The Art of Network Vulnerability Assessment

By: Irfan Shakeel

INFOSEC INSTITUTE

www.infosecinstitute.com

Contents

Module 1: Introduction to Vulnerability Assessment 3

What is Vulnerability Assessment? 3

Why we need Vulnerability Assessment? 3

Types of Vulnerability Assessment 4

Network-based Vulnerability Assessment 4

Host-based Vulnerability assessment 4

The Approach to Vulnerability Assessment (Automated test and Manual) 5

The Vulnerability Assessment Process 5

Determine the Target Systems 6

Locating the live systems 6

Listing Services (one-by-one) 6

Recognizing services 7

Identification of Applications 7

Identification of Vulnerabilities in network 7

Reporting the vulnerabilities discovered 7

Vulnerability Assessment VS Penetration testing 7

Module 2: Nessus, its Configuration & Vulnerability Assessment 8

Introduction: 8

The Most Widely Deployed Vulnerability Assessment & Management Solution 8

Nessus Architecture: 8

Nessus Editions 9

Installing Nessus: 9

USER ACCOUNTS: 11

COMMUNICATION: 13

ADVANCE SETTINGS 14

SCANNING THE ENVIRONMENT 15

CREATING YOUR FIRST POLICY: 16

CREATING YOUR OWN POLICY: 18

Discovery: 18

Port Scanning 20

Service Discovery: 21

ADVANCED 21
ASSESSMENT 22
SCAN RESULT ANALYSIS: 24
Web Application Scan Policy 27
Importing the Result in Metasploit 30
End Note: 32

Module 1: Introduction to Vulnerability Assessment

In this modern era, the need to analyze and eliminate vulnerabilities in your networks has become the most important task for any security expert and network administrator. We all know that today the only way to protect your organization's network from any possible attack is by locating and fixing the security holes in the network. Even if an organization has a well-managed firewall, an updated antivirus, and intrusion detection system, an attacker can still get the unauthorized access by exploiting the vulnerabilities.

Historically, we have seen many organizations that fell victim to a hacking attack thought that they could never be a target of cyber criminals. Often, we have seen small organizations that didn't take their network security seriously because of a genuine misperception that only large organizations are the target of cyber criminals. However, in the past, we have found many small companies fell victim to the different types of attacks because they did not focus on network security. What we realized with time is that the motive of an attacker is not always his profit. An attacker can be an unhappy customer, dissatisfied employee, or even a disgruntled contractor. Any of these individuals can target an organization for just the sake of self-satisfaction and revenge.

The objective of this eBook is not just to discuss vulnerability assessment and its process, but to practically show you an effective way of conducting vulnerability assessment test for any network environment. At the end of this chapter you will learn why vulnerability assessment testing should be conducted continuously on your network, and what tools you should be using to run these tests successfully. Selecting the right tool is one of the most important steps of vulnerability assessment because it will have an enormous impact on security of your organization's network.

What is Vulnerability Assessment?

“Vulnerability Assessment” or “Vulnerability Analysis” is the process of identifying and classifying security holes in an organization's system, network, or its communication infrastructure. The biggest advantage of a vulnerability assessment test is that it can predict the success of proposed countermeasures and examine the actual success rate after it was put into use.

To put it simply, suppose a network infrastructure has been set up in an organization, all the routers, access points, computers, printers and other electronic devices have been configured and attached with the network. Is this network secure from hacking attack? The answer is no. Now the vulnerability assessment comes, where an expert actually performs the test to find the vulnerabilities exist in the system and network.

Why we need Vulnerability Assessment?

Vulnerability assessment process analysis broad range of network issues, and then pinpoints the weakness in the network that needs to be fixed. This process also identifies vulnerabilities like misconfiguration and policy noncompliance. A network administrator can get a complete picture of all his systems and devices (connected through Wi-Fi) connected with the specific network.

Recently a research was conducted by “Computer Security Institute” which shows 90% of its responding organizations had experienced a security breach in last 12 months. 8% of these organizations have suffered in heavy financial losses in aftermath of these breaches. Many of these organizations didn’t have a certified security professional; neither they hired any outsider to check the security of their network. Their network and systems were extremely vulnerable; this could be the main reason behind the success of the attacks.

Another advantage of a vulnerability assessment is that it will always keep you one step ahead of the attackers. It is the most powerful proactive process of securing an organization's security. Since Vulnerability assessment already identifies all the security holes an attacker can exploit, a network administrator just needed to patch them. All he needs to do is to keep running this test from time to time, just to keep track of new vulnerabilities.

Types of Vulnerability Assessment

Vulnerability assessment can be divided into two major parts:

1. Network-based assessment
2. Host-based assessment

The network-based vulnerability assessment tools allow a network administrator to identify and eliminate his organization's network based security vulnerabilities. On the other hand, host-based scanning tools help the network administrator to secure his organization's internal systems by providing an extra layer of security. Providing limited access to the hosts it prevents him from accessing confidential data of the organization. In a nutshell, network-based analysis is to test and keep an eye on the entire network, while host-based analysis is to keep an eye on specific hosts.

Network-based Vulnerability Assessment

When you compare the two types of vulnerability assessment, network-based come on top because of its ability to identify vulnerable systems on a network. A network administrator should adopt this process first, while conducting the vulnerability assessment tests. A network-based test provides the immediate results of highly severe vulnerabilities that needed a quick fix. A firewall not configured correctly or vulnerable web server, which is considered very severe vulnerabilities, can be detected easily by running a network vulnerability test.

Some common tools are:

1. Nessus
2. OpenVAS

Host-based Vulnerability Assessment

The host based vulnerability assessment works on client-server model where client performs the scan and sends the report back to the server/manager. In this situation, client files should be installed on every machine that you want to check. The main advantage of host-based vulnerability assessment is to keep an eye on a suspect. Let's say, you want to monitor the activities of an employee in the workplace,

the suspect might create problems and might introduce vulnerabilities and malware in the network, so go ahead and use host-based vulnerability assessment.

The host vulnerability assessment enables a network administrator to eliminate the security risks from inside his organizations. This vulnerability assessment tool runs the tests from the perspective of a user who is assigned, a local account on his system. Once a user connects with the local network, even from guest account, he can exploit the security holes in the local servers and could end up taking control of organization's local systems. The most common tools are:

- Enterprise Configuration Manager
- Symantec Enterprise Security Manager

The host-based vulnerability assessment enables a network administrator to evaluate security risks inside his organization's network. These security risks can be caused by his malicious users, ignorant users (who don't follow the security protocols) and also users in between them.

The Approach to Vulnerability Assessment (Automated test and Manual)

The result of vulnerability assessment highly depends on the selected approach; there are numerous tools, both open-source and commercial are available that can make an individual confuse. But, before selecting the tools you should finalize your approach. How you will conduct the test, the automated test or manual? Both approaches have their own merits and demerits, and the combination of both approaches can take your test to the next level.

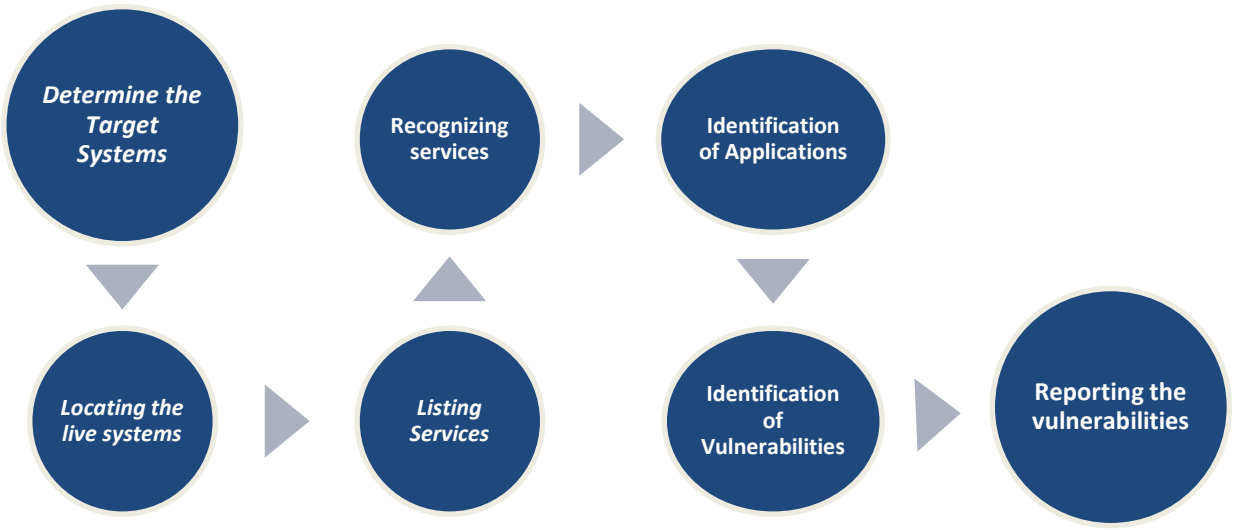
The manual check-list based approach needs an intensive review or analysis of the codes, firewall rules, network policies and every aspect of the network security. Having such an approach is costly nowadays because it requires an independent assessment of vulnerabilities in your systems. It may also require organization to hire a designated security analyst from outside, an approach which can be time consuming. But this is where an Automated Vulnerability assessment test comes to an organizations rescue; it's pretty cost effective when you make a comparison with hiring security analysts from outside.

Automated test signals out the highly severe vulnerabilities in the organization's networks or systems. But sometimes it fails to identify the vulnerabilities which are not highly severe in nature, and it also gives false positive and false negative response too. This is why manual approach is there. Although manual approach is time-consuming and requires more human resource than automated test, but it can also provide the accurate results.

The manual approach is important, but that doesn't mean you should ignore the need of an automated approach of vulnerability assessment. For examples: An automated approach makes easier to find bugs and defects if there is any.

The Vulnerability Assessment Process

The effective and efficient vulnerability assessment is based on a systematic approach and a standard process. No matter what tool and strategy are using, you are most likely following the generalized vulnerability assessment process.



Determine the Target Systems

The first stage of a vulnerability assessment process is to define the IP (internet protocol) a network administrator wants to target on his network. He needs to identify the span of IP addresses which can be mapped to his online systems. His every IP address specified by the computer or user, enquirers is sent to extract a response or answer. Once the response is received in return of probes, the system will mark that IP address as a valid host.

Locating the live systems

Once the network administrator is done with the first stage of vulnerability assessment process, he will then perform many fingerprinting techniques to detect the live host and their information. This shows what kind of system is found at each IP address in the process of "determining the target systems". These techniques of finger-printing range from simple Network Management Protocol queries to complex TCP/IP stack based operating system identification.

Listing Services (one-by-one)

When a network administrator completes the first and second step of vulnerability assessment process, he needs to start scanning ports. A port scanning is one of the most important step of this test because it will allow him to find out vulnerable ports on his network and the services associated with specific port numbers. Through implementing port scanning, a network administrator can discover the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) services which are open in his network or system. There are different scanning types that you should use while scanning to avoid firewalls and IDS; TCP ACK and TCP window scanning techniques are the recommended. If any of his port responded with a message that a particular port is open. The address or port number will be logged and will be saved for later usage.

Recognizing services

The fourth step of the vulnerability assessment process is recognizing the services on every open port of a network (which are identified in stage 3). The test begins with sending similar requests frequently and assessment tool will examine the responses against the set of signatures. Once a match is made between signatures of known application, the data will be saved for later use and tool will start running tests on other services.

Identification of Applications

This is one of the most important step in all vulnerability assessment process. Once a network administrator moves from recognizing services stage he needs to pinpoint vendor and type of every service which was discovered in stage 4. The basis on which we rate this stage most critical is because we have to see vulnerability test of one application is not effecting or crashing other applications. If there is an application, which is the cause of other application crashing then the results network administrator will get cannot be rated as accurate. It may also cause some assessment tools to identify false vulnerability or false positives. The common cause of a false positive is imperfect application identification before the test was conducted.

Identification of Vulnerabilities in network

In this the system is ready to run the test. Since all of the ports open on a network are mapped, all familiar services are also mapped to a particular application. The vulnerability assessment test will begin, In the next step of this process active configuration probes are conducted and in the end a set of custom attacks on network which will define either a stated vulnerability exists in a system or not.

Reporting the vulnerabilities discovered

This is the final stage of vulnerability assessment process, where the vulnerabilities will be reported which are discovered in the system or network. The report will indicate which vulnerabilities are highly severe and which are not. The report will also provide solutions to a network administrator how the reported vulnerabilities will be fixed. One thing which most of the assessment tools have in common is the ability to show tendency report of how a tested network progressed over time. The network administrator can also choose the report summary to present it to his organization's management.

Vulnerability Assessment VS Penetration testing

These two are the most common practices of the cyber security field. But, sadly people often get confused between them. As discussed, vulnerability assessment is the process of finding the vulnerabilities in the system, while pen testing is the additional step where you actually perform the attacks like an attacker does.

The penetration testing process has the vulnerability assessment in it, where the specialist first performs the vulnerability assessment to find the issues and then he/she act as an attacker to exploit the found vulnerabilities. The objective is to provide the proof-of-concept and to demonstrate the attacking vectors; or simply the objective is to show how risky and vulnerable the network is.

Module 2: Nessus, its Configuration & Vulnerability Assessment

Introduction:

In 1998 Renaud Deraison started the Nessus project with an aim to provide the world a free and open source remote security scanner. And, since then Nessus has been one of the most used vulnerability assessment tool all over the world. This is not a hypothetical statement, it was backed by the sectools.org survey, conducted few time back. Nessus is the three-time award winner of "Most popular vulnerability scanner", in the last decade.

Nessus is an ideal assessment tool for the large networks and its popularity increased with time because it costs effective for every enterprise. Its extensibility allows its users to leverage their own expertise in developing vulnerability checks.

Renaud Deraison established a company named Tenable Network Security, so he can provide the paid support for Nessus Vulnerability Scanner. It was a big move for the success of Nessus because it silences all its critics.

The Most Widely Deployed Vulnerability Assessment & Management Solution

There are more than 1 Million users around the globe who deployed Nessus. Why? Because it is available on cloud and it has the industry's broadest vulnerability check library, the secret of success is Nessus supports more technologies than any other tool available and it can be used on a very small to very large corporate networks effectively.

So, anyone who denies the importance of Nessus needed to get his facts right, because the biggest fact is Nessus is the only vulnerability assessment tool which has reached such high- level of success since its launched. Because of its high demand the certified Nessus specialists are able to earn big payrolls in an organization.

Nessus Architecture:

The core reason behind the success of Nessus is its architecture. The architecture of Nessus is unique in many ways when you compare it with other assessment tools. The flexibility and resourcefulness of the Nessus architecture has taken every element of the security life cycle into consideration.

Some keys thing which makes Nessus stand apart from other assessment tools is its large scale batch execution of vulnerability scans, Graphical and hyperlink data report (which are easier to present to bosses).

Previously, vulnerability scanners were client based solutions; the specialist brings his machine (laptop) to the client's offices or organization and run the assessment tests. The organizations pay those specialists thousands of dollars to find the vulnerabilities in their systems. They just work for a day or two depending on the depth of the organization's network. The machine (laptop) of those assessments specialists is unusable until the scan is running.

The Nessus tried to eliminate this aspect of the vulnerability assessment test. To conquer this problem and many others, the Nessus Project adopted a client/server model for its foundation. This allows the Nessus specialist to work on his machine (laptop) while the Nessus Vulnerability assessment test is running on the back. This is another advantage Nessus tool provides to its specialists.

The Nessus server, nessusd, is the one that performs the actual vulnerability tests. It notices the incoming connections from Nessus clients, where certified specialist had configured and scanned the assessment tests. The Nessus client needs the authentication from its servers before the scanning starts. This architecture makes it easier for specialists to administer the Nessus installation.

Nessus Editions

There are numerous tools available for the security analyst or pen tester to conduct the vulnerability assessment. But, as discussed Nessus is the renowned amongst them. Now the next question one could ask about the version, what version or edition of Nessus is right for me? The right answer is, it depends. Yes, it depends on your need, every organization is different, their objectives are different and this is why Nessus provides fours editions to fulfill the need of every organization.

- Nessus home edition
- Nessus professional
- Nessus manager
- Nessus cloud

Nessus home edition is free and for non-commercial, it has some restrictions and limitation over the other editions of Nessus. It can scan only up to 16 IP addresses per scanner and you can't perform the compliance check and content audits.

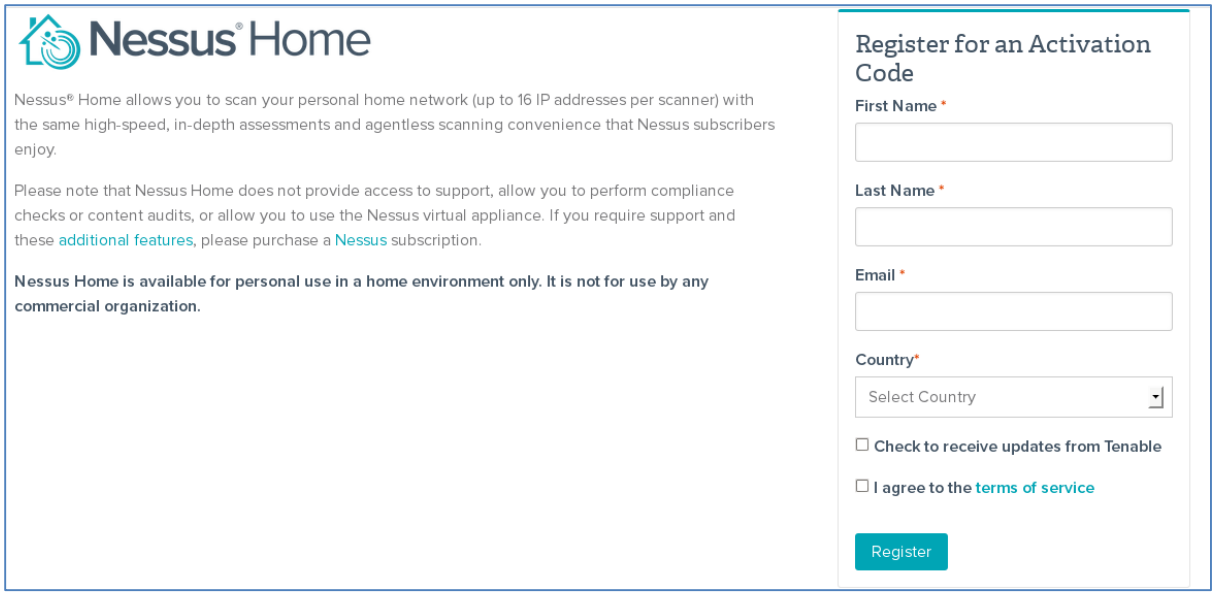
Whereas, Nessus professional is the common choice and it has all the functionalities to conduct a successful vulnerability analysis.

Nessus manager is an advance and one step farther than professional edition. Nessus manager can be configured on the premises for continuous monitoring, threat detection, resource sharing and get added vendors in your vulnerability test.

Nessus cloud is cloud-based vulnerability management system. It allows you to test the public IP that an attacker might do, perform the web vulnerability assessment, PCI approved scanning and get continuous coverage from the cloud.

Installing Nessus:

The core objective is to get the activation key and the software installer. Locate the edition of your choice and put your personal information to get the activation key:

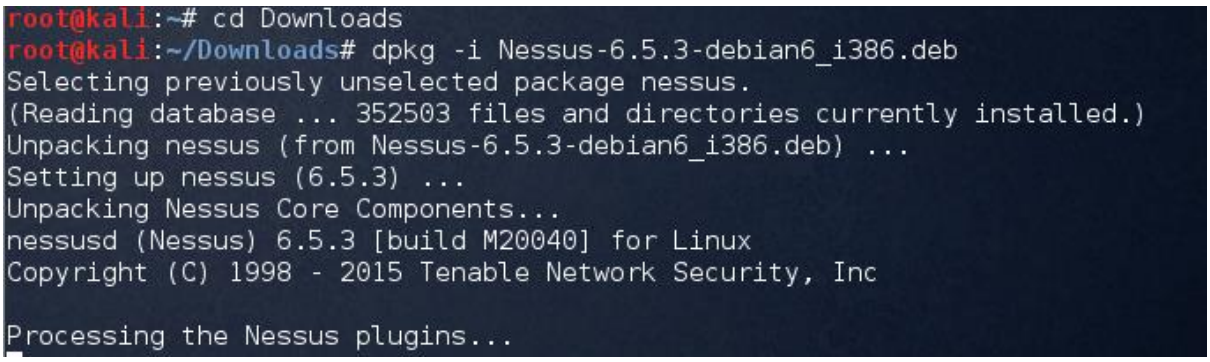


Once you get the activation key, download Nessus for your operating system. Nessus is available for almost all known and common operating systems, whether you are using Linux, Windows, MAC and FreeBSD.

After getting the installer, the next step is to install it. Kali Linux has been selected to demonstrate the installation and configuration process.

Open the terminal and locate the directory where you have stored the downloaded file. Use the command:

```
$ dpkg -i nessus_file_name.deb
```

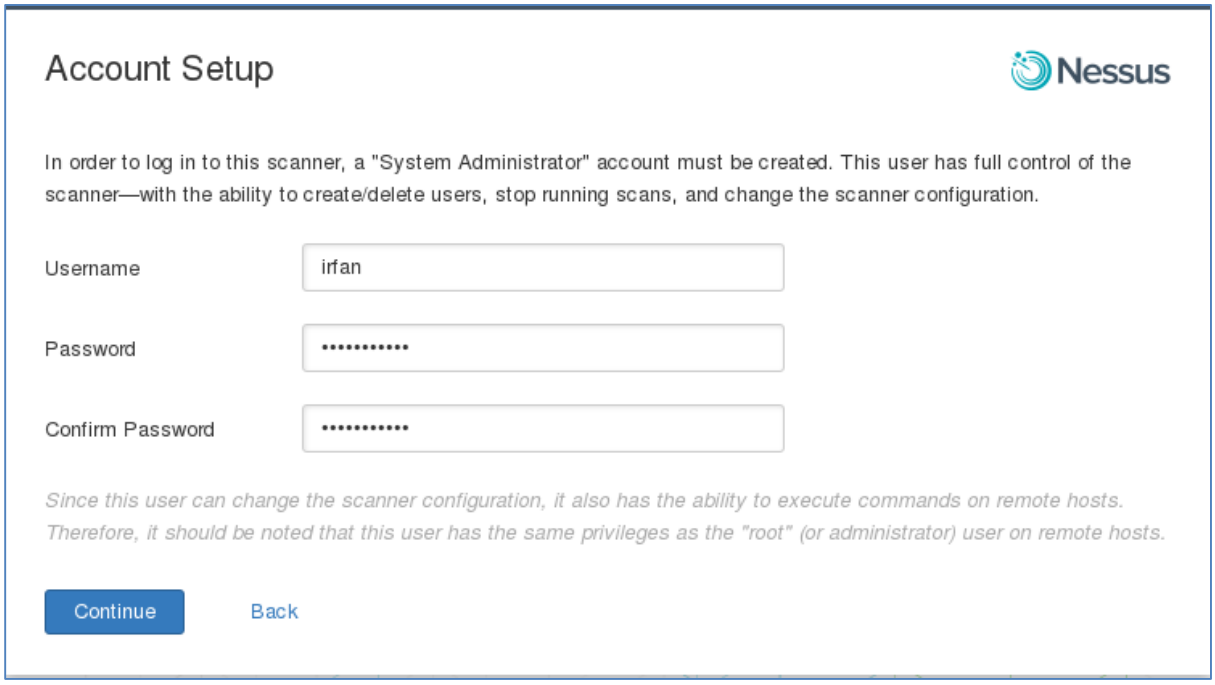


Since Nessus works on the client-server module, so your client connects to the server to download all the plugins and necessary files to configure the Nessus.

```
All plugins loaded (2116sec)

 - You can start Nessus by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner
```

Once all the plugins downloaded, start the Nessus service and locate the localhost on port number: 8834 and setup the System Administrator account (account roles will be discussed).



On the next window put the activation code to active the Nessus functionalities. More or less, the installation process for every OS is the same. After installing Nessus, open it through web interface (http://localhost:8834) login by using the system administrator account created during the installation process.

User Accounts:

User management is a magnificent feature of Nessus. Consider an environment where multiple people have to work on Nessus scanner from different accounts and different locations; it can be managed through user management setting. There are primarily two roles:

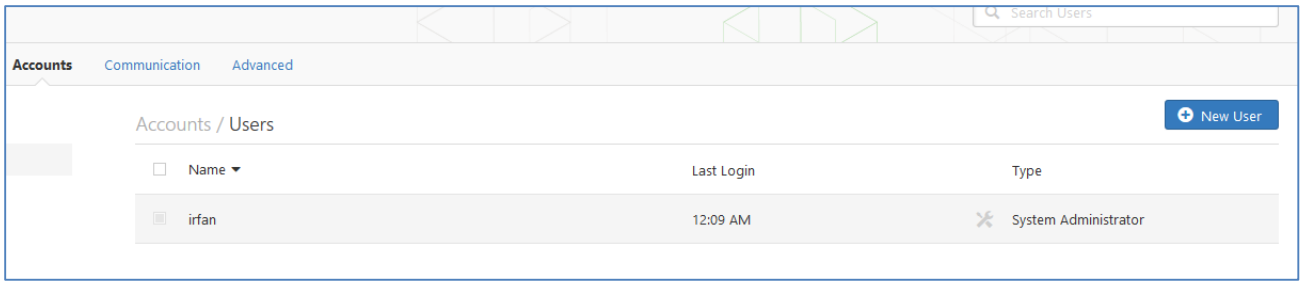
- System administrator
- Standard role

System administrator is an admin account and has full control of the scanner while standard role does not have all the access and control including:

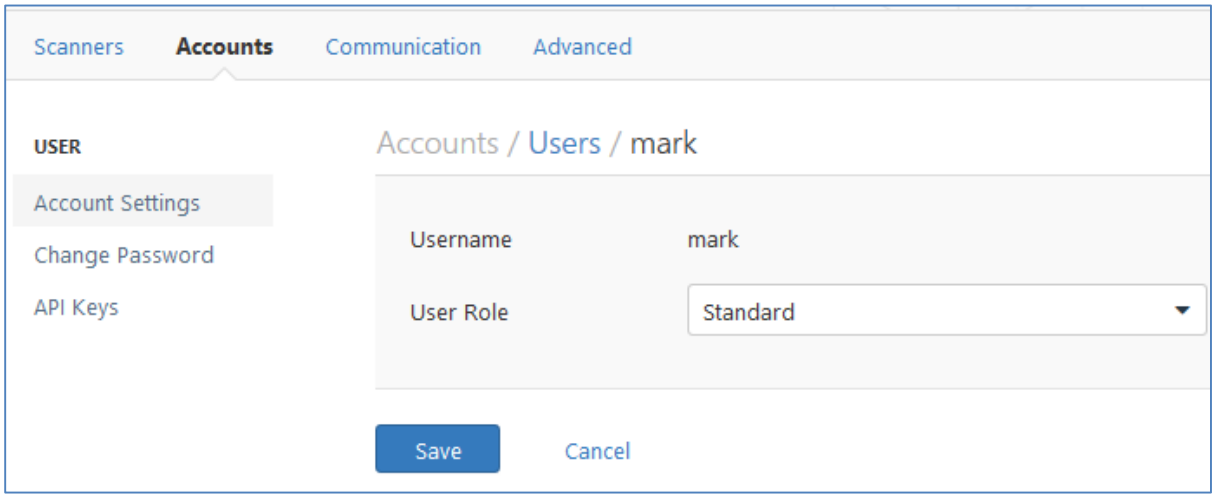
- User management

- Communication setup (proxy & SMTP)
- Advance scanner setting
- Basic scanner setting

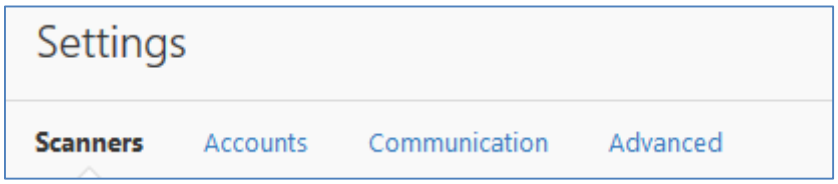
However, users with standard access can perform the vulnerability assessment. But, this account should have to follow the created guidelines. If you are operating in a large corporate environment, then you should have many accounts with standard access.



Click on **New User** under the **Accounts** tab to add new users. Fill the required information (username, password and role) to setup an account. The system admin account can change the role and even delete any account, whenever they need. There is no way for the users having standard access to recover the lost password; they need to contact the admin account to reset the password.



Admin has to manually change the password and role for that matter. You will witness the following menu items while browsing using an admin account:



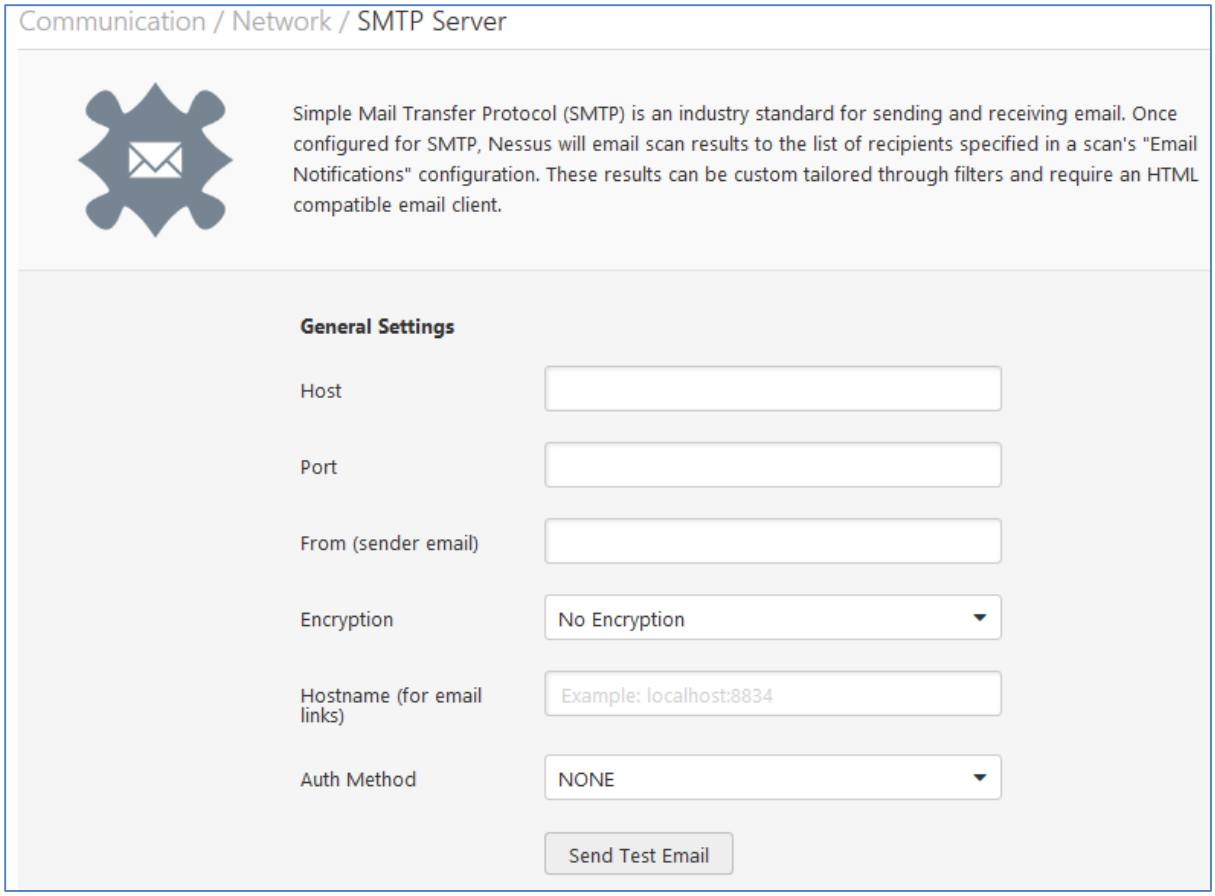
The first tab “scanner” provides the details of the installed Nessus scanner, the activation code, expiry, software version and other relevant information, while the “accounts” tab has already been discussed.

Communication:

Generally, the organization does not let internal network connect to external directly, they use proxy servers to manage the incoming and outgoing traffic. Nessus has to face the same situation, if you are configuring Nessus at your workplace, then Nessus is not likely to get the latest plugins downloaded from the server because of the network connection issue. To this problem, you should provide the proxy server information, so that Nessus can connect with the internet. Under the communication tab, there is an option to provide the proxy server information.

Host	The server IP address or host name
Port	The port number to connect the server
Username	The authorized username
Password	The password of the said user
User-agent	If the server filter specific http user-agent

Another great feature of Nessus is its ability to send the report of the scan through email. Consider a situation where an admin has configured the account and scan, he left the office, but he wants to get the report of the scan on his cell phone or any device via email. This can be done automatically by the SMTP server (standard protocol to send/receive email). This is the second option that you will find under the communication tab:



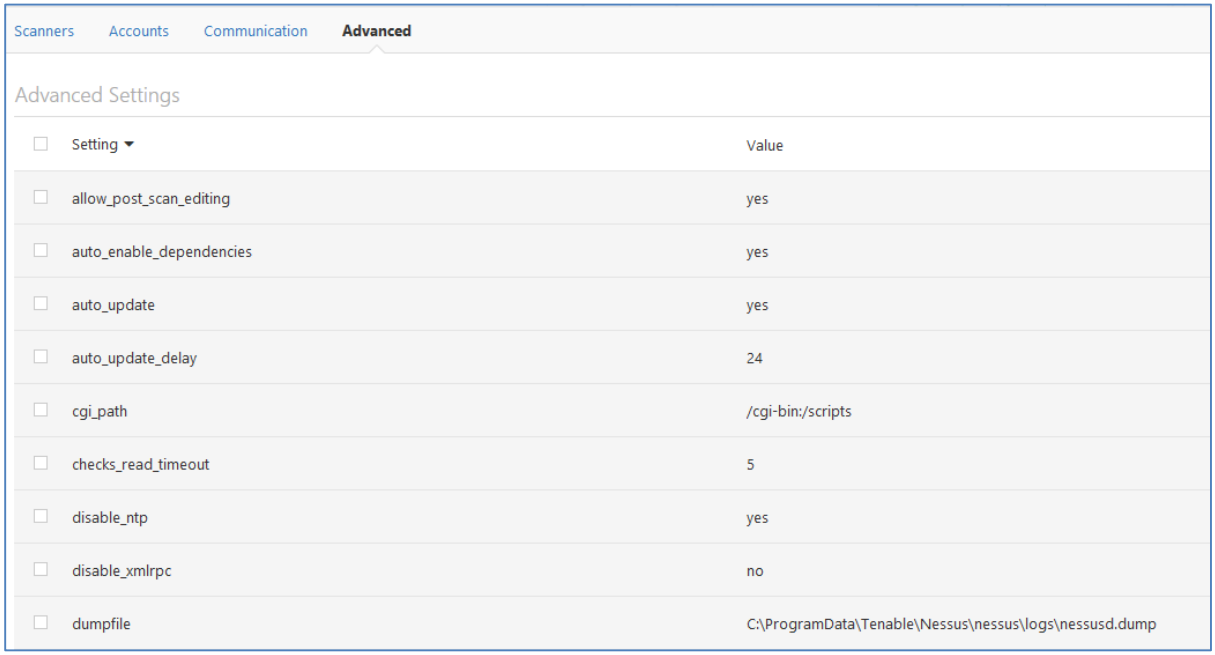
Host	The email server IP or hostname
Port	The email server port number to connect
From	The send email ID (e.g. nessureport@abc.com)
Encryption	Secure the data transfer by using SSL
Host (for email)	The SMTP hostname that will use by Nessus server. Make sure it is up and Nessus can connect with it.
Auth method	Supported methods are: Plain, NTLM, Login and CRAM-MD5 (provide the username and password so that Nessus will send email)

Advance Settings

The performance of the scanner can be controlled and altered using the advance setting. The users having standard access can't change the advance settings, only the system admin can see and configure the settings. Keep in mind that, this setting is for the scanner not for a single scan, so the modifications will affect every individual scan and ever user of this scanner. You can alter the default values and it depends on the nature of your scan; the details of some important options are as follows:

global.max_hosts	The default value is 520, it represents the number hosts to scan
global.max_scans	It represents the parallel scan, zero is the default value
max_checks	The default value is 5 means the maximum number of parallel checks against each hosts
max_hosts	The maximum number to check at one time during the scan.

listen_address	The IP address for incoming connection.
listen_port	The port to listen the incoming connections
cgi_path	While conducting the web application test, get the files from the location
log_whole_attack	If set yes, then the scanner create log of everything. It is good to debug the issues, if you are facing any.
port_range	Define the range of the ports to be scanned. You may use All, Default or even specify the range as 21-99



The advance settings should be used carefully as it impacts the overall performance of the scanner.

Scanning the Environment

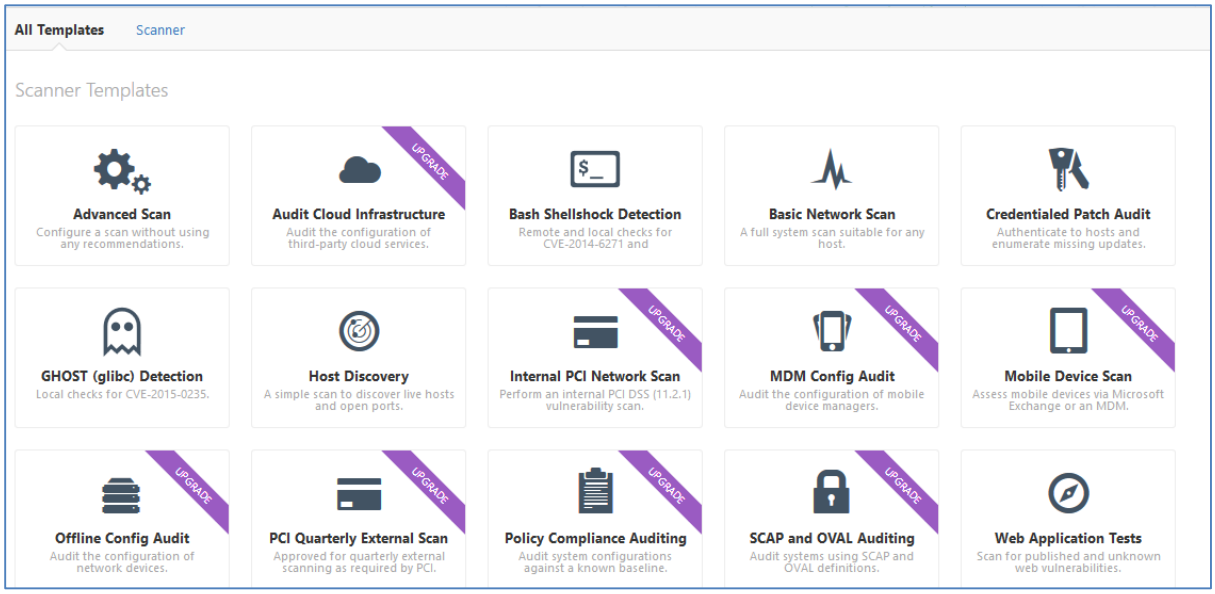
There are many important things to ponder before scanning the environment, as the risks are associated with the benefit. Some questions that you should ask before scanning:

- Do we have all the approval documents in place?
- Do we have the credentials to place in Nessus scanner? This allows Nessus to scan behind the authentication wall.
- Is there any firewall or IDS blocking the traffic? If yes, then alter the rule and direct firewall to allow Nessus incoming and outgoing traffic smoothly
- Do we have the incident handling policies? And what about the backup make sure to keep a backup of the important data.
- What policy should be used? Policy depends on the objective, network type and the overall requirement. Creating the policy will discuss later.

- Have the risks evaluated yet? The network might treat Nessus scan as a DOS (denial of service) attack. Let the authorities sit and discuss the issue with Network lead and let them to provide the enough bandwidth that can cover the scan and alter the IDS rules.
- Network support team should there while you perform the scan, they should continuously monitor the performance of the network and the target systems, let the systems don't get crashed.

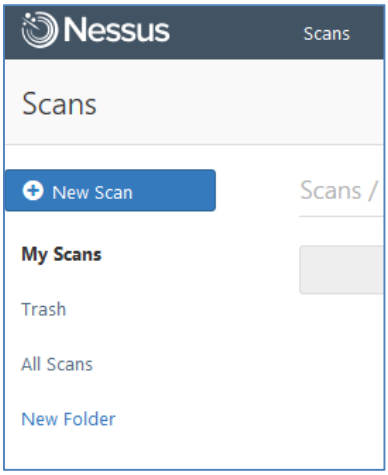
Creating your first policy:

Creating policy is not a choice, but an essential step that you have to do before scanning the environment. Nessus policy configuration means you are telling Nessus to optimize the scanning on the basis of given/defined parameters and those parameters depend on the target network. While defining the policy, you must take care of the system discovery, scanning, vulnerability discovery and the report pattern (how you want Nessus to create the report). Nessus provides the list of pre-defined policies; you can select the policy on the basis of your objective.

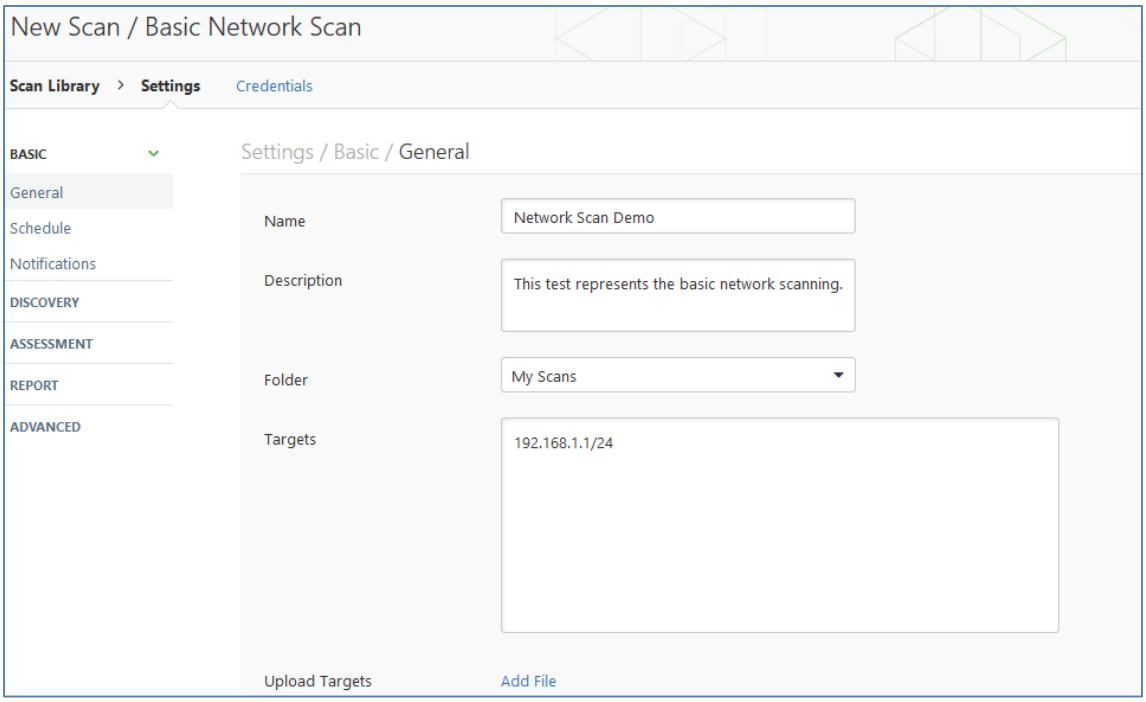


Let say you want Nessus to test the web application, then select the respective policy and same goes with the others.

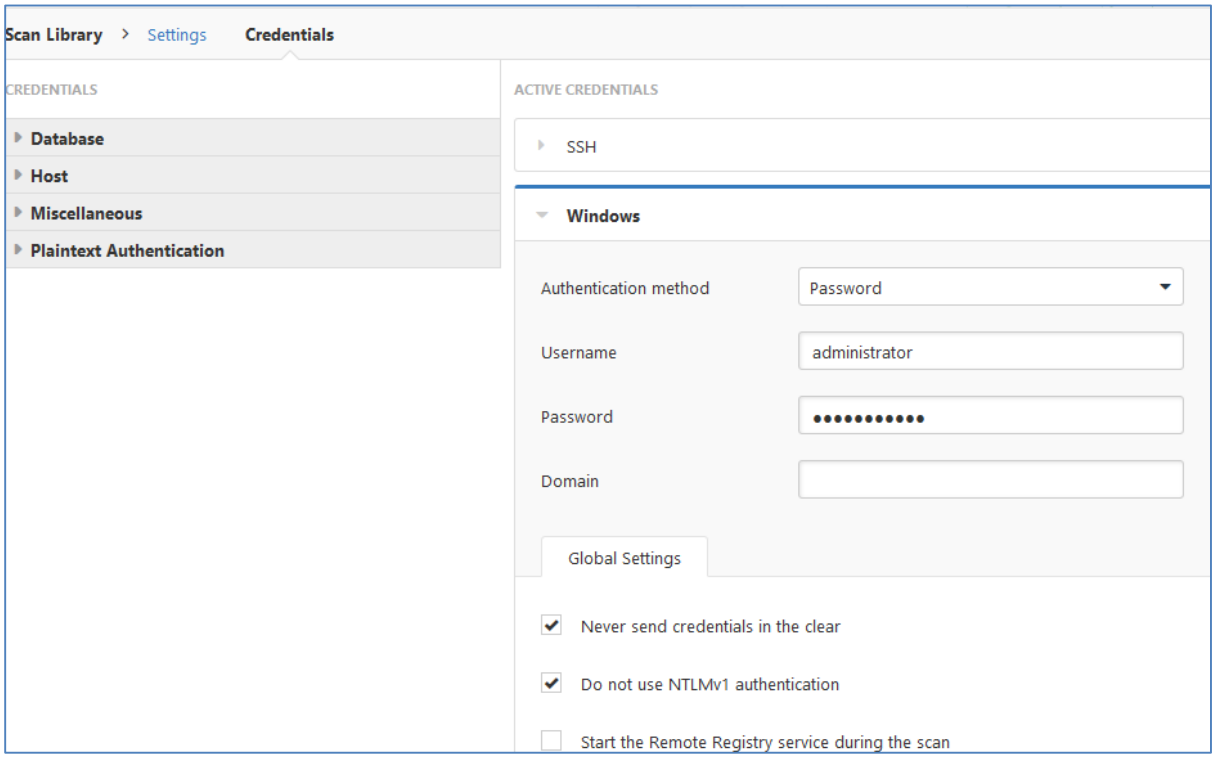
Let's do a basic network scan. Click on the **New Scan** and select the basic network scan policy:



Name	Assign a unique name that reflects the nature, client or objective of this scan.
Description	Write the detail of the scan. For example, Network configuration test for ABC client.
Folder	Multiple folders can be created in the scanner to organize the work process. You can create folders for every client and you can also categorize the folders on the basis of scan types. We will discuss the procedure to create and maintain the folders.
Targets	Put the target IP address, you can also put the range here. E.g. 192.168.1.1-100 or the entire subnet 192.168.1.1/24
Upload targets	The alternate option is to upload the target list (for example you can use nmap to find and locate the live systems and then browse the result file).



The second important factor that you should not forget is the **credentials**. You should provide the necessary credentials before scanning the network. If you want Nessus to scan the machines behind an authentication wall, then you should provide the required credentials, although this is an optional feature. You can add credentials for the Windows, SSH, Databases (MySQL, Oracle and etc.), virtual machines and the ports (FTP, POP3 and etc.):



Once you are done with the credentials, save and launch the scanner.

Creating Your Own Policy:

In the previous topic, the procedure to create the policy using the available templates has been discussed. We will discuss the techniques of reading and understanding the reports, and how to manage the data. But, the foremost objective is to discuss the advance policy and how to create one. Creating your own policy is very important and you should understand the science behind the available templates.

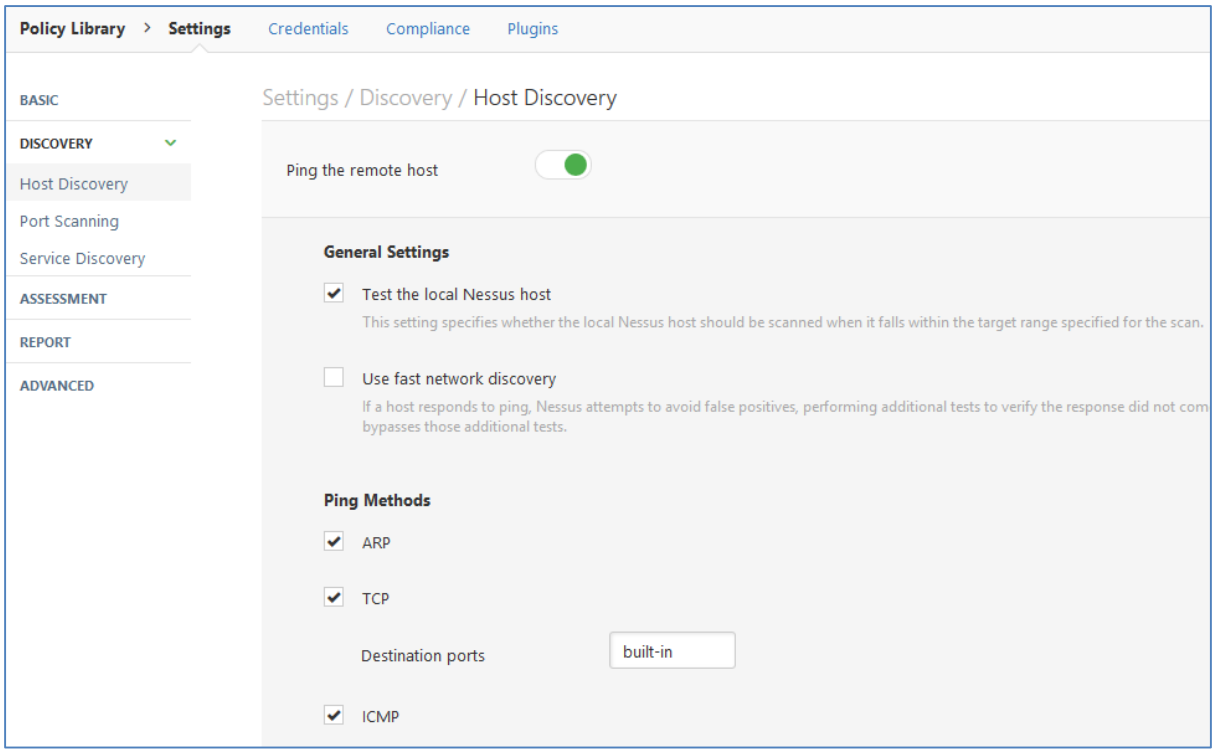
The first step is to give a memorable and unique name to your policy, set permission:

1. The other users can access this policy
2. Only me

Discovery:

How you want Nessus to discover and find the machines associated with the target network, what ports to scan? What protocols to use? And many other factors should setup under the discovery tab. The discovery module has been divided into three parts:

- Host discovery
- Port scanning
- Service discovery



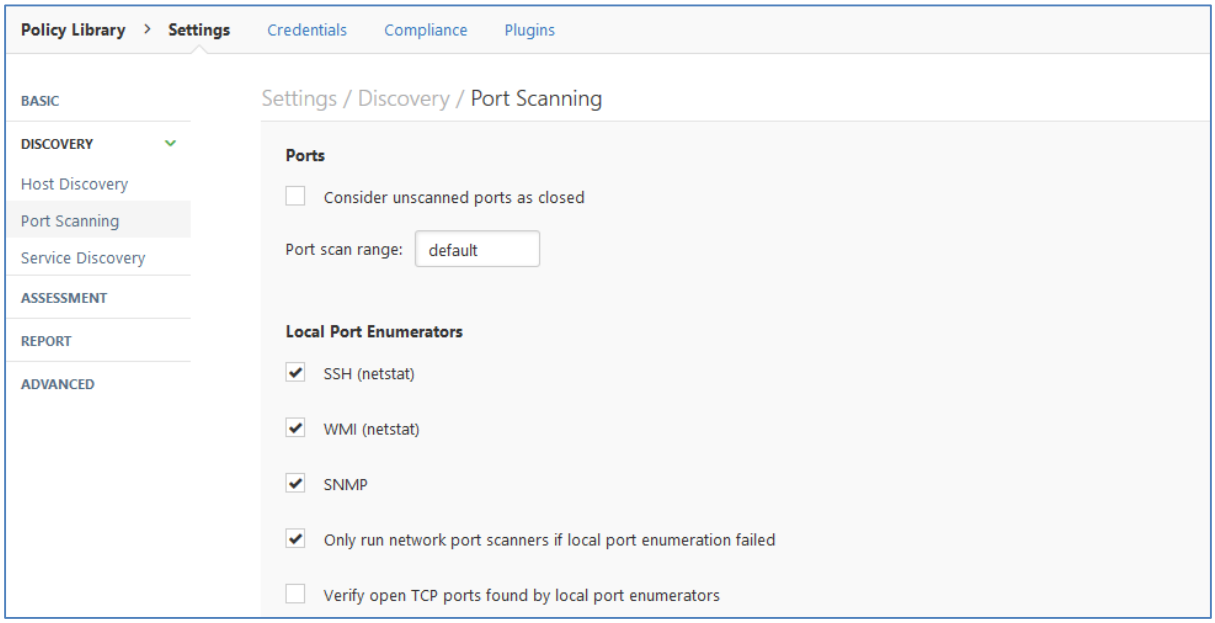
"Ping remote host" gets the information of the live systems. "Test the local Nessus host" if the scanner machine is included in the target range, then whether scanner should scan it or not. If you want Nessus to test the host machine, then select this option. "Fast network discovery" is when you want Nessus to finish the scanning as soon as possible. You might go in the wrong direction, if this option selected, as Nessus will not probe deeply.

There are different ping methods are available. Select "TCP" to let Nessus ping the TCP ports, the specific port numbers can also be defined. For example, the objective is to get the list of machines having port 23 open. If you are not sure about the port numbers, then leave it to built-in. You may use the ICMP to check the machine status. Don't select the "Assume ICMP unreachable from the gateway means the host is down" because firewalls used to filter the specific ports and in return send the ICMP unreachable message. If this option selected, the Nessus will consider the host down, but in actual it might up.

UDP is not the reliable service because it connectionless protocol and sometimes not detectable. You can also upload the list of MAC addresses to scan, and if you want Nessus to scan the associated printers, then select the fragile devices option.

Port Scanning

- **Consider unscanned port as closed:** If Nessus fail to scan any port due to any reason, then Nessus will treat it as close. Other tools such as Nmap can be used to double check the ports.
- **Port range:** The ports that you want to scan. "Default" means, the 4790 common ports listed in Nessus. While "**All"** represents all the 65365 ports to scan. The range of port numbers can also be selected, e.g. 23-400



The port scanning is divided into two portions:

- Local port enumerators
- Network port scanners

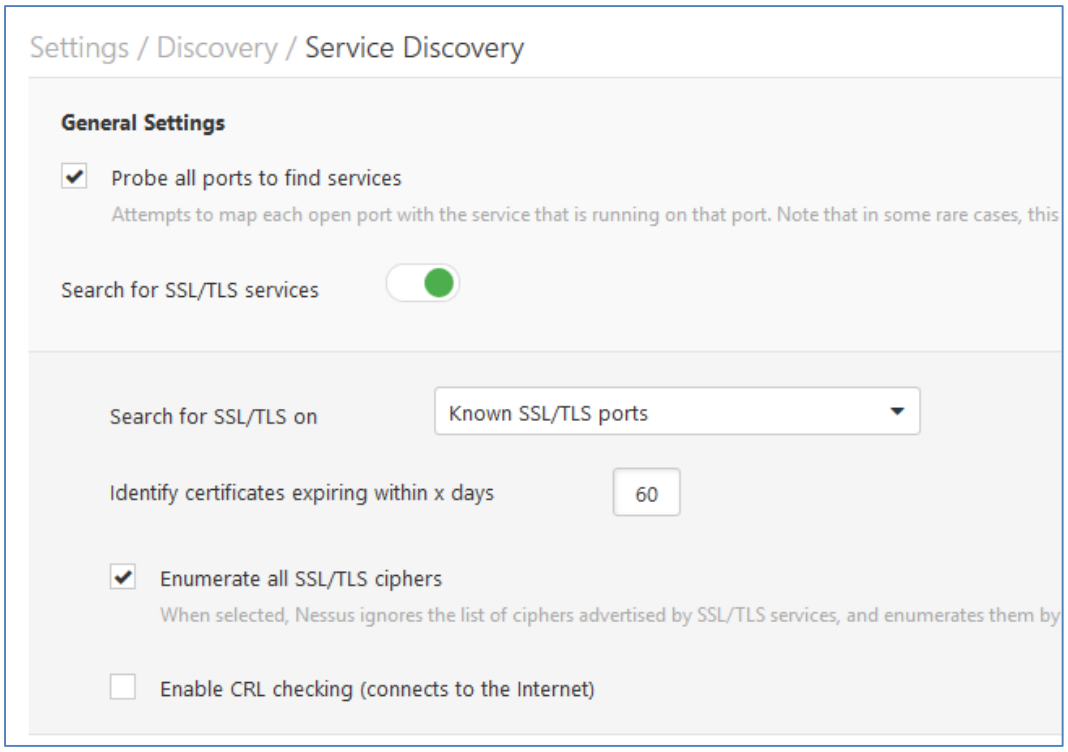
The local port enumerators required credentials to scan. Netstat (SSH) is specifically for Unix-based system and it uses netstat command to find the open ports. Whereas, WMI (netstat) is for windows-based systems and it also requires the credentials to utilize the netstat commands. Simple Network Management Protocol (SNMP) test is very important to test the routers and other networking devices. The version of the device can be predicted by looking at the SNMP reply. Uncheck the option to let the Network port scanner work in parallel with the local port enumerators.

SYN is the recommended approach as it is the part of 3-way handshaking process of TCP. If selected, then the scanner sends the SYN packet to the target and decides upon getting the ACK message from the target machine.

Service Discovery:

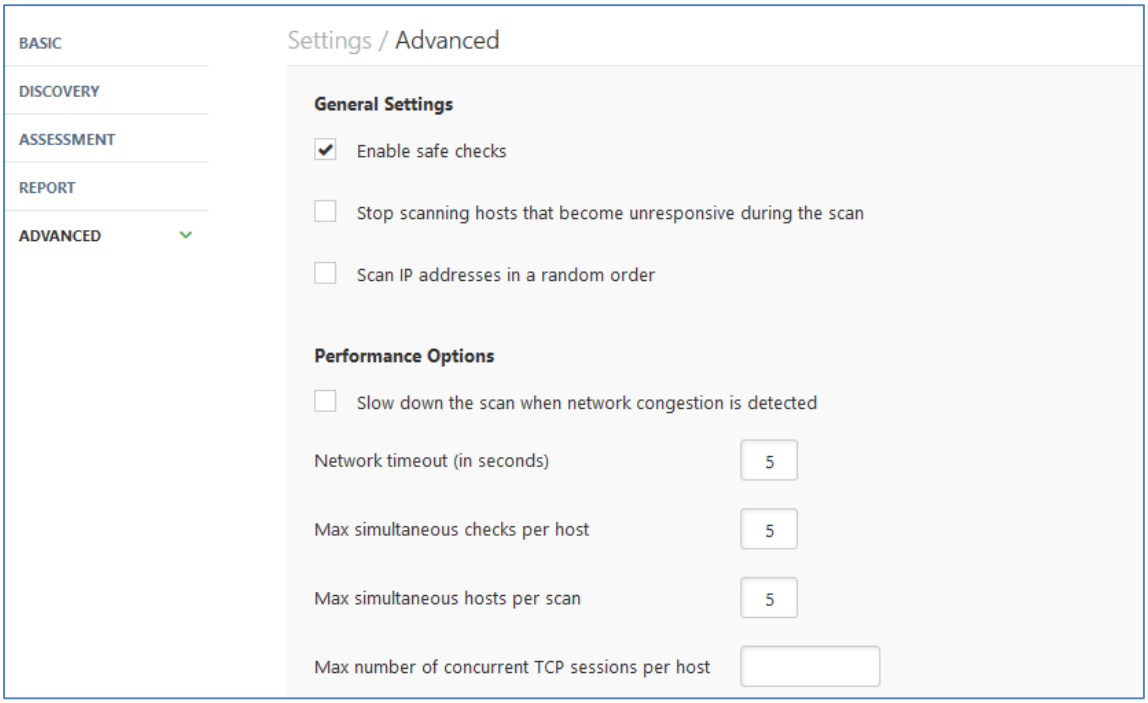
This is where you configure the Nessus setting to find the services associated with port numbers. Probe all ports to find services: if you want Nessus to check every open port and to find the services running on every port.

Search for SSL based services: if selected the know SSL ports, then Nessus will probe the port 443 and if selected all ports, then Nessus will check SSL on every port. Enable CRL checking (connects to the Internet): if selected, then Nessus will check the certificates revocation list



Advanced

The configuration options under the advanced tab provides control of the scanner, it also impacts the performance of the scanner.



Network timeout (in sec)	It depends on your network connection; the default time is 5 seconds. Nessus waits for 5 seconds to get a response from the host
Max simultaneous checks per host	This option allows you to limit the simultaneous against a single target machine at one time.
Max simultaneous hosts per scan	You can limit the number of hosts Nessus scan at one time
Max number of concurrent TCP sessions per host	You can limit the number of TCP sessions against a single machine at one time
Max number of concurrent TCP sessions per scan	Number of TCP sessions established in the scan
Enable safe checks	If selected, then the plugins that may have an adverse effect gets disabled

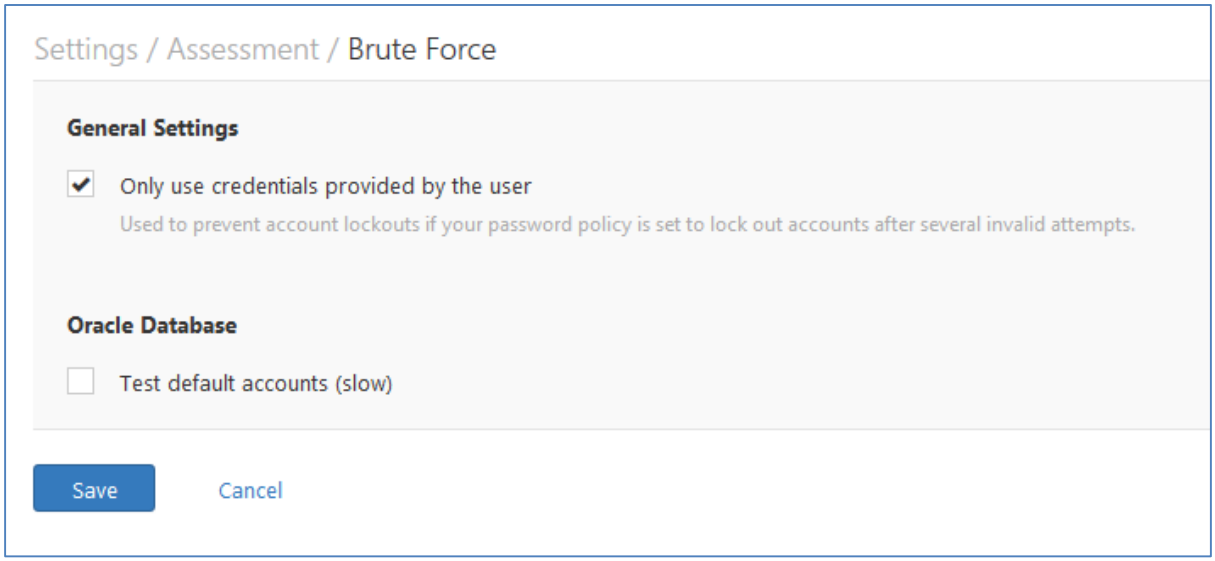
Assessment

Assessment setting is divided into different categories:

- General
- Brute force
- Web applications
- Windows

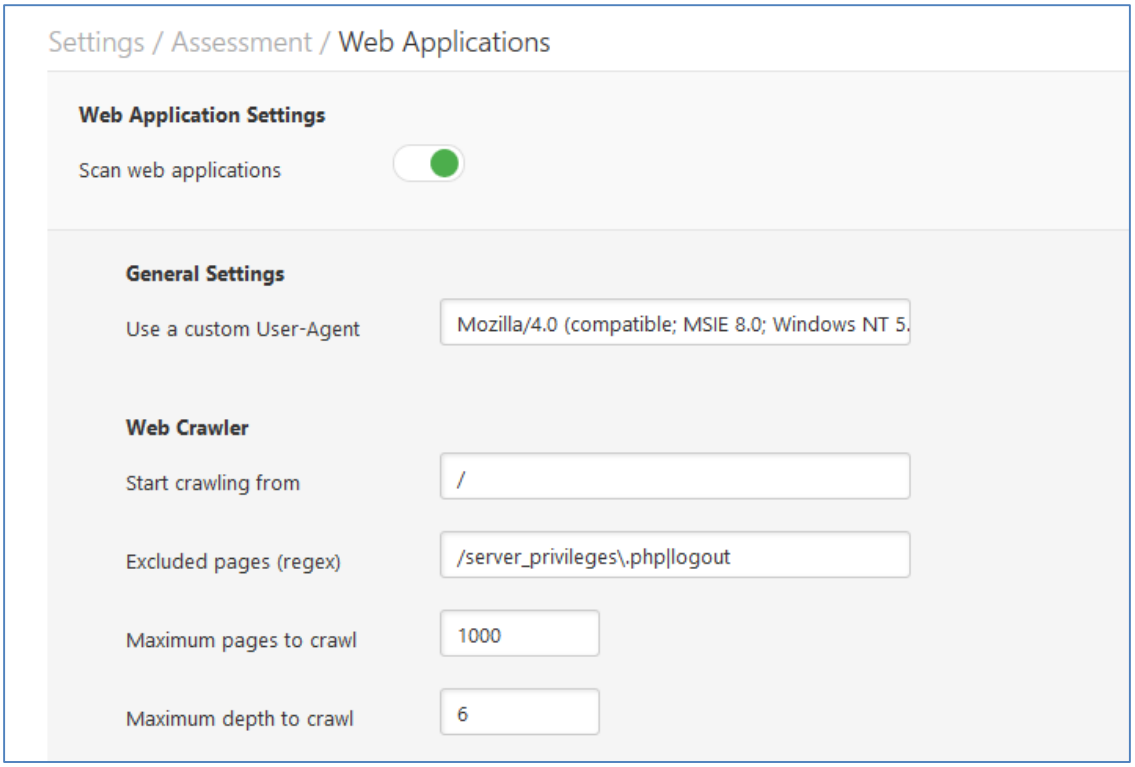
The most important setting under the general tab is about the false positive response. If you want Nessus not to report the vulnerabilities if there is any uncertainty, then select “Avoid potential false

alarms". If the objective is to report every vulnerability, whether you have the strong reason or not, then select the "Show potential false alarms" option.



Select the first option of brute force tab to not let Nessus lock accounts. Nessus will try to login using the provided credentials. And, if you want to test security, then you may select the second option of using the default accounts.

You may enable the web application scanning option, if you want to Nessus to perform the web app test. Many important options to ponder at this moment, if you want to exclude the specific pages, then "Excluded pages (regex)" is the right option.

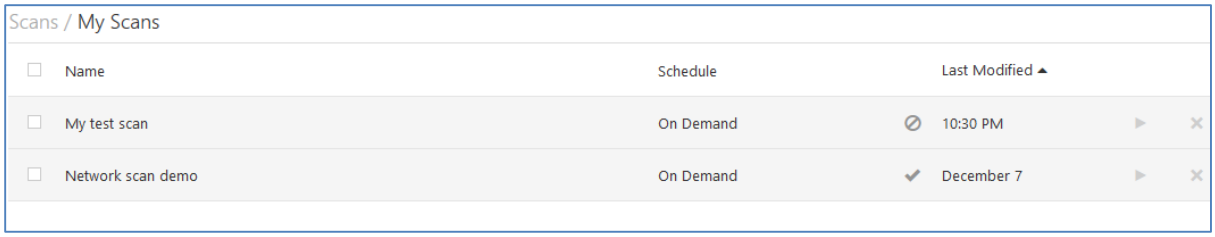


Start crawling from	The default is "/" means the home page. You may specify the other pages using colon operator. ("/:/about")
Maximum pages to crawl	How many maximum pages do you want to crawl?
Maximum depth to crawl	You may limit the crawling depth
Follow dynamically generated pages	Some web app generates dynamic pages, if requested.
Maximum run time (min)	The default is 5. The maximum time allows spending on each individual attacking vector or test.

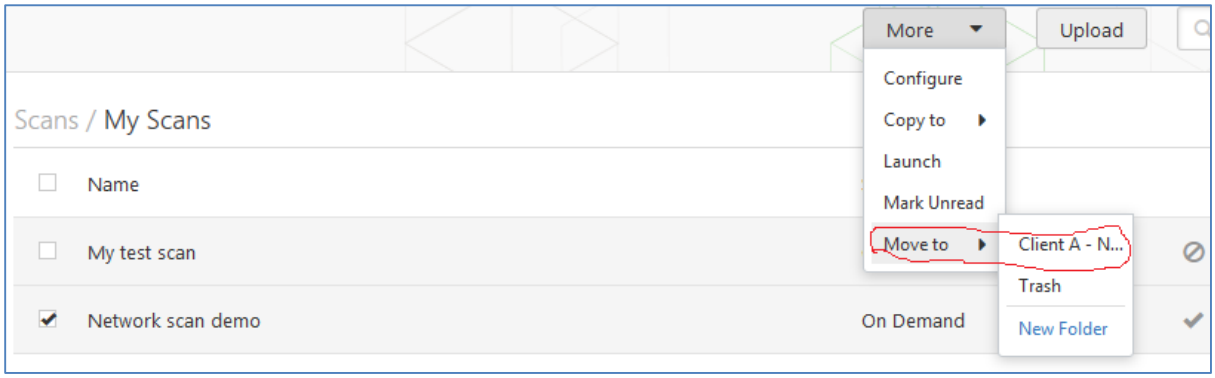
Under the **Windows** option tab, you can configure the domain user's enumeration values. Configure the UID values for reverse domain lookup. If you have a list of bad MD5 hashes, then you can upload it and tell Nessus to treat the match as malware. If you want Nessus to avoid checks on specific hosts during the test, then upload the whitelist host file.

Scan Result Analysis:

Analyzing the scan report is the crucial part of vulnerability assessment; you should understand the false positive and negative responses, and the procedure to create an effective vulnerability assessment report. Nessus gives you an opportunity to download the scan report. But, creating your own report based on the findings is the recommended approach as you should know the audience of your report and then, act accordingly.



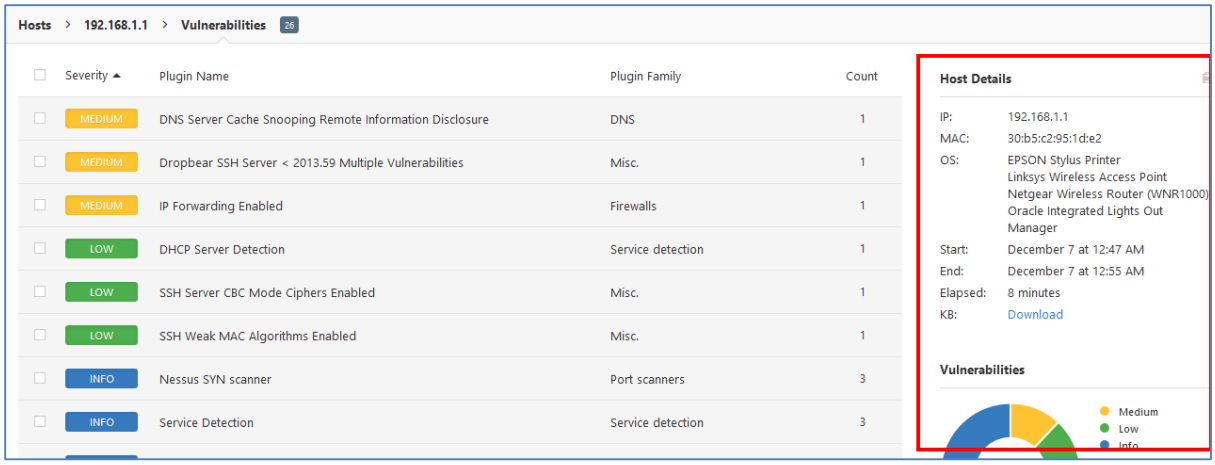
Click on the completed scan to analyze the results. You can also create folders to organize the scan reports, click on New Folder and give a unique name to this folder. Select the scan that you want to move and click “More” button to copy or move this scan to another folder.



Nessus categorized the vulnerabilities into 5 different parts (from low to high):

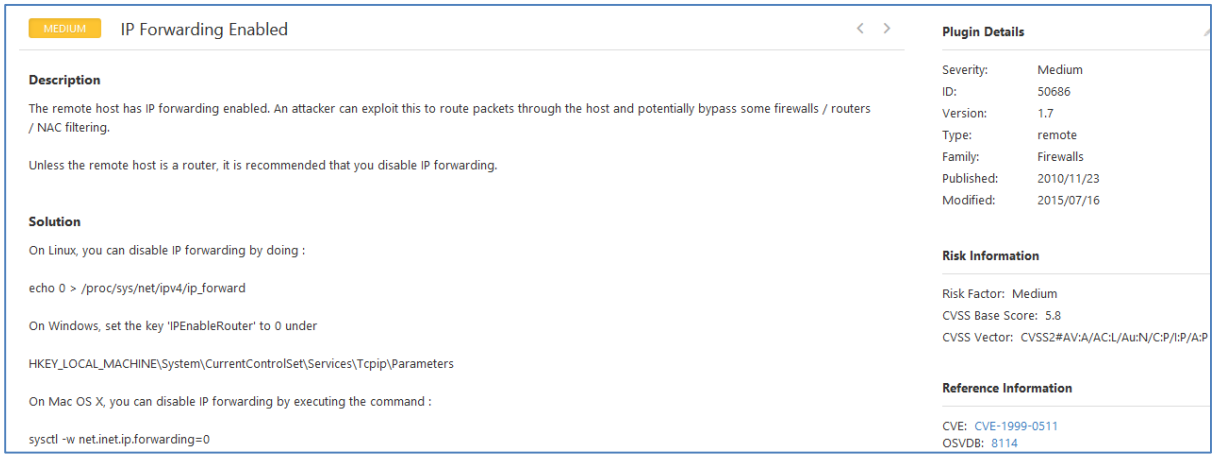
- Info
- Low
- Medium
- High
- Critical

Nessus organize the report by listing host and vulnerabilities. It also provides the scan details (when started, the elapsed time, nature of scan, policy selected and etc.). It also provides the detail information of the scanned host; you will see the OS information, IP and MAC addresses, the found vulnerabilities and their detail. KB or knowledge base is the raw text file that contains the information about what exactly Nessus did to find the said information. You can download this file and it can be used as logs and while troubleshooting the issues.



Click on the vulnerability to see the details:

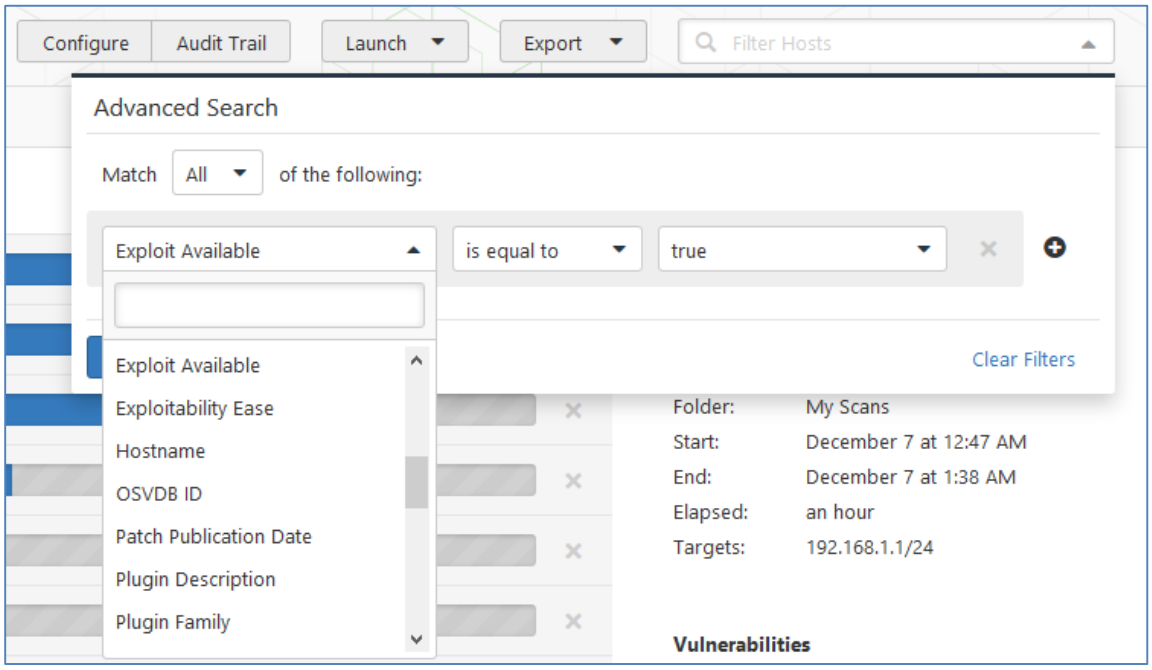
- Description
- Possible solution
- Risk information (CVSS score, risk factor)
- Reference information (CVE and OSVDB details)
- Output information (port number and etc.)
- Software/solution that can exploit the vulnerability
- External references (blog post and published articles)



Nessus has a very intelligent filter. You can filter the results based on so many factors, but the most important are:

- Exploit available
- CVE number
- Port number
- OSVDB ID

- And many more.

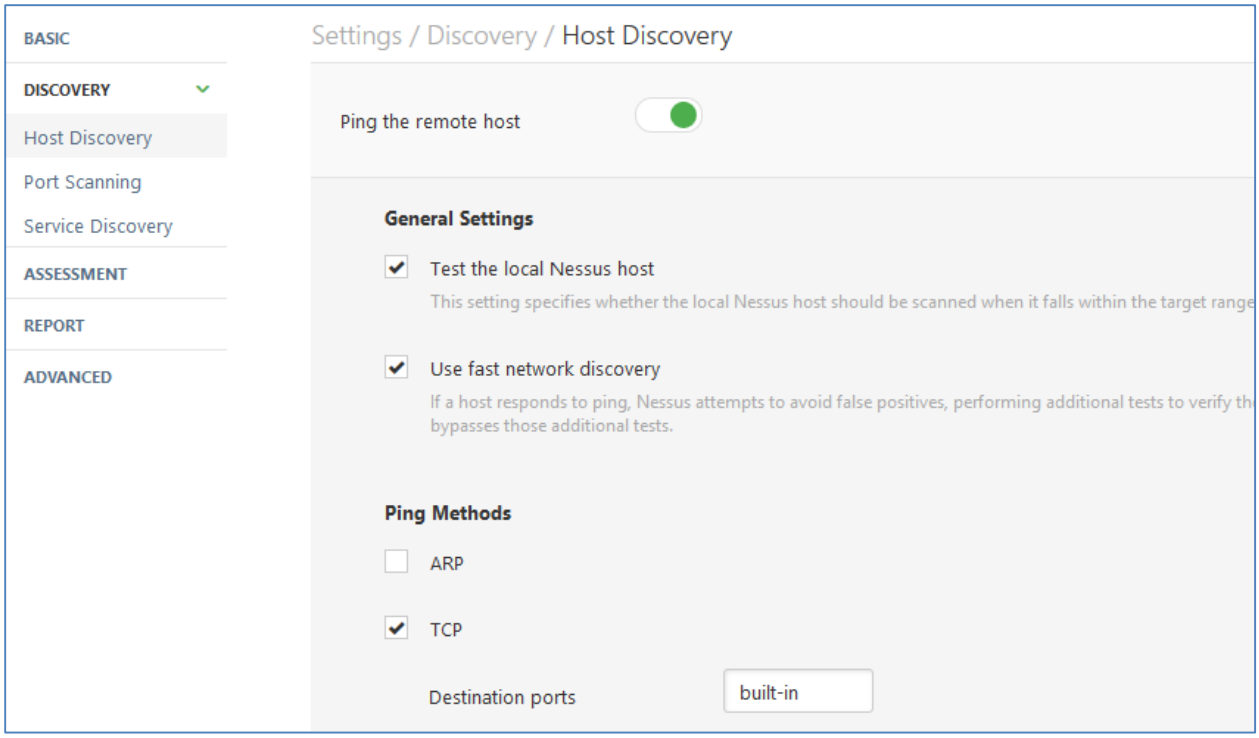


You can see the following options right side of the filter bar:

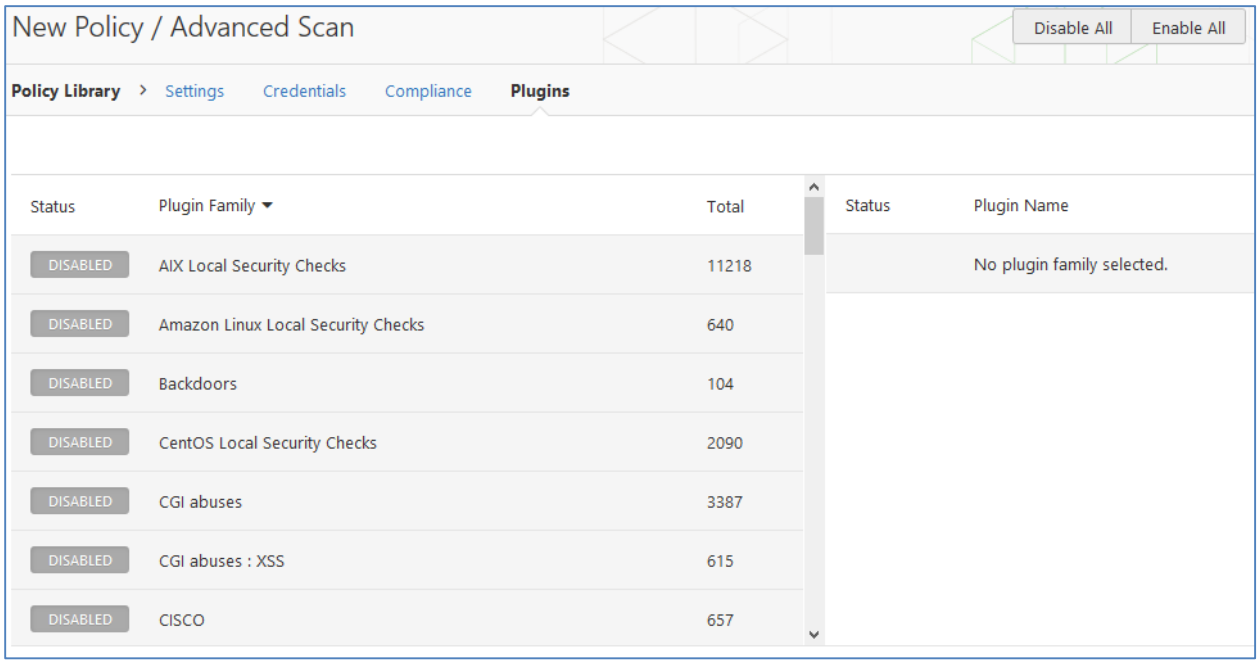
Configure	If you want to reconfigure the scan
Audit Trail	You can see the performance of every individual plugin against the specific host. This option allows you to audit the performance of a plugin
Launch	You can re-launch the scan
Export	The report can be exported (PDF, HTML, CSV and Nessus format)

Web Application Scan Policy

In this section, we will see the necessities to create an effective web application scan policy. In the very first step, click on **Web Application Tests** from the policy library; provide the basic information such as name and description. In the "host discovery" select the ping and TCP scanner; uncheck the ARP and other option (we need to get the information of the live systems only).



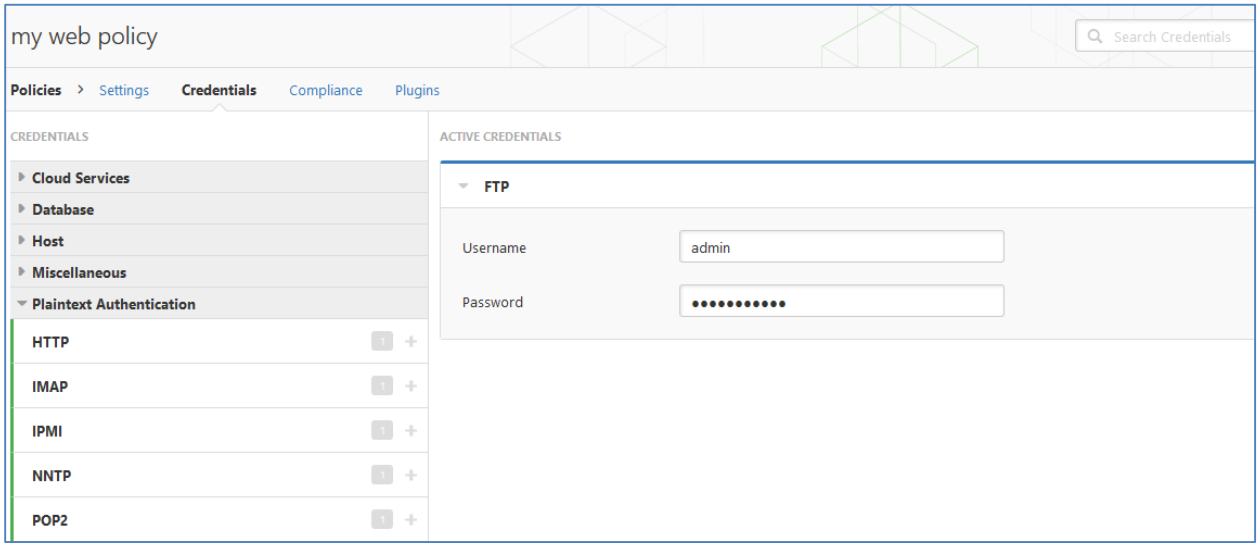
Put the “default” in the “port scanning” tab to scan the all common ports listed in the Nessus configuration. In the plugins tab, disable all the plugins to enable only the required plugins.



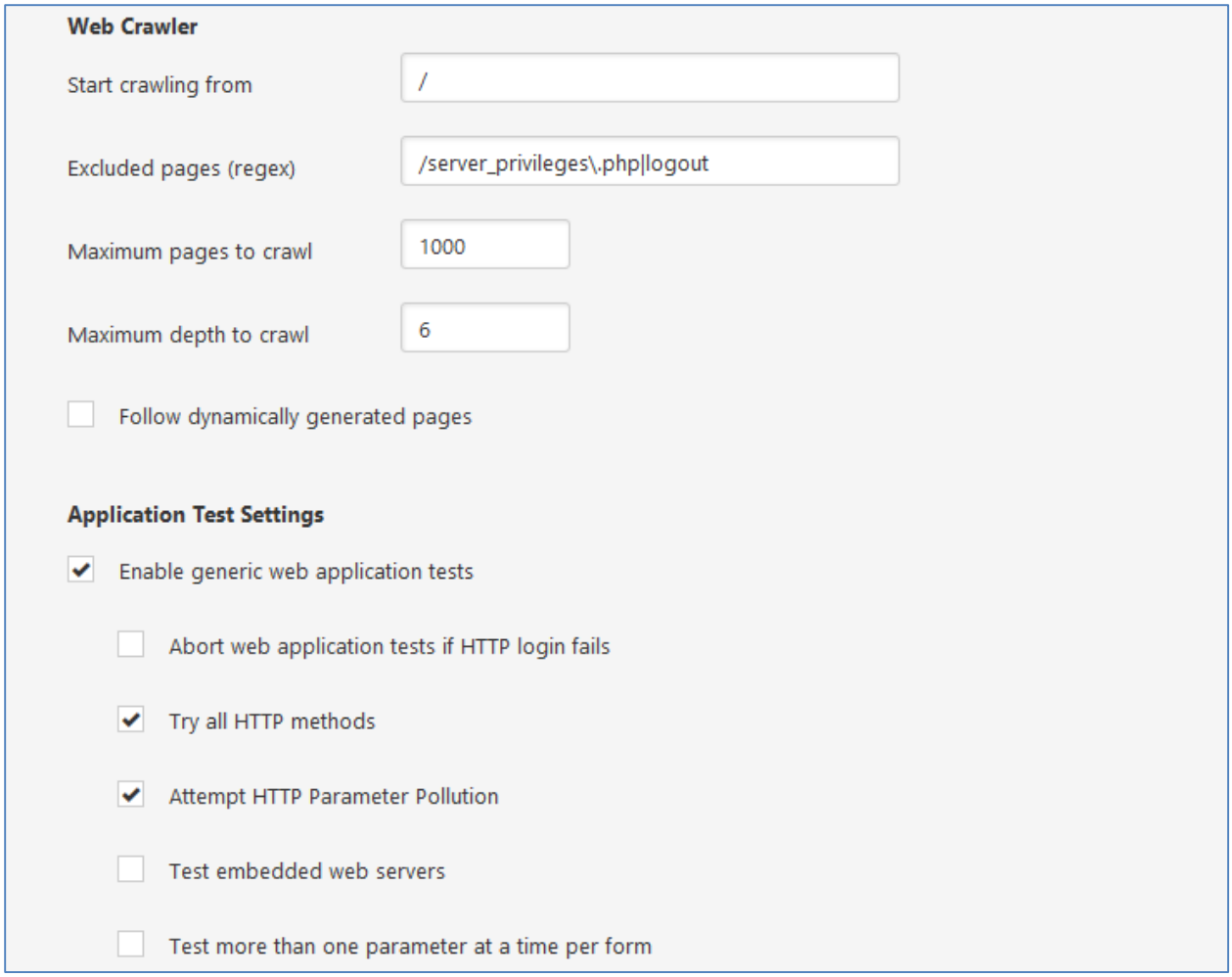
Manually enable the following plugins:

CGI abuses	CGI abuses: XSS	FTP	Firewalls
SMTP problems	SNMP	Gain a shell remotely	Databases
General	Settings	Web server	Windows

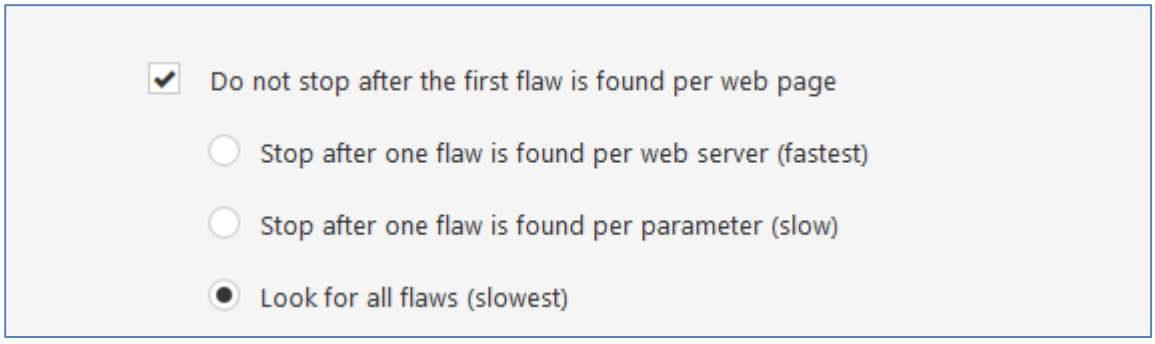
Check “Prob all ports to find service” under service discovery tab. Under the credentials tab, provide the credentials to authenticate the services, brute force attack can also be selected in the “assessment” tab; it depends on the objective.



Make sure to enable “Web application settings” under assessment tab. To test the web application, enable the “generic web application tests”, select “Try all HTTP methods” which includes banner grabbing too.



Do not let the scanner stop after the first flaw is found, make sure to select “look for all flaws”; it takes time but this is the most effective way to find all the vulnerabilities of a web page.



Save your policy and now it is ready to scan. Create a new scan and use the created policy.

Importing the Result in Metasploit

Nessus result can be imported in Metasploit. All you need to do is to export the report from Nessus and on Metasploit use the db_import command:

```
db_import Nessus_report.nessus
```

```
Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.4-2015071403                   ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post        ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > db_status
[*] postgresql connected to msf
msf > db_import Network_scan_demo_tqub3p.nessus
```

You can see the list of hosts, their OS and other basic information by using the hosts command:

```
msf > hosts

Hosts
=====

address         mac               name          os_name                os_flavor  os_sp  purpose  i
fo  comments
-------         ---               ----          -------                ---------  -----  -------
--  --------
192.168.1.1     30:B5:C2:95:1D:E2 192.168.1.1   EPSON Stylus Printer                     printer
192.168.1.100   00:23:CD:CF:BC:2E 192.168.1.100 VxWorks                                  device
192.168.1.105   C8:A8:23:3C:FD:F9 192.168.1.105
192.168.1.107   00:EE:BD:92:CF:80 192.168.1.107
192.168.1.108   34:23:BA:65:86:DE 192.168.1.108
192.168.1.110   F8:A9:D0:63:CE:2A 192.168.1.110
```

You can see the open ports, the services and status by using the services command:

```
msf > services 192.168.1.1

Services
========

host          port  proto  name  state  info
----          ----  -----  ----  -----  ----
192.168.1.1   22    tcp    ssh   open
192.168.1.1   53    udp    dns   open
192.168.1.1   67    udp          open
192.168.1.1   80    tcp    www   open
192.168.1.1   1900  tcp    www   open
```

The list of found vulnerabilities can be search and use to exploit the system/network:

```
msf > search cve:2010-2075

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  UnrealIRCD 3.2.8.1 B
or Command Execution
```

To load any specific exploit:

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Once the vulnerability loaded, you can exploit:

```
msf exploit(unreal_ircd_3281_backdoor) > info

       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
  Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Provided by:
  hdm <hdm@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target
```

End Note:

The end of this mini course is the beginning of your practice. Reading the eBook is not enough; reading might give you immense information and knowledge. But, it can't train you to act practically. Vulnerability assessment & penetration testing is the job that requires practical experience, the more you do; more you understand the systems, issues and the possible solutions. Your scenario might different than what discussed in the eBook, you should follow the said assessment process and approach, but make little tweaks where required, as it all depends on the circumstances.

Undoubtedly, Nessus is the renowned and an effective vulnerability assessment scanner. But, other scanners are also competing in the market, and I recommend you to explore. After reading this eBook, you can explore the other scanners, as the basic foundation and work process of every scanner are same (more or less).

Best of luck for your practice.