Install configure Metasploitable2
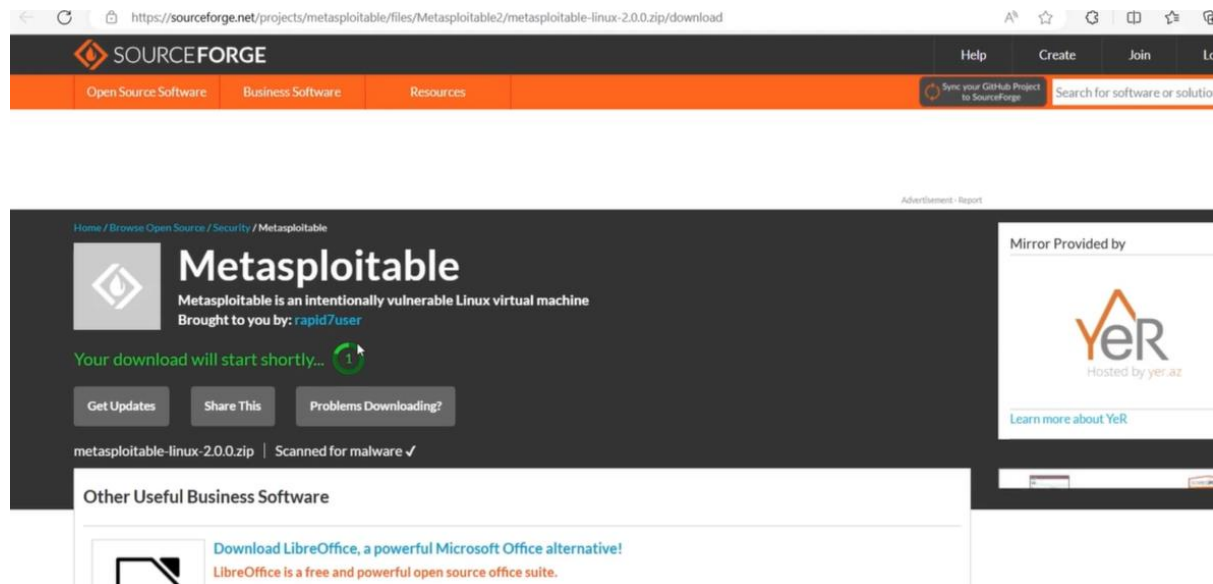
Download the zip file of metasploitable2 frm the below link.

http://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download
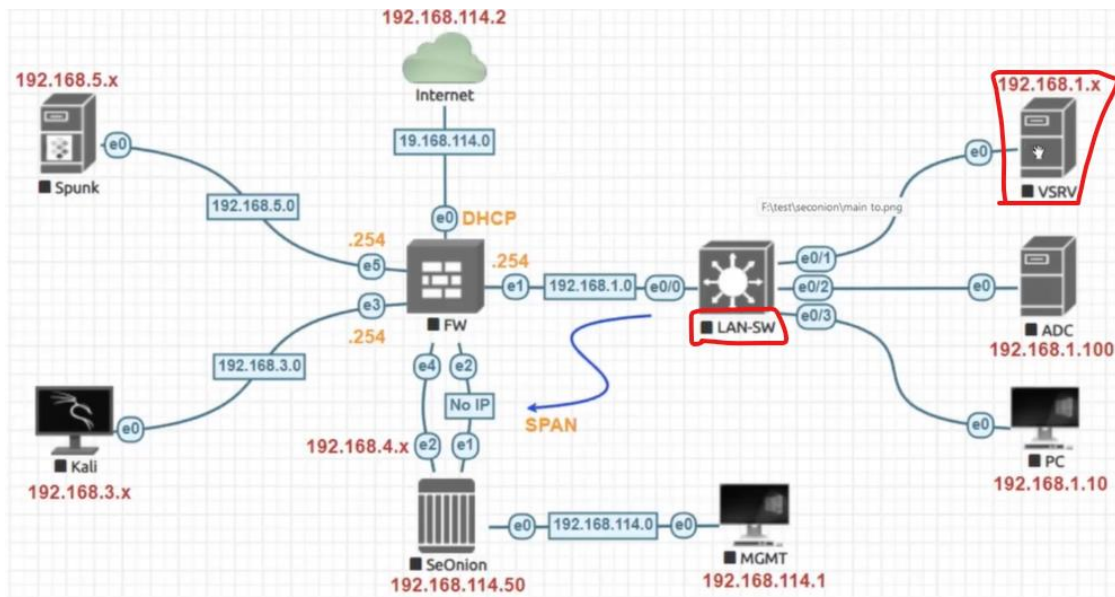

- Unzip the file.
- Open in vm as like do for kali linux.
- Network adapter will also change as do in kali linux but here we select the network adapter **vmnet 2** at custom.
- If more than one adapter are have then remove others.

Username and password is **msfadmin .**

Login using these credentials.

According to topology the Metasploit sever place shown below.
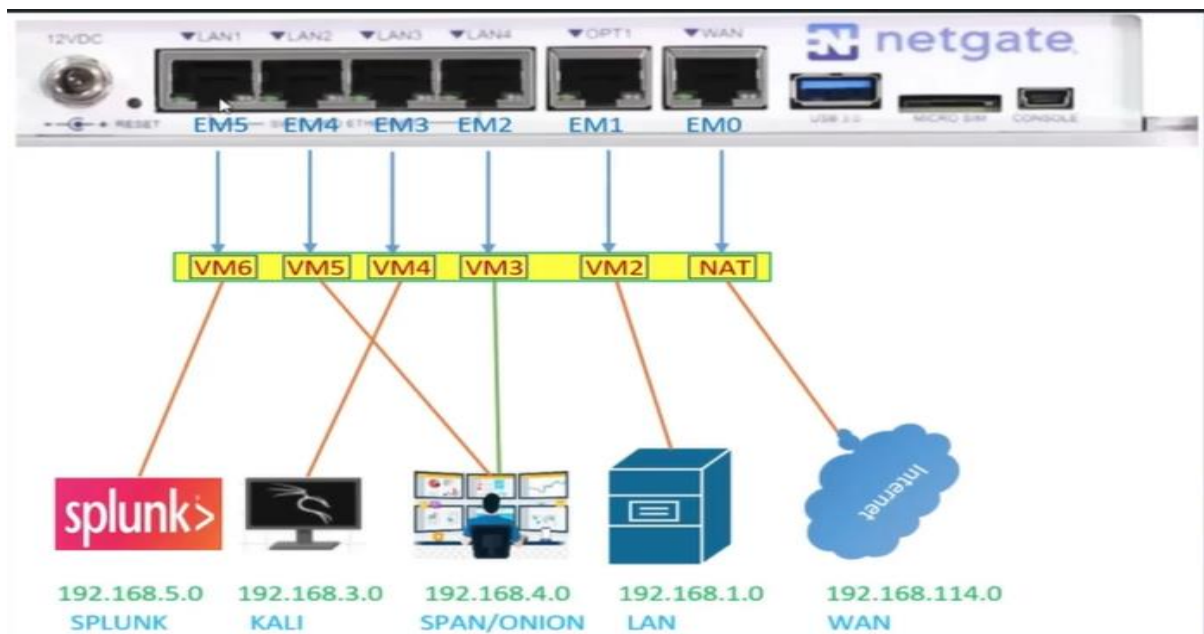
How vmnet were working it explain below.

Pfsense firewall have ports/interface from em0-em6.

Em0 connected with NAT for access internet.

Em1 for VM2(LAN) connect with window11, and both vulnerable server.

Other interfaces are also as shown in diagram.

Main point is that vm's act as virtual switch for connectivity.

So login to the Metasploit machine.

Then run command **ifconfig** to confirm the ip address .

It is linux based.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bf:6a:7e
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febf:6a7e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4478 (4.3 KB)  TX bytes:7358 (7.1 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:~$
```

complete