## OLD DOMINION UNIVERSITY

## CYSE 301 Cybersecurity Techniques and Operations

## Assignment #4 Ethical Hacking

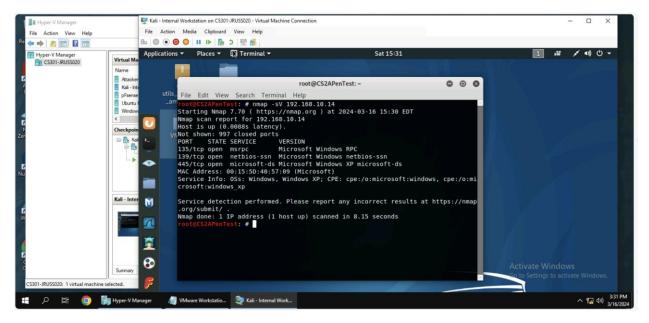
Joshua Russell

Task A.

Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

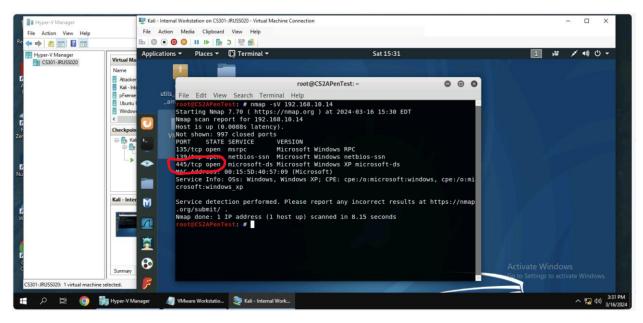
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. Run a port scan against Windows XP using nmap command to identify open ports and services.



(The above screen shot shows a nmap scan of the Windows XP Server 192.168.10.14 to find open ports and services. The option -sV was used to detect version information).

2. Identify the SMB port number (default: 445) and confirm that it is open.



(In the above screenshot, port 445 the SMB port is open)

3. Launch Metasploit Framework and search for the exploit module: ms08\_067\_netapi

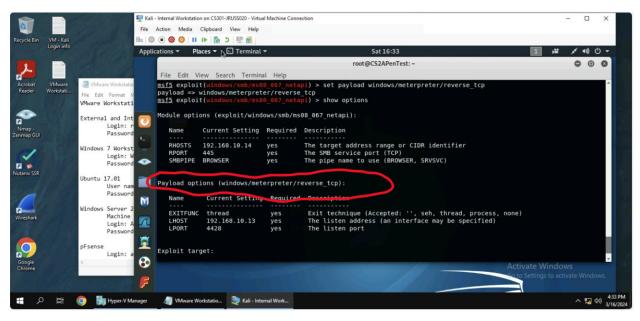
Hyper-V Manager	-	ali - Internal Workstation on CS301-JRUSS020 - Virtual Machine Connection			110	
ile Action View Help	File					
• 🔿 🙍 🚮		◎ ● ◎ ◎ ॥ ▶ ⓑ > № ñ				
Hyper-V Manager	Ар	plications 🔻 Places 🔻 😥 Terminal 👻 Sat 15:41		1	18 /	• • • • •
CS301-JRUS5020	Virtual Ma	root@CS2APenTest: ~				0 0 0
	Name	File Edit View Search Terminal Help				
	Attacker Kall - Inte	+== 3 evasion				
	pFsense					
	Ubuntu 6	msf5 >				
	Windows	<u>msf5</u> > search ms_08_067netapi				
	<	[-] No results from search msf5 > search "ms 08 067netapi"				
	Checkpoin	msis > search ms 08 00/hecapi				
	E-R Kal S.	Matching Modules				
	0- <b>1</b>					
		▶ # Name tion	Disclosure Date	Rank	Check	Descrip
		<pre>0 auxiliary/admin/appletv/appletv_display_image</pre>		normal	No	Apple T
	Kali - Inter	V Image Remote Control				
		1 auxiliary/admin/appletv/appletv_display_video V Video Remote Control		normal	No	Apple T
				normal	No	Veritas
		Backup Exec Windows Remote File Access				
		3 auxiliary/admin/chromecast/chromecast_reset		normal	No	Chromec
		ast Factory Reset DoS				
		4 auxiliary/admin/cisco/cisco_asa_extrabacon SA Authentication Bypass (EXTRABACON)		normal	Yes	Cisco A
		SA AUCHENCICALION BYPASS (EXTRADACON)		Activate Wi	ndows	
	Summary			Go to Settings		
01-JRUSS020: 1 virtual machine s	elected.			- In the second		
o = 🎧 📲	Hyper-V Manager	🔊 VMware Workstatio 🤰 Kali - Internal Work				^ 🌇 🕼 🖁

(In the above screenshot, a search for ms 08 067 netapi was performed)

4. Use ms08\_067\_netapi as the exploit module and set meterpreter reverse\_tcp as the payload.

			🖳 Kali	- Internal Workstation on CS301-JRUSS020 - Virtual Machine Connection				- 🗆 X
			File	Action Media Clipboard View Help				
ycle Bin	VM - Kali Login info		B 0	💌 🐵 🕲 🔲 🕪 🔂 🖄 🚟 👬				
	Login into		Appli	cations - Places - 🕞 Terminal -	Sat 16:18			1 ば 💉 🕪 🕛 🗝
0				root	@CS2APenTest: ~			000
٨				File Edit View Search Terminal Help				
robat	VMware	VMware Workstatio		<pre>16 exploit/windows/fileformat/varicad_dwb</pre>	2010-03-17	great	No	VariCAD 2010-2.05 EN (*
ader	Workstati	File Edit Format V		DWB File) Stack Buffer Overflow 17 exploit/windows/ftp/globalscapeftp input	2005-05-01		No	GlobalSCAPE Secure FTP
		VMware Workstati		Server Input Overflow	2002-02-01	great	NO	GLODALSCAPE Secure FIP
		External and Int		18 exploit/windows/http/hp_nnm_toolbar_01	2009-01-07	great	No	HP OpenView Network No
nap -		Login: r	2	<pre>de Manager Toolbar.exe CGI Buffer Overflow     19 exploit/windows/http/sysax create folder</pre>	2012-07-29	normal	No	Sysax Multi Server 5.6
nap GUI		Password	6	4 Create Folder Buffer Overflow	2012-07-25	normat	NO	Sysax Hatti Server 5.0
		Windows 7 Workst		20 exploit/windows/http/xitami_if_mod_since	2007-09-24	average	Yes	Xitami 2.5c2 Web Serve
		Login: W	-	<pre>r If-Modified-Since Overflow 21 exploit/windows/scada/indusoft webstudio exec</pre>	2011-11-04	excellent	Yes	InduSoft Web Studio Ar
۵		Password	~	bitrary Upload Remote Code Execution				
nix SSR		Ubuntu 17.01	-	22 exploit/windows/smb/ms03_049_netapi kstation Service NetAddAlternateComputerName Overflow	2003-11-11	good	No	MS03-049 Microsoft Wor
		User nam		23 exploit/windows/smb/ms06 040 netapi	2006-08-08	good	No	MS06-040 Microsoft Ser
		Password	M	ver Service NetpwPathCanonicalize Overflow				
		Windows Server 2		24 exploit/windows/smb/ms06_070_wkssvc kstation Service NetpManageIPCConnect Overflow	2006-11-14	manual	No	MS06-070 Microsoft Wor
shark		Machine Login: A		<pre>25 exploit/windows/smb/ms08_067_netapi</pre>	2008-10-28	great	Yes	MS08-067 Microsoft Ser
	Password	-	ver Service Relative Path Stack Corruption					
			1					
		pFsense Login: a	-	<pre>msf5 &gt; use exploit/windows/smb/ms08_067_netapi</pre>				
ogle		<		<pre>msf5 exploit(windows/smb/ms08_067_netapi) &gt;</pre>				ctivate Windows
ome							A	to Settings to activate Windows.
			F					Strange to activate windows.
								-
م	ă,	🧿 📑 Hyper-V Ma	inager	🧾 VMware Workstatio 🛛 💐 Kali - Internal Work				^ 🌆 ሳ») 🔒

(In the above screenshot, the ms08 067 netapi exploit is used)



(In the above screenshot the meterpreter is set to a reverse tcp as payload)

5. Use XXXX (follow the lab instruction) as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

