Amul Shrestha

Setup of Metasploitable 2 on Vmware

Following are the steps to setup metasploitable 2 on Vmware workstation on host windows.

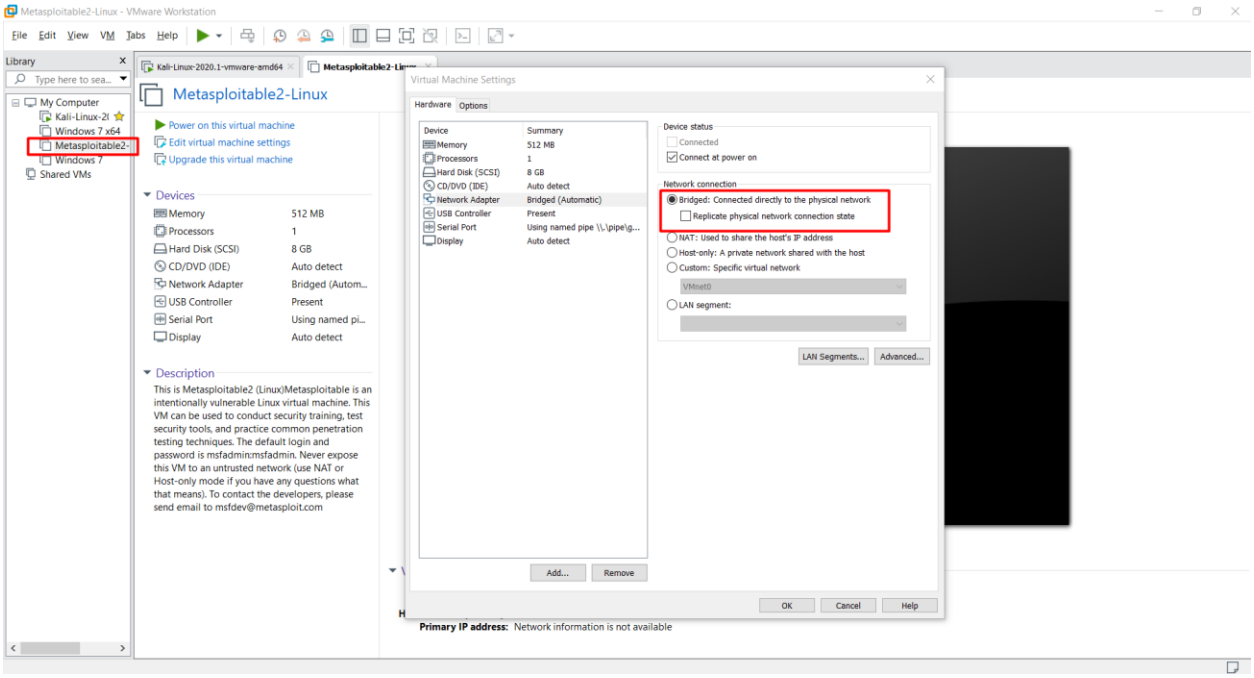
Step 1: First of all, download the metasploitable 2 vulnerable machine on your host using the following link:

https://information.rapid7.com/download-metasploitable-2017-thanks.html

or https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Step 2: After completing the download, open Vmware and create new virtual machine using the metasploitable 2 vulnerable machine file:

Step 3: Now in Network adapter setting of metasploitable 2, use the Bridged mode as shown below:

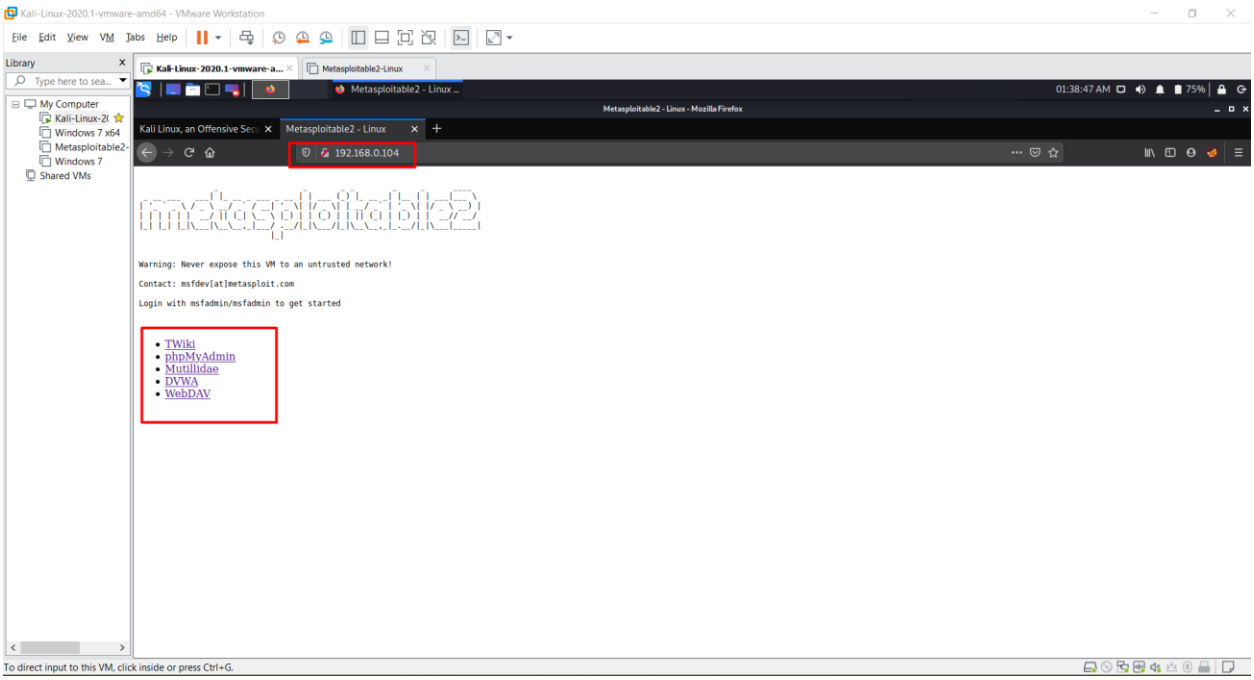


Amul Shrestha

Step 4: Now Power on both the attacking (kali) and the metasploitable 2 machine. Use msfadmin for username and password for metasploitable 2 and check the ip of that machine using the command ifconfig or ip addr.

```
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:5b:23:09 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.104/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::20c:29ff:fe5b:2309/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Step 5: Use that ip address in attacking machine (kali) to access the metasploitable 2 machine to practice as shown below:



By using those steps, we can setup the metasploitable 2 vulnerable machine to conduct security training, test security tools, and practice common penetration testing techniques on our own system.

Thank you.