**Name: Shangirne Kharbanda**

**Registration Number: 20BAI1154**

**ISAA FAT LAB**

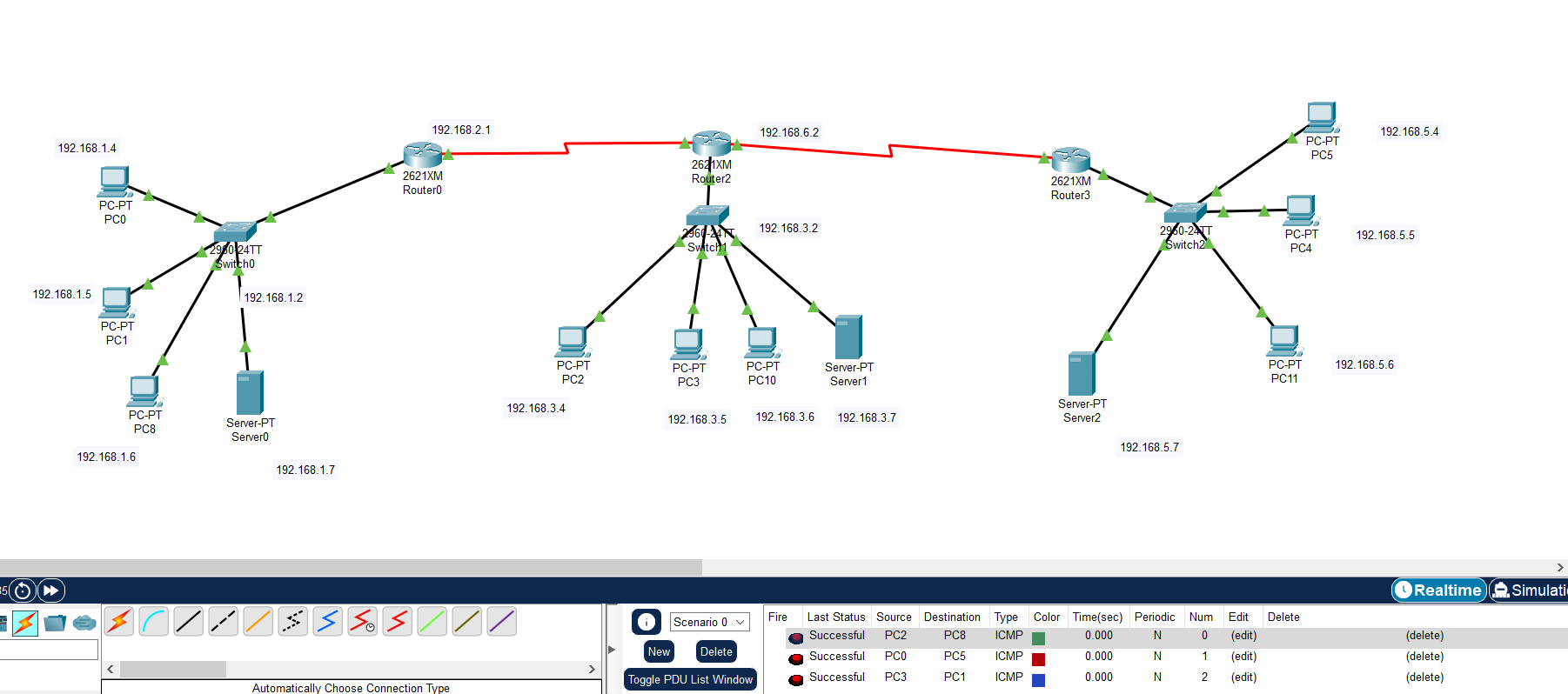
**Question 1. Create a network with three subnets and 4 computers in every subnet and complete the basic routing.**

**Create ACLs for the following cases**

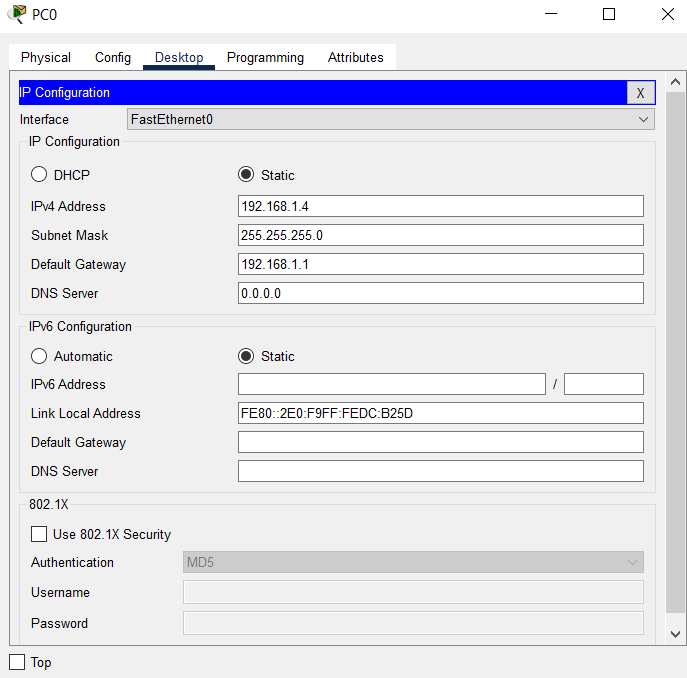
**All the subnets should have a server and three clients. The clients are given the IP address sequentially. All the odd-numbered clients can send the packets to the odd-numbered clients in the local and other subnets. All the even-numbered clients can send the packets only to the even numbers clients in the local and other subnets.**

**Answer 1:**

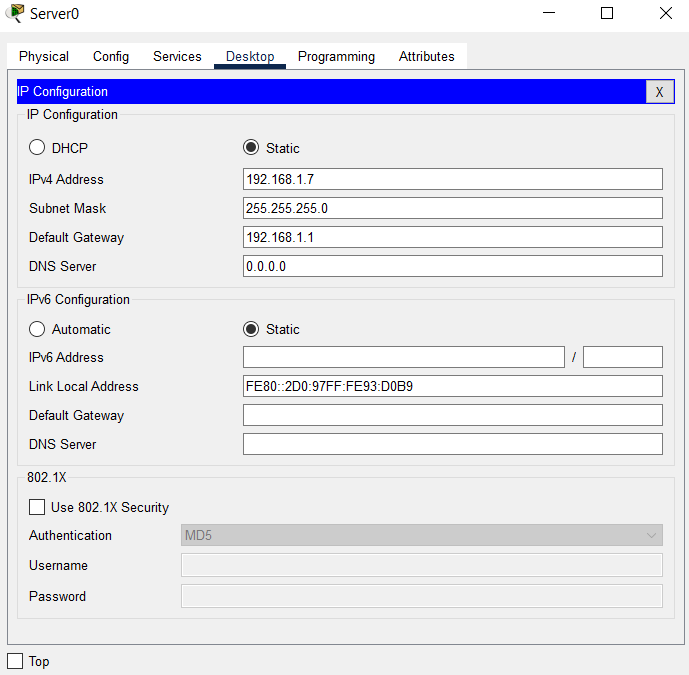
First we will create a network with 3 subnets and 4 computers in every subnet as follows.



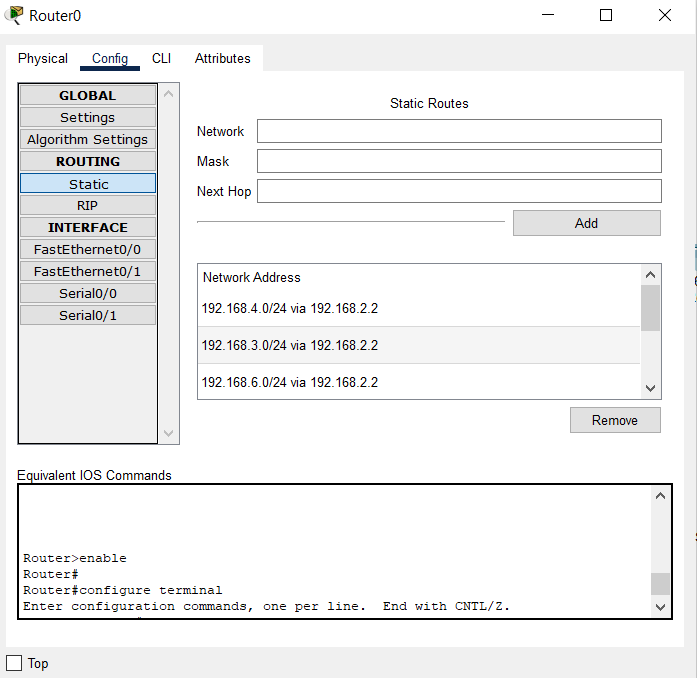
We will configure the PCs as follows:



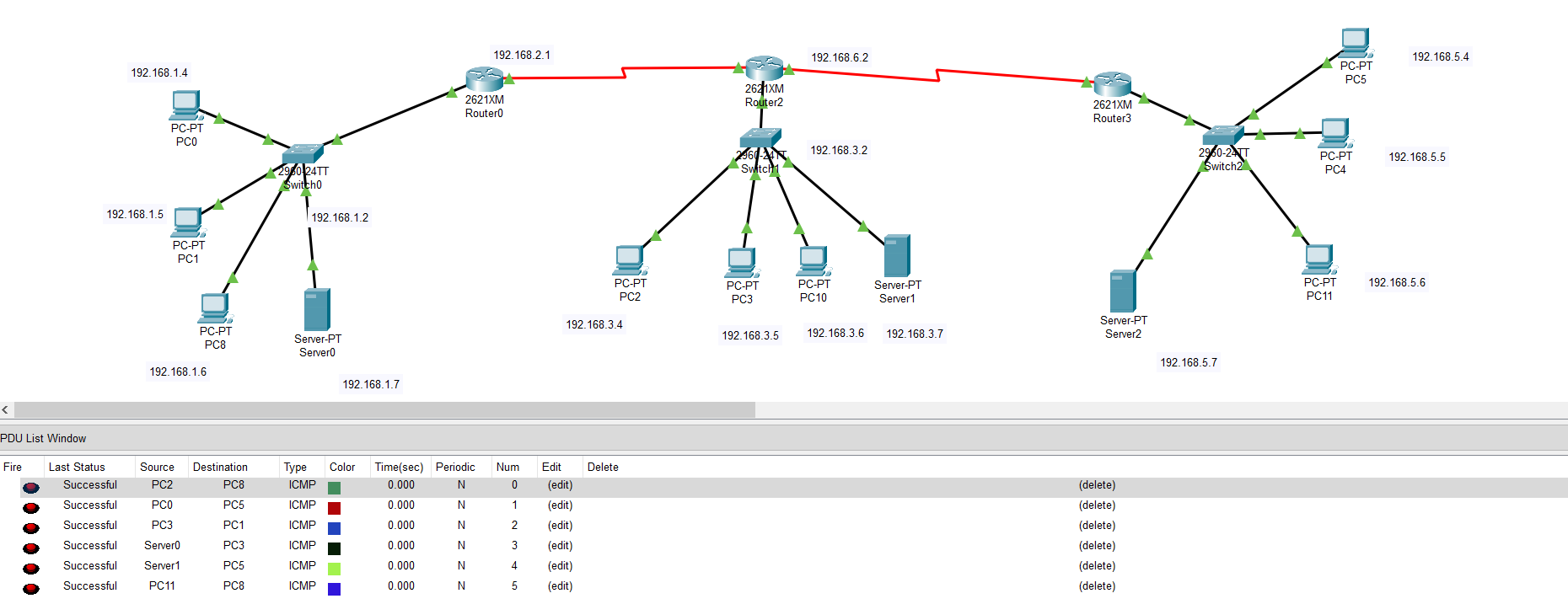
We will configure the servers as follows:



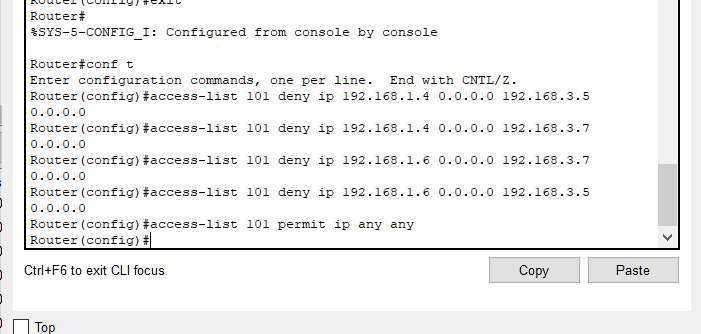
We will configure the router interfaces and perform static routing as follows to make the network work.



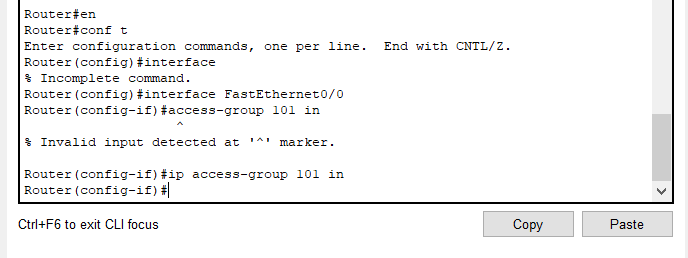
After performing static routing and configuring all the devices in our network, we can see from the following screenshot that our network has successful routing.



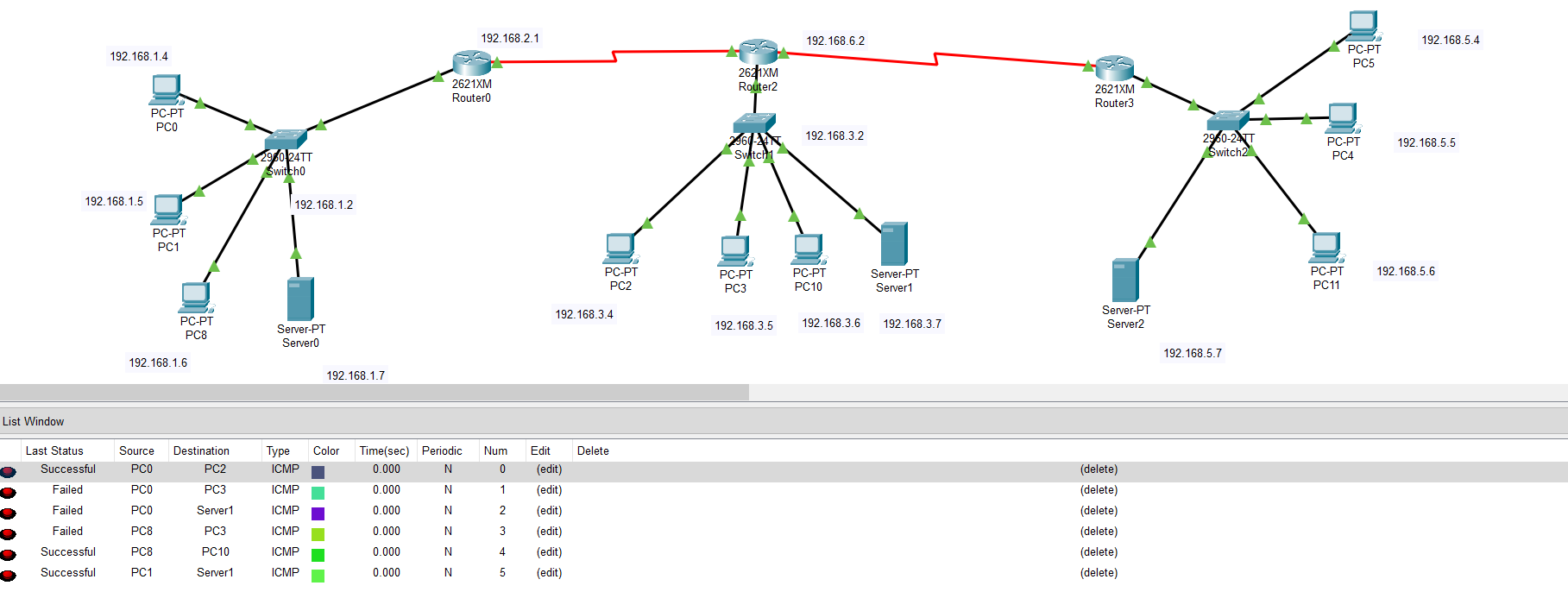
We will now write the **Extended Access-list** for even numbered devices to be able to send packets to only even numbered devices and odd numbered devices to be able to send packets only to odd numbered devices by writing command **access-list 101 deny ip 192.168.1.4 0.0.0.0 192.168.3.5 0.0.0.0** and so on as seen in the below screenshot.



We will enable the access-list as follows by using **ip access-group 101 in** command.



After applying the list, we see that the odd numbered devices can only communicate with odd numbered devices and even numbered devices can only communicate with even numbered devices from the following screenshot.

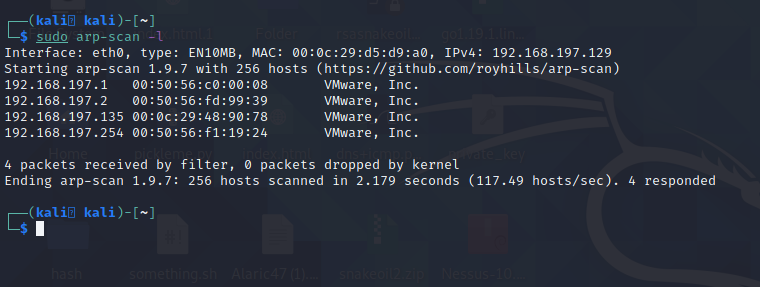


**Similarly, we have done this for other routers as well. Therefore, the task was successful.**

**Question 2. Using Kali and Metasploitable2.  
  Identify the vulnerability and exploit auxiliary/scanner/http/axis\_login.**

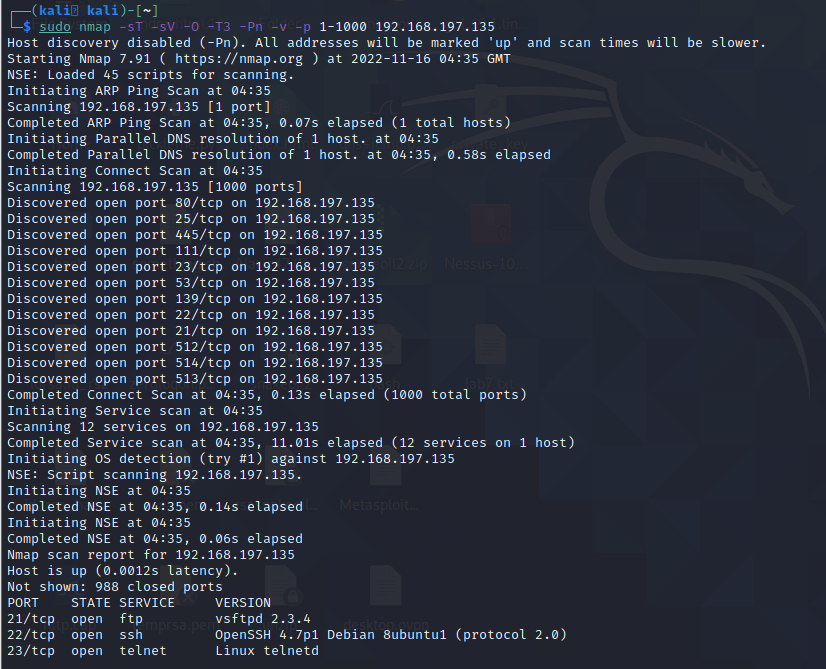
**Answer 2:**

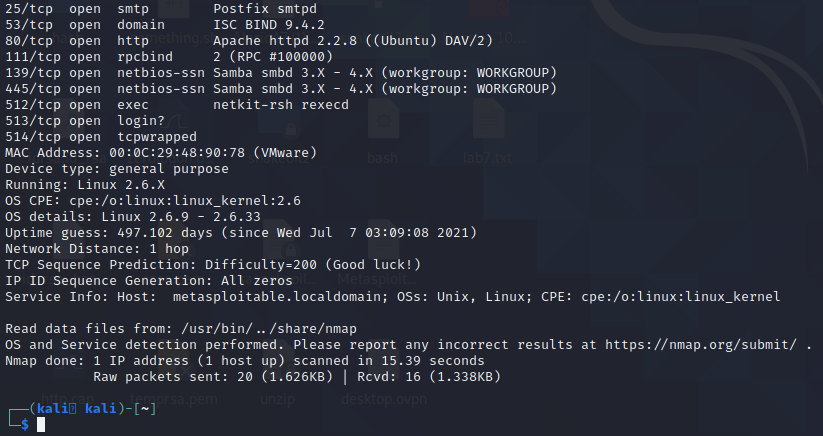
First, we perform an **arp-scan** on our kali machine to find the IP of the Metasploitable2 machine.



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

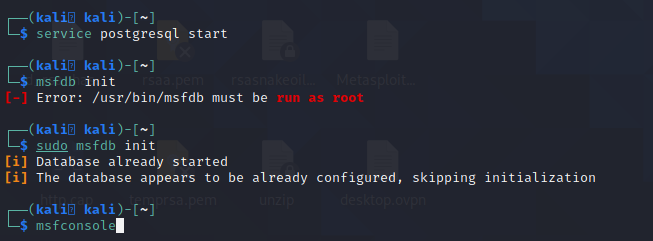
We will now perform an **Nmap scan** on the target machine to see which ports and services are open on it.





We see that http server Apache httpd 2.2.8 is running on port 80 from the Nmap scan.

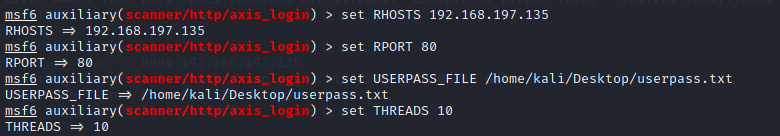
Now we will open up Metasploit by typing **msfconsole** in the terminal and starting the **postgresql** database service and initializing the database.



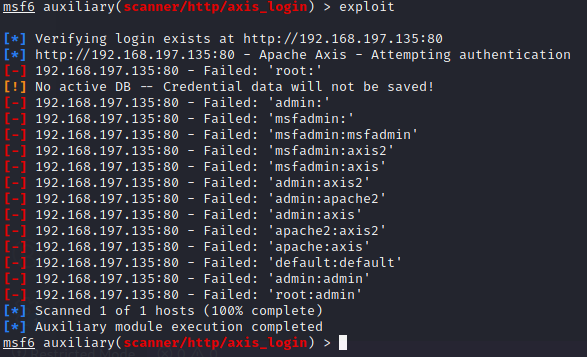


We will now try to use the module auxiliary/scanner/http/axis\_login to login to the Apache instance on the target machine.

We will now set the options, RPORT as 80 as that’s the port that our Apache service is running on, RHOSTS as the IP of Metasploitable2 i.e. 192.168.197.135 and USERPASS\_FILE as a userpass file.



Now we will hit exploit and try to brute force into the Apache instance of the machine using this module.



We see that we have attempted to brute force into the Apache server of the target machine using this module and we couldn’t brute force the password of the Apache server using the “userpass.txt” file.

Our exploit is now complete.