# 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 <u>https://127.0.0.1:8834</u>

Username: root Password: toor



C Q. Search	☆ 自 ♣ 余 ♥
Nessus N	
■ root	
Remember Me Sign In	

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.

) 👏 Nessus Home / Folde	×\+		
🗲 🛈 🍋   https://127.0.0.	1:8834/#/scans/folders/my-scans	C Search	☆ 自 ♣ ☆ ♥ ☰
Nessus 🔊	Scans Settings		🔺 root 💶
FOLDERS My Scans All Scans Trash	My Scans	This folder is empty. Create a new scan.	Import New Folder Rew Scan
RESOURCES Policies Policy Plugin Rules			

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

Scan Templates Gack to Scans					
Scanner Select Adr	vanced Scan from available Sca	an Templates			Search Library Q
2 <sup>0</sup>		È.	\$	···•\/	1
Advanced Scan Configure a scan without using any recommendations.	Audit Cloud Infrastructure Audit the configuration of third-party cloud services.	Badiock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.	Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.	Basic Network Scan A full system scan suitable for any host.	Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.
		V	ta anger	0	Constant of the second
DROWN Detection Remote checks for CVE-2016-0800.	Host Discovery A simple scan to discover live hosts and open ports.	Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.	Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.	Malware Scan Scan for malware on Windows and Unix systems.	MDM Config Audit Audit the configuration of mobile device managers.
	Citary Citary		E Charge	C CREAT	
Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.	Offline Config Audit Audit the configuration of network devices.	PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.	Policy Compliance Auditing Audit system configurations against a known baseline.	SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.	Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
		<b></b>			
Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754	WannaCry Ransomware Remote and local checks for MS17-010.	Web Application Tests Scan for published and unknown web vulnerabilities.			



This document is licensed with a Creative Commons Attribution 4.0 International License ©2017 Catalyzing Computing and Cybersecurity in

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.

ettings	Credentials	Compliance	Plugins		
ASIC	~				
General		Name		Test	Name the scan profile na
Schedule Notification	าร	Description		Windows server 2012 Vulnerability scan	Add description for furt detail
ISCOVERY	>				Select Folder from drop
SSESSMENT	>	Folder		My Scans	down menu. Select My
EPORT	>	<b>T</b>			Scans as default value.
DVANCED	>	largets		192.168.180.133	ress
		Upload Targets		Add File	

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	s								Filter windows	0	٨	root 👤
New Scan Back to Scan T	/ Advance	d Scan							C Enter Plugin Keyword	Disable All	Enab	ble All
Settings	Credentials	Compliance	Plugins							Show Ena	bled   S	ihow All
STATUS	PLUGIN FAMILY	f .			TOTAL	^	STATUS	PLUGIN NAME		PL	UGIN ID	^
ENABLED	Windows				3940	2011 (101) (101) <sup>4</sup> P.11 (		No plugin family selected.				
ENABLED	Windows : Mic	crosoft Bulletins			1437							
ENABLED	Windows : Use	er management			28							
		Avail	able 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



This document is licensed with a Creative Commons Attribution 4.0 International License ©2017 Catalyzing Computing and Cybersecurity in

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.

ngs (	Credentials Compliance Plugins			Show Enabled   S
ATUS	PLUGIN FAMILY 🛦	TOTAL STATUS	PLUGIN NAME	PLUGIN ID
ISABLED	Windows	3940	No plugin family selected.	
SABLED	Windows : Microsoft Bulletins	1437		
Star	Windows : User management tus of plugins after Enabling	28		
IISABLED	Windows : User management	28		

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 ur 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 Q 1Scan		
Name	Schedule	Last Modified V
Test	On Demand	N/A click to launch scan $\Box$ > > ×

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 Q 1Scan						
Name	Schedule		Last Modified	Ŧ		
Test	On Demand	Scan in progress 🖒 🔿	Today at 9:10	РМ	П	

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



This document is licensed with a Creative Commons Attribution 4.0 International License ©2017 Catalyzing Computing and Cybersecurity in

My Scans		Im	nport Ne	w Folder	🕂 New	/ Scan
Search Scans Q 1 Scan						
□ Name	Schedule	Completed as	st Modified v			
Test	On Demand	🗸 Tod	day at 9:18 PM		Þ	×

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



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.



St ick to My S	icans					
Hosts 1	Vulnerabilities 23 History 1					
ilter 👻 S	Sealed Vulnerabilities Q 23 Vulnerabilities				Scan Details	
Sev *	Name 🛦	Family 🛦	Count v		Name:	Test
HIGH	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1	1	Status: Policy:	Completed Advanced Scan
MEDIUM	SMB Signing Disabled Select the vulnerabilities to see details.	Misc.	1	1	Scanner: Start:	Local Scanner Today at 9:09 PM
MEDIUN	Unencrypted Telnet Server	Misc.	1	/	End: Elapsed:	Today at 9:18 PM 8 minutes
INFO	Nessus SYN scanner	Port scanners	6	1	Vulnerabilitie	•5
INFO	Service Detection	Service detection	3	/		Critical
INFO	DNS Server Detection	DNS	2	1		High     Medium
INFO	Common Platform Enumeration (CPE)	General	1	1		Low     Info
INFO	Device Type	General	1	1		
INFO	Ethernet Card Manufacturer Detection	Misc.	1	1		
Inei	rabilities in detail. ugin #33447		¢	Configure	Audit Trail	Launch 👻 Export
Iner st / Pl ack to Vul Hosts 1	rabilities in detail. ugin #33447 nerabilities Vulnerabilities 24 History 2		¢	Configure	Audit Trail	Launch 👻 Export
IIner est / Pli ack to Vul Hosts 1 HIGH	rabilities in detail. ugin #33447 nerabilities Vulnerabilities 24 History 2 Multiple Vendor DNS Query ID Field Prediction Cache Poi	soning	c	Configure	Audit Trail Plugin Details	Launch 👻 Export
HIGH HIGH High hoison the hution	Asverity Level rabilities in detail. ugin #33447 nerabilities Vulnerabilities 24 History 2 Multiple Vendor DNS Query ID Field Prediction Cache Poi NS resolver does not use random ports when making queries to third-party DNS se remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites DNS server vendor for a patch.	Soning rvers. An unauthenticated, remote attacker can explo s.	t this	Configure >	Audit Trail Plugin Details Severity: ID: Version: Type: Family: Published: Modified:	Launch  Export Export High 33447 SRevision: 1.30 \$ remote DNS July 9, 2008 December 6, 2016
Inc.	severity Level rabilities in detail. ugin #33447 nerabilities vulnerabilities 24 History 2 Multiple Vendor DNS Query ID Field Prediction Cache Poi NS resolver does not use random ports when making queries to third-party DNS se remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites DNS server vendor for a patch. net.com/news/massive-coordinated-dns-patch-released/ register.co.uk/2008/07/21/dns_ftaw_speculation/	Soning rvers. An unauthenticated, remote attacker can explo s.	t this	2onfigure >	Audit Trail Plugin Details Severity: ID: Version: Type: Family: Published: Modified: Risk Information	Launch  Export  High 33447 SRevision: 1.30 \$ remote DNS July 9, 2008 December 6, 2016
High Hosts / PI/ Hosts 1 High Aborts 1 High Abort 2 Also Also Also Also Also Also	Asvertiy Level rabilities in detail. ugin #33447 nerabilities Vulnerabilities 24 History 2 Multiple Vendor DNS Query ID Field Prediction Cache Poi NS resolver does not use random ports when making queries to third-party DNS se remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites DNS server vendor for a patch. net.com/news/massive-coordinated-dns-patch-released/ register.co.uk/2008/07/21/dns_flaw_speculation/	Soning rvers. An unauthenticated, remote attacker can explo	it this	> ·	Audit Trail Plugin Details Severity: ID: Version: Type: Family: Published: Modified: Risk Information Risk Factor: Hig CVSS Base Soc	Launch  Export Export High 33447 Revision: 1.30 \$ remote DNS July 9, 2008 December 6, 2016 December 6, 2016 Dn I (Lown 0 0)
And the second s	severity Level rabilities in detail. ugin #33447 nerabilities Vulnerabilities 24 History 2 Multiple Vendor DNS Query ID Field Prediction Cache Poi NS resolver does not use random ports when making queries to third-party DNS se remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites DNS server vendor for a patch. net.com/news/massive-coordinated-dns-patch-released/ pregister.co.uk/2008/07/21/dns_flaw_speculation/ ete DNS server uses non-random ports for its used ports : erver: 99.60.84.227 : S8273	Soning rvers. An unauthenticated, remote attacker can explo 3.	t this	>	Audit Trail Plugin Details Severity: ID: Version: Type: Family: Published: Modified: Risk Informatiod CVSS Base Soc CVSS Temporal CVSS Vector: C /1:C/A:C CVSS Temporal IAVM Severity:	Launch  Export  High 33447 SRevision: 1.30 \$ remote DNS July 9, 2008 December 6, 2016  ph ore: 9.4 I Score: 8.9 2VSS2#AV:N/AC:L/Au:N/C:N I Vector: CVSS2#E:F/RL:ND/RC:1 I
Hillner est / Pi ack to Vul Hosts 1 1 Hosts 1 1 Hosts 1 Hosts 1 Hosts 1 Hosts 1 Hosts 4 Hosts 4	severity Level rabilities in detail. ugin #33447 merabilities Vulnerabilities	Soning rvers. An unauthenticated, remote attacker can explo	it this	> · ·	Audit Trail Plugin Details Severity: ID: Version: Type: Family: Published: Modified: Risk Factor: Hig CVSS Base Sc CVSS Temporal CVSS Veetor: C 1.C/A:C CVSS Temporal IAVM Severity: Vulnerability In	Launch       Export         High       Stata         SRevision: 1.30 \$       remote         DNS       July 9, 2008         December 6, 2016       Stata         one:       9.4         I Score: 8.9       VSS2#A:N/AC:L/AI::N/C:N         I Vector:       CVSS2#E:F/RL:ND/RC:I         I       I
HIDEST / PI ack to Vul Hosts 1 Heat Hosts 1 Heat Hution Socioson the e Also Socioson the e Also Socioson the the remember that The remember that The remember Ports for Ports fo	severity Level rabilities in detail. ugin #33447 nerabilities vulnerabilities vulnerabilities 24 History 2 Multiple Vendor DNS Query ID Field Prediction Cache Poi NS resolver does not use random ports when making queries to third-party DNS se remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites DNS server vendor for a patch. net.com/news/massive-coordinated-dns-patch-released/ pregister.co.uk/2008/07/21/dns_flaw_speculation/  pte DNS server uses non-random ports for its used ports : rver: 99.60.84.227 is8273 is8274 bots	soning rvers. An unauthenticated, remote attacker can explo	it this	>	Audit Trail Plugin Details Severity: ID: Version: Type: Family: Published: Modified: Risk Informatic Risk Factor: Hig CVSS Base Sc CVSS Tempora IAVM Severity: Vulnerability Ir Exploit Available Exploit Ease: E	Launch ▼       Export         High       33447         SRevision: 1.30 \$       remote         DNS       July 9, 2008         December 6, 2016       December 6, 2016         on       July 9, 2008         Jose 8, 9       System 1, 10/RC: L         VSS2#AV:N/AC: L/AU:N/C:N       I         Vector: CVSS2#E:F/RL:ND/RC: I       I         tormation       e: true         xploits are available       I

# WHAT TO SUBMIT

## Submit your response with detailed screenshots.

