Chapter 5: Vulnerability Analysis

Technology Brief

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

Vulnerability Assessment Concept:

This is a fundamental task for a penetration tester to discover the vulnerabilities in an environment. Vulnerability assessment includes discovering weaknesses in an environment, design flaws and other security concerns which can cause an operating system, application or website to be misused. These vulnerabilities include misconfigurations, default configurations, buffer overflows, Operating System flaws, Open Services, and others. There are different tools available for network administrators and Pentesters to scan for vulnerabilities in a network. Discovered vulnerabilities are classified into three different categories based on their security levels, i.e., low, medium or high. furthermore, they can also be categorized as exploit range such as local or remote.

Vulnerability Assessment

Vulnerability Assessment can be defined as a process of examination, discovery, and identification of system and applications security measures and weaknesses. Systems and applications are examined for security measures to identify the effectiveness of deployed security layer to withstand attacks and misuses. Vulnerability assessment also helps to recognize the vulnerabilities that could be exploited, need of additional security layers, and information's that can be revealed using scanners.

Types of Vulnerability Assessments

- ***Active Assessments:*** Active Assessment is the process of Vulnerability Assessment which includes actively sending requests to the live network and examining the responses. In short, it is the process of assessment which requires probing the target host.
- ***Passive Assessments:*** Passive Assessment is the process of Vulnerability Assessment which usually includes packet sniffing to discover vulnerabilities, running services, open ports and other information. However, it is the process of assessment without interfering the target host.

- ***External Assessment:*** Another type in which Vulnerability assessment can be categorized is an External assessment. It the process of assessment with hacking's perspective to find out vulnerabilities to exploit them from outside.

- ***Internal Assessment:*** This is another technique to find vulnerabilities. Internal assessment includes discovering vulnerabilities by scanning internal network and infrastructure.

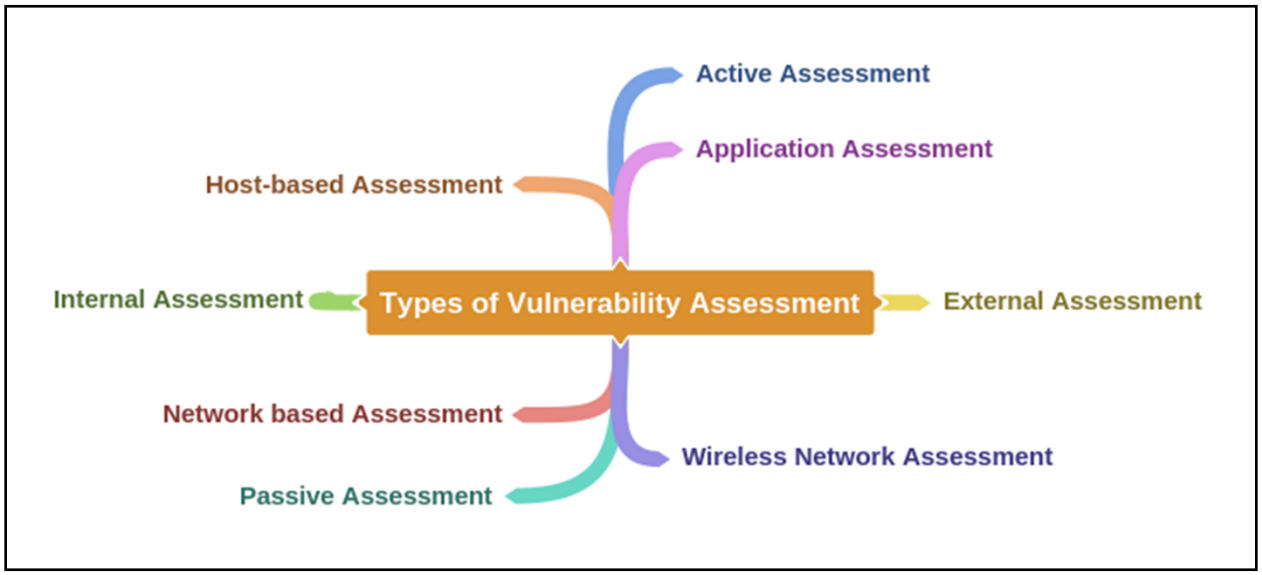

Figure 5-01 Types of Vulnerability Assessment

Vulnerability Assessment Life-Cycle

Vulnerability Assessment life cycle includes the following phases:

Creating Baseline

Creating Baseline is a pre-assessment phase of the vulnerability assessment life-cycle in which pentester or network administrator who is performing assessment identifies the nature of the corporate network, the applications, and services. He creates an inventory of all resources and assets which helps to manage, prioritize the assessment. furthermore, he also maps the infrastructure, learns about the security controls, policies, and standards followed by the organization. In the end, baseline helps to plan the process effectively, schedule the tasks, and manage them with respect to priority.

Vulnerability Assessment

Vulnerability Assessment phase is focused on assessment of the target. The assessment process includes examination and inspection of security measures such as physical security as well as 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 using assessment tools. Once scanning is complete, findings are ranked in terms of their priorities. At the end of this phase, vulnerability assessment report shows all detected vulnerabilities, their scope, and priorities.

Figure 5-02 Vulnerability Assessment Lifecycle

Risk Assessment

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

Remediation

Remediation phase includes remedial actions for these detected vulnerabilities. High priority vulnerabilities are addressed first because they can cause a huge impact.

Verification

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

Monitor

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

Vulnerability Assessment Solutions

Different approaches for Vulnerability Assessment

- ***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 for dedicated for internal (private) network.

Service-based solutions are third-party solutions which offers security and auditing to a network. These solutions can be host either inside or outside the network. As these solutions are allowed to the internal network, hence a security risk of being compromised.

- ***Tree-based Assessment Vs. Inference-based Assessment***

Tree-based assessment is the assessment approach in which auditor follows different strategies for each component of an environment. For example, consider a scenario of an organization's network where different machines are live, the auditor may use an approach for Windows-based machines whereas another technique for Linux based servers.

Inference-based assessment is another approach to assist depending on the inventory of protocols in an environment. For example, if an auditor found a protocol, using inference-based assessment approach, the auditor will investigate for ports and services related to that protocol.

Best Practice for Vulnerability Assessment

The following are some recommended steps for Vulnerability Assessment for 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. It will help to select appropriate tool to extract your desired information.
- Make sure about the assessment tool that it will not cause any sort of damage or unavailability of services running on a network.
- Make sure about the source location of scan to reduce the focus area.
- Run scan frequently for vulnerabilities.

Vulnerability Scoring Systems

Common Vulnerability Scoring Systems (CVSS)

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as 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 website https://www.first.org.

Common Vulnerabilities and Exposure (CVE)

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

U.S. National Vulnerability Database (NVD) was launched by National Institute of Standards and Technology (NIST), The CVE List feeds NVD, which then builds upon the information included in CVE Entries to provide enhanced information for each entry such as fix information, severity scores, and impact ratings. As part of its enhanced information, NVD also provides advanced searching features such as by OS; by vendor name, product name, and/or version number; and by vulnerability type, severity, related exploit range, and impact.

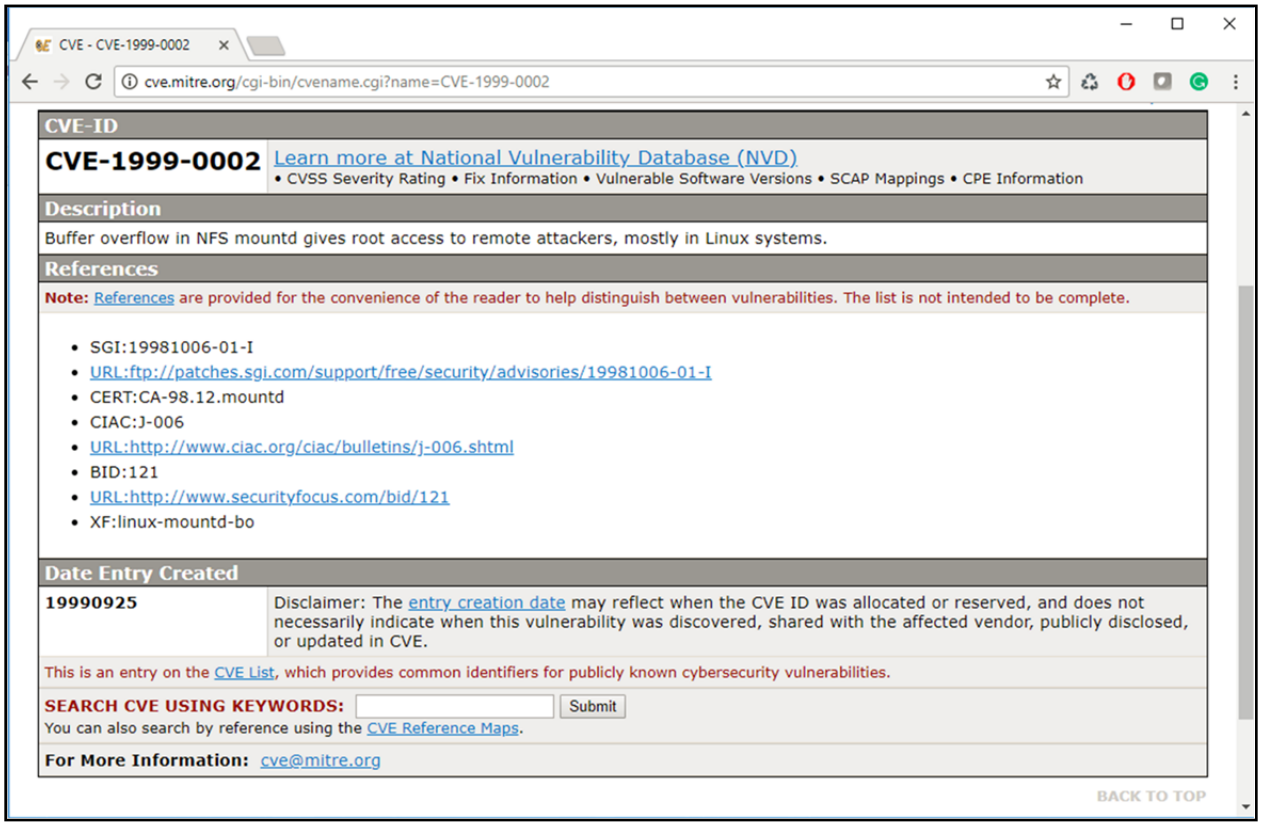

Figure 5-03 Common Vulnerability and Exposures (CVE)

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

Vulnerability Scanning

In this era of modern technology and advancement, finding vulnerabilities in an existing environment is becoming easy using different tools. Various tools, automated as well as manual tools, are available to help you in finding vulnerabilities. Vulnerability Scanners are automated utilities which are specially developed to detect vulnerabilities, weakness, problems, and holes 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, and many other tools.

These tools not only inspect running software and application to find risk and vulnerabilities by Security experts but also by the attackers to find out loopholes in an organization's operating environment.

Vulnerability Scanning Tool

1. GFI LanGuard

GFI LanGuard is a network security and 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

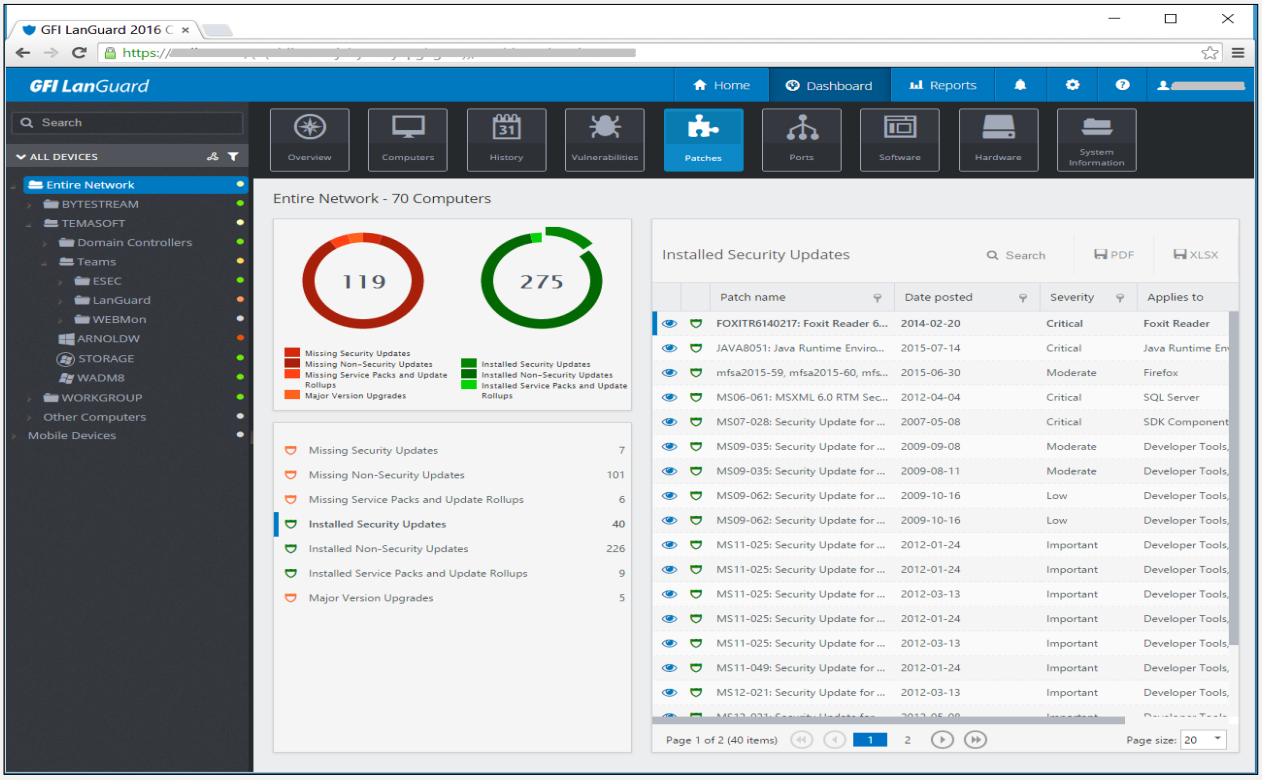

Figure 5-04 GFI Lan Guard Vulnerability Scanning Tool

2. Nessus

Nessus Professional Vulnerability Scanner is a most comprehensive vulnerability scanner software powered by Tenable Network Security. This Scanning Product focuses on

vulnerabilities and configuration assessment. Using this tool, you can customize and schedule scans and extract reports.

3. Qualys FreeScan

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

- Network Vulnerability scan for Server and App
- Patch
- OWA SP Web Application Audit
- SCAP Compliance Audit

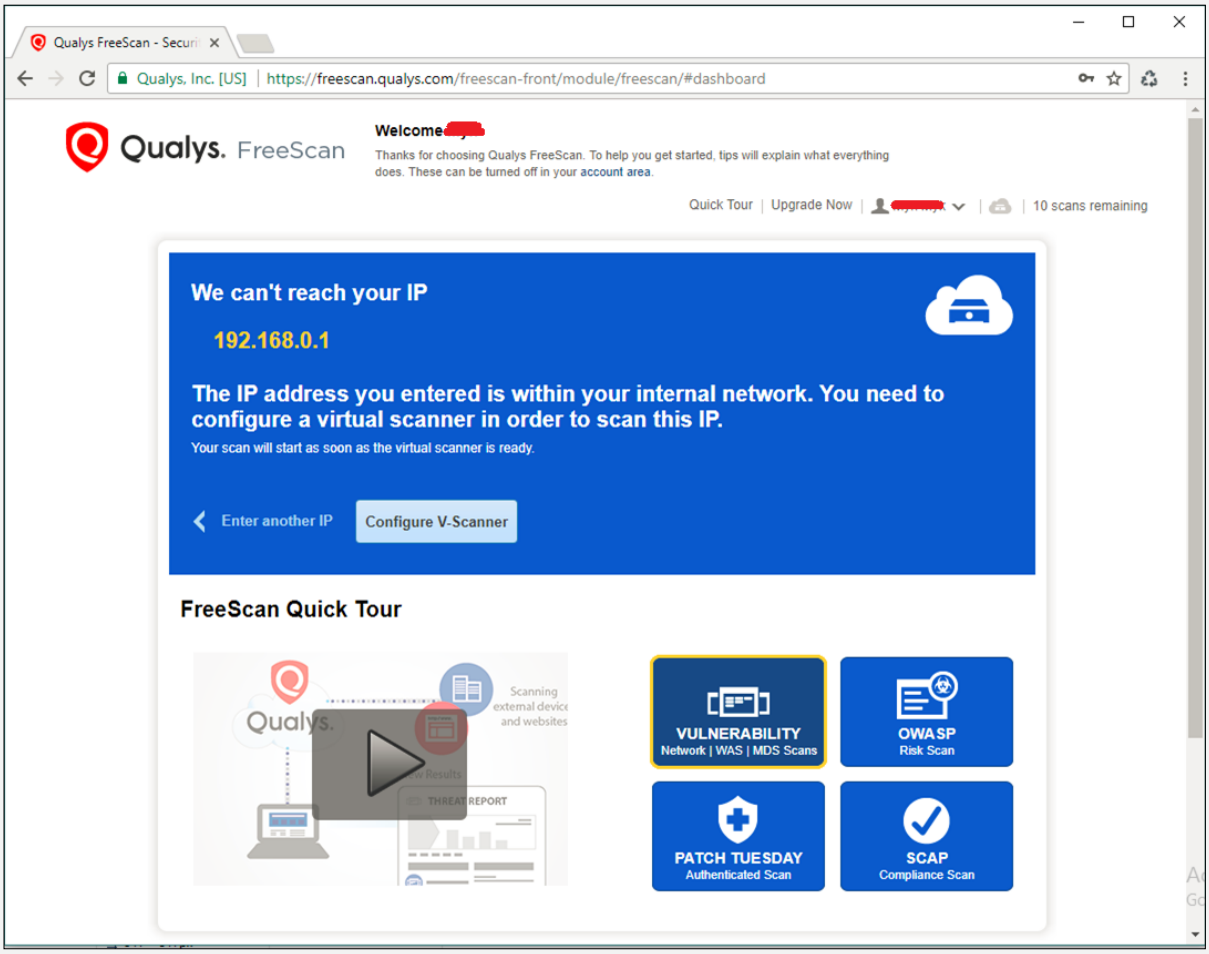

Figure 5-05 Qualys FreeScan Vulnerability Scanning Tool

Go to http://www.qualys.com to purchase the Vulnerability scanning tool or register for the trial version and try to scan. To Scan Local Network, Qualys offers Virtual Scanner which can be virtualized on any Virtualization hosting environment. The following figure is showing the result of Vulnerability scan for a targeted network.

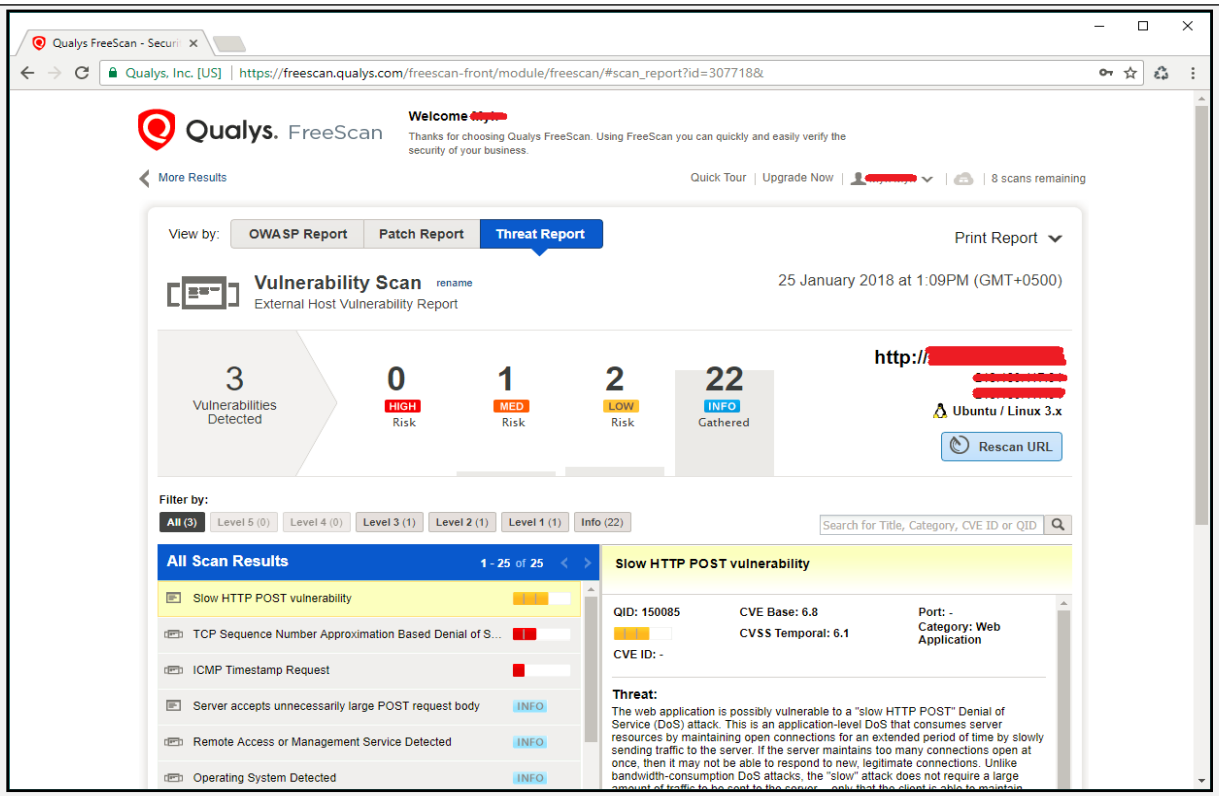

Figure 5-06 Qualys FreeScan Vulnerability Scanning Tool

Vulnerability Scanning Tools for Mobile

List of Vulnerability Scanning tools for Mobile are as follows: -

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 Mobile

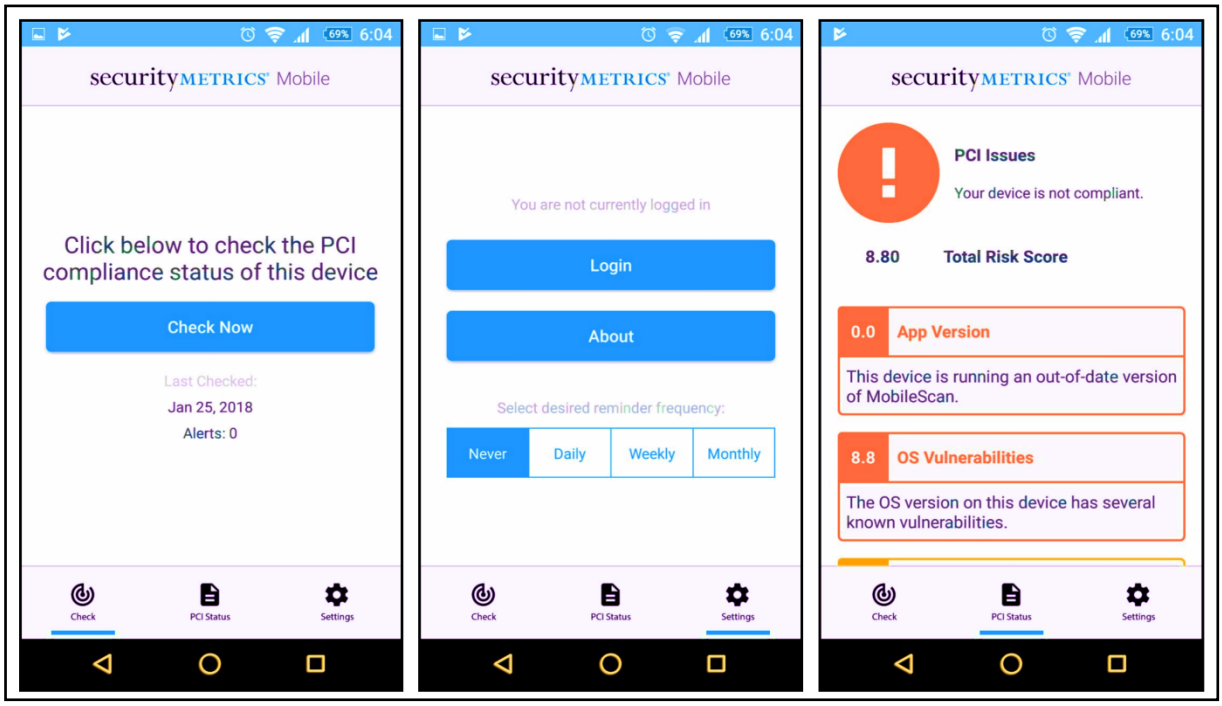

Figure 5-07 Security Metrics Mobile Scan

Lab 5.1: Vulnerability Scanning using 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 vulnerability scanning tool. This lab is performed on Windows 10 virtual machine using Nessus vulnerability scanning tool. You can download this tool from Tenable's website https://www.tenable.com/products/nessus/nessus-professional.

Configuration:

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

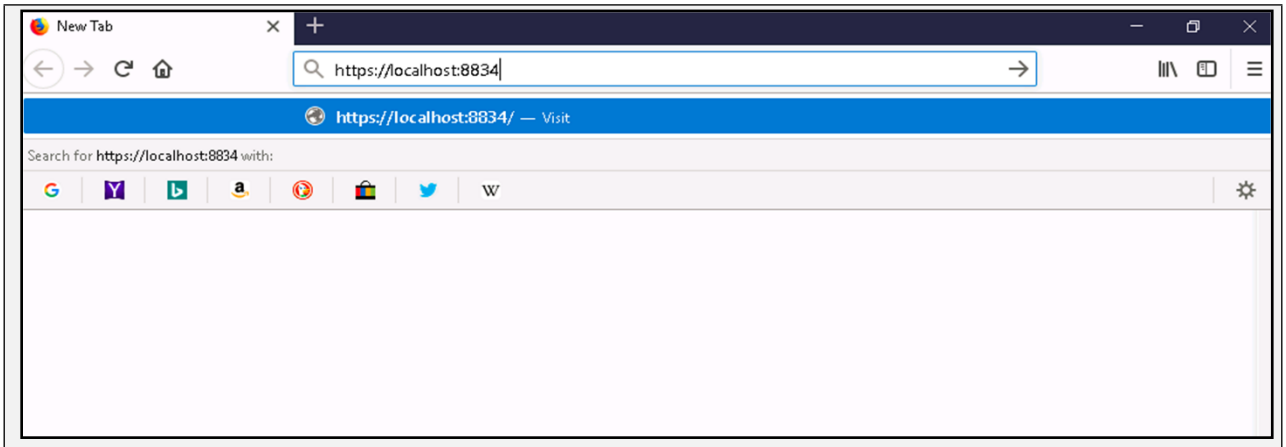

Figure 5-08 https://localhost:8834

4. Click on **Advanced** Button.

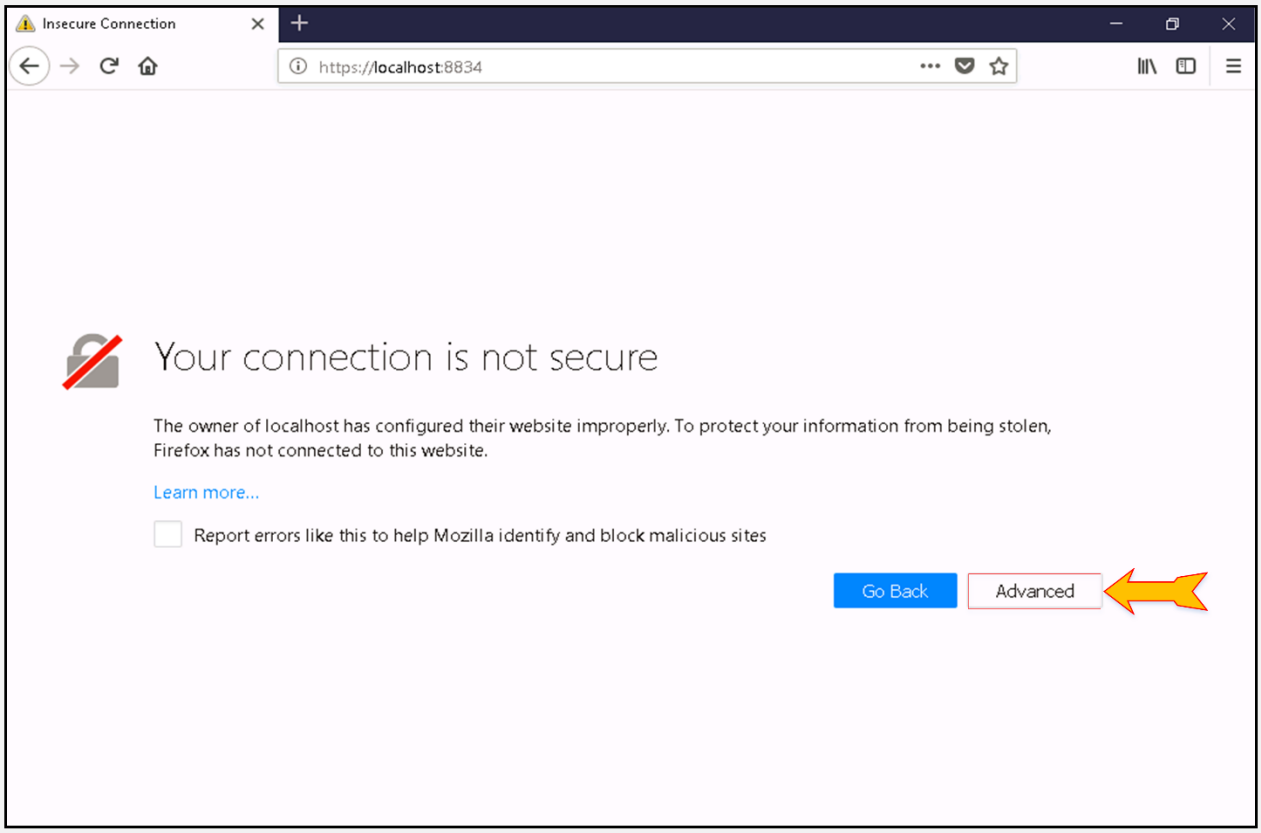

Figure 5-09 Security Exception required

5. Proceed to Add Security Exception.

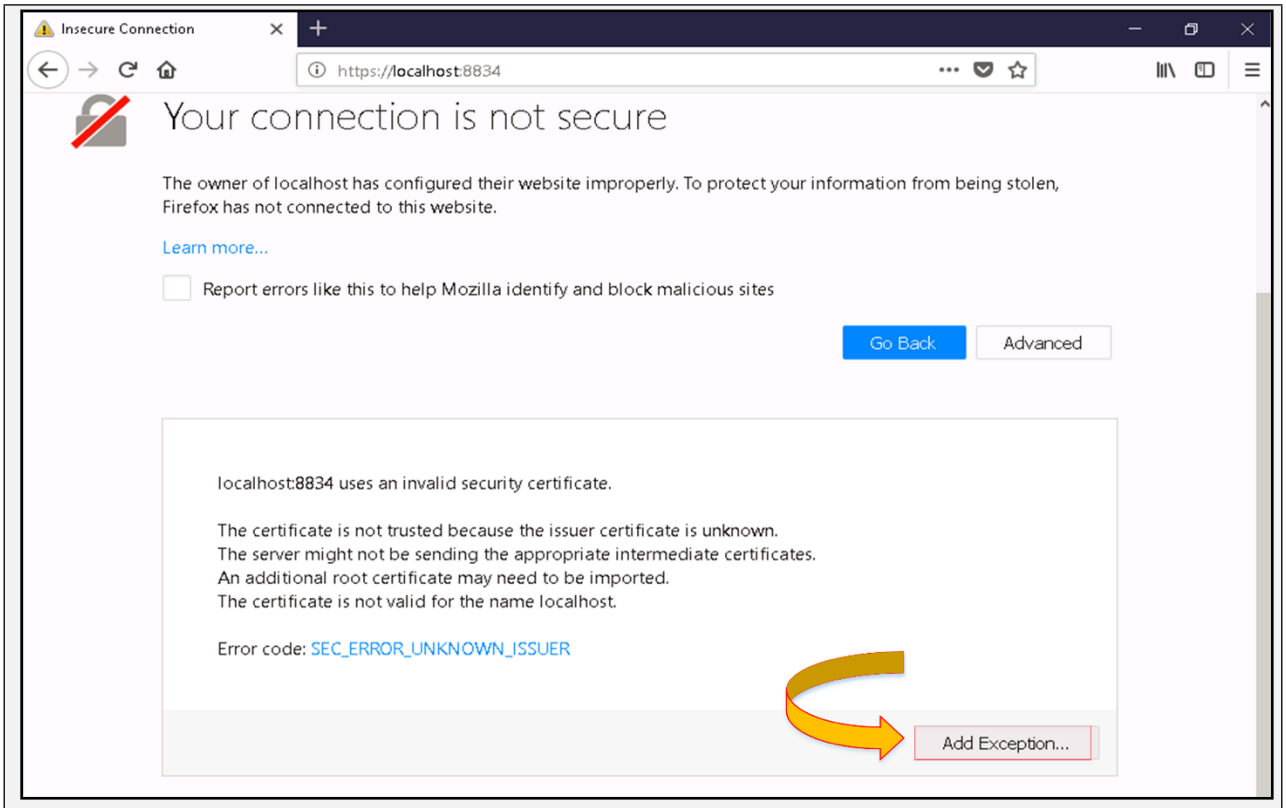

Figure 5-10 Add Security Exception

6. Confirm Security Exception.

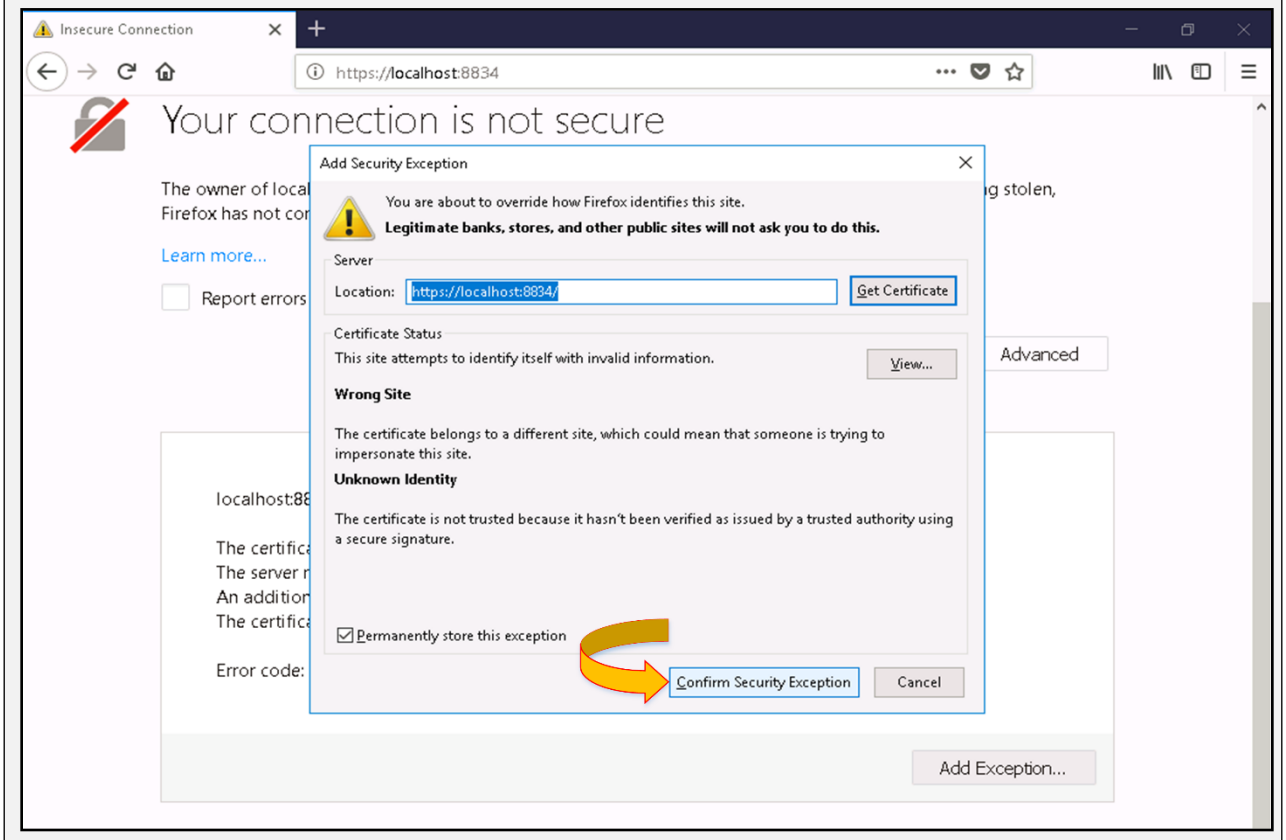

Figure 5-11 Confirm Security Exception

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

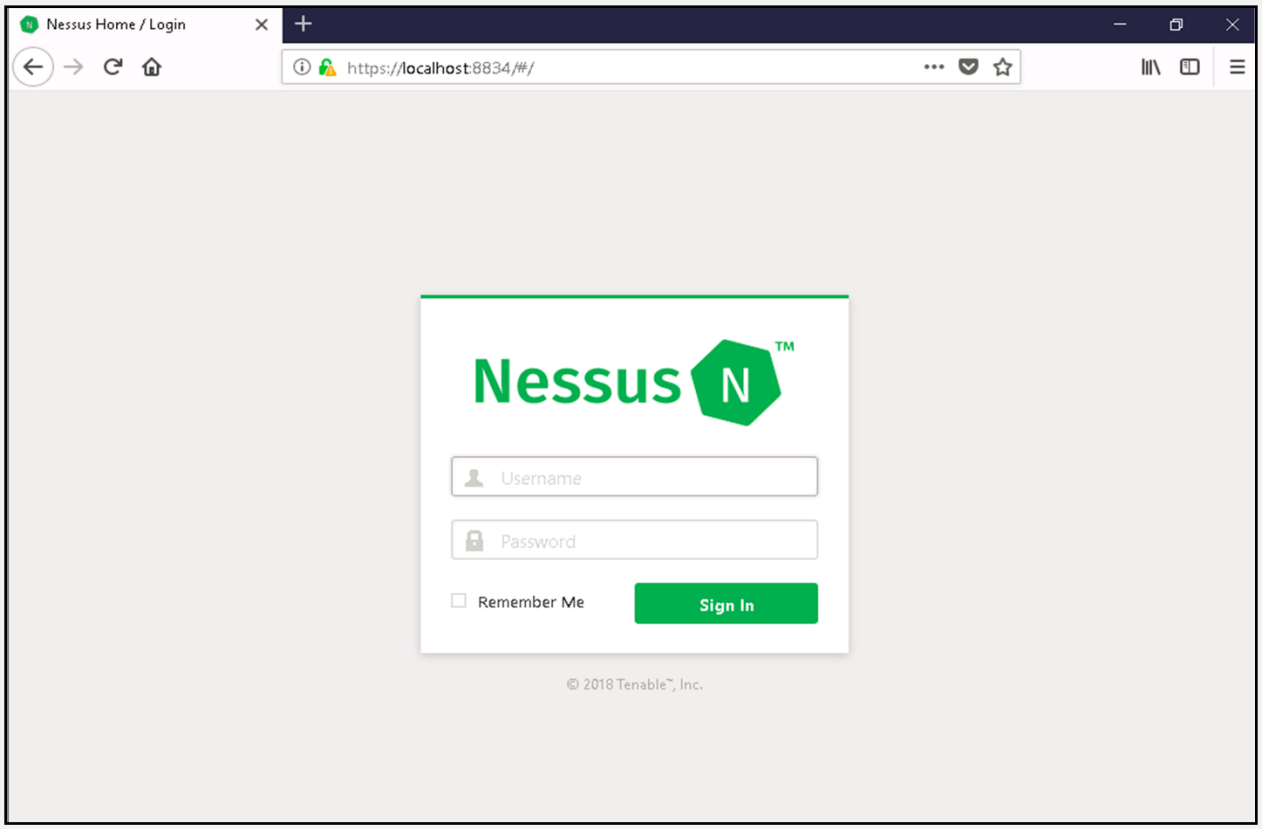

Figure 5-12 Nessus Login Page

8. Following dashboard will appear.

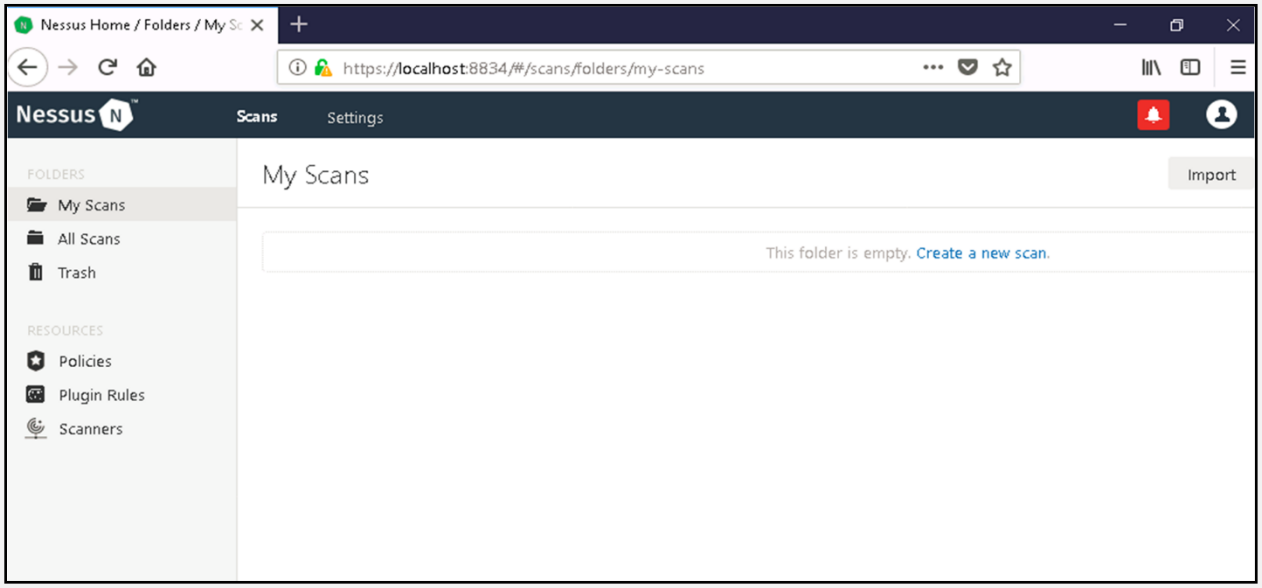

Figure 5-13 Nessus Dashboard

9. Go to **Policies** Tab and Click **Create New Policy.**

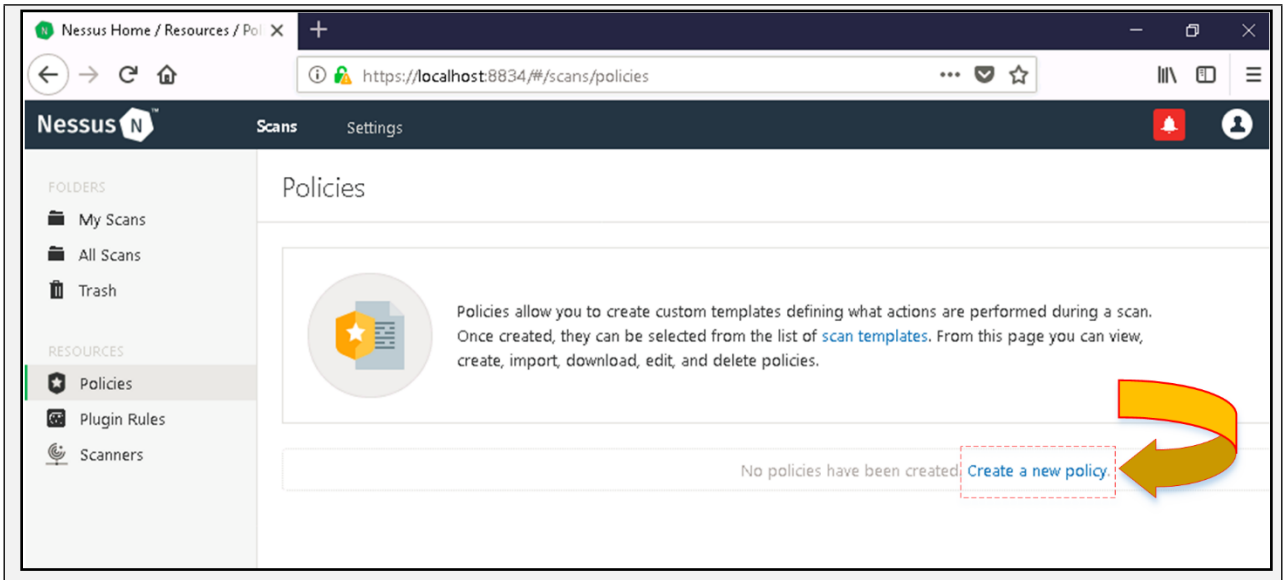

Figure 5-14 Create new policy

10. In Basic Settings, Set a name of the Policy.

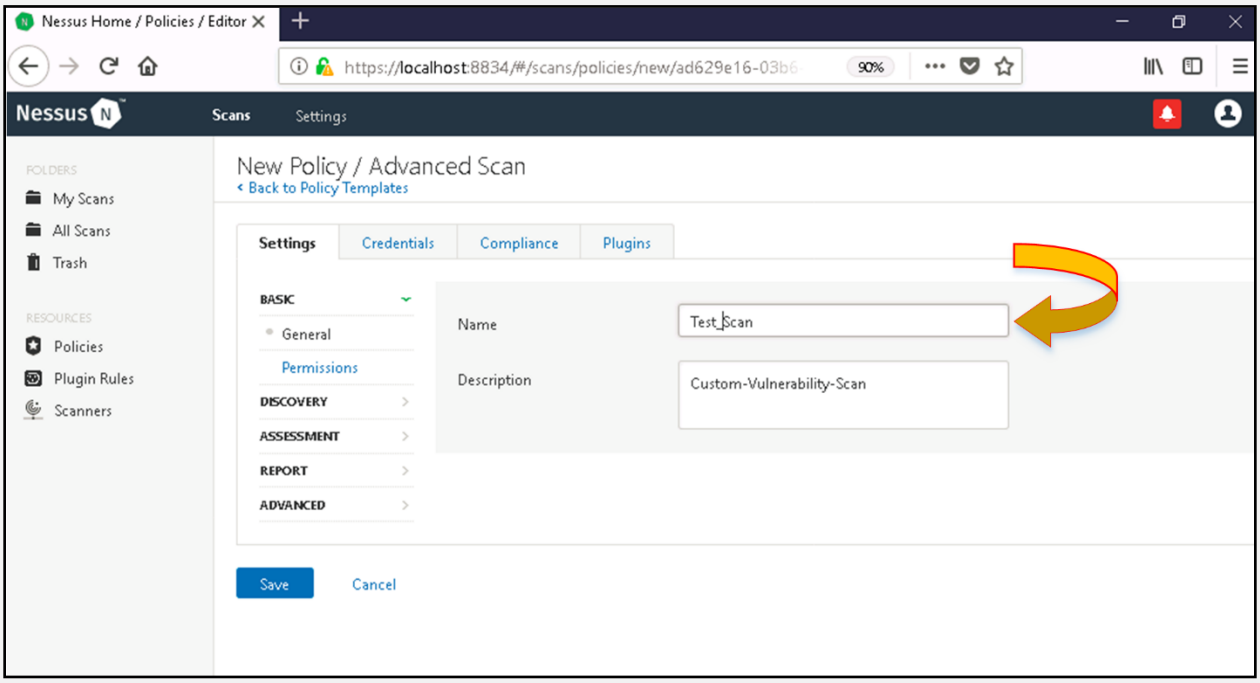

Figure 5-15 Configuring Policy

11. In **Settings** > **basics** > **Discovery**, Configure discovery settings.

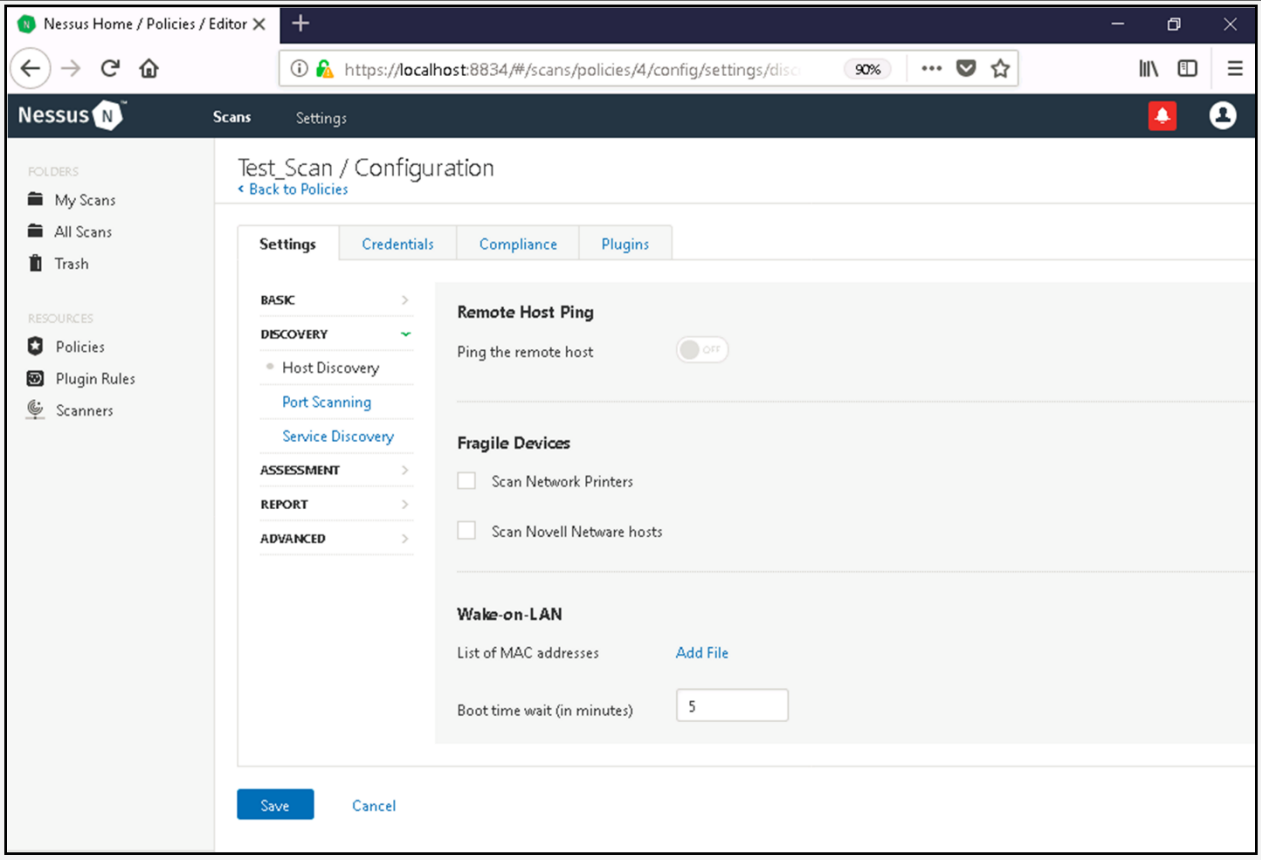

Figure 5-16 Configuring Policy

12. Configure Port Scanning Settings under **Port Scanning** Tab.

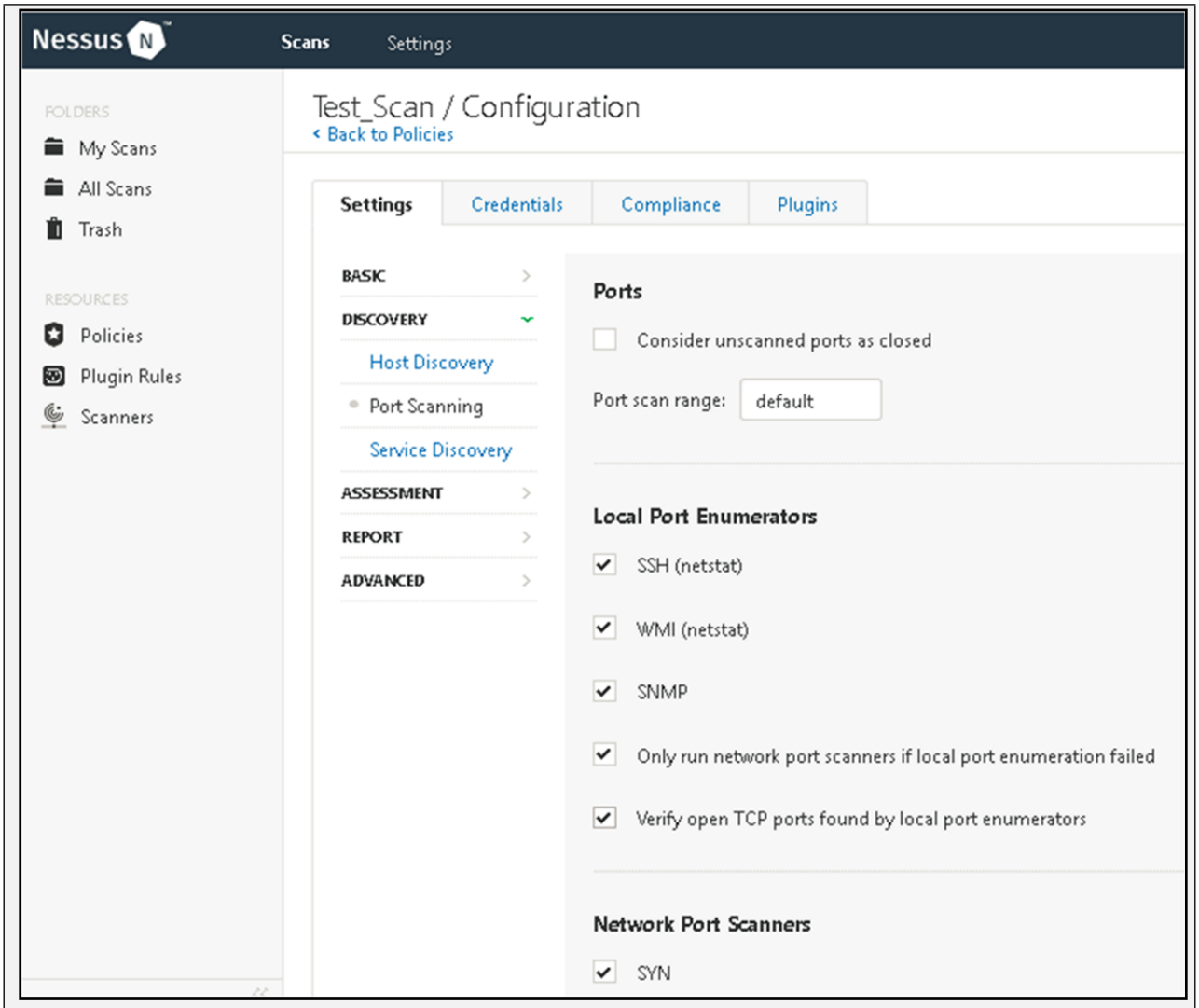

Figure 5-17 Configuring Policy

13. Under Report tab, configure settings as required

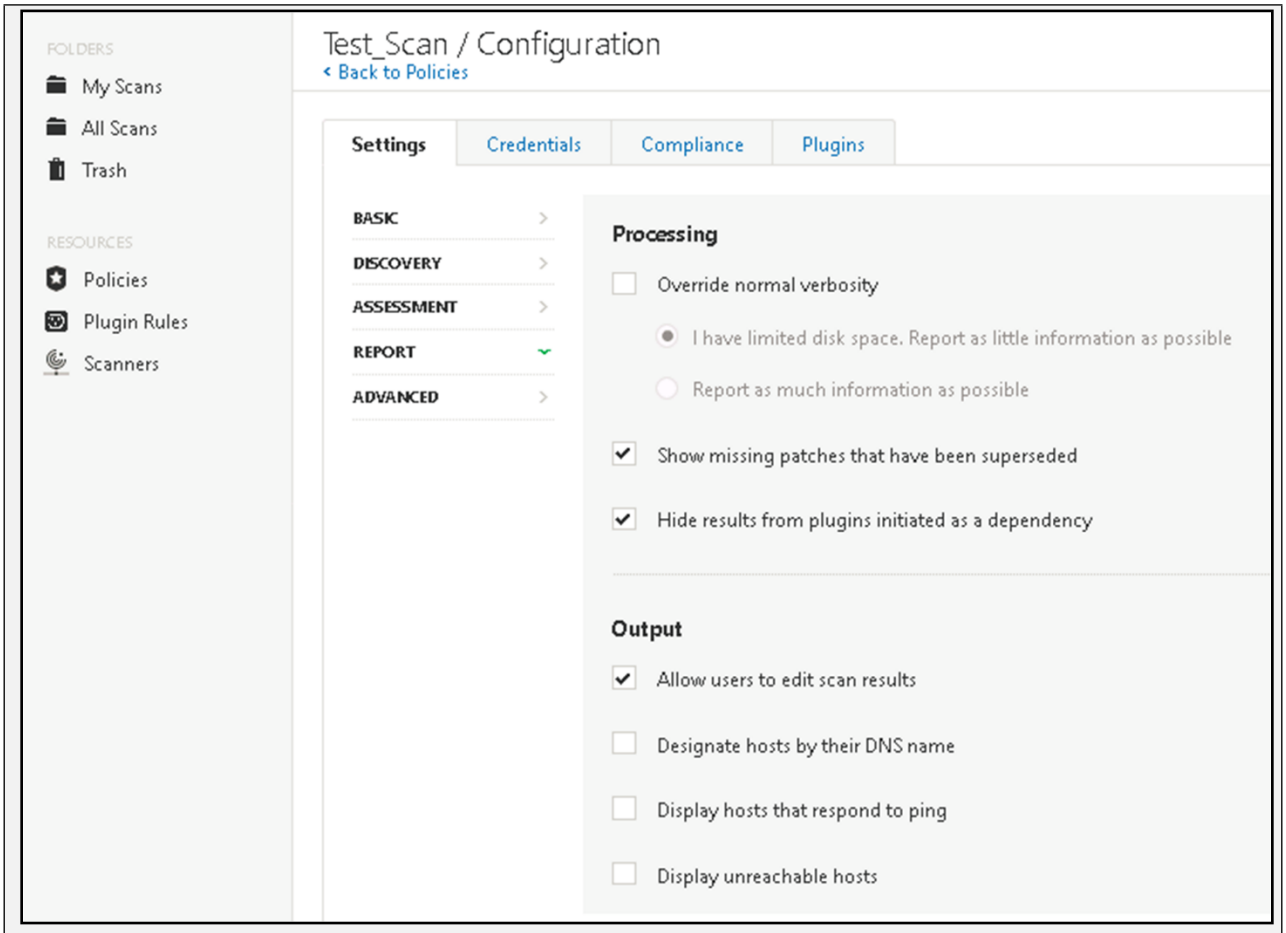

Figure 5-18 Configuring Policy

14. Under **Advanced** tab, configure parameters:

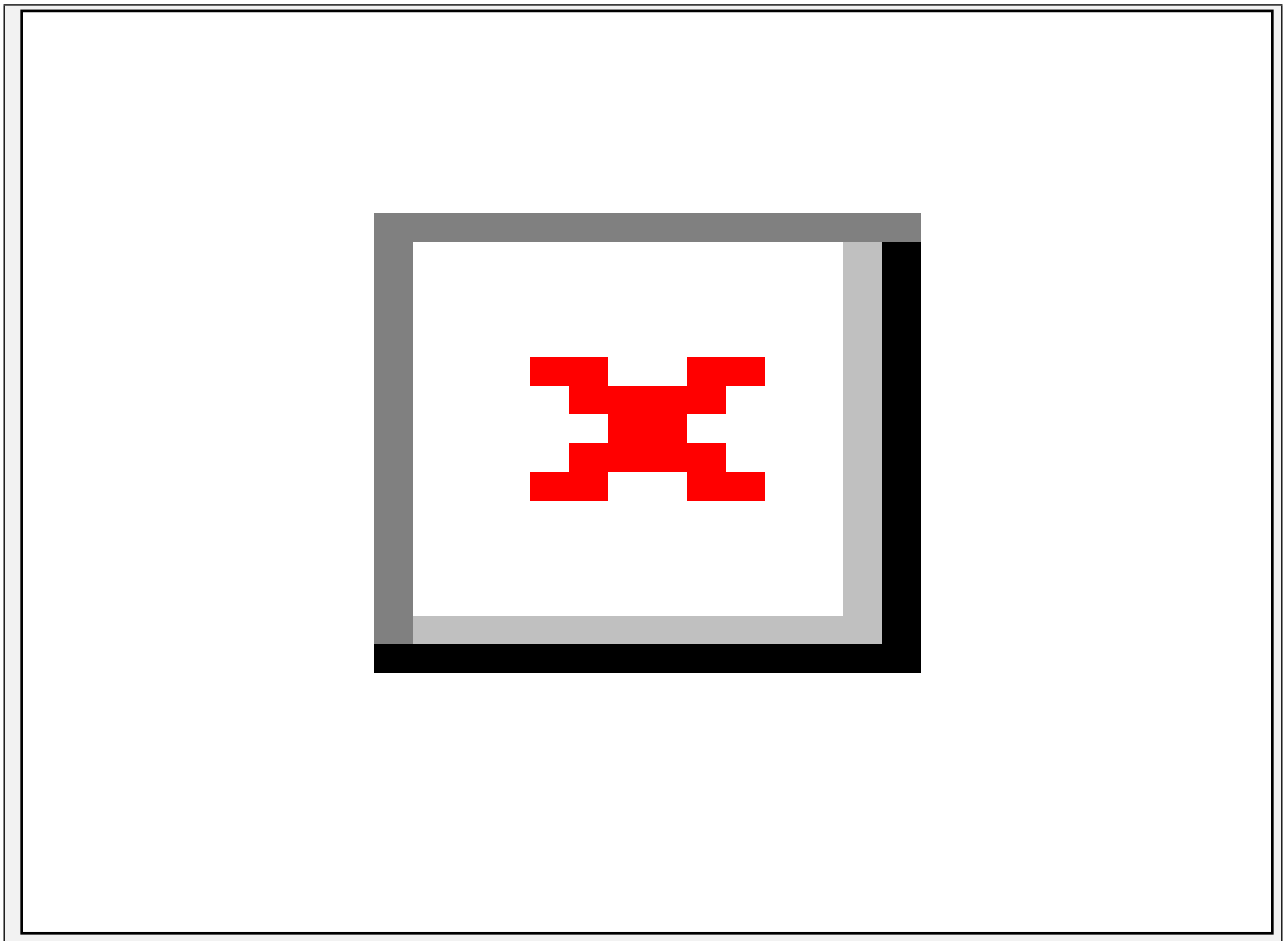

Figure 5-19 Configuring Policy

15. Now go to **Credentials** tab to set credentials.

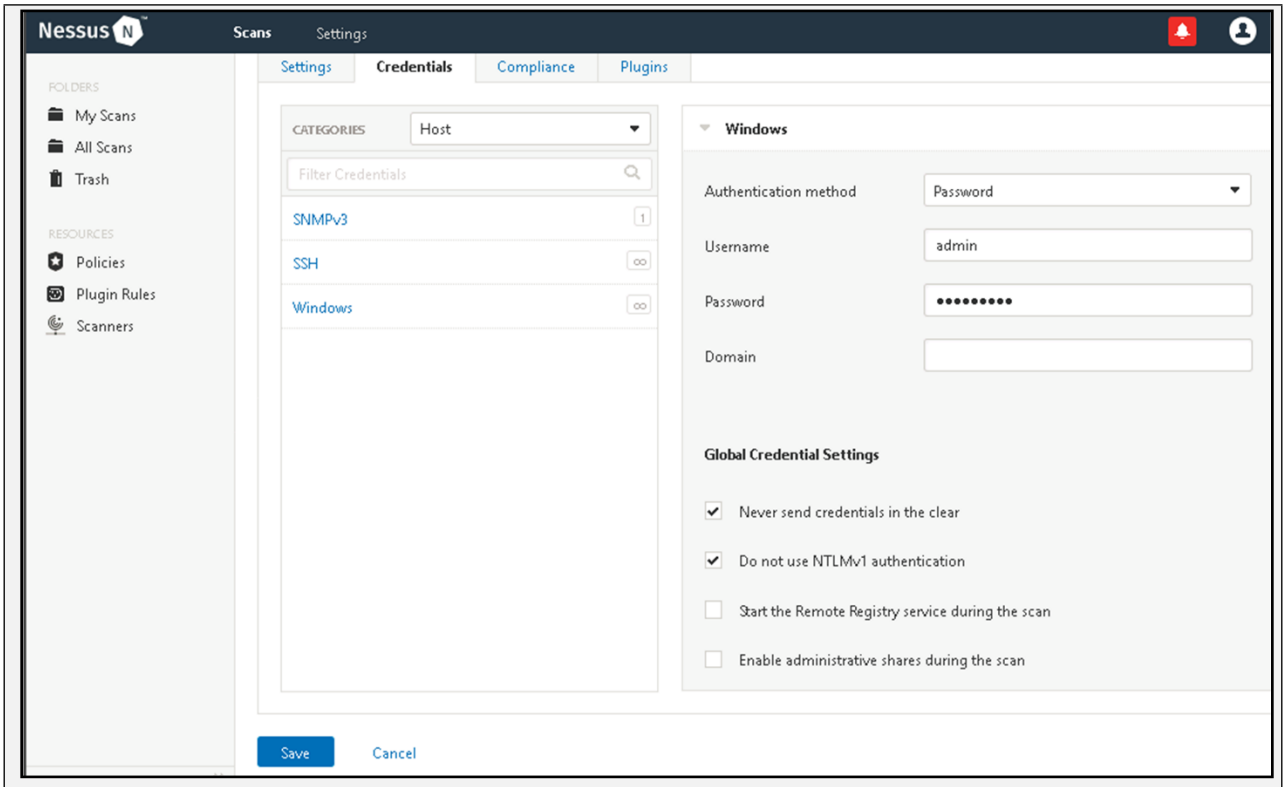

Figure 5-20 Configuring Policy

16. Enable / Disable desired Plugins.

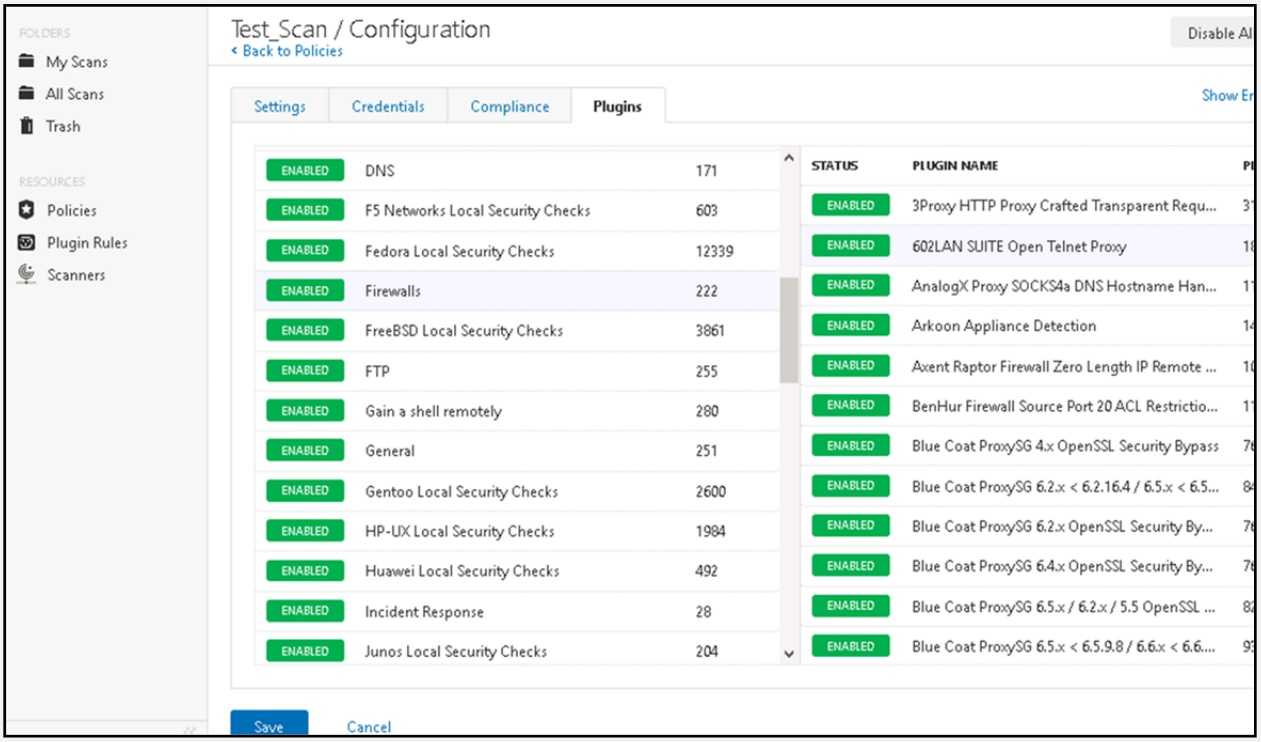

Figure 5-21 Configuring Policy

17. Check the Policy, if it is successfully configured

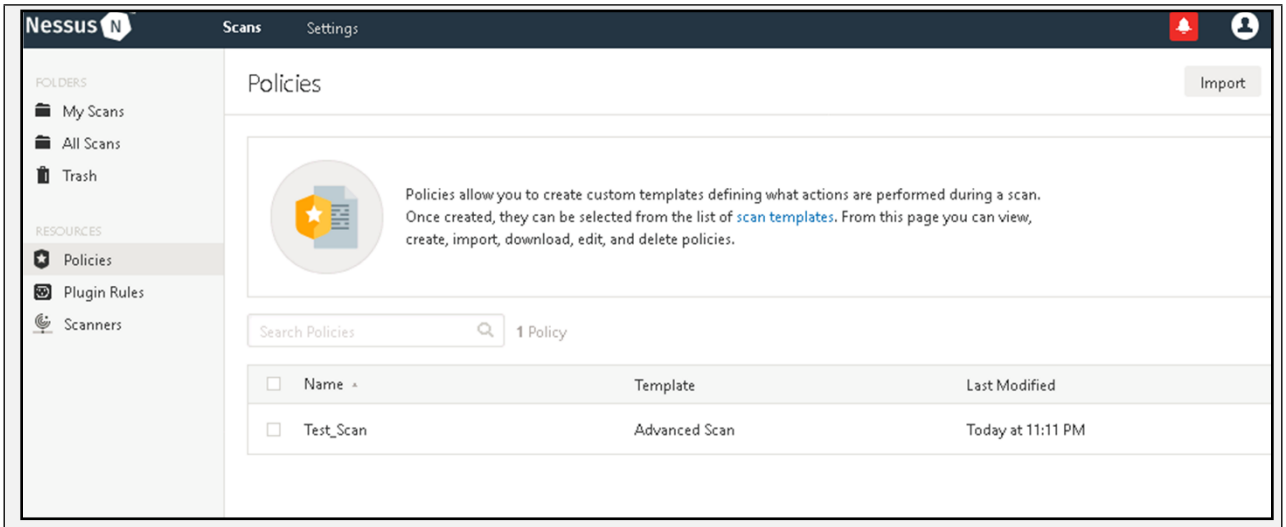

Figure 5-22 Verify Policy

18. Go to **Scan > Create New Scan**

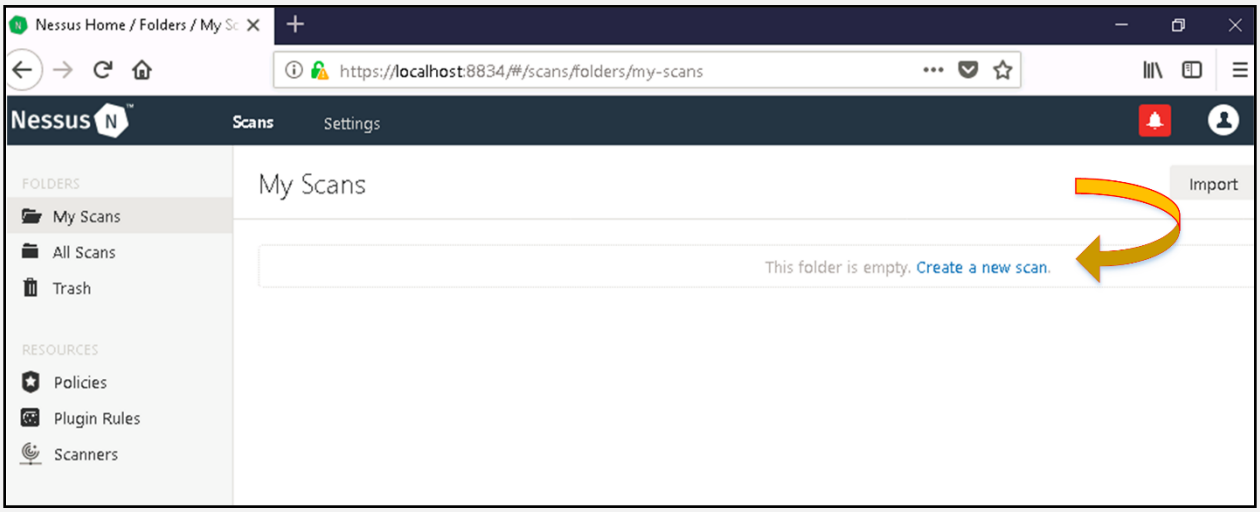

Figure 5-23 Configuring Scan

19. Enter the name for New Scan

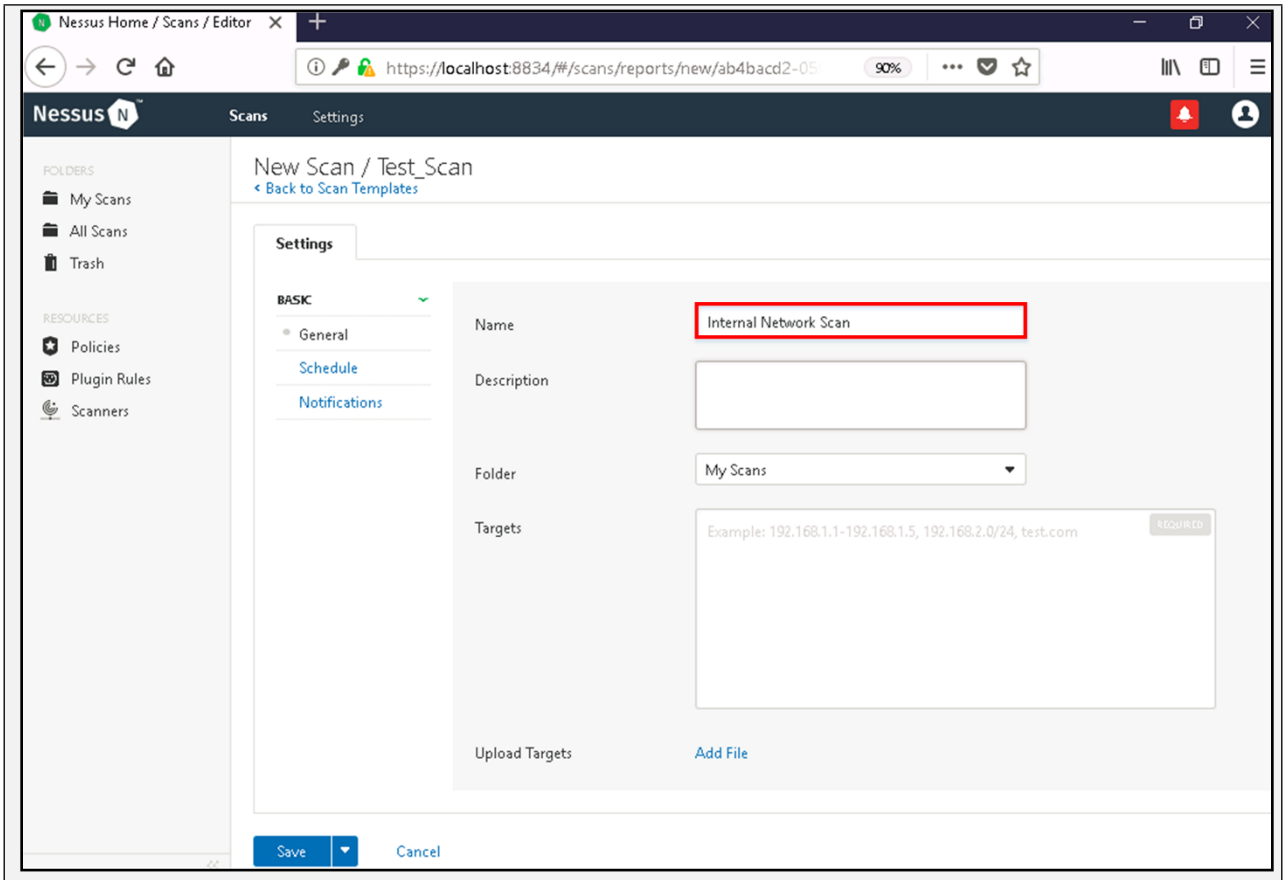

Figure 5-24 Configuring Scan

20. Enter Target Address

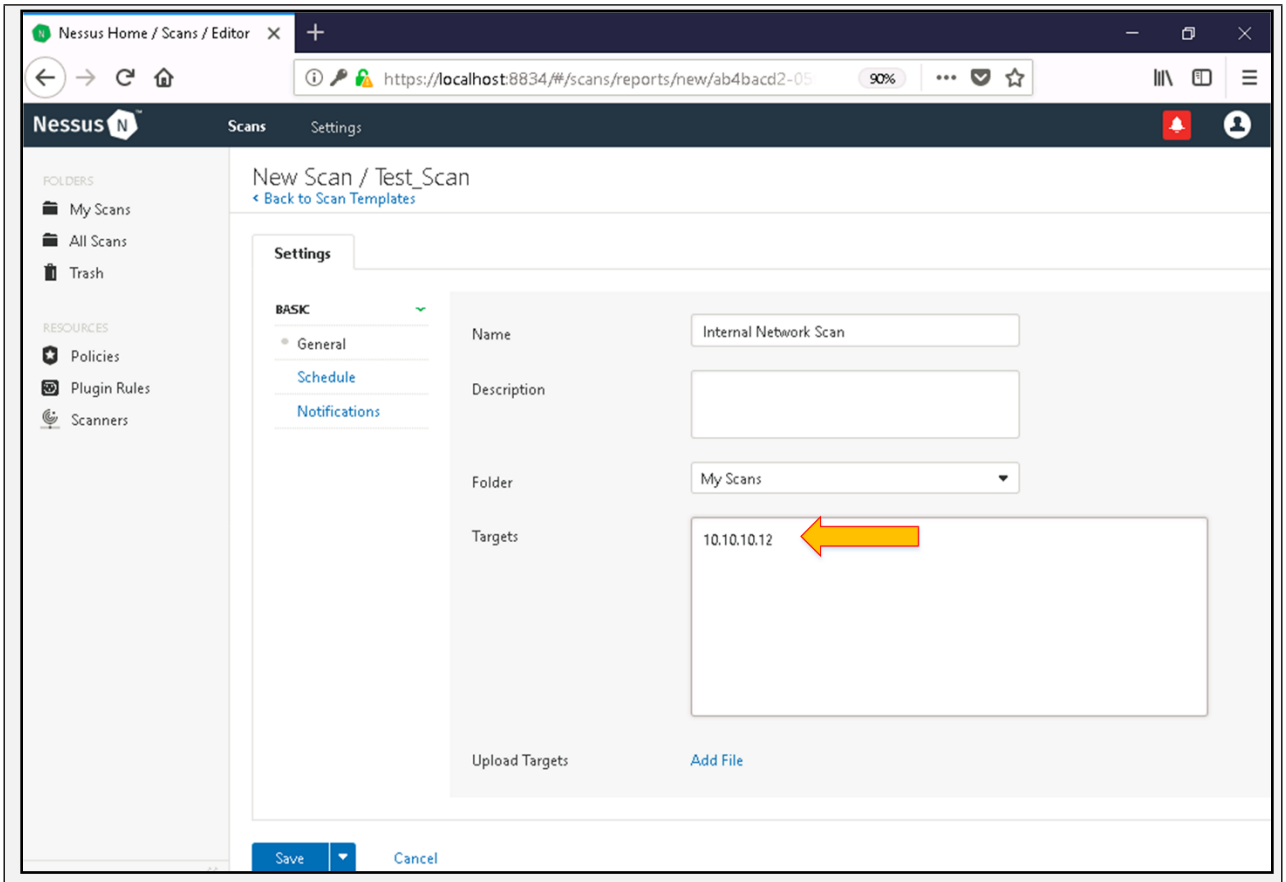

Figure 5-25 Configuring Scan

21. Go to **My Scan**, Select your created Scan and Launch.

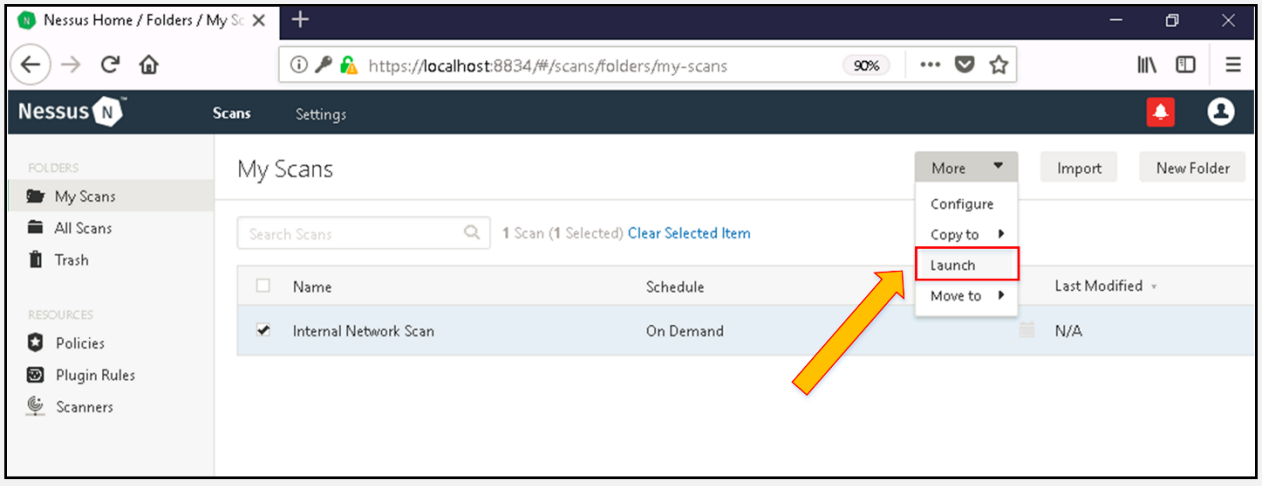

Figure 5-26 Launching Scan

22. Observe the status if scan is successfully started.

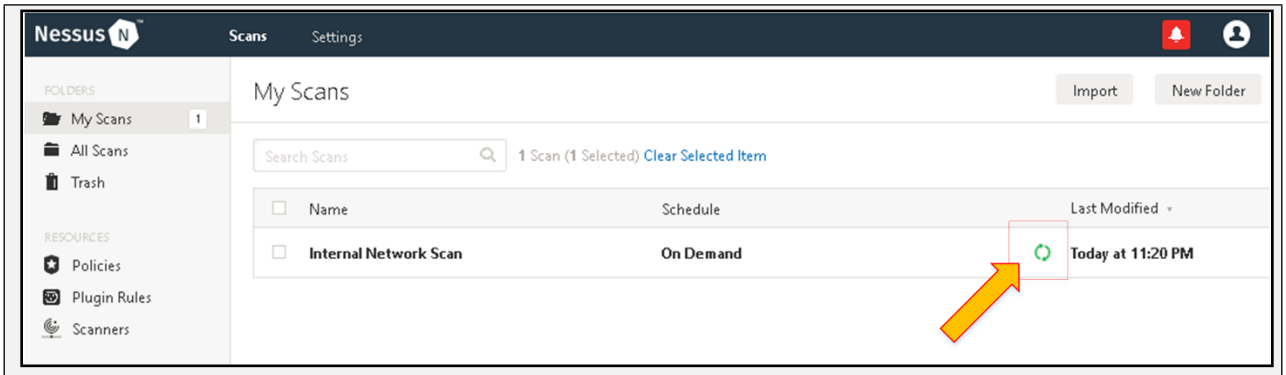

Figure 5-27 Scanning

23. Upon completion, observe the result.

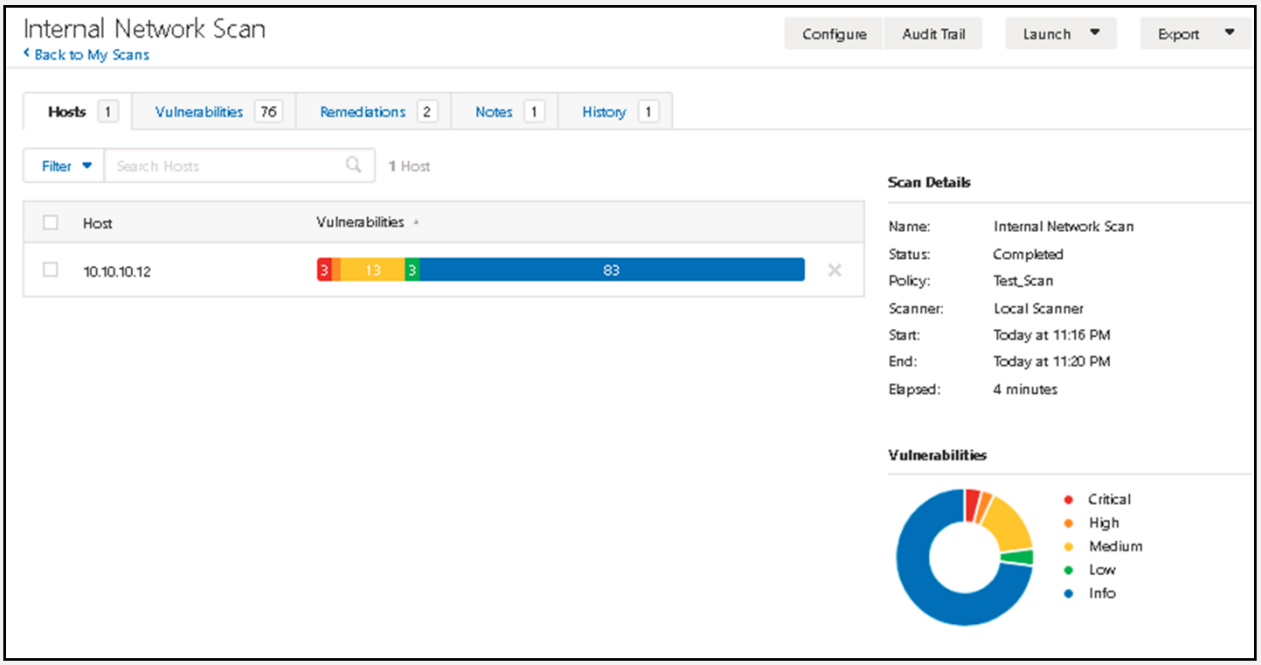

Figure 5-28 Scan results

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

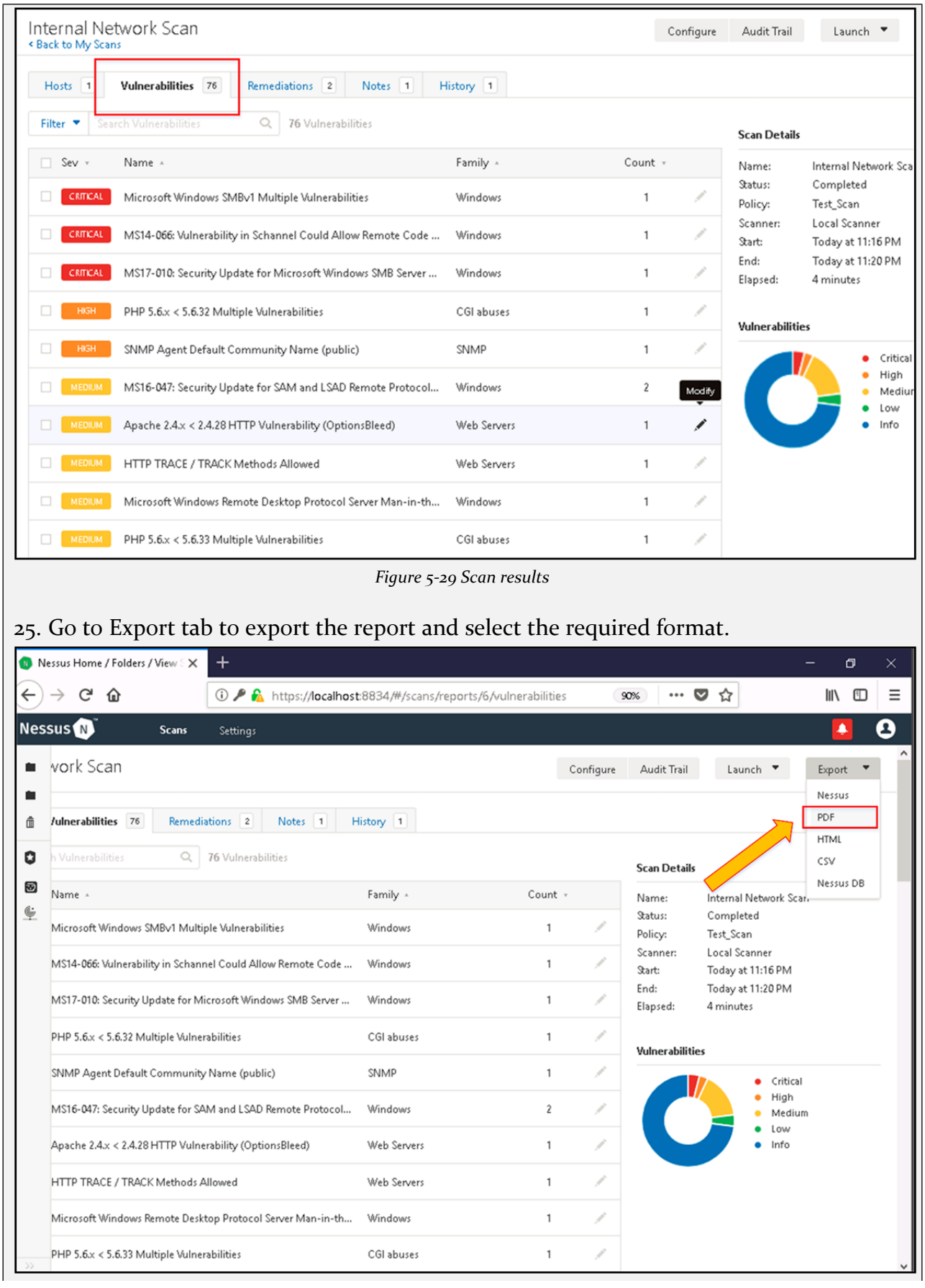

Figure 5-29 Scan results

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

Figure 5-30 Scan results

26. The following is the preview of Exported report in pdf format.

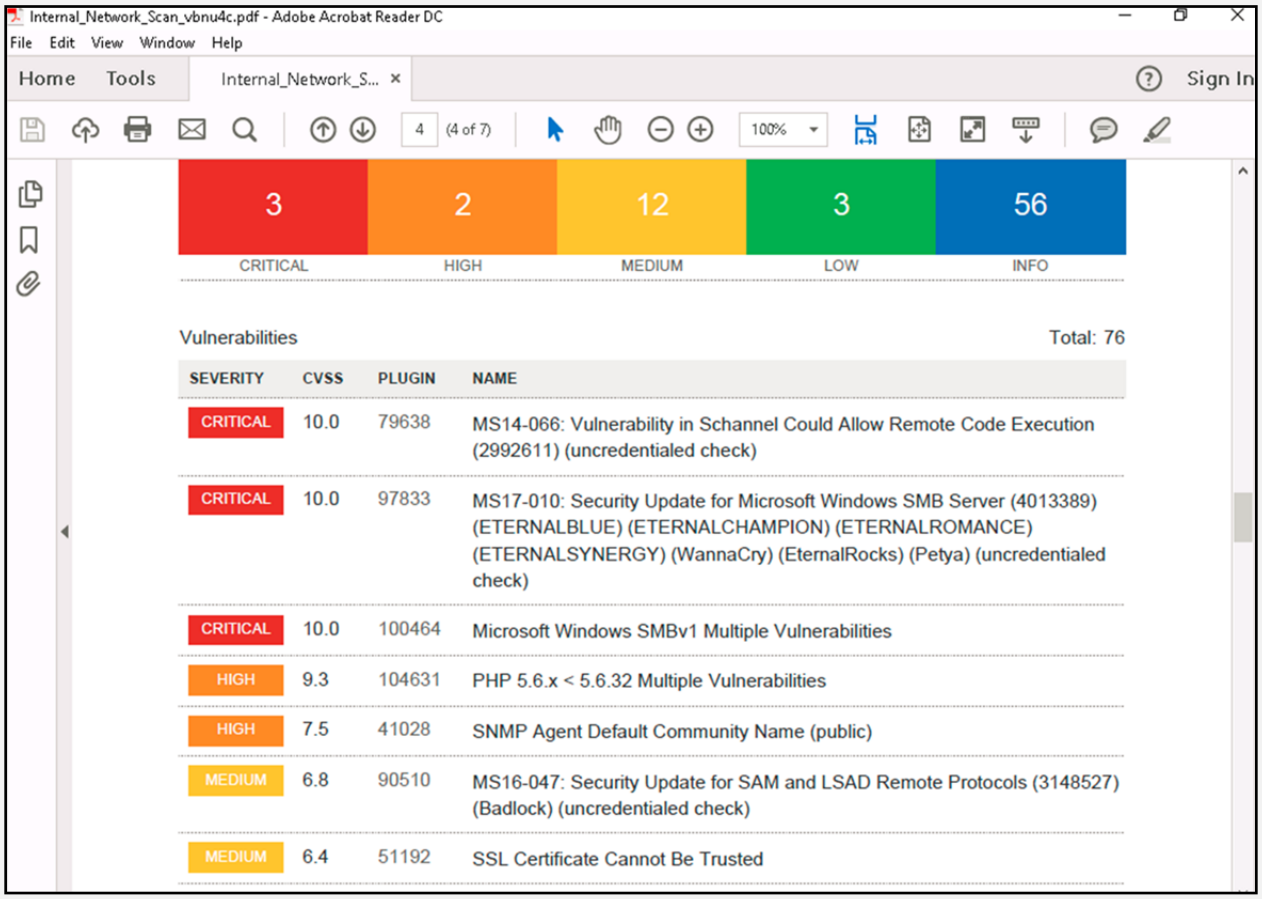

Figure 5-31 Scan results