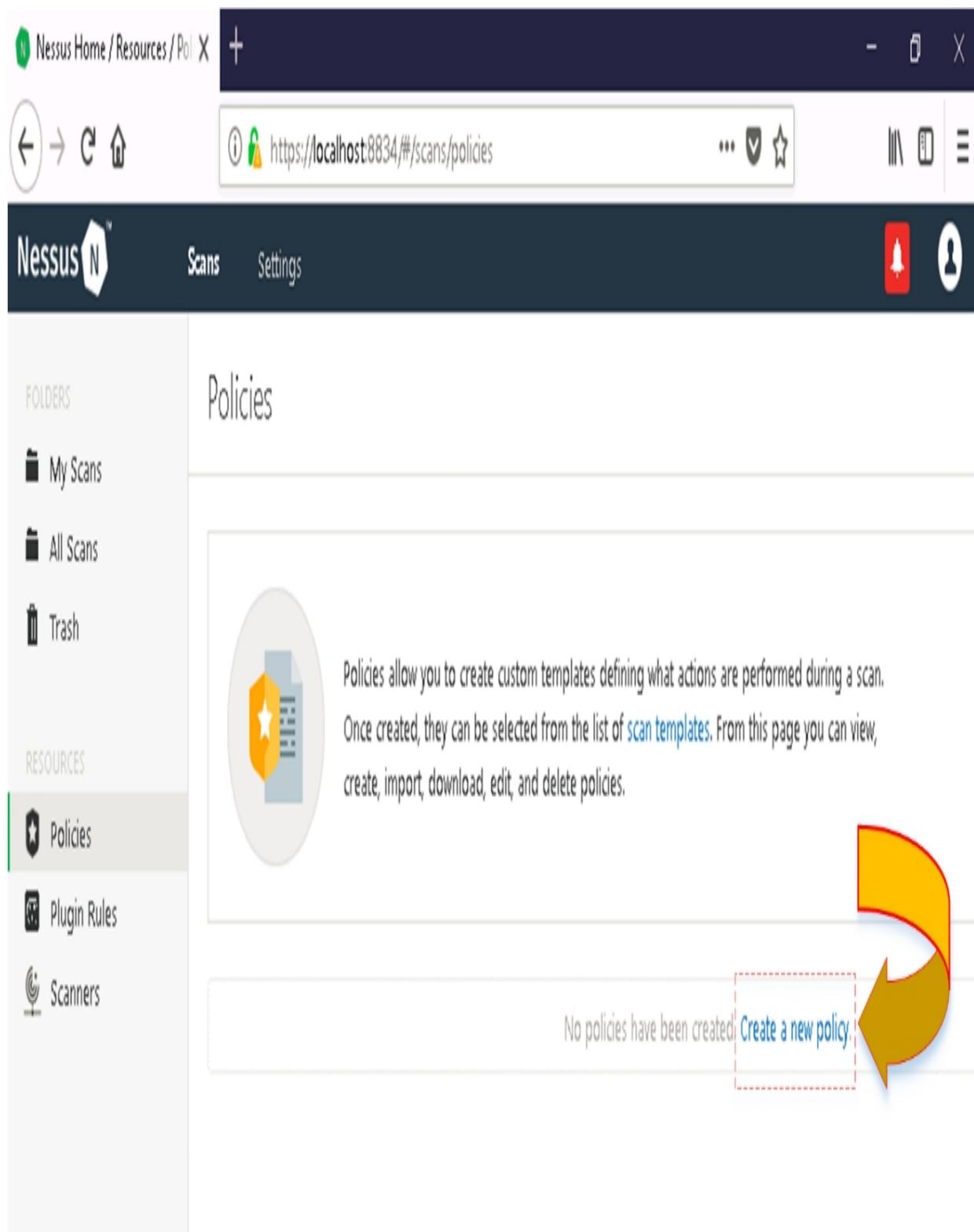


Figure 5–14: Create New Policy

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

Nessus Home / Policies / Editor X

https://localhost:8834/#/scans/policies/new/ad629e16-03b6-4f3d-83c3-0a2a2a2a2a2a

90% ⚡ ⚡ ⚡

Nessus Scans Settings

New Policy / Advanced Scan

Back to Policy Templates

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

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 X

https://localhost:8834/#/scans/policies/4/config/settings/discovery

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)

Save Cancel

The screenshot shows the Nessus Home / Policies / Editor interface. The main title bar says "Nessus Home / Policies / Editor X". The address bar shows the URL "https://localhost:8834/#/scans/policies/4/config/settings/discovery". The top navigation bar has tabs for "Scans" and "Settings", with "Settings" currently active. On the left, there's a sidebar with sections for "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Scanners). The main content area is titled "Test\_Scan / Configuration" and has a link to "Back to Policies". Below the title, there are four tabs: "Settings" (selected), "Credentials", "Compliance", and "Plugins". Under "Settings", there are several sections: "BASIC", "DISCOVERY" (with "Host Discovery" selected), "Port Scanning", "Service Discovery", "ASSESSMENT", "REPORT", and "ADVANCED". In the "DISCOVERY" section, there's a "Remote Host Ping" section with a checkbox labeled "Ping the remote host" which is checked and set to "off". There's also a "Fragile Devices" section with two unchecked checkboxes: "Scan Network Printers" and "Scan Novell Netware hosts". In the "ADVANCED" section, there's a "Wake-on-LAN" section with a "List of MAC addresses" field and an "Add File" button, and a "Boot time wait (in minutes)" field containing the value "5". At the bottom of the configuration screen are "Save" and "Cancel" buttons.

*Figure 5–16: Configuring Policy*

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

## 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 closedPort scan range: 

## 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****General Settings** Enable safe checks Stop scanning hosts that become unresponsive during the scan Scan IP addresses in a random order**DISCOVERY****ASSESSMENT****REPORT****ADVANCED****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

Settings Credentials Compliance Plugins

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

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

This screenshot shows the 'Credentials' tab in the Nessus web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Scanners). The main area has 'Categories' set to 'Host'. A 'Filter Credentials' search bar is present. Below it, three credential types are listed: 'SNMPv3', 'SSH', and 'Windows'. For the 'Windows' credential, the 'Authentication method' is set to 'Password', with 'Username' as 'admin' and 'Password' masked as '\*\*\*\*\*'. A 'Domain' field is also present. At the bottom, there's a section for 'Global Credential Settings' with four checkboxes: 'Never send credentials in the clear' (checked), 'Do not use NTLMv1 authentication' (checked), 'Start the Remote Registry service during the scan' (unchecked), and 'Enable administrative shares during the scan' (unchecked). At the very bottom are 'Save' and 'Cancel' buttons.

*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 AI](#)[Settings](#)[Credentials](#)[Compliance](#)[Plugins](#)[Show Er](#)

STATUS	PLUGIN NAME	PI
ENABLED	3Proxy HTTP Proxy Crafted Transparent Requ...	31
ENABLED	602LAN SUITE Open Telnet Proxy	18
ENABLED	AnalogX Proxy SOCKS4a DNS Hostname Han...	11
ENABLED	Arkoon Appliance Detection	14
ENABLED	Axent Raptor Firewall Zero Length IP Remote ...	10
ENABLED	BenHur Firewall Source Port 20 ACL Restrictio...	11
ENABLED	Blue Coat ProxySG 4.x OpenSSL Security Bypass	7t
ENABLED	Blue Coat ProxySG 6.2.x < 6.2.16.4 / 6.5.x < 6.5...	8
ENABLED	Blue Coat ProxySG 6.2.x OpenSSL Security By...	7t
ENABLED	Blue Coat ProxySG 6.4.x OpenSSL Security By...	7t
ENABLED	Blue Coat ProxySG 6.5.x / 6.2.x / 5.5 OpenSSL ...	8t
ENABLED	Blue Coat ProxySG 6.5.x < 6.5.9.8 / 6.6.x < 6.6....	9t

[Save](#)[Cancel](#)

*Figure 5–21: Configuring Policy*

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

The screenshot shows the Nessus web interface with the title "Nessus N". The top navigation bar includes "Scans", "Settings", and user icons for notifications and profile. On the left, a sidebar lists "FOLDERS" with "My Scans", "All Scans", and "Trash"; "RESOURCES" with "Policies" (which is selected and highlighted in grey), "Plugin Rules", and "Scanners". The main content area is titled "Policies" and contains a large icon of a document with a star. A descriptive text block states: "Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of [scan templates](#). From this page you can view, create, import, download, edit, and delete policies." Below this is a search bar labeled "Search Policies" with a magnifying glass icon, showing "1 Policy". A table lists the single policy: "Test Scan" (Template: Advanced Scan, Last Modified: Today at 11:11 PM).

	Name	Template	Last Modified
<input type="checkbox"/>	Test Scan	Advanced Scan	Today at 11:11 PM

*Figure 5–22: Verify Policy*

18. Go to “Scan” > “Create New Scan” .

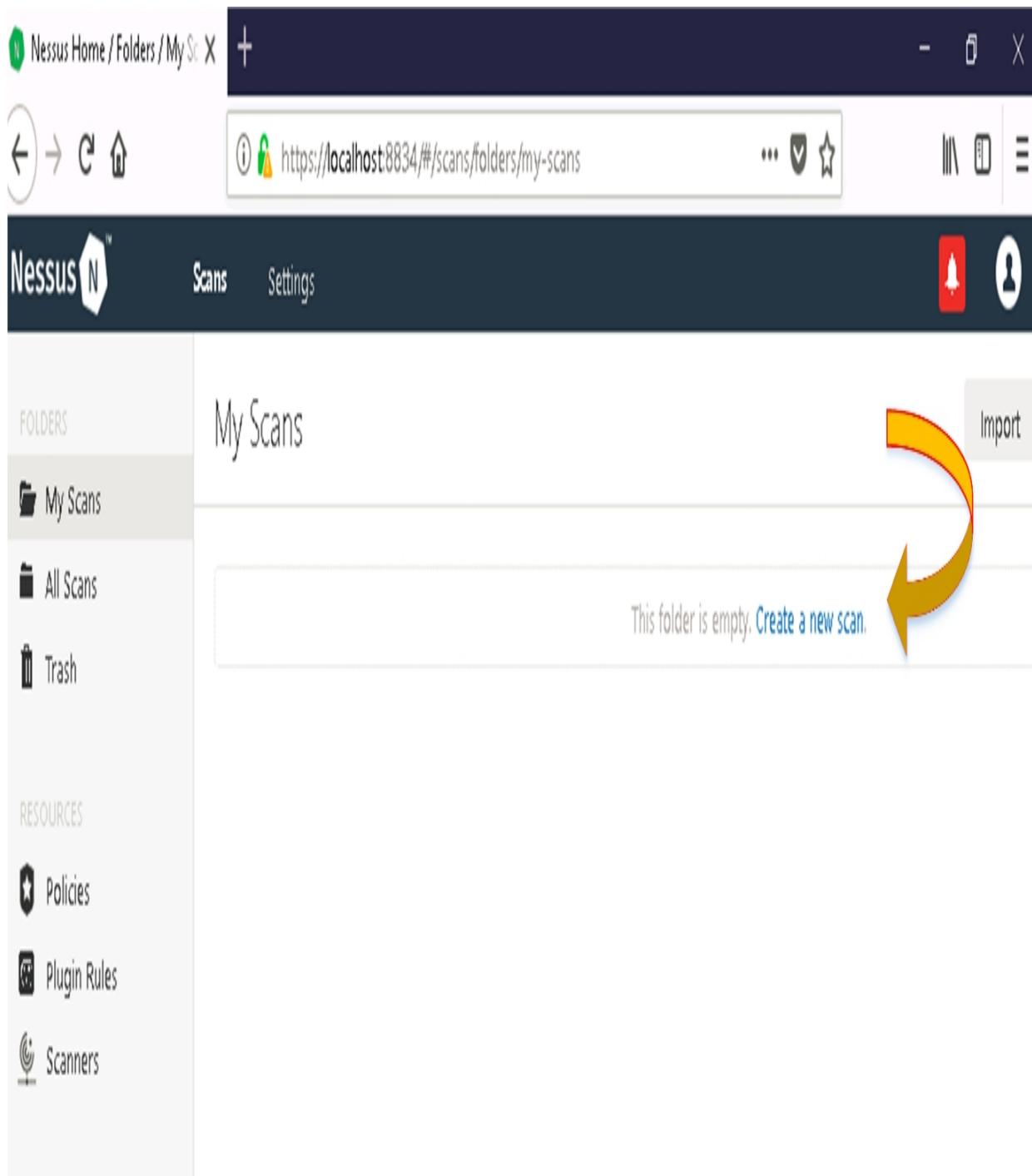


Figure 5–23: Configuring Scan

19. Enter the name for a new scan.

N Nessus Home / Scans / Editor X

← → C ⌂

https://localhost:8834/#/scans/reports/new/ab4bacd2-05 90% ⌂ ⌂ ⌂ ⌂

Nessus N 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

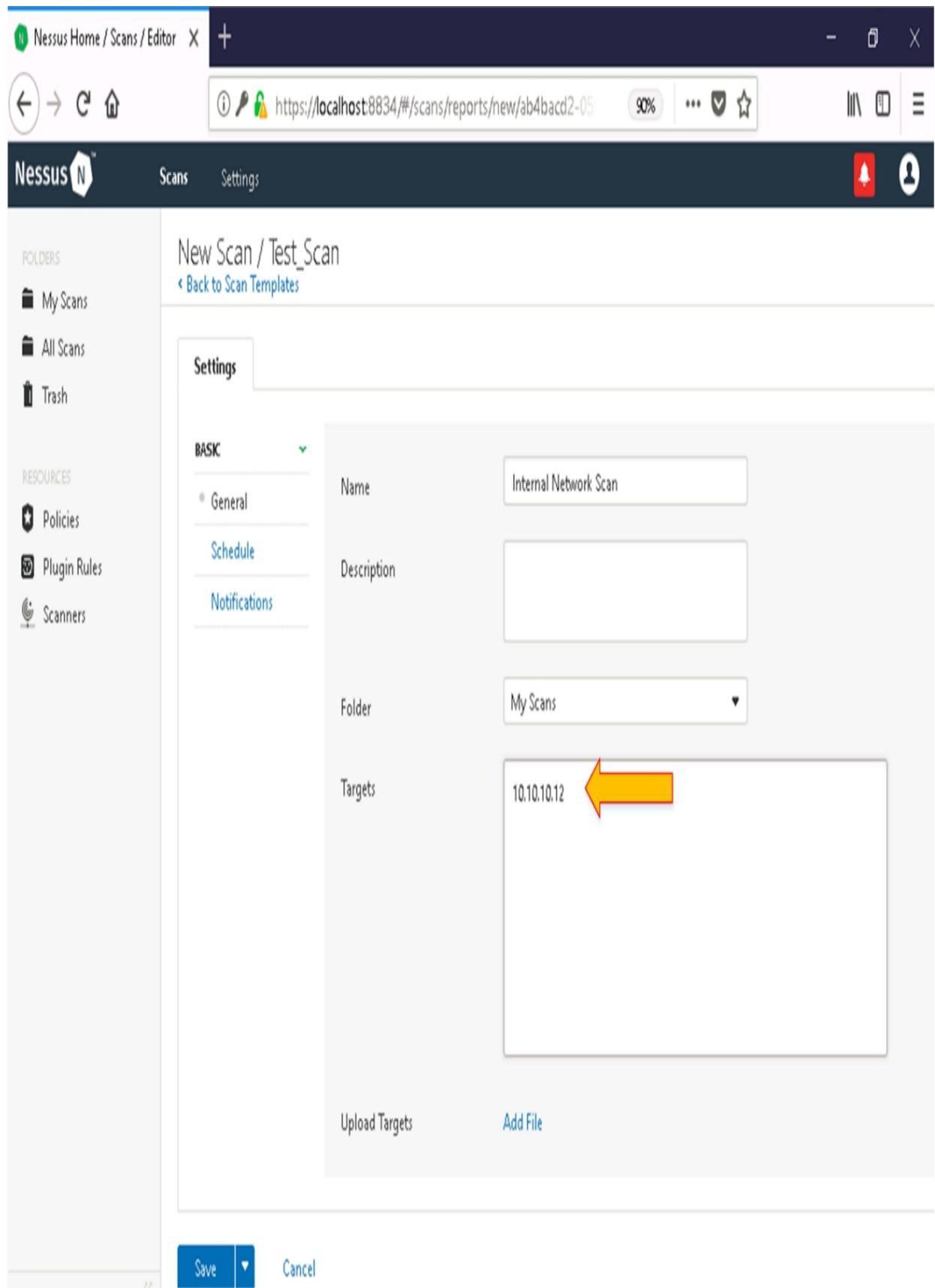
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Upload Targets Add File

Save Cancel

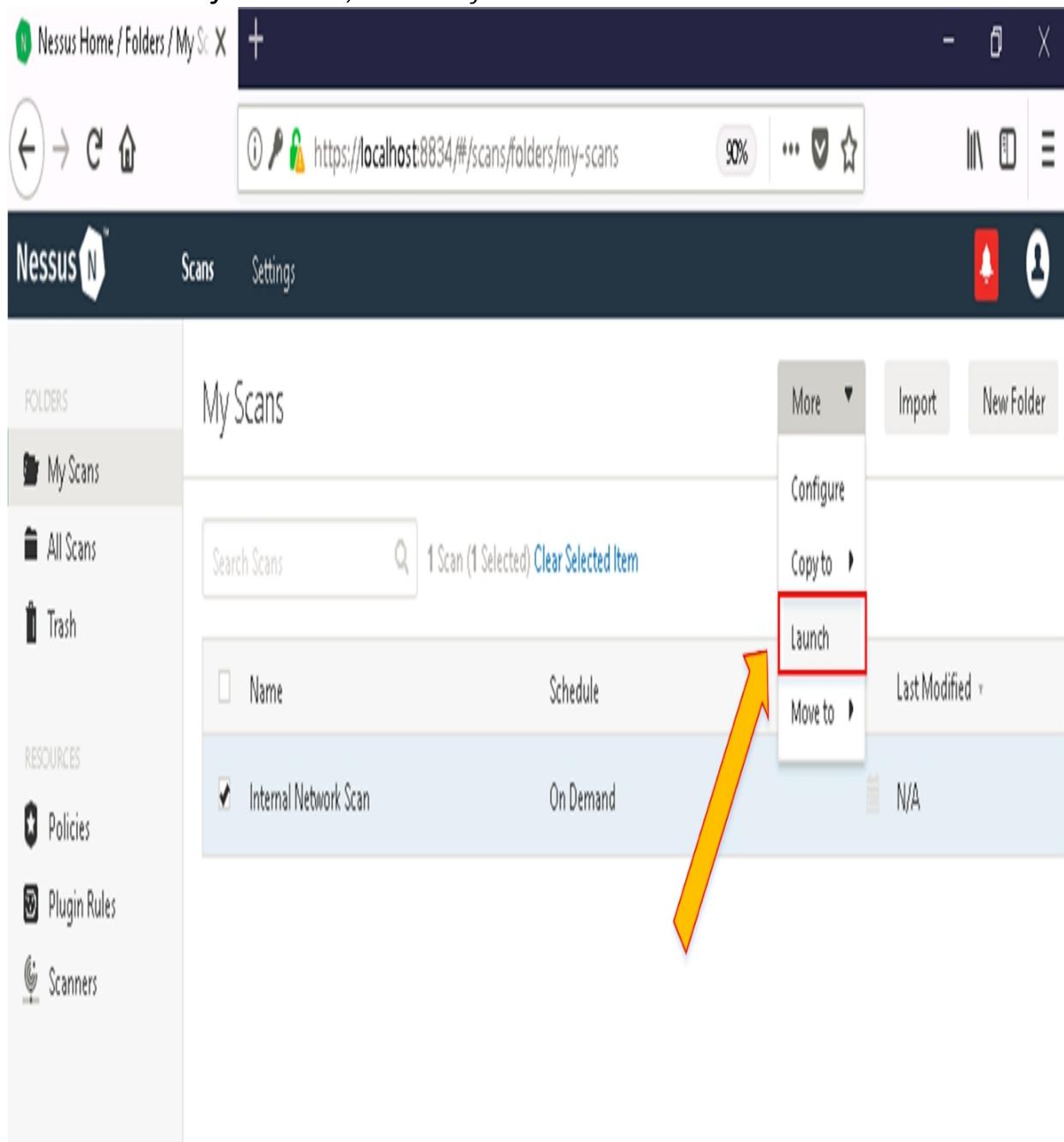
*Figure 5–24: Configuring Scan*

20. Enter target address.



*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 Critical   13 High   3 Medium   83 Low   0 Info

## Scan Details

Name: Internal Network Scan

Status: Completed

Policy: Test\_Scan

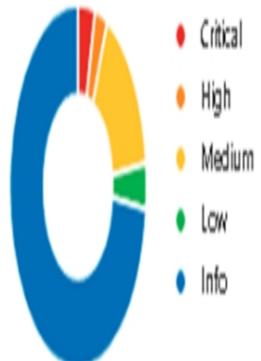
Scanner: Local Scanner

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.



*Figure 5–30: Scan Results*

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

Home Tools

Internal\_Network\_S...

?

Sign In



## Vulnerabilities

Total: 76

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unprivileged check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged 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) (unprivileged 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