**Name: Shangirne Kharbanda**

**Reigstration Number: 20BAI1154**

**ISAA LAB ASSESSMENT**

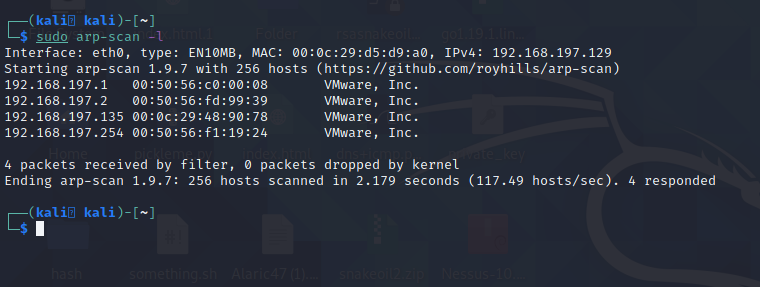
**Question:**

**Using Kali and Metasploitable2**

**Kali found that port for file transfer protocol(FTP) is open and exploit the port by removing a file in the victim system.**

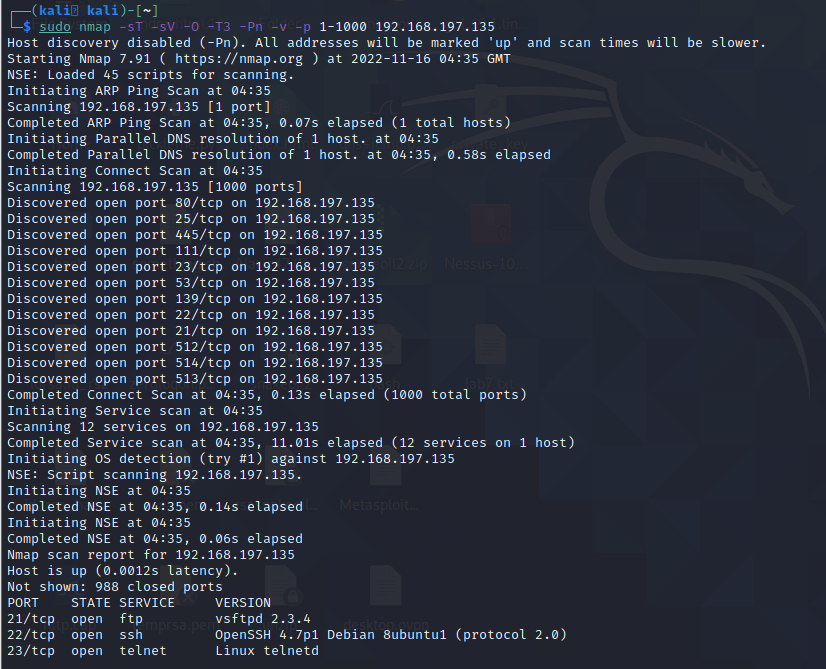
**Answer:**

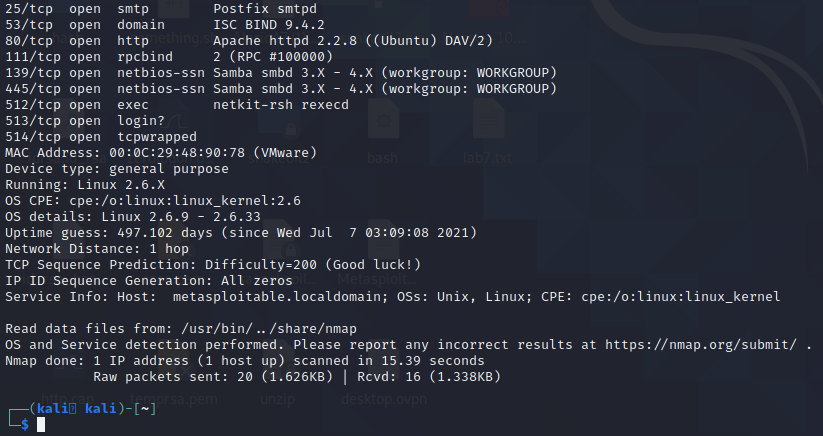
First, we perform an **arp-scan** on our kali machine to find the IP of the Metasploitable2 machine.



We can see that the IP of our target machine is **192.168.197.135**.

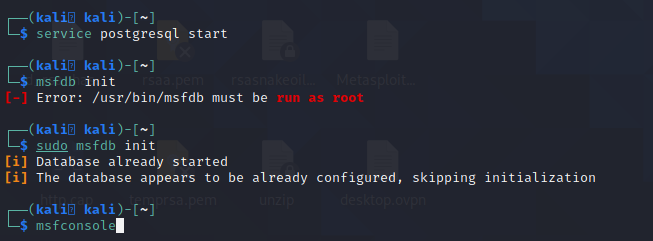
We will now perform an **Nmap scan** on the target machine to see which ports and services are open on it.





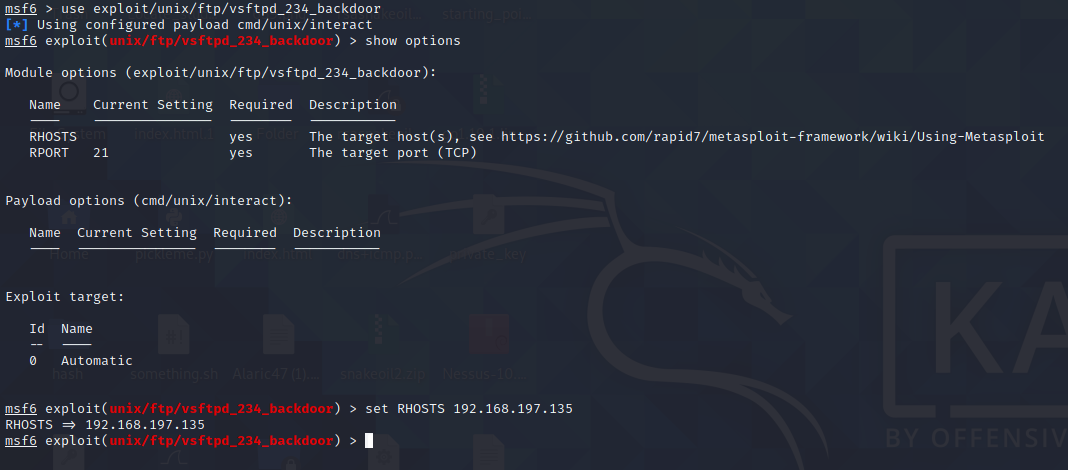
We see that ftp is running on the machine on **port 21**.

Now we will open up Metasploit by typing **msfconsole** in the terminal and starting the **postgresql** database service and initializing the database.

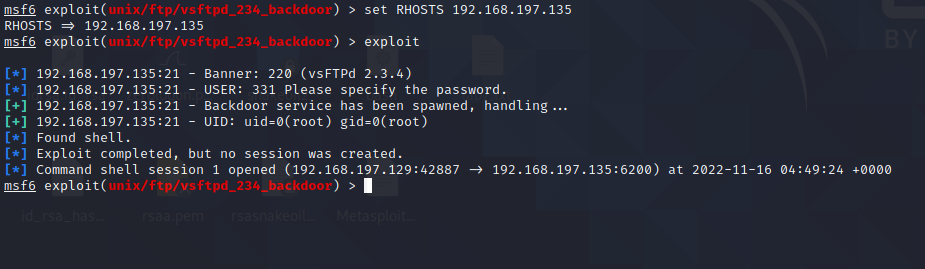


We know that the ftp version running on the target machine is **vsftpd 2.3.4**.

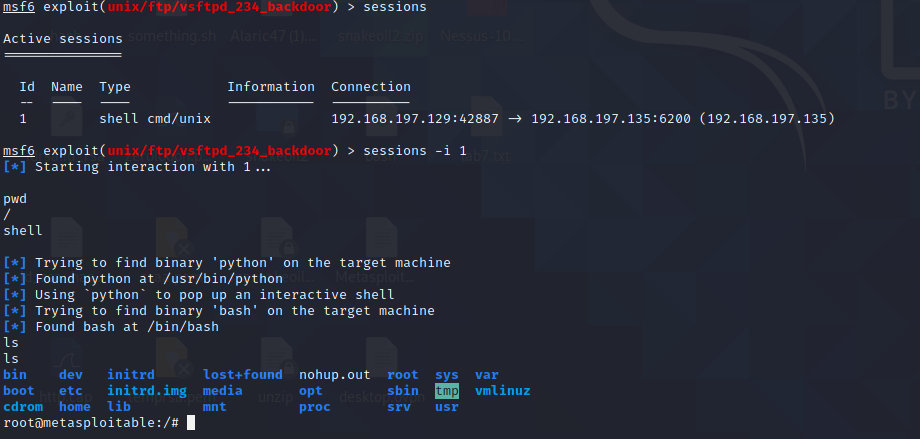
We will use the module **exploit/unix/ftp/vsftpd\_234\_backdoor** to exploit the target machine.



We will set our **RHOSTS to 192.168.197.135** which is the target machine Metasploitable2 and exploit the system.

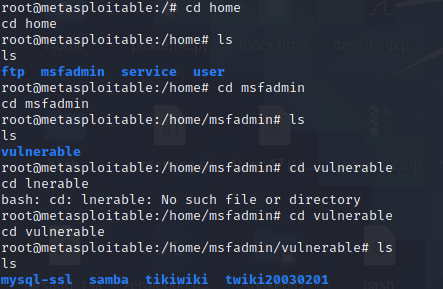


We can see that we have gotten a shell back. We will now **interact with the session and get a shell on our target machine**.

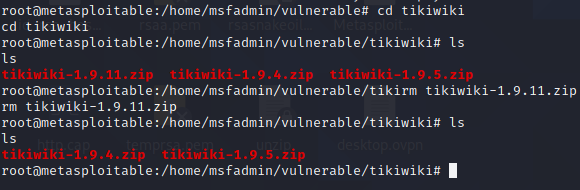


We have now gained root access to the machine using our exploit.

We will now navigate to the home directory and then the msfadmin directory.



We will navigate to one of the folders here and exploit the system by removing a file.



From the screenshot above, We can see that we have **removed a file from the target system successfully**.

The exploit is now complete and the target machine has been fully compromised and we have full root access to it.