**Name: Shangirne Kharbanda**

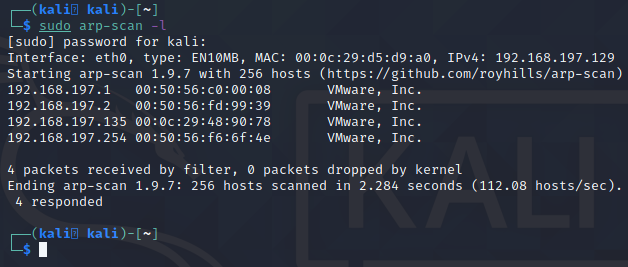
**Registration Number: 20BAI1154**

**ISAA LAB-3**

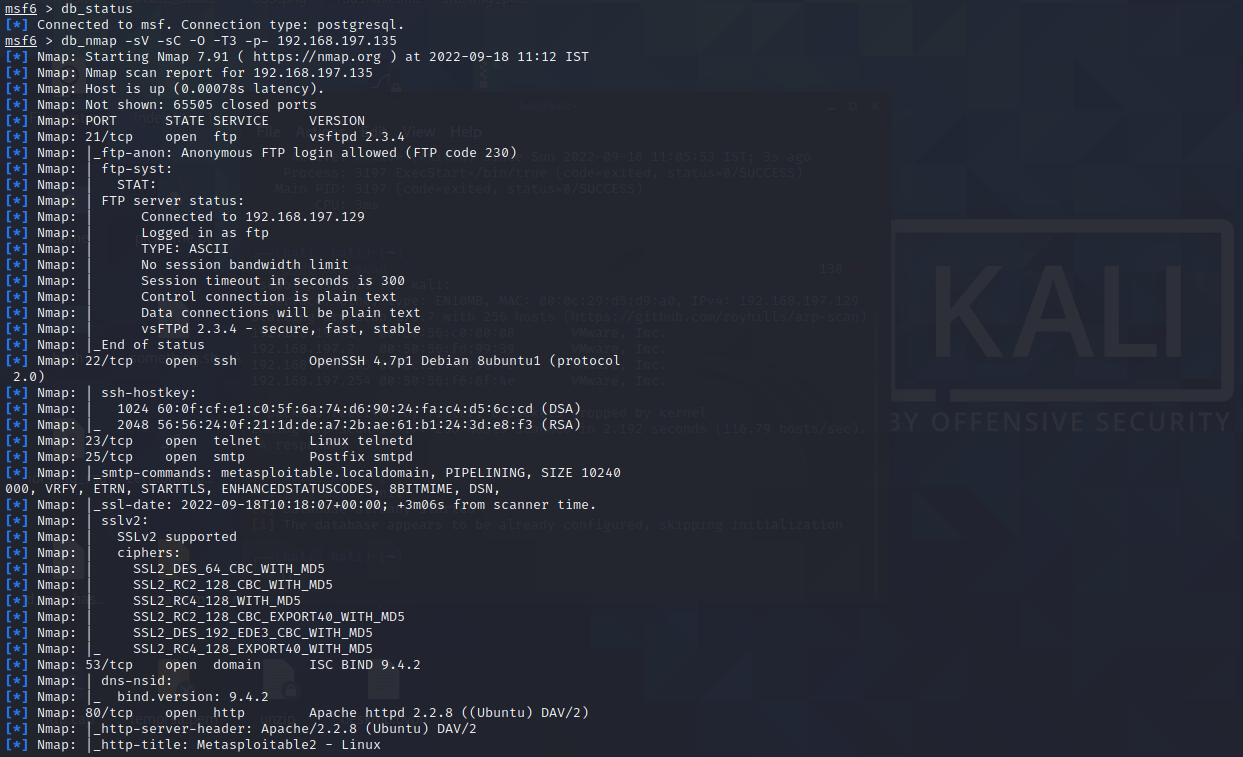
**SCANNING AND ENUMERATION OF TCP,FTP, UDP PROTOCOLS**

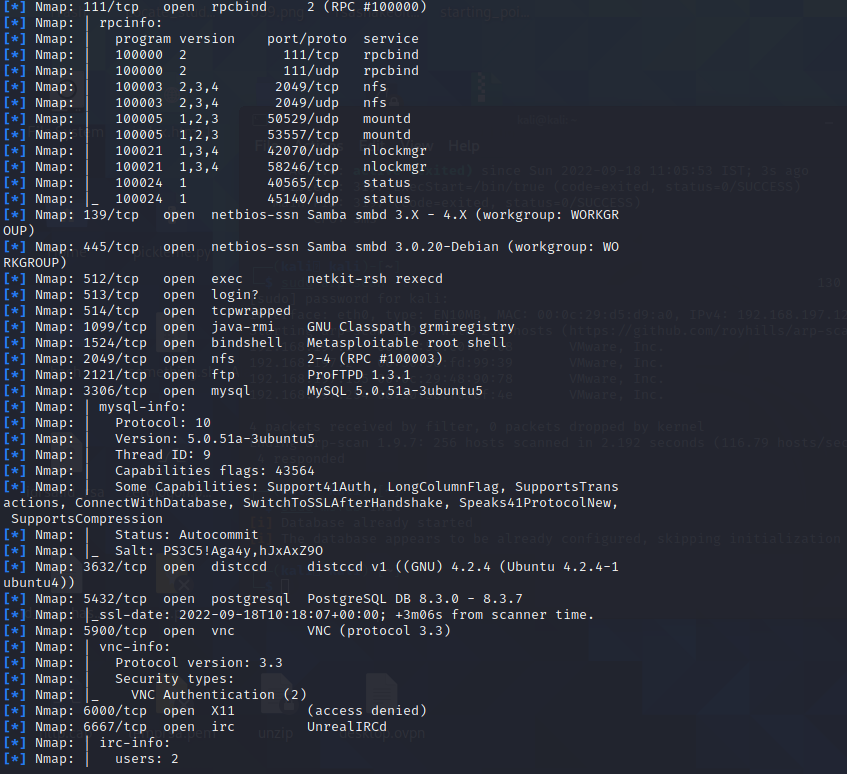
**Scanning of Target Machine:**

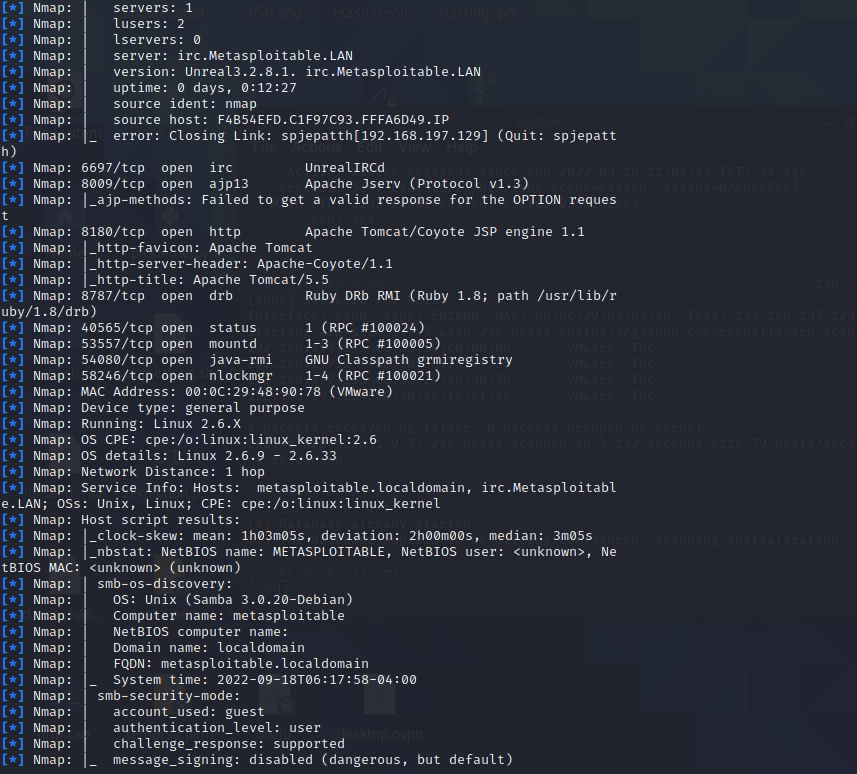
We can see our machines IP on the network as **192.168.197.135** in the following screenshot

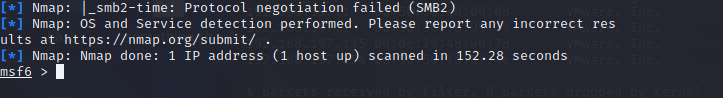


Now we will start up msfconsole and run an Nmap scan on the machine in metasploit to see which ports and services are open.

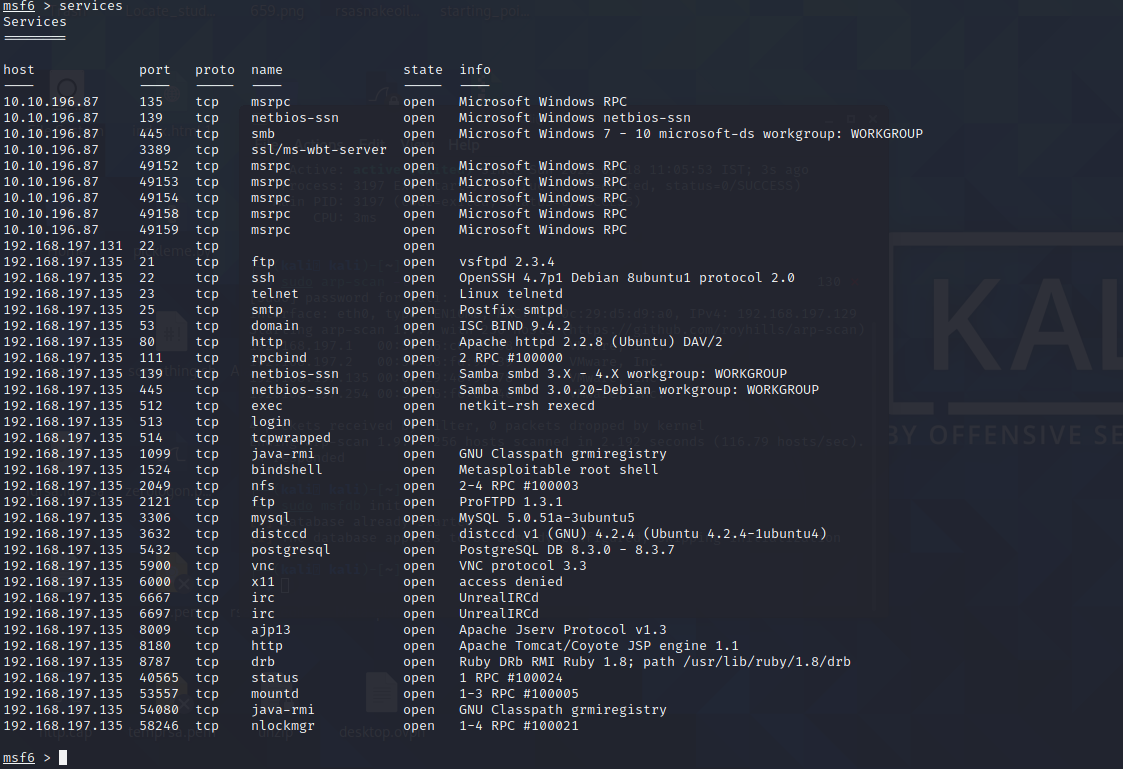






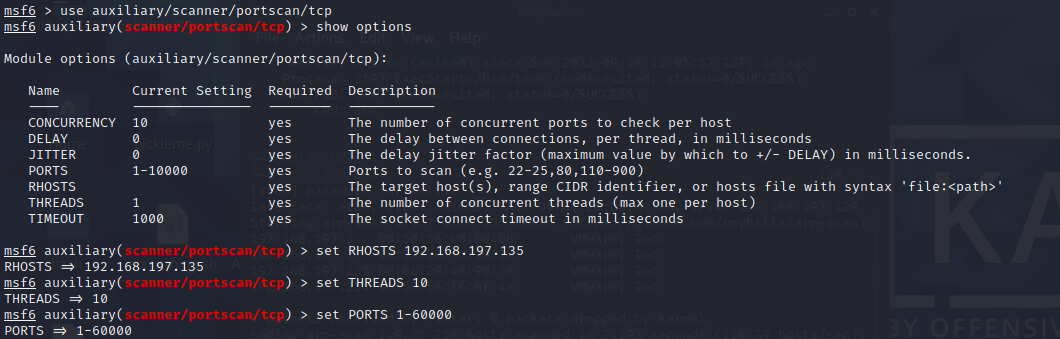


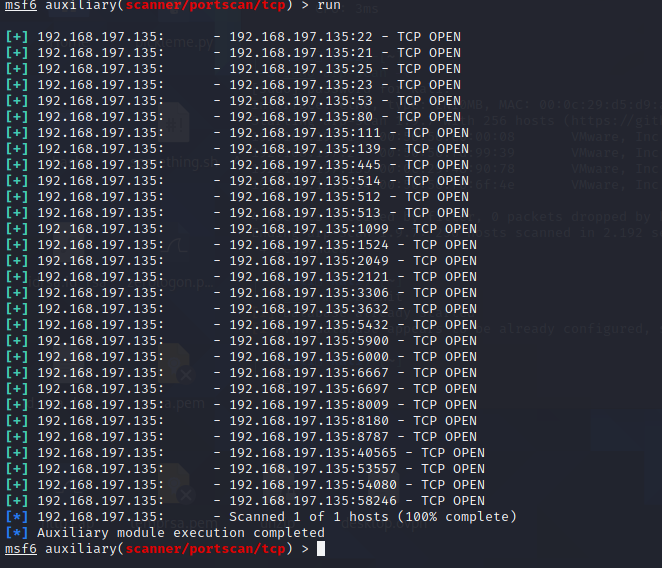
To see which services are open on the target machine, we simply type services in msfconsole as we have our nmap scan results now stored in the database.



**TCP Protocol:**

To scan TCP protocols on our target machine In metasploit, we are going to use a metasploit module called **auxiliary/scanner/portscan/tcp**. Refer to the following screenshots to see how to use it in metasploit.



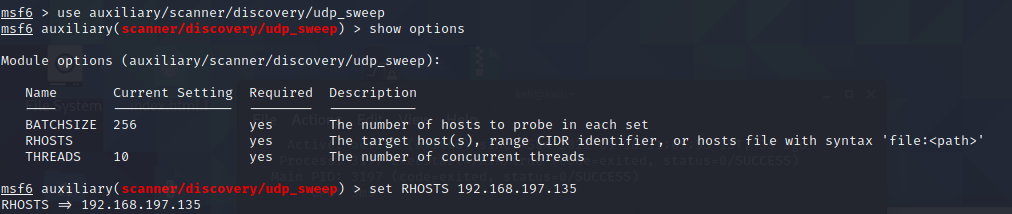


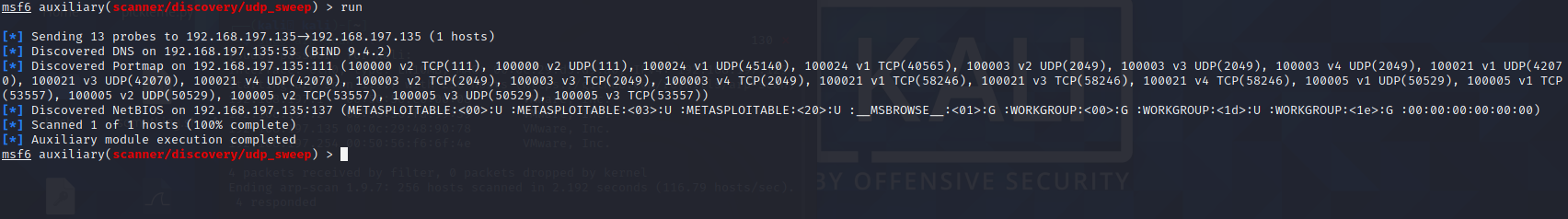
We can see which TCP protocols are open and we are done scanning the TCP ports of the target machine.

**UDP Protocol:**

Now we are going to perform a UDP sweep on our target machine to see which UDP ports are open on it in metasploit.

To do this, we are going to use the metasploit module called **auxiliary/scanner/discovery/udp\_sweep**. Refer to the following screenshots to know how to use this module in metasploit.





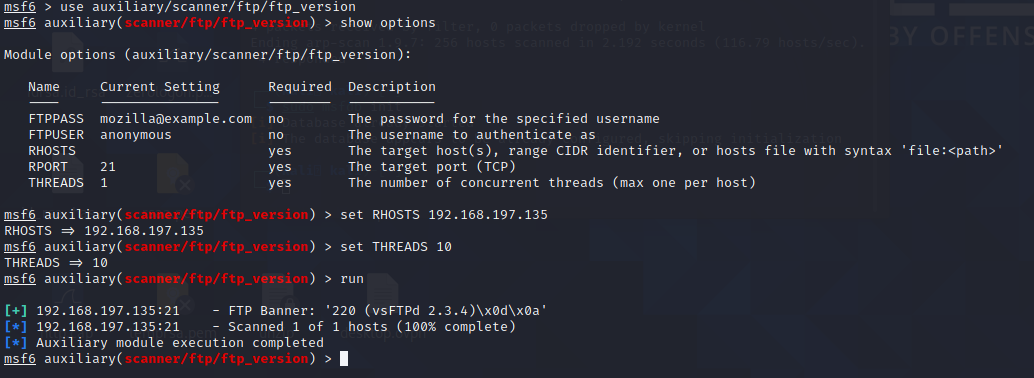
From the results, we have discovered DNS, Portmap and NetBIOS services running on our target machine.

Thus, we are done with scanning our machine for UDP ports and services.

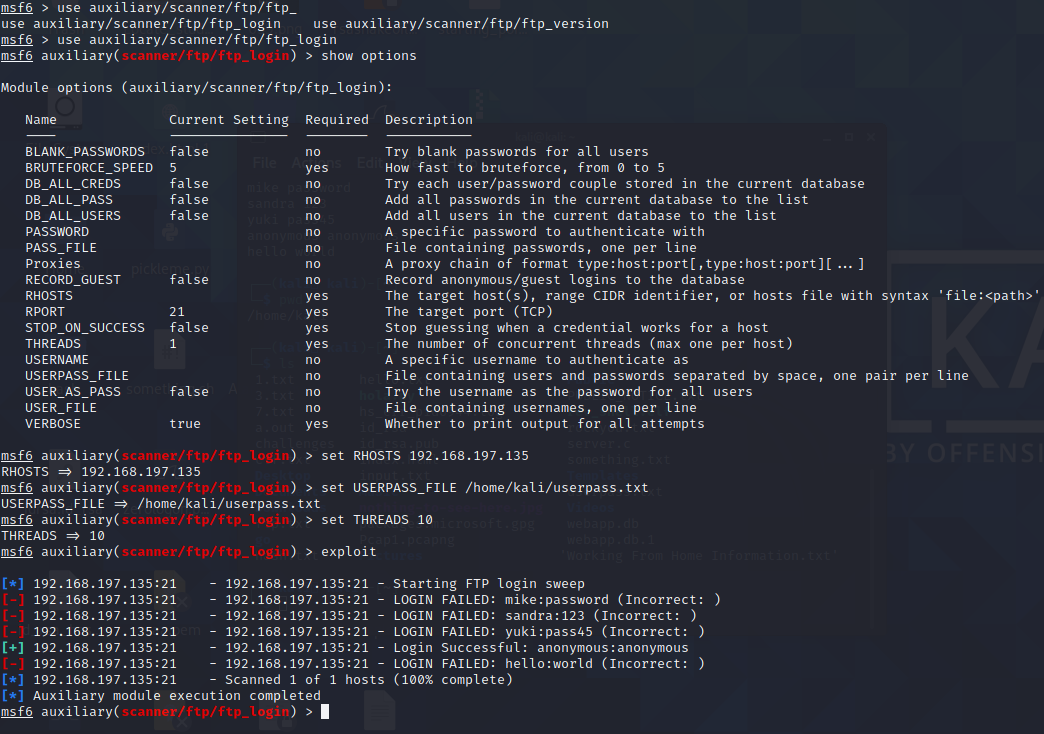
**FTP Protocol:**

From our previous enumeration of the target machine, we saw that the FTP service was running on the target machine.

Let us try to find a way to login to the FTP server running on our target machine. Let us try to find which variant of FTP is running on the target machine. We will do this by using the metasploit module **auxiliary/scanner/ftp/ftp\_version**.

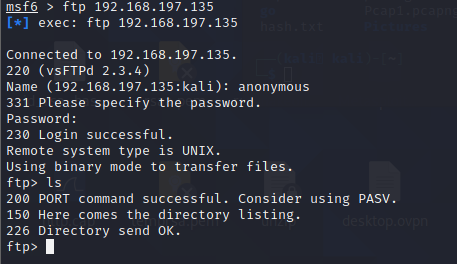


We will now try to bruteforce the FTP login in metasploit using the module **auxiliary/scanner/ftp/ftp\_login**.



We can see that the **FTP anonymous login** was **successful**.

We can now try to log into the FTP server using those credentials.



We have **successfully logged into the FTP server of our target machine**.