**Name: Shangirne Kharbanda**

**Registration Number: 20BAI1154**

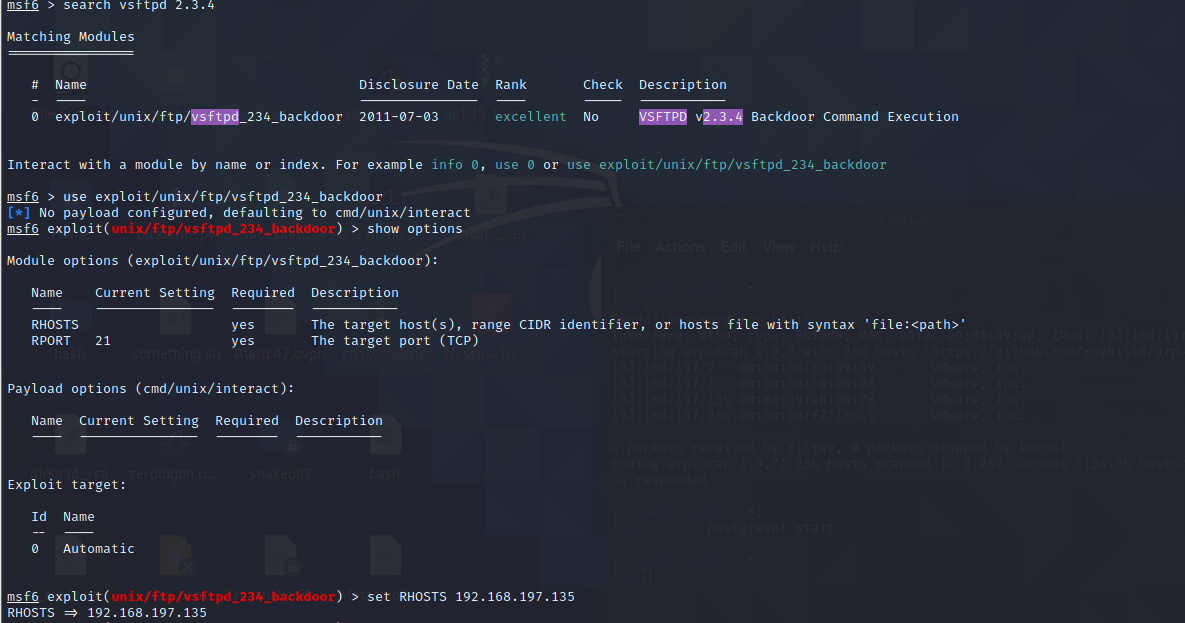
**ISAA LAB-7**

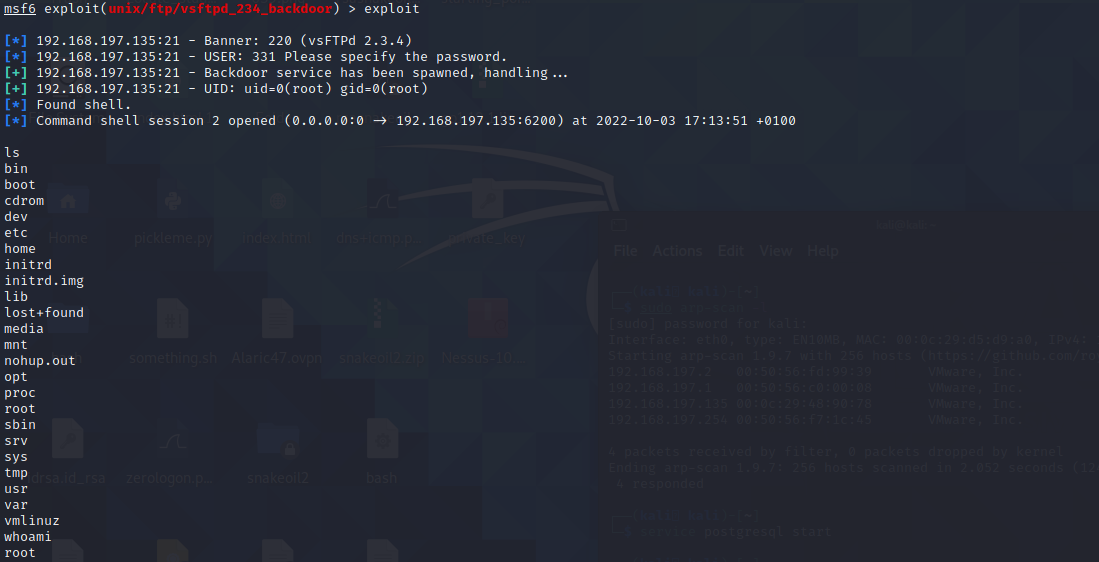
**Exploiting FTP service:**

Now we will exploit the FTP service that’s running on port 21.

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.

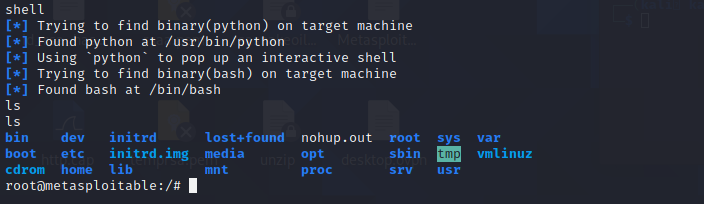
We will use the module **exploit/unix/ftp/vsftpd\_234\_backdoor** for this.





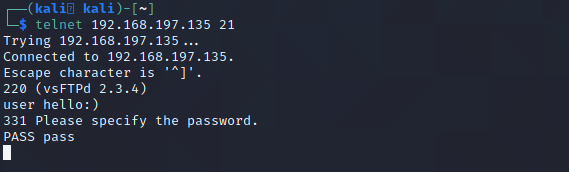
By using this exploit, we can see that we have gotten a shell back.

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

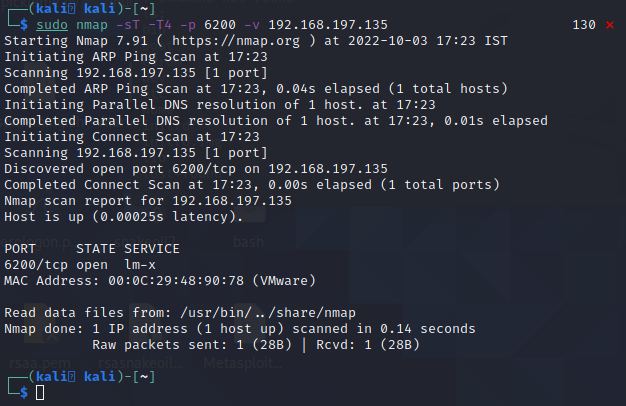


**Manually Exploiting FTP service:**

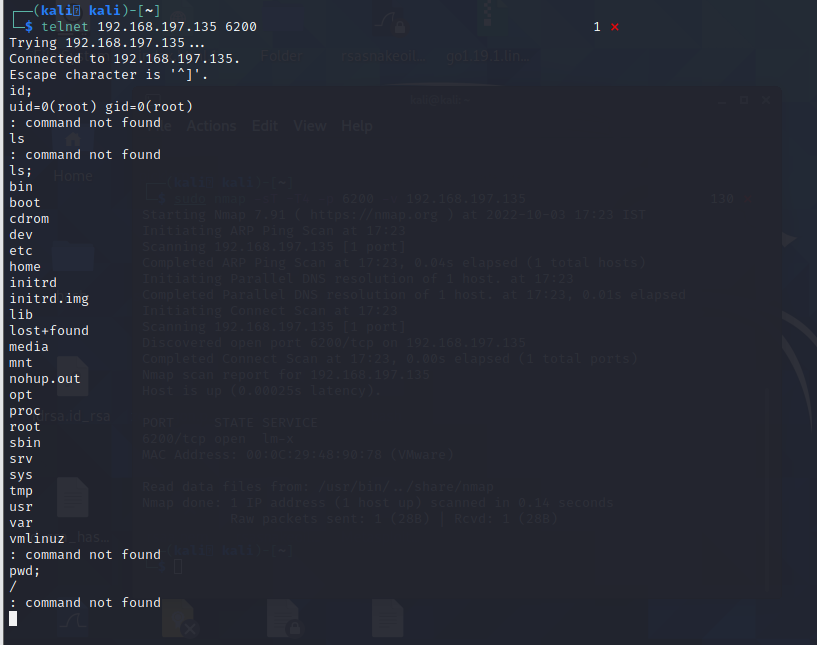
We will use telnet to connect to our target machine and exploit FTP on it manually.



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.

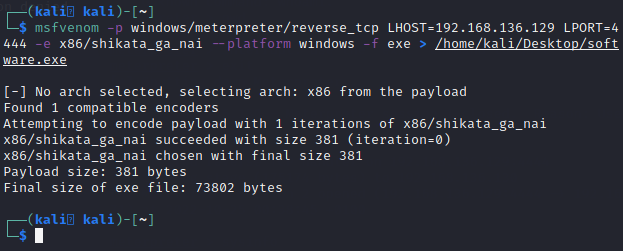


Thus, we have manually exploited the FTP service here.

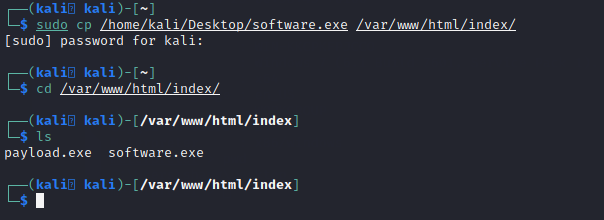
**Windows Exploit:**

First we will use msfvenom to generate a payload which the Windows 7 user will run on their machine.

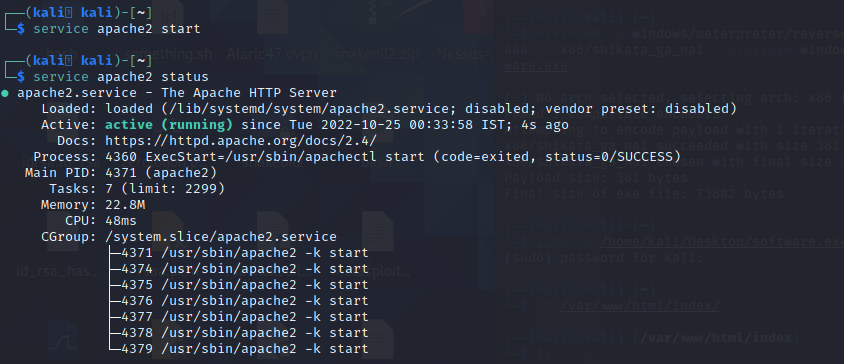
We will do that as follows:



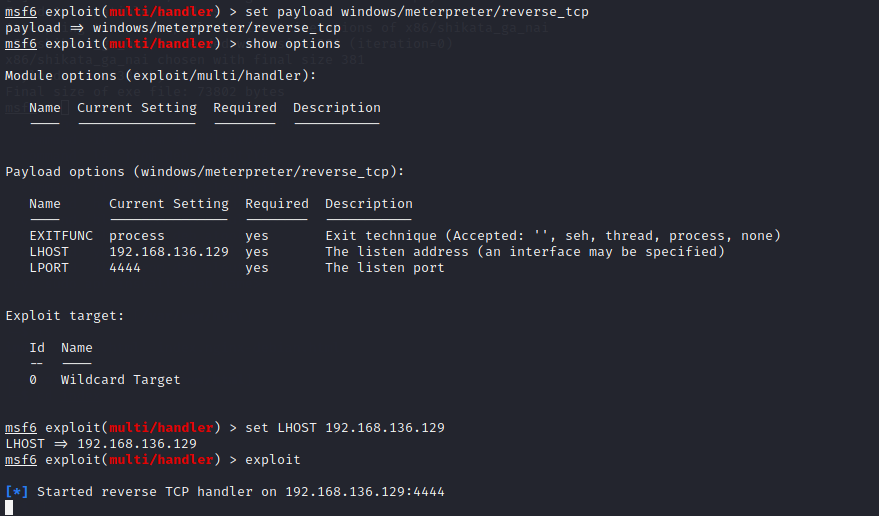
Now we will copy this payload to /var/www/html



Now we will start the apache2 service to host an http server.

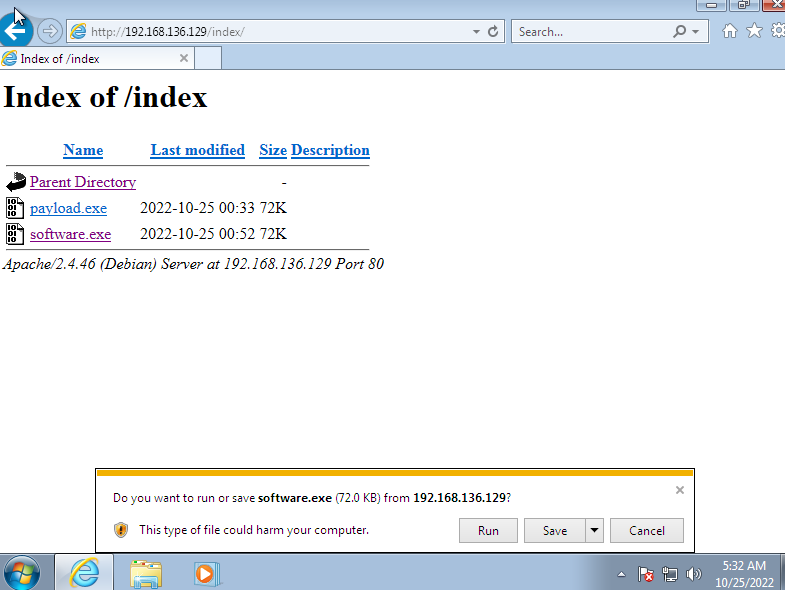


Now we will move to Metasploit and use the exploit multi/handler and set payload as windows/meterpreter/reverse\_tcp.

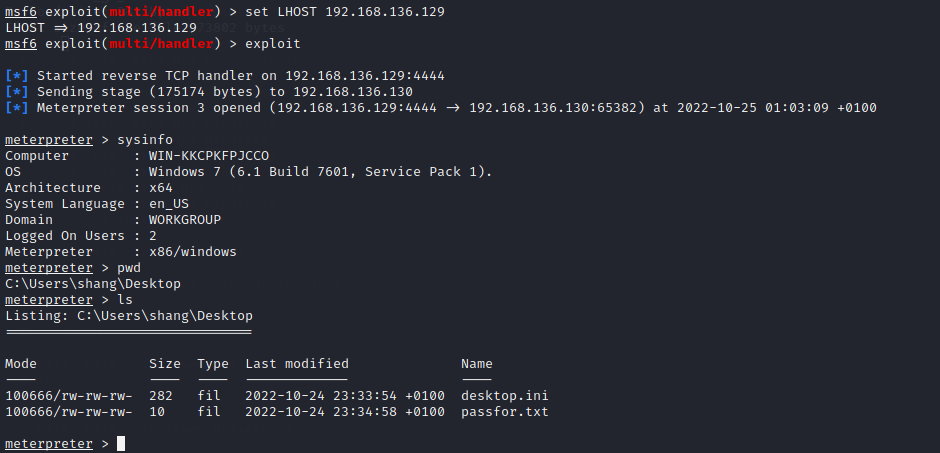


Now we are listening in on port 4444.

Now we will host our payload on an http server for the victim to download and run on their Windows 7 machine.



As soon as the victim runs this file, we get a reverse meterpreter shell on our Kali machine.



Therefore, we have successfully exploited this windows vulnerability.