Lab 9: Pen Testing (NESSUS)

Aim:

To provide a foundation in using NESSUS for vulnerability scanning.

Time to complete: Up to 90 minutes.

Activities:

- **Complete Lab 9**: Introduction to NESSUS.
- **Complete Test 9**.

Leaning Activities:

At the end of these activities, you should understand:

- How to use NESSUS for scans.
- How to follow through with a vulnerability.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- How often do you think you would want to run a vulnerability scan on a corporate Web site?
- Is just running NESSUS and looking at the results enough for vulnerability scanning?
- How often do you think an IT Administrator should patch servers?

Lab 8: Pen Testing (NESSUS)

1 Details

Aim: To provide a foundation in a Pen Testing using NESSUS.

2 Activities

L1.1 From your Windows 2003 virtual image, run NESSUS from Start->Programs->Tennable Network Security->Web Client. Login with a username of **bill** and a password of **bill**.

L1.2 **Create a new policy.** From NESSUS, go to the **Policy** tab and select **Create a new policy**. Next select a **Port Scan policy**. Next select a **Basic** setting type, enter a name of your test as **My Scan** (Figure 1). Next go to the Plugs-In tab and **Disable all**. Save your new policy.

L1.3 **Create a template.** From NESSUS, go to the **Template** tab and select **New scan**. Next give the scan template a name and select your scan policy you just created (Figure 2). Final enter the IP address for your Ubuntu host, and then select the scan type of **Run Now**. Click on Create Scan and it should now scan the Ubuntu host.

L1.4 **Analyse results of Ubuntu.** From NESSUS, go to the **Results** tab and wait for the scan to complete.

Outline the ports that are open on the Ubuntu:

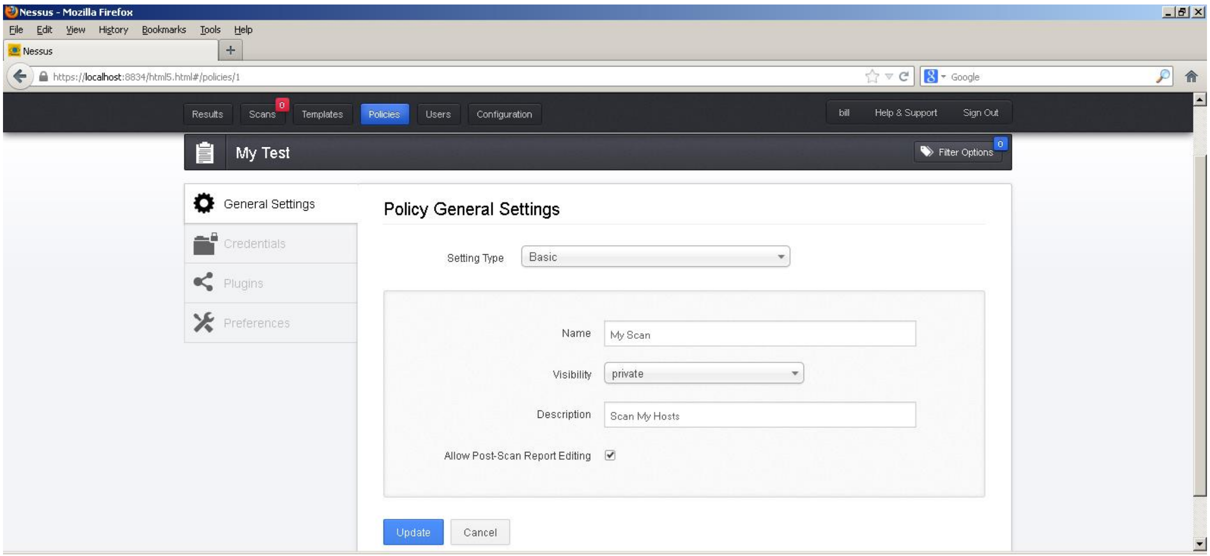
L1.5 **Analyse results of Windows 2003.** Perform the same steps as previously but this time use the IP address of the Window 20003 virtual image. In this case we are scanning the local machine that has the scanner on it.

Outline the ports that are open on the Windows 2003:

L1.6 **Analyse results of Metasploitable.** Perform the same task for the Metasploitable image.

Outline the ports that are open on the Metaspoitable image:

What can you observe from the Metaspoitable image and why would you not run this image on a real network:



Setting Type: Basic

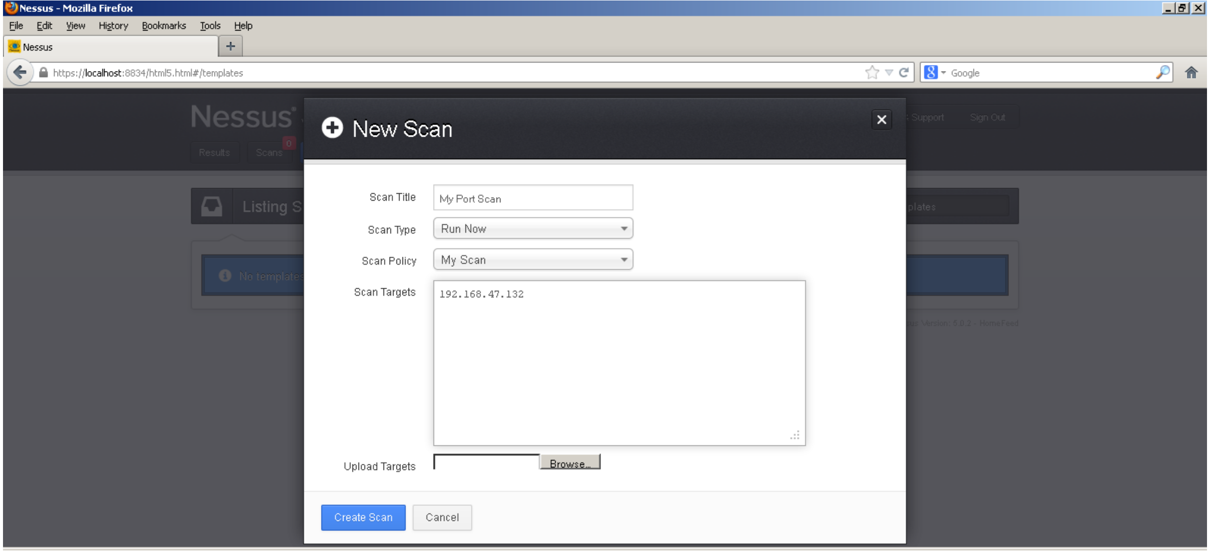
Name: My Scan

Visibility: private

Description: Scan My Hosts

Allow Post-Scan Report Editing ☑

Figure 1:


Nessus - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Nessus
https://localhost:8834/html5.html#/templates
Nessus
New Scan
Upload Targets
Browse...
Create Scan
Cancel

Scan Title: My Port Scan

Scan Type: Run Now

Scan Policy: My Scan

Scan Targets: 192.168.47.132

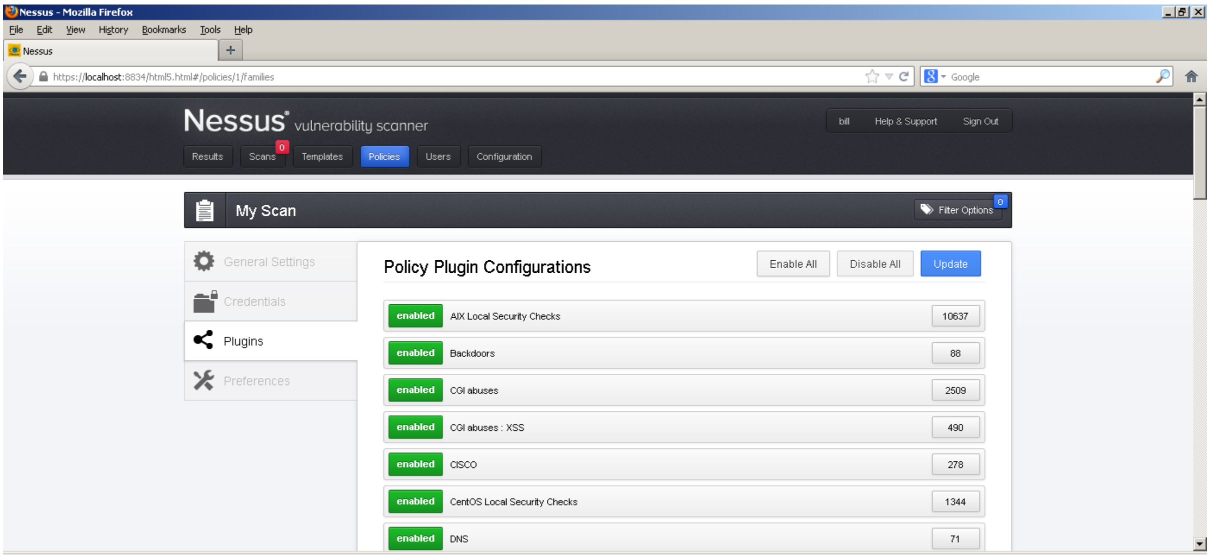
Figure 2:

L1.7 Now go back and create a policy which has the following plug-ins enabled and rescan each machine (Figure 3):

How many critical, medium and low level vulnerabilities are there on Ubuntu:

How many critical, medium and low level vulnerabilities are there on Windows 2003:

How many critical, medium and low level vulnerabilities are there on Metaspoitable:



My Scan

Policy Plugin Configurations

enabled	AIX Local Security Checks	10637
enabled	Backdoors	88
enabled	CGI abuses	2509
enabled	CGI abuses : XSS	490
enabled	CISCO	278
enabled	CentOS Local Security Checks	1344
enabled	DNS	71

Figure 3:

L1.8 For each scan has NESSUS determined the correct operating system:

Operating systems identified:

L1.9 The Metasploitable image has an Anonymous login for FTP vulnerability. Go ahead and see if you can log into its FTP server with an Anonymous login. You can do this by either using the command line option of:

telnet [Metasploitable IP] 21

and enter the commands to login, or you can download an FTP client and connect.

L1.10 The Metasploitable image has a critical VNC vulnerability. Go ahead and see if you can exploit this vulnerability (do this by downloading a VNC client for your Windows 2003 instance).

L1.11 The Metasploitable image has vulnerably on the Web server. Access the Web server on the image by opening a browser on the Windows 2003 host and enter the IP address.

Outline some of the technical information you can gain from the site:

There is a file phpinfo.php on the site. What information does this file release to an intruder:

L1.12 The Metasploitable image has the vulnerability of **rsh Unauthenticated Access (via finger Information)**. Go ahead and try and exploit this vulnerability.

Information on the steps you have taken:

L1.13 The Metasploitable image has a number of folders that can be viewed from the standard user account. Go ahead and see which folders are viewable from Windows 2003.

Information on the steps you have taken:

L1.14 The Metasploitable image has a shared folder which can be viewable (/doc). Go ahead and see if you can exploit this vulnerability.

Information on the steps you have taken:

3 Patching

L1.15 For the vulnerabilities defined for the Windows 2003 host. Investigate the information on the vulnerabilities, and see if you can fix some of them.

Metasploitable Image
(Username: user, Password: user OR Username: msfadmin, Password: msfadmin).