Kali Linux: Task 3.3D

Name of Student

Institutional Affiliation

**Lab Details**

Virtual Box is installed on the host machine and the operating systems installed by specifying the type of operating system, amount of memory, storage, and network properties. This is shown in Figure 1. The network properties are configured as NAT Network in order to enable the machines to be on the same network. The IP range provided for the network is 192.168.1.1 – 192.168.1.254. The IP address for Metasploitable 2 can be viewed in the ifconfig results on Figure 2. The IP addresses for the machines is shown in the table in Figure 3.

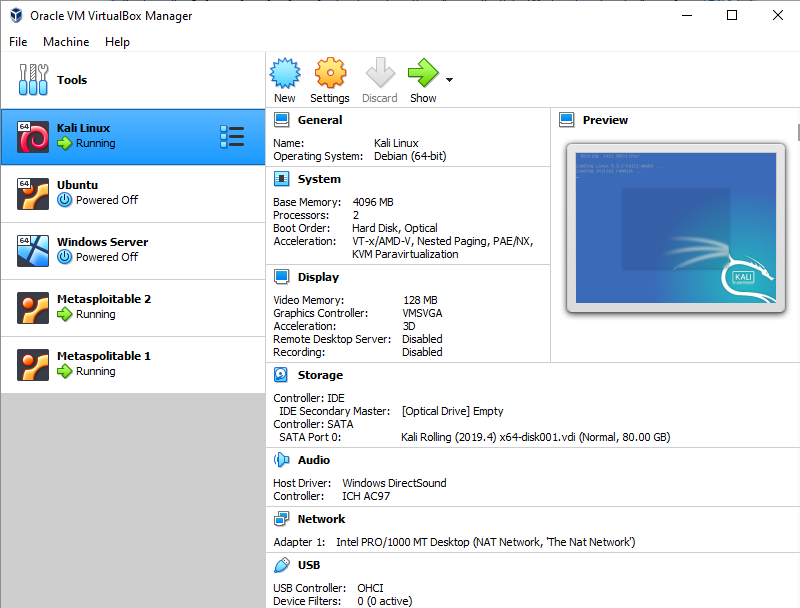
The exploitation process begins with an Nmap scan of the ports as shown in Figure 4. This helps to identify open ports in the machine. On viewing the ftp port is open, the next step is running an ftp scan as shown in Figure 5. The process shows the connection to vsFTPd 2.3.4. This can then be exploited using Metasploit Framework as shown in Figure 6. After searching for the vulnerability, a backdoor is identified which can then be exploited as shown in Figure 7 by setting the RHOST to the IP of the target.

The attacking platform now has access to the target machine’s command shell. To test if this is true, a “reboot” command is performed. The results as shown in Figure 8 show that the command works and the target machine reboots.

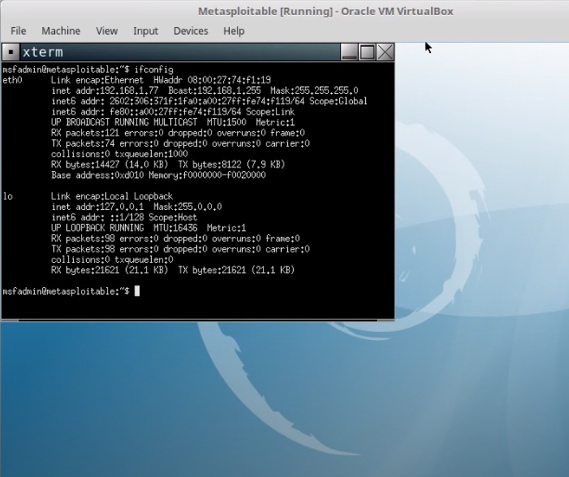
# **Summary**

The attack of the target virtual machine (Metasploitable) using Kali Linux is successful since the vulnerability is discovered, the backdoor used, and remote commands to the system made to reboot it. The Appendix section contains the figures which are screenshots of the virtual machines in operation.

**Figure 1**



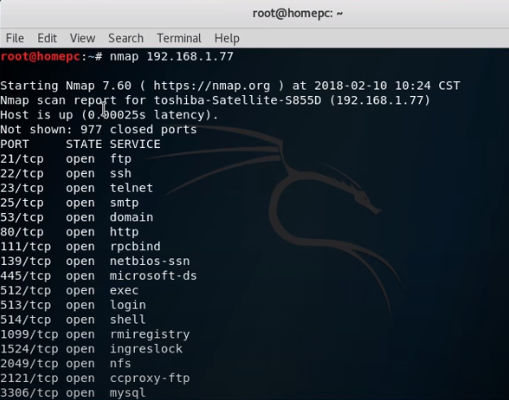
**Figure 2**



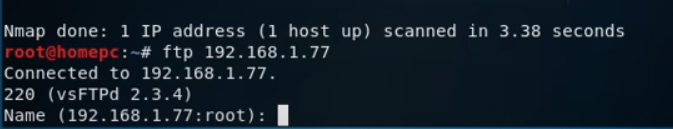
**Figure 3**

|  |  |
| --- | --- |
| **Machine** | **IP Address** |
| Kali Linux | 192.168.1.76 |
| Metasploitable 1 | 192.168.1.78 |
| Metasploitable 2 | 192.168.1.77 |

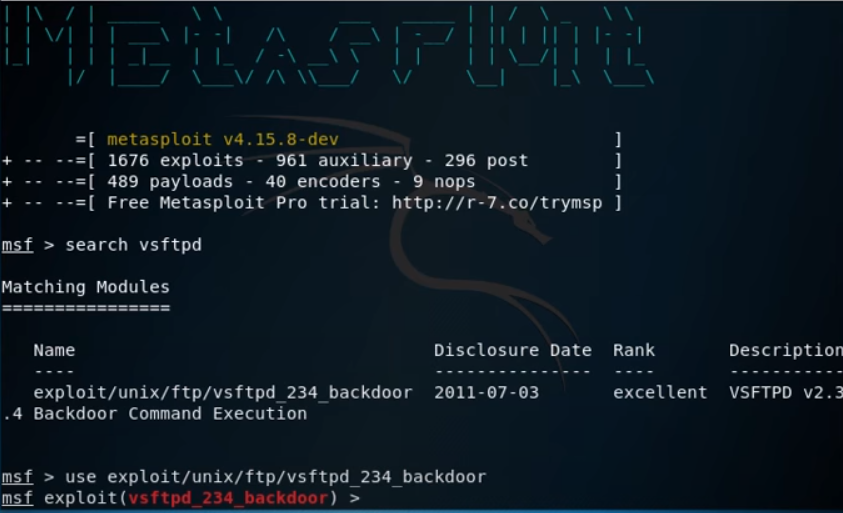
**Figure 4**



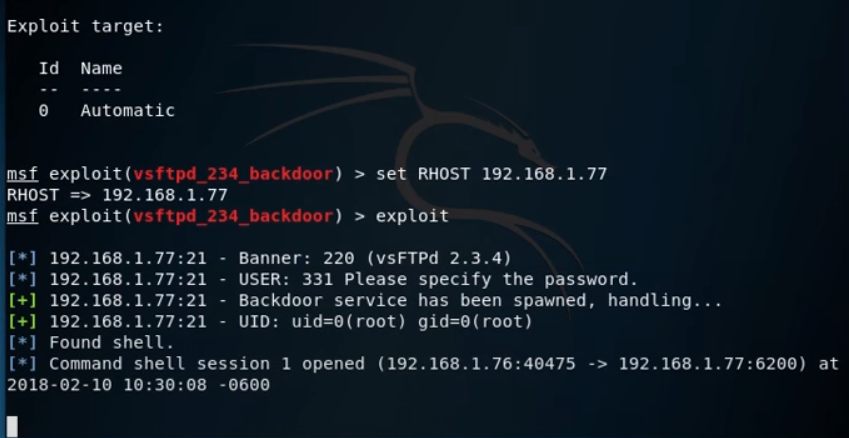
**Figure 5**



**Figure 6**



**Figure 7**



**Figure 8**

