**Name: Shangirne Kharbanda**

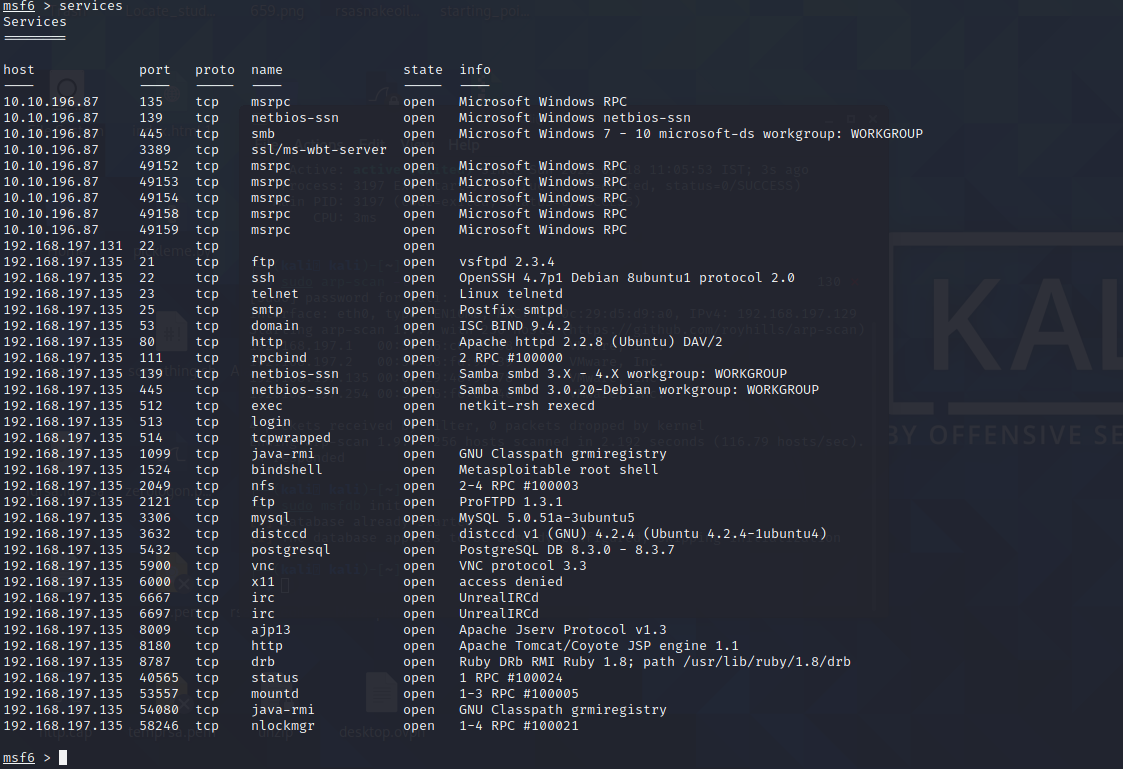
**Registration Number: 20BAI1154**

**ISAA LAB-6**

**Exploiting FTP service and other services using metasploit**

We did our nmap scan in ISAA Lab-5 on our target i.e. **192.168.197.135** and so the results from that nmap scan are stored in the database and now we can access those results.

We will again type services in metasploit to see what services are running on our target machine.



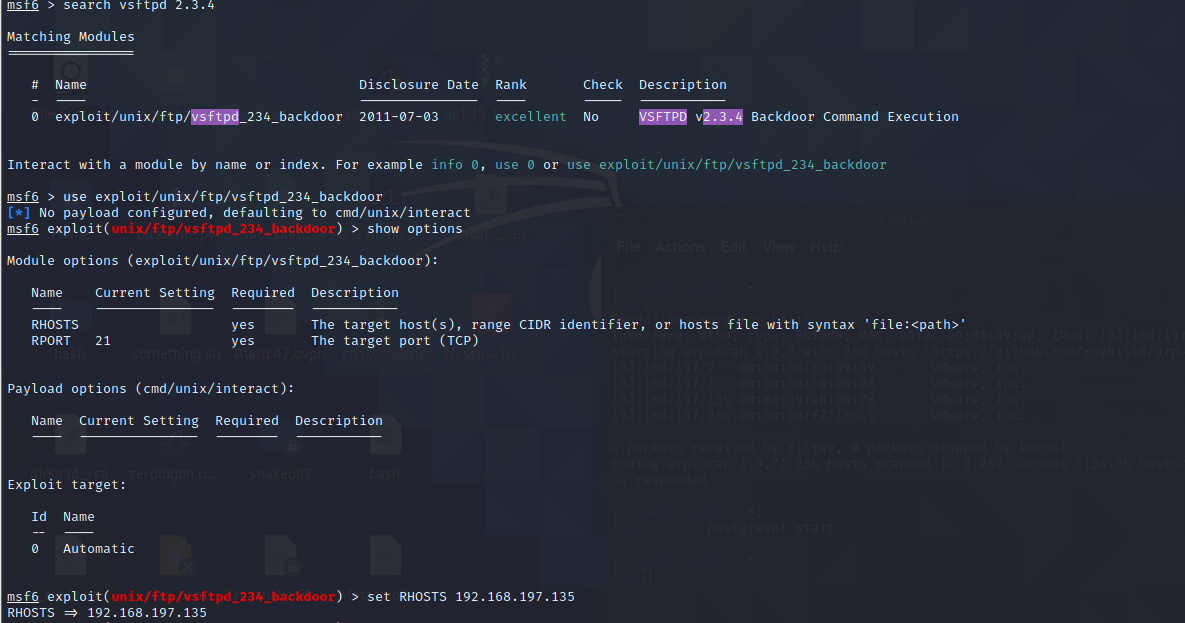
**1. FTP Exploit:**

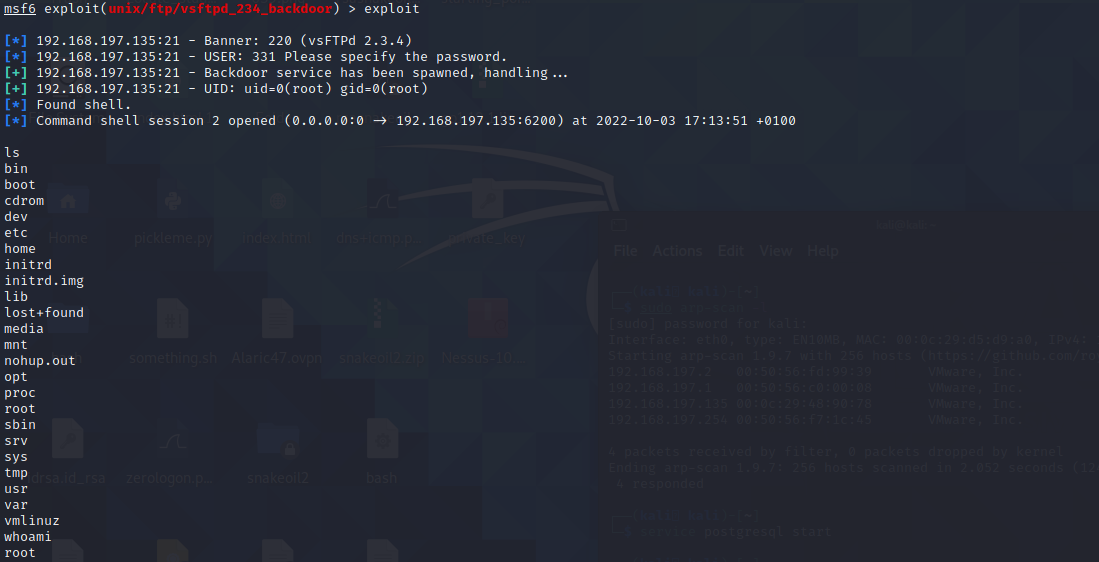
Now we will exploit the FTP service that’s running on port 21 on the machine in two ways.

Method 1:

We will use the popular vsftpd 2.3.4 exploit that will open up a backdoor on the target machine and get us a shell back. Lets try it.

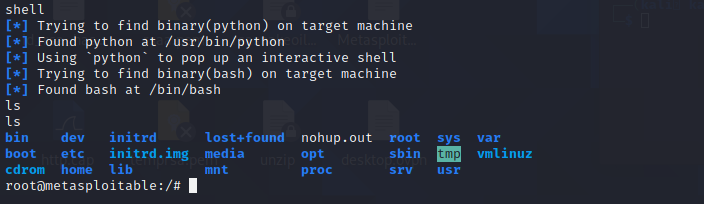
We will use the module **exploit/unix/ftp/vsftpd\_234\_backdoor** for this.





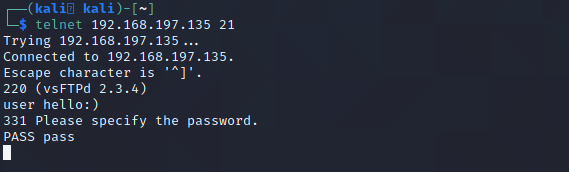
By using this exploit, we can see that we have gotten a shell back.

To get an interactive shell, we will simply type in shell now and gain an interactive shell on the target machine as shown.

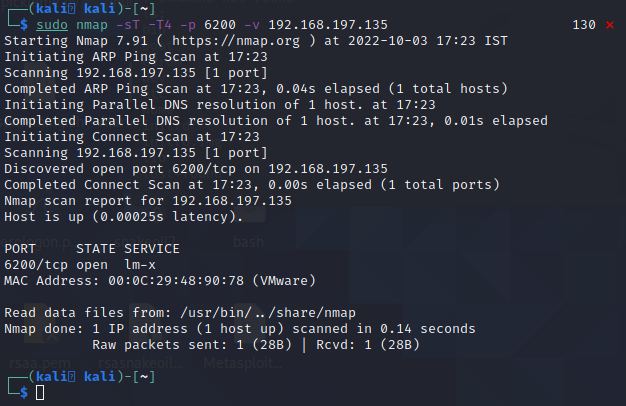


Method 2:

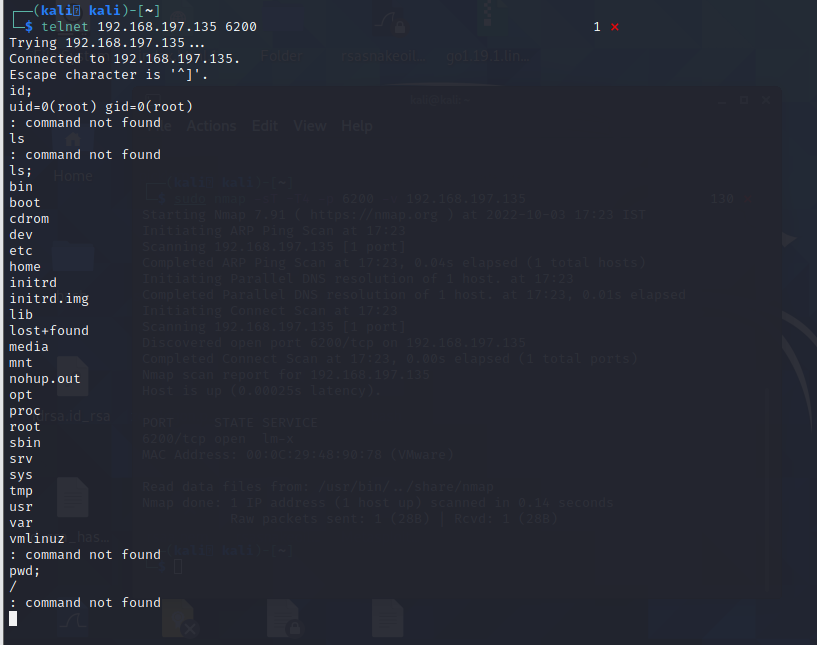
We will use telnet to connect to our target machine and exploit FTP on it.



We will specify a username with a ☺ character and that will open up a listening shell on port 6200. Lets see if port 6200 is open on our target machine or not.



Port 6200 is open so now we can connect to it and gain access to the target machine.

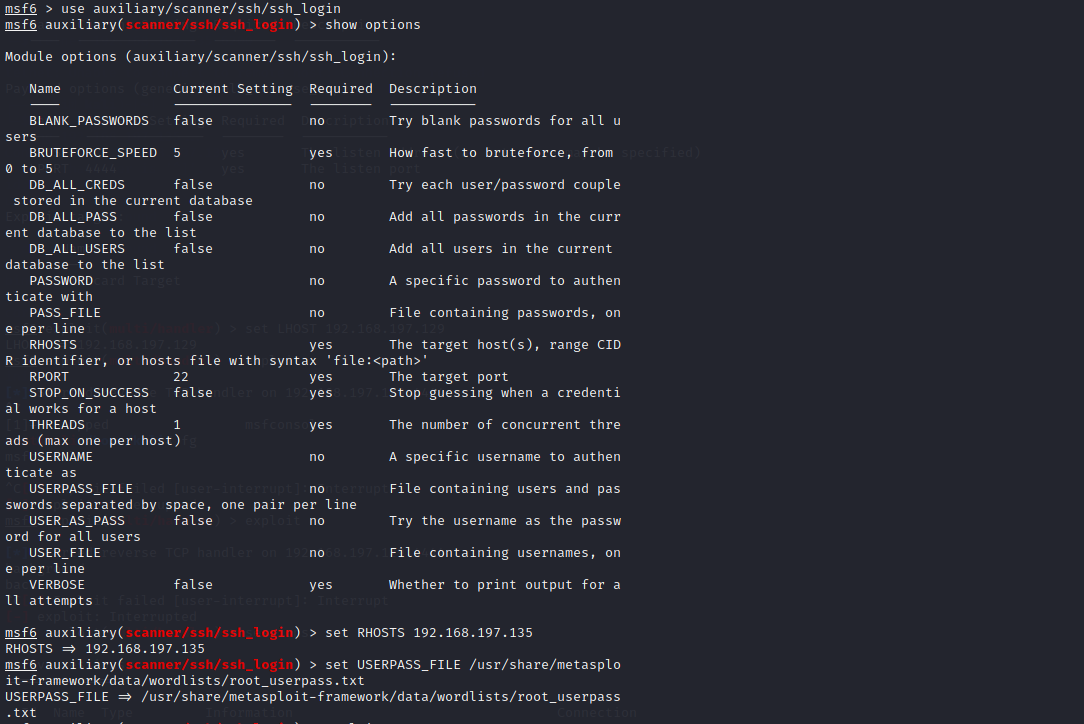


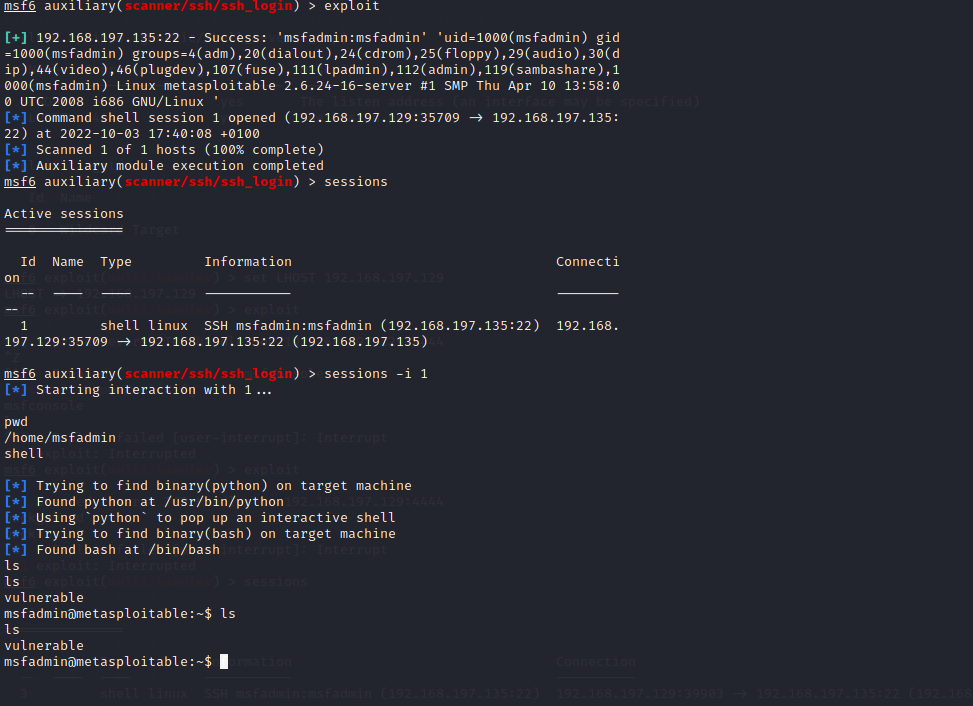
Therefore, we have exploited the FTP service using two methods.

**2. SSH Exploit:**

We know that port 22 is open on our machine that is SSH. We will now try to exploit SSH on the machine using metasploit.

We will use the module **auxiliary/scanner/ssh/ssh\_login** for this purpose.



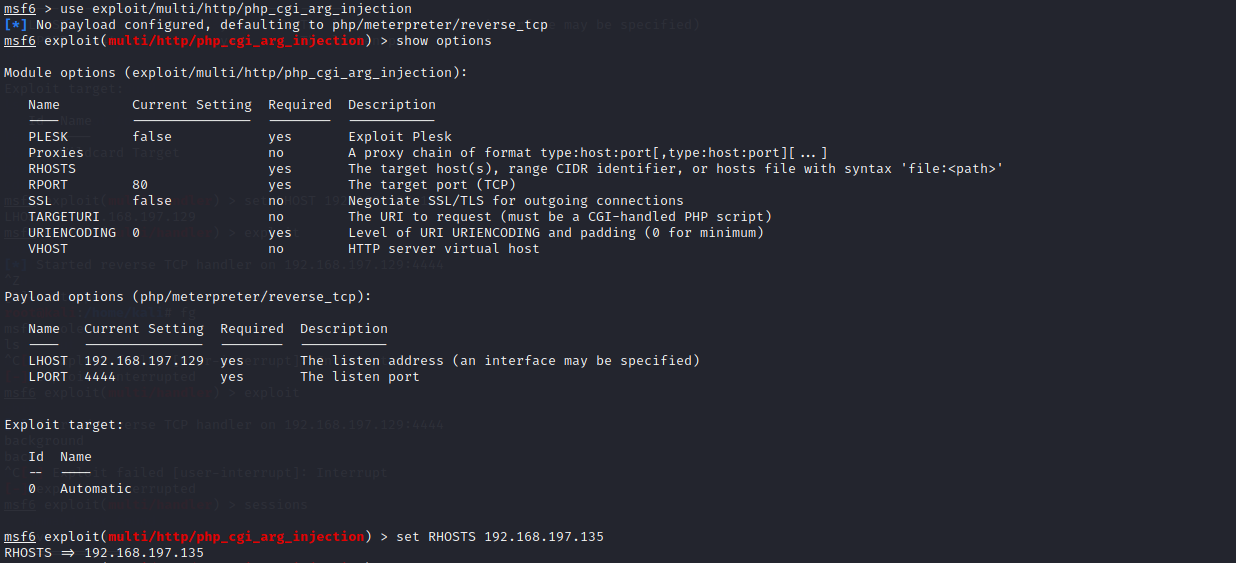


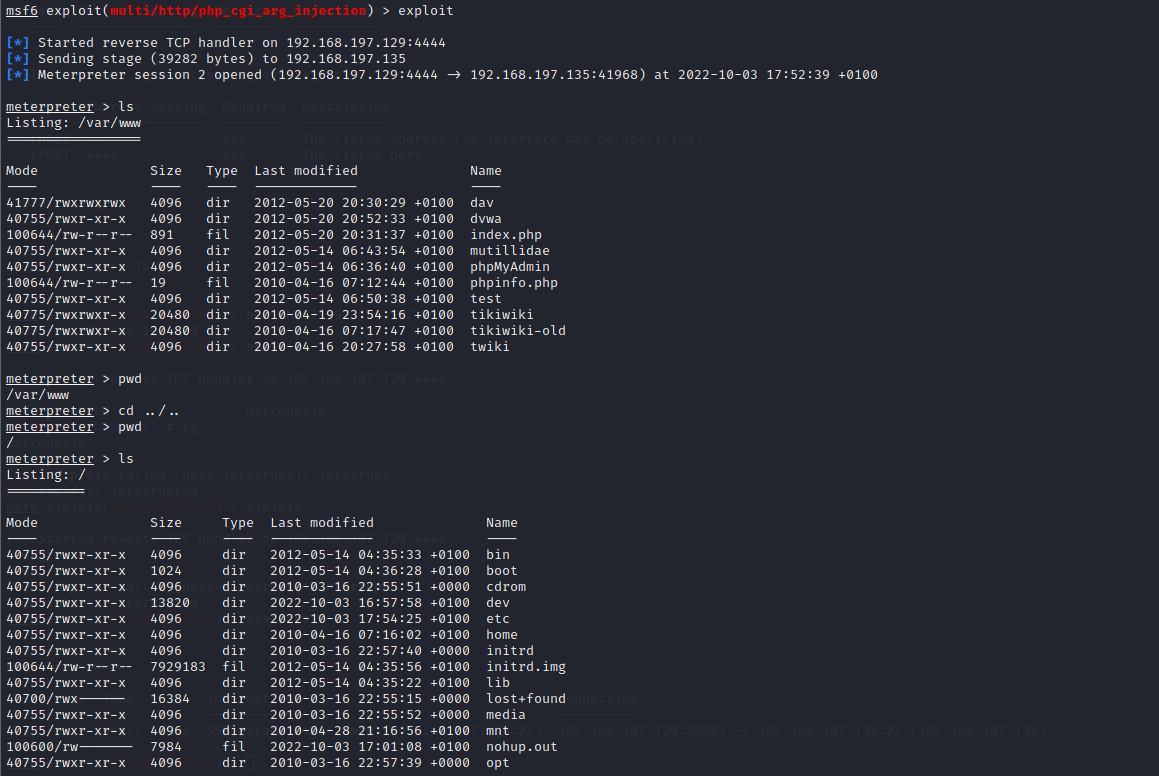
We have successfully brute-forced SSH login and gained a shell on our target machine.

**3. PHP Exploit:**

We see that theres an Apache HTTP server running on port 80 that uses PHP. We will use a metasploit module to gain a shell on the HTTP web server running on port 80.

We will use the module **exploit/multi/http/php\_cgi\_arg\_injection** to do this.

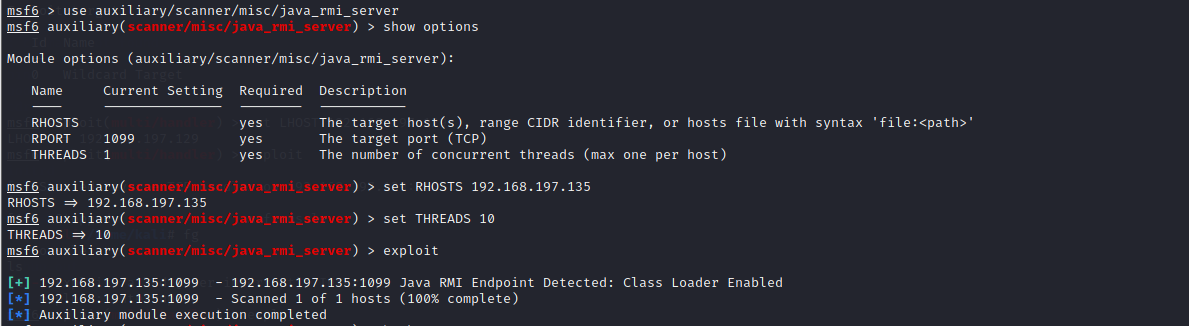




**4. Java-rmi server exploit:**

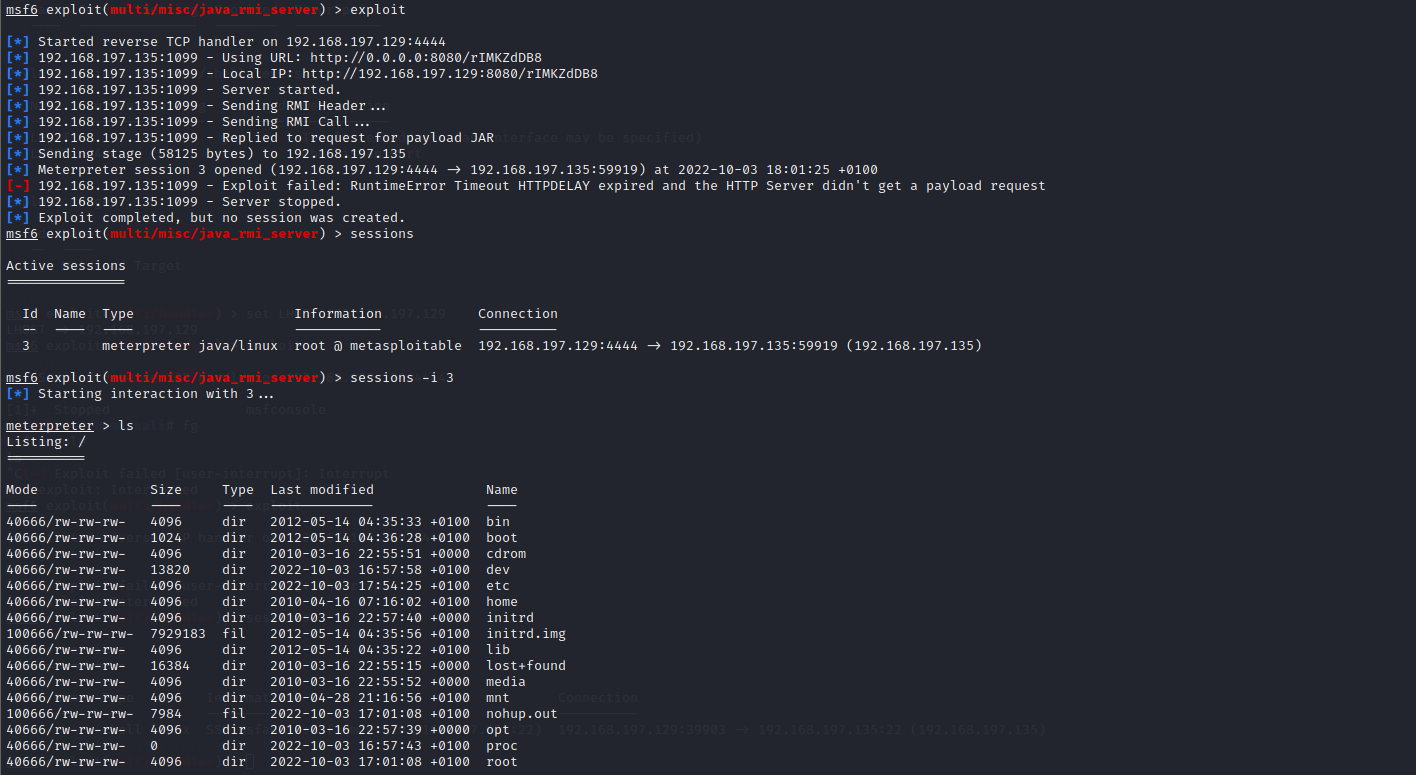
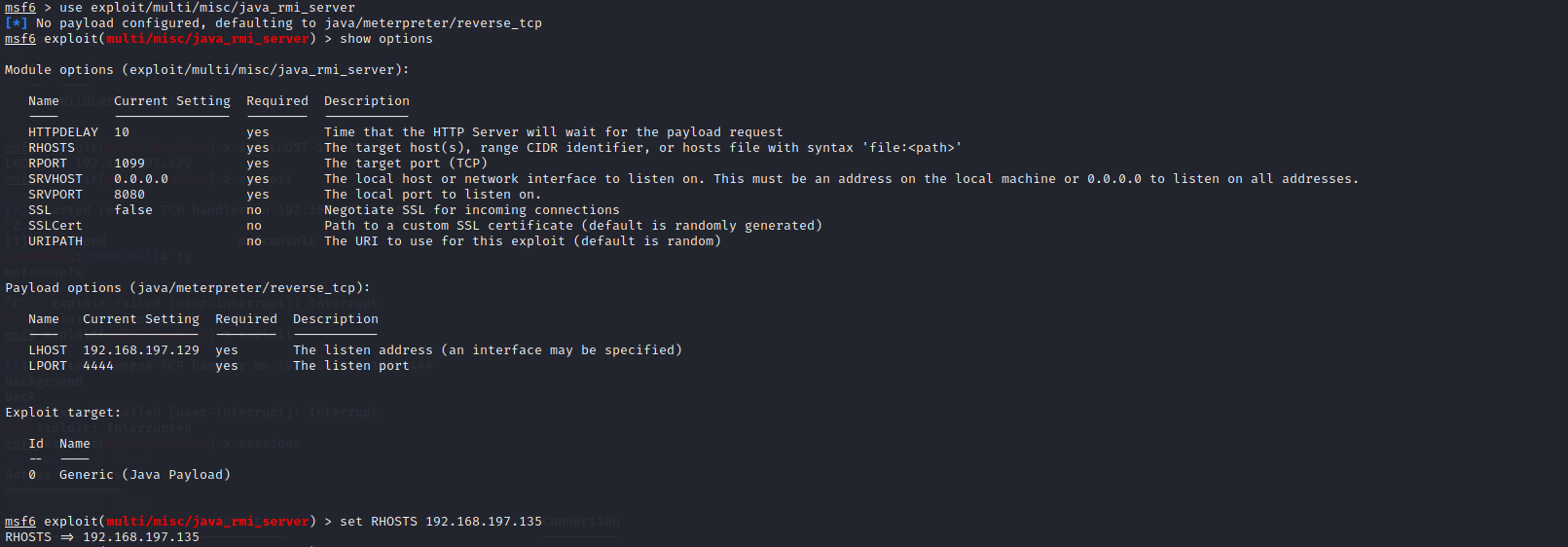
We see that Java-rmi service is running on port 1099 and we will now try to exploit that.

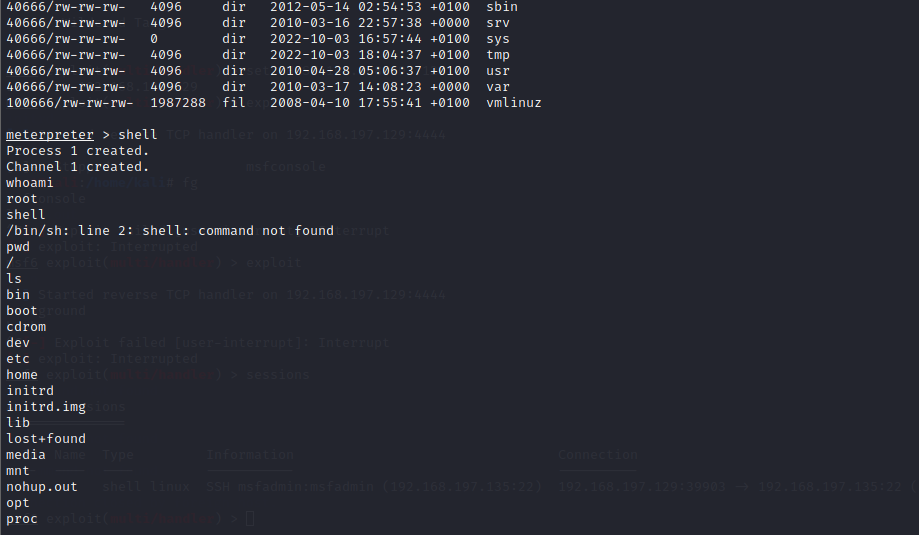
We will first use the module **auxiliary/scanner/misc/java\_rmi\_server** to see if the Java-rmi server running on the target machine is vulnerable to the java insecure code execution exploit that we are going to run on it.



Now we have everything to run our exploit.

We will use the module **exploit/multi/misc/java\_rmi\_server** to be able to exploit this vulnerability.





Therefore, we have successfully gained a shell on our target machine using this exploit.