

ETHICAL HACKING

LAB: VULNERABILITY IDENTIFICATION

LEARNING OBJECTIVES

- Understand vulnerability Identification with Nessus tool
-

The 10 First Principles Covered by Lesson 4

- Data\Information Hiding
- Resource Encapsulation
- Straightforwardness
- Domain separation
- Process separation

LEARNING CONTENT

For this lab we'll be using Nessus to do vulnerability identification. Nessus is one of the top vulnerability identifications. Nessus is one of the top vulnerability scanners in existence. Nessus has a very robust set of plugins. These plugins are basically instructions and signatures that it uses to check for a specific vulnerability. We'll be scanning 2012 Windows Server VM using Nessus.

Virtual Machines Needed: Windows 2012 Windows Server VM, Linux Attack server (Kali) VM.

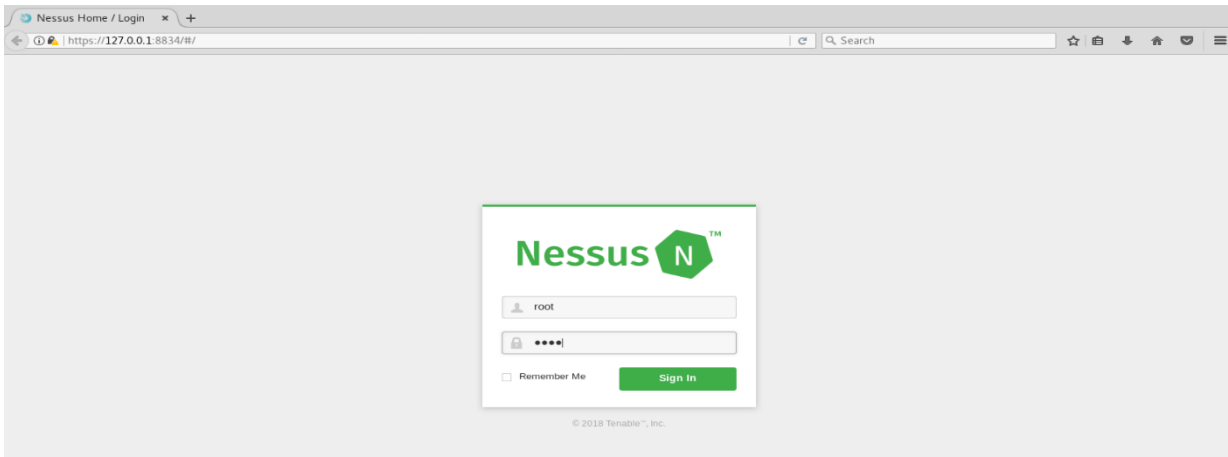
Scan vulnerability test on Windows Server 2012

Enter following URL on your web browser to login Nessus web interface for vulnerability scan <https://127.0.0.1:8834>

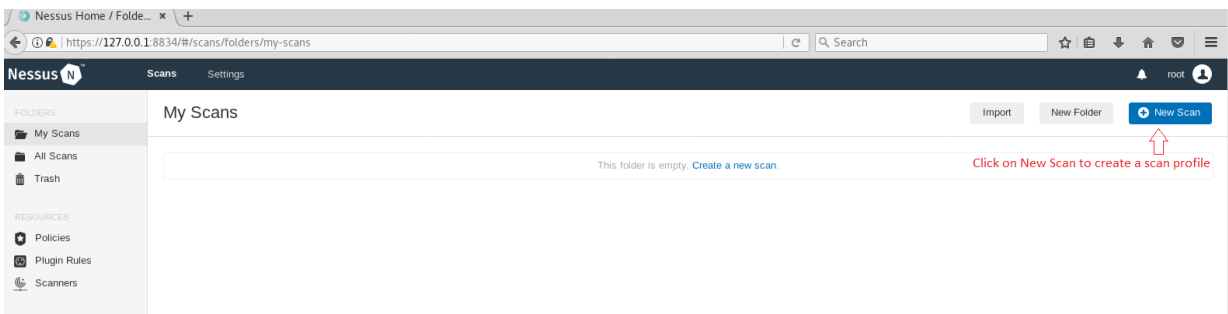
Username: root

Password: toor

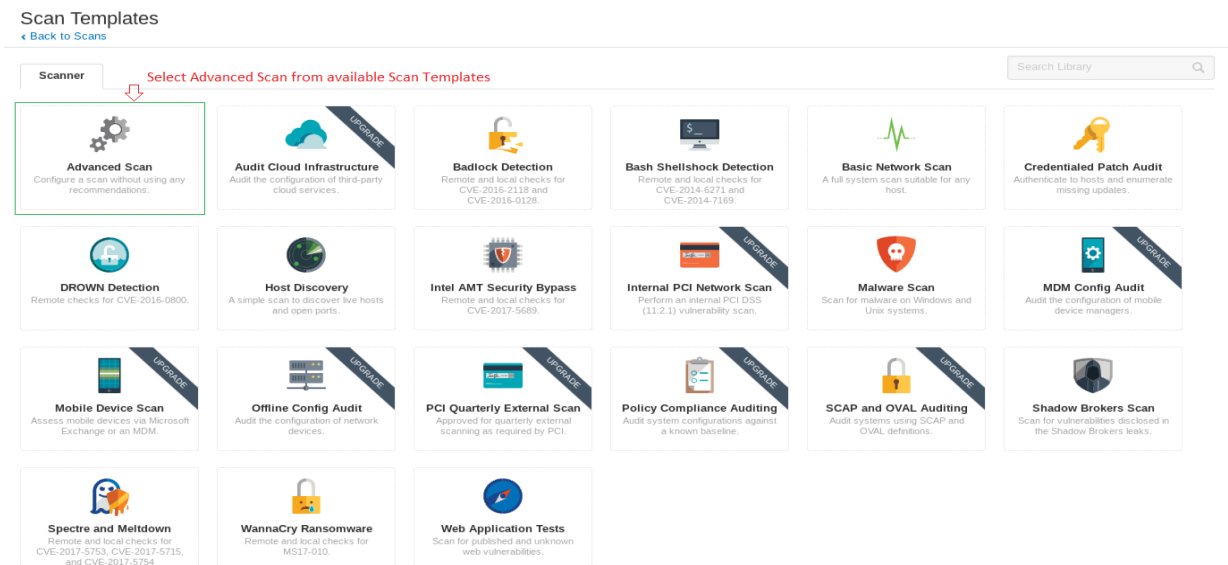




You're now at the default "My Scans" page. Next, you'll need to create a scan profile in order to run a scan with Nessus.



Number of Scanner option will be show on scan templates screen select Advanced Scan. It will lead you to scan configuration screen.



Fill out the information under General BASIC settings. Name your scan profile, add description, define the Target host machine IP Address. After adding the desired field under General Basic setting click on Plugins tab at the top.

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings | Credentials | Compliance | Plugins

BASIC ▾

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Test ← Name the scan profile name

Description: Windows server 2012 Vulnerability scan ← Add description for further detail

Folder: My Scans ← Select Folder from drop down menu. Select My Scans as default value.

Targets: 192.168.180.133 ← List the target host machine IP Address

Upload Targets [Add File](#)

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

If you scroll through this list of plugins, you'll see that it is quite the list. Since we'll only be scanning our 2012 Active Directory VM here, we won't need to do all the scan such as Linux, etc. At the top right corner of your screen you'll see the Filter search bar we can search the "Filter Plugin Families". Simply type Windows on that search bar. A filter result will appear as show below.

Scans | Settings | Filter: windows | root

New Scan / Advanced Scan ← Back to Scan Templates Enter Plugin Keyword Disable All Enable All

Settings | Credentials | Compliance | **Plugins** Show Enabled | Show All

STATUS	PLUGIN FAMILY	TOTAL
ENABLED	Windows	3940
ENABLED	Windows : Microsoft Bulletins	1437
ENABLED	Windows : User management	28

Available Plugins Results ↑

As we can see we only see three plugins. You'll now want to click the enabled button on all but the three Windows plugins we see now and the Web Servers



plugins. By clicking the enabled button you'll see that it toggles to Disabled. When you're done your selection should look like mine. See below.

New Scan / Advanced Scan Disable All Enable All

[Back to Scan Templates](#) Show Enabled | Show All

Settings **Credentials** Compliance **Plugins**

STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	Windows	3940	No plugin family selected.		
DISABLED	Windows : Microsoft Bulletins	1437			
DISABLED	Windows : User management	28			

↑ Status of plugins after Enabling

↓ Click on save button to save your can profile settings.

Save Cancel

Now click the blue Save button on bottom Left corner of your plugin setting screen. You'll see a quick flash showing the successful saving of you new policy and returns to My Scans home screen. You will now see your new policy profile with On Demand schedule to run the scan and N/A ui ▶ Last Modified indicating no scan has been performed along with small grey paly button to launch the scan.

My Scans Import New Folder New Scan

Search Scans 1 Scan

Name	Schedule	Last Modified
Test	On Demand	N/A click to launch scan ➡ ▶

Now go ahead and select the Launch button at the right side of your new policy profile. You should notice that the green activity icon is now spinning. This means the scan is currently running.

My Scans Import New Folder New Scan

Search Scans 1 Scan

Name	Schedule	Last Modified
Test	On Demand	Scan in progress ➡ ⏳ Today at 9:10 PM

A small grey tick arrow will appear once the scan is completed within the profile with time stamp.



Name	Schedule	Status	Last Modified
Test	On Demand	Completed	Today at 9:18 PM

Click on your new policy profile to see vulnerabilities scan results.

Test Configure Audit Trail Launch Export

← Back to My Scans

Hosts 1 Vulnerabilities 23 History 1


Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.180.133	28

Scan Details

Name: Test
 Status: Completed
 Policy: Advanced Scan
 Scanner: Local Scanner
 Start: Today at 9:09 PM
 End: Today at 9:18 PM
 Elapsed: 8 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Select Vulnerabilities tab on top to list the details. If you'll notice in the results we see one HIGH; Multiple Vendor DNS Query ID Field Prediction Cache Poisoning two MEDIUM; SMB Signing Disabled, Unencrypted Telnet Server. The rest of the results are classed as informational only. Let's drill down into the High one. Do this by selecting the "HIGH" vulnerabilities. Read the description for the vulnerability. Also notice towards the bottom there is a link to read more. Go ahead and note this vulnerability, our job as penetration tester would be to validate that these vulnerabilities exist though exploitation. In truth, you should know that Nessus can only find published vulnerabilities. Not zero-day vulnerabilities, or more aptly, vulnerabilities which have not been disclosed to the general public or source software vendors. If time allows, feel free to run Nessus again any of your other virtual machines. You can close out of Nessus when you're done.

Test

[Back to My Scans](#)

[Configure](#) [Audit Trail](#) [Launch](#) [Export](#)

Hosts 1 Vulnerabilities 23 History 1

Filter Search Vulnerabilities 23 Vulnerabilities

select vulnerabilities tab to list the scan results.

Sev	Name	Family	Count
HIGH	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1
MEDIUM	SMB Signing Disabled	Misc.	1
MEDIUM	Unencrypted Telnet Server	Misc.	1
INFO	Nessus SYN scanner	Port scanners	6
INFO	Service Detection	Service detection	3
INFO	DNS Server Detection	DNS	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1

Severity Level

Select the vulnerabilities to see details.

Scan Details

Name: Test
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Start: Today at 9:09 PM
End: Today at 9:18 PM
Elapsed: 8 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Vulnerabilities in detail.

Test / Plugin #33447

[Back to Vulnerabilities](#)

[Configure](#) [Audit Trail](#) [Launch](#) [Export](#)

Hosts 1 Vulnerabilities 24 History 2

HIGH Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Description

The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.

Solution

Contact your DNS server vendor for a patch.

See Also

<https://www.cnet.com/news/massive-coordinated-dns-patch-released/>
http://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/

Output

```
The remote DNS server uses non-random ports for its DNS requests. An attacker may spoof DNS responses.
List of used ports :
+ DNS Server: 99.60.84.227
- Port: 58272
- Port: 58273
- Port: 58274
- Port: 58275
```

Port	Hosts
53 / udp / dns	192.168.180.133

Plugin Details

Severity: High
ID: 33447
Version: \$Revision: 1.30 \$
Type: remote
Family: DNS
Published: July 9, 2008
Modified: December 6, 2016

Risk Information

Risk Factor: High
CVSS Base Score: 9.4
CVSS Temporal Score: 8.9
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:ND/RC:ND
IAVM Severity: I

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: July 8, 2008

WHAT TO SUBMIT

Submit your response with detailed screenshots.

