# Lab 3 – Metasploitable2 VM and Familiarity with Kali Linux

Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

| NAME – Student ID | COURSE CODE | WEIGHT |
|---|---|---|
| Click or tap here to enter text. | CYT130 | 5% |

## Homework Objectives

Upon completion of this homework, you will be able to perform the following:

- Install Metasploitable2 Virtual Machine (VM);
- Kali Linux commands;

## Lab Materials

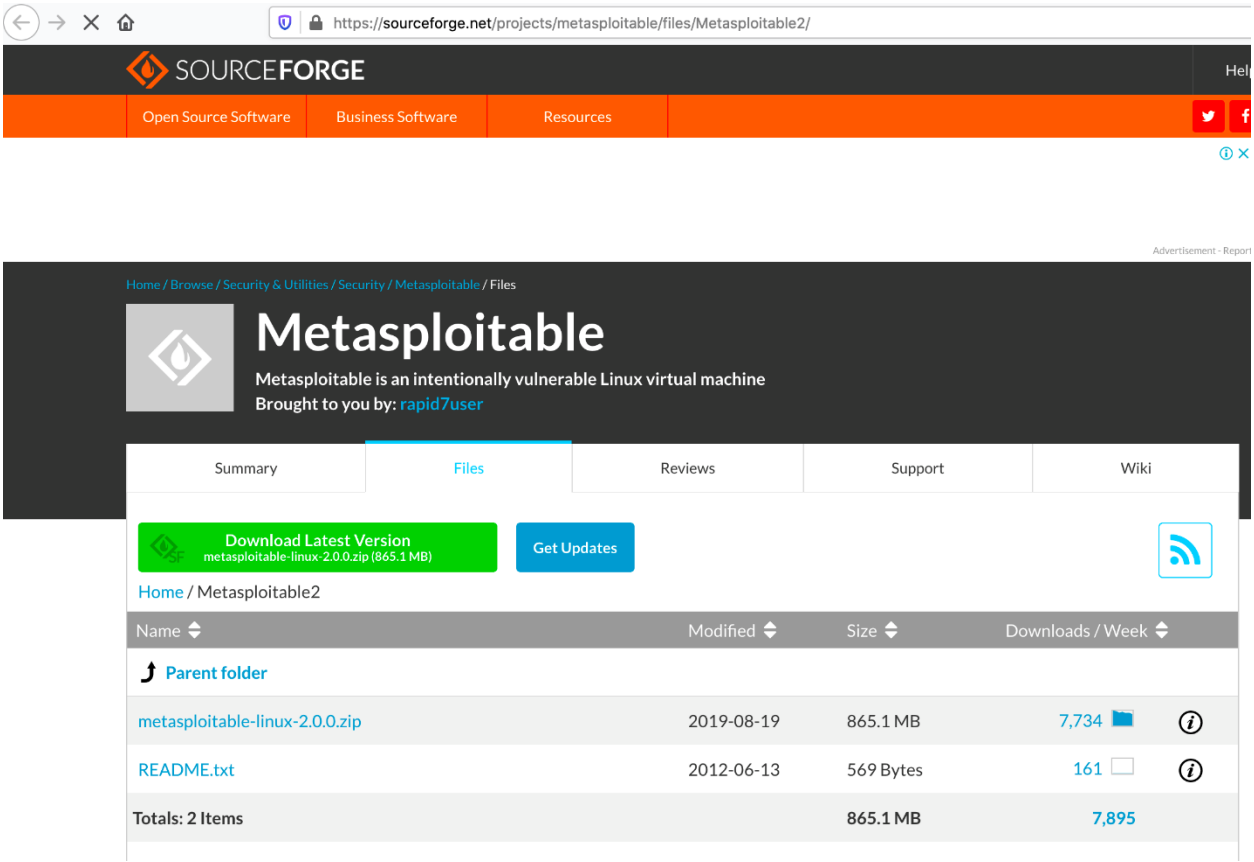
- VMWare Workstation Pro
- Metasploitable2 VM;
- Kali Linux

## Lab Instructions

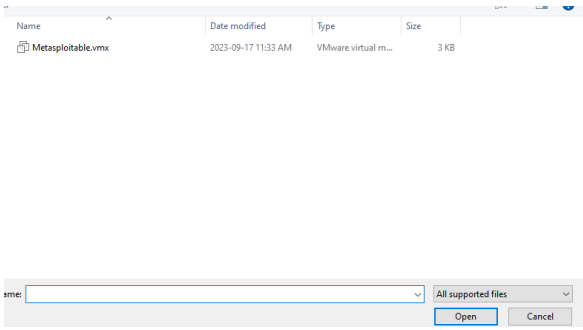
- Donwload and import Metasploitable VM;
- Enter your name and student ID above (Example: Michael Smith– 3683xxxx);
- Answer questions and add screenshots into the corresponding questions;
- Save the file on your computer for future reference;
- Save this file again as a "`.pdf`" file;
- Submit the PDF file with ***<yourname>_<student ID>_Lab_3*** for grading.

## Part 1: Download and Import Metasploitable VM

1. *Metasploitable2* is an intentionally vulnerable Linux virtual machine. We will use it to conduct security training, test security tools, and practice common penetration and ethical hacking techniques.
2. Head to SourceForge web site, click the **Download Latest Version** button to download the VM image for Metasploitable2.




3. Once the file is downloaded unzip it to your external SSD when you keep your other VMs.
4. Open VMWare Workstation and click the **File**, and then **Open**. Navigate to the location where you stored the unzipped VM, and choose the file **Metaploitable.vmx**.




5. Once the VM is open, make sure that it's network adaptor is connected to NAT, and then click **Power on this virtual machine**. If asked "This virtual machine might have been moved or copied", choose **I Mover It**.
6. Login into *Measploitable* with user **msfadmin** and a password **msfadmin** .

Never expose this VM to an untrusted network (use **NAT,** or **Host-only** mode for the network interface)!

## Part 2: Checking Lab Setup

1. After logging in, type the following command:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.29.141  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4361 (4.2 KB)  TX bytes:7084 (6.9 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

2. Find IP address for the **eth0** network interface. In the above example, the IP address is *192.168.29.141*. It may be different in your environment.
3. Check that your Kali VM network card is also set to be connected to NAT.
4. Start your *Kali Linux VM*.

5. Login into *Kali Linux* with the username and password that you have setup in lab 1
6. Open **Terminal Emulator** and find the IP address of your Kali VM using **ifconfig** command.
7. Check the connectivity of your Kali VM to the Metasploitable VM using the following command: ping -c 3 192.168.29.141 (change the IP address to the IP address of you metasploitable machine that you found in step 2)

```
┌──(kali㉿kali)-[~]
└─$ ping -c 3 192.168.29.141
PING 192.168.29.141 (192.168.29.141) 56(84) bytes of data.
64 bytes from 192.168.29.141: icmp_seq=1 ttl=64 time=0.348 ms
64 bytes from 192.168.29.141: icmp_seq=2 ttl=64 time=0.259 ms
64 bytes from 192.168.29.141: icmp_seq=3 ttl=64 time=0.270 ms

--- 192.168.29.141 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.259/0.292/0.348/0.039 ms

┌──(kali㉿kali)-[~]
└─$
```

8. Ping *Kali* from *Metasploitable*. Make sure that both machines can “see” each other.

```
msfadmin@metasploitable:~$ ping -c 3 192.168.29.129
PING 192.168.29.129 (192.168.29.129) 56(84) bytes of data.
64 bytes from 192.168.29.129: icmp_seq=1 ttl=64 time=0.194 ms
64 bytes from 192.168.29.129: icmp_seq=2 ttl=64 time=0.211 ms
64 bytes from 192.168.29.129: icmp_seq=3 ttl=64 time=0.234 ms

--- 192.168.29.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.194/0.213/0.234/0.016 ms
msfadmin@metasploitable:~$ _
```

## Part 3: Proof of Lab

1. Take a screenshot of your *ping* command output on *Metasploitable VM* (Host + e) and insert it in the form below (See step #7 from the previous section).

2. Answer the following questions:
    a. What is the ping command in Unix
    b. What is the ping command on Windows
    c. Show the command used to ping 5 times in Unix
    d. Show the command used to show IP address in Unix

3. On your Kali Linux machine
    a. Create a new directory called “Week_3” (take screenshot)
    b. Create a new file using “touch”
    c. Navigate to “Week_3” and start recording your script to “<name>_script.txt”. The recorded script must include (please include your commands in the screenshots):
        i. Ping to your metasploitable 2 machine
        ii. What is NMAP?
        iii. Run NMAP (Ping scan) – Google for “Nmap ping scan” and output the result to “NMAP.txt”

    Click or tap here to enter text.

## Part 4: Submit your Lab


- **Doublecheck all your answers.**
- **Save the file on your computer for future reference.**
- **Save the file again as a “`.pdf`” file.**
- **Submit the PDF file for grading.**