**Name: Shangirne Kharbanda**

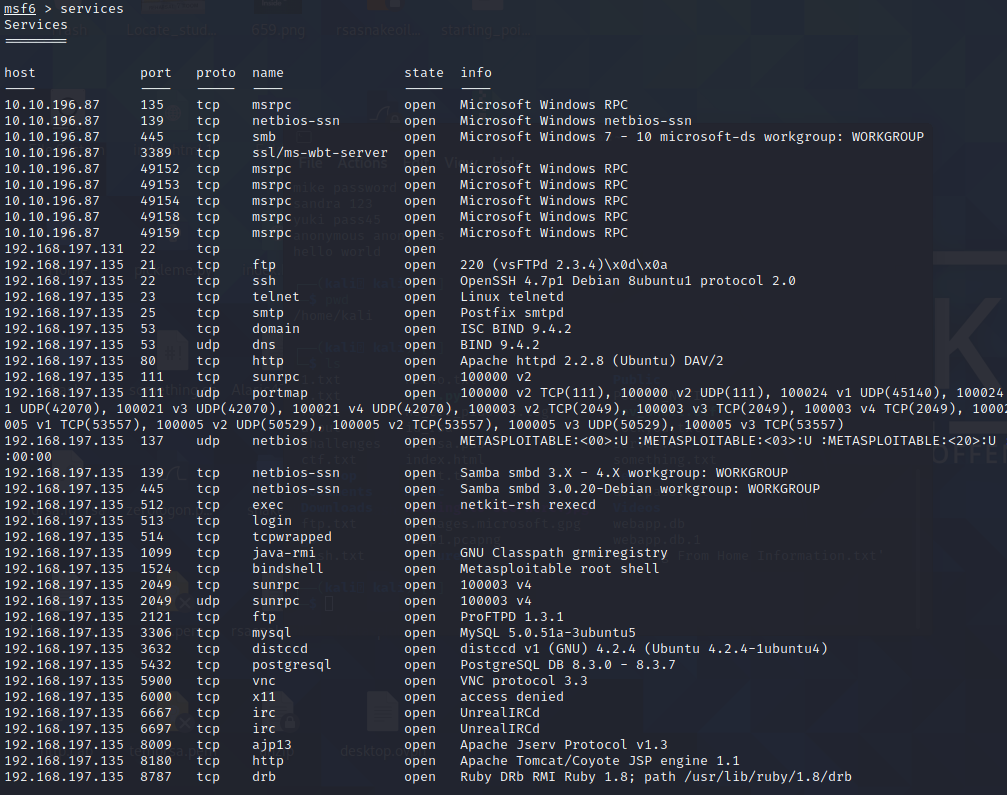
**Registration Number: 20BAI1154**

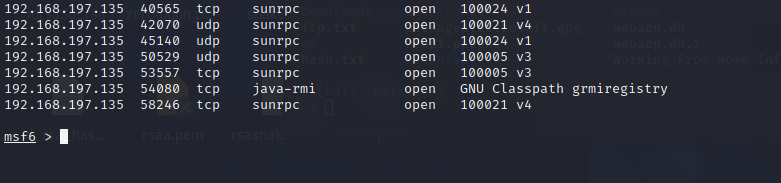
**ISAA LAB-4**

**SCANNING AND ENUMERATION OF HTTP, SMTP, SSH PROTOCOLS**

We know that the IP of our target machine is **192.168.197.135** and what services are running from our previous enumeration of the machine in previous lab(ISAA LAB-3). We ran an Nmap scan on the target machine for the same and stored our scan results in the metasploit database running postgresql.

We can bring up the services running on our target machine by typing **services** in metasploit.

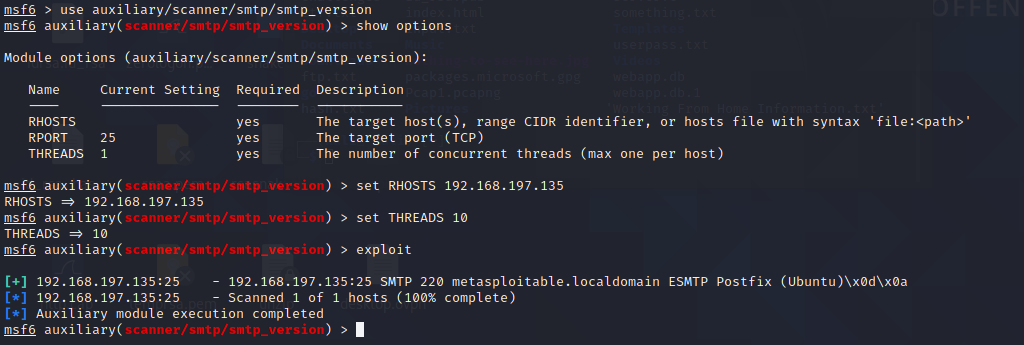




**SMTP Protocol:**

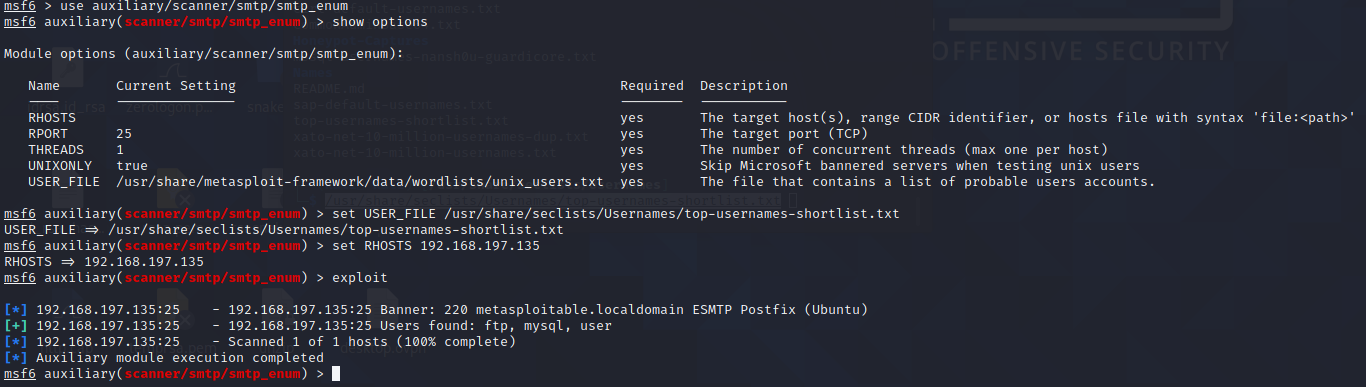
We know from our enumeration of the target machine that SMTP is running on port 25.

We will find the version of the SMTP running on our target machine by using the metasploit module **auxiliary/scanner/smtp/smtp\_version**.



The SMTP service has two internal commands that allow the enumeration of users: VRFY (confirming the names of valid users) and EXPN (which reveals the actual address of user’s aliases and lists of e-mail (mailing lists). Using these SMTP commands, we can reveal a list of valid users.

We can do this manually, over a telnet connection- however Metasploit comes to the rescue again, providing a handy module appropriately called "smtp\_enum" that will do the legwork for us! Using the module is a simple matter of feeding it a host or range of hosts to scan and a wordlist containing usernames to enumerate. We will use the module **auxiliary/scanner/smtp/smtp\_enum**.



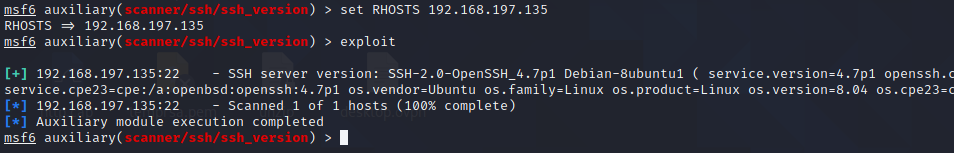
We can see that there were some users returned to us namely **ftp, mysql, user**.

Our enumeration of SMTP protocol is now complete.

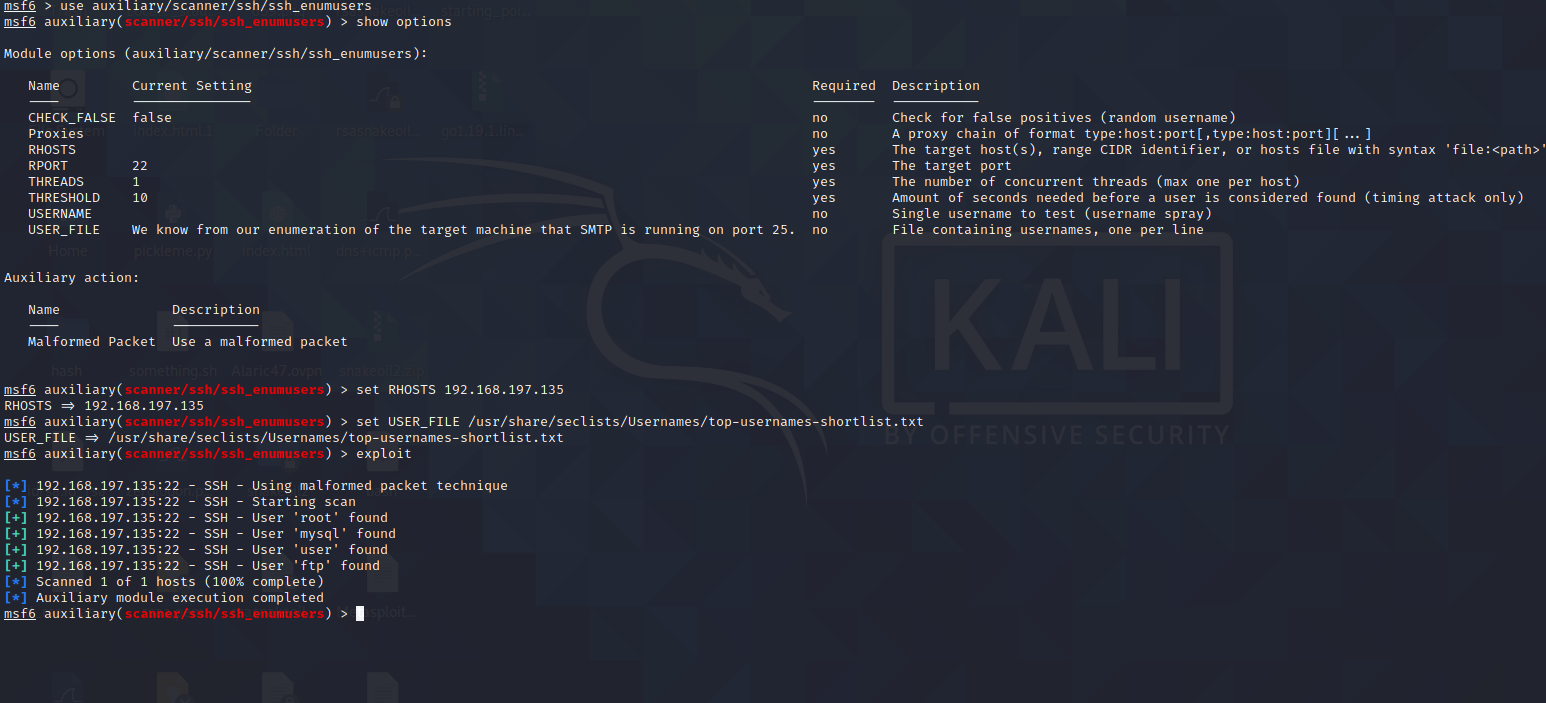
**SSH Protocol:**

We know from our enumeration of the target machine that SSH is running on port 22.

We will find the version of the SSH running on our target machine by using the metasploit module **auxiliary/scanner/ssh/ssh\_version**.



Now we can enumerate the users on SSH by using the metasploit module **auxiliary/scanner/ssh/ssh\_enumusers**.



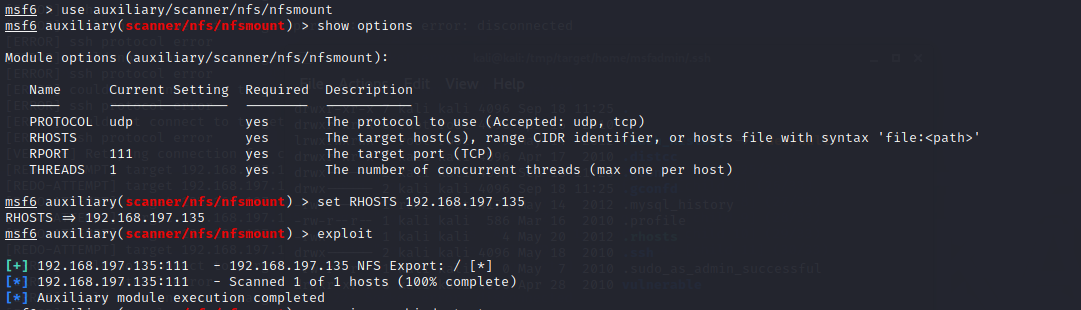
We have found 4 users namely **root, mysql, user,ftp**.

Now we are going to try to log into SSH.

To do this, we are going to look for an SMB or an NFS share.

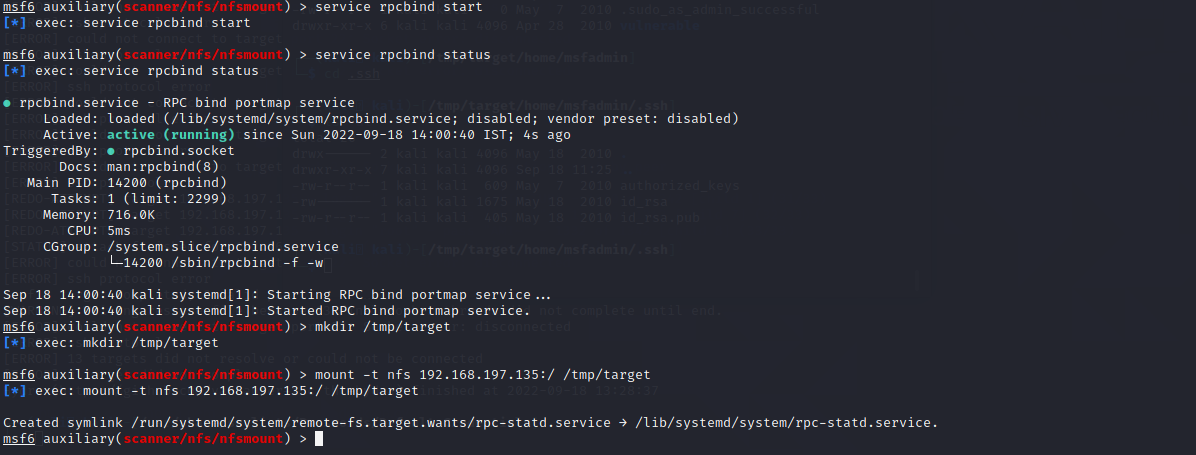
We found out during our enumeration of SMB that there are no SMB shares on the target machine.

So we will try to see if there is an NFS share that we can mount by using the module **auxiliary/scanner/nfs/nfsmount**.

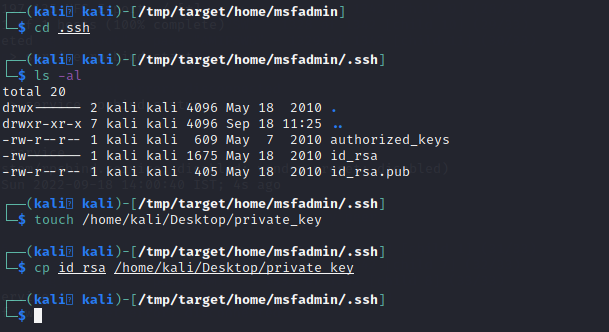


We see that there is a NFS share “/” that we can mount on our attacker machine.

We are going to make a directory in /tmp folder namely target and we are going to mount this nfs share on there.

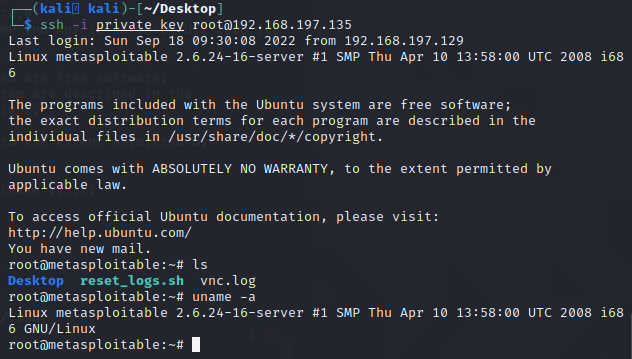


Now we will look for the SSH private key in the NFS share that we just mounted in /tmp/target..



Now that we have the private key, we can log into SSH of one of the users that we have found from our previous user enumeration of SSH.

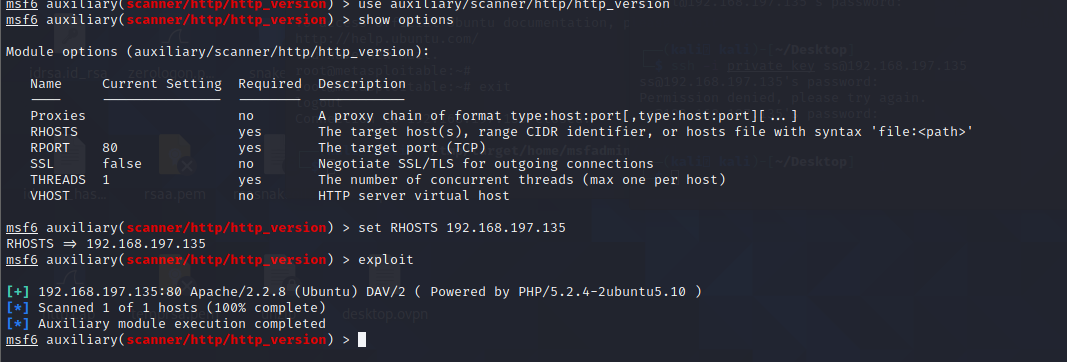
We will try to SSH into the target machine as “root” user.



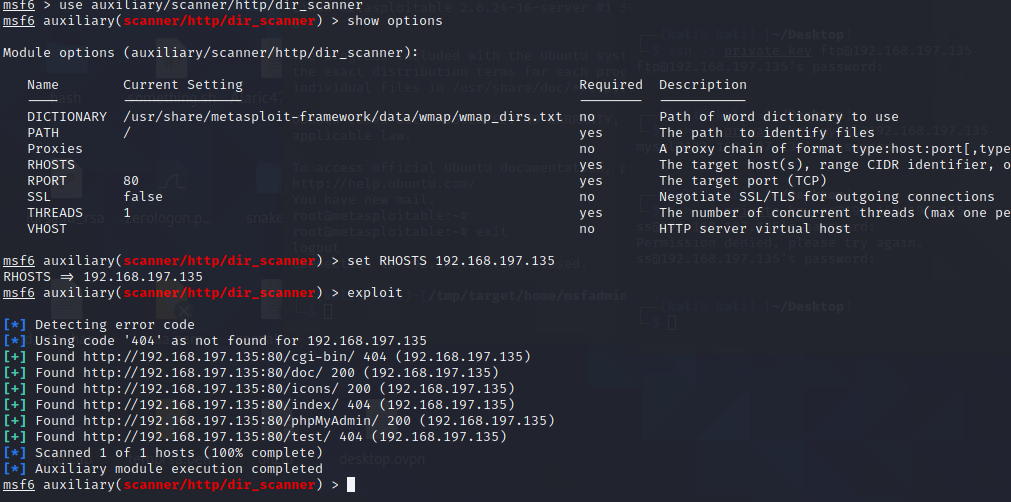
Now that we have successfully infiltrated our target machine by SSHing into it and with the help of the private key of the target machine, we have got a root shell on our target machine.

**HTTP Protocol:**

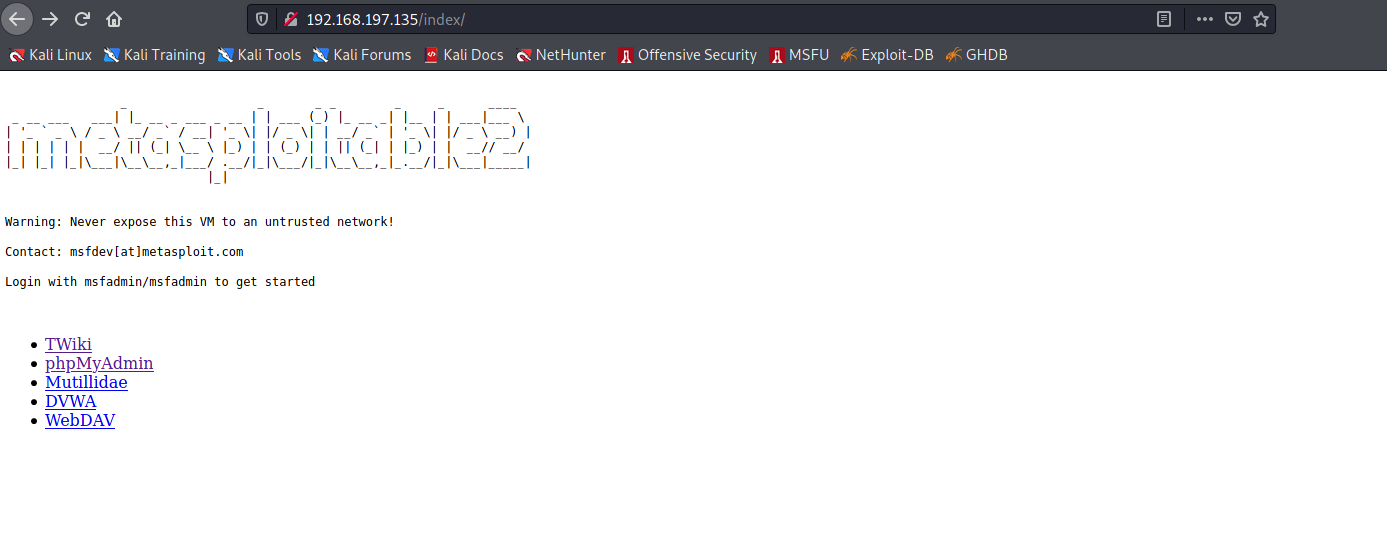
We will see which version of HTTP is running on the target machine by using the module **auxiliary/scanner/http/http\_version**.



We can scan the directories on this HTTP website by using the module **auxiliary/scanner/http/dir\_scanner**.



We can visit <http://192.168.197.135:80/index/> to look for any web vulnerabilities on our target machine and go from there.



We are done with our enumeration and scanning of HTTP protocol on our target machine.