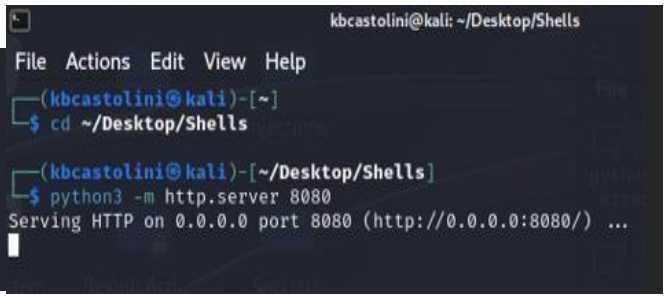
Establishing a reverse shell client

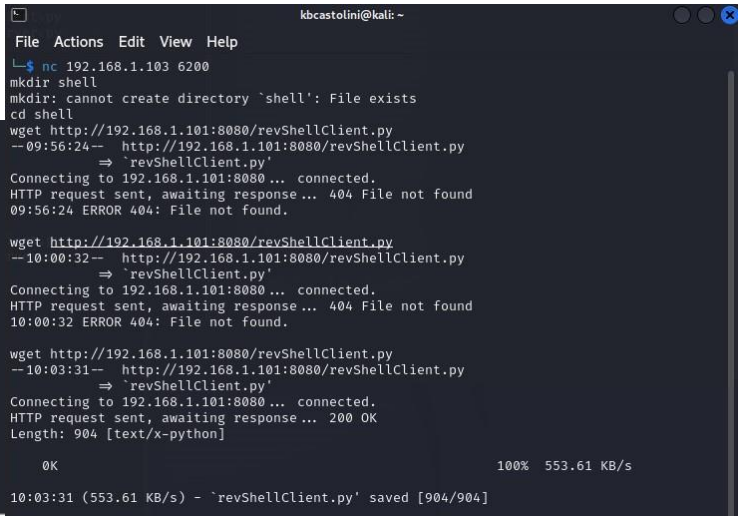
Using python, I wrote a reverse shell client, in which it's purpose is to be installed on the machine I am attacking and it will initiate a connection from within the network to the attackers computer that is outside of the network. This gets around a firewall and NAT from a companies network. Next, I wrote a bind shell, which allows me to execute commands remotely from my computer to the compromised machine. In my case, I am attacking a vulnerable Metasploitable virtual machine from my kali linux virtual machine.

a

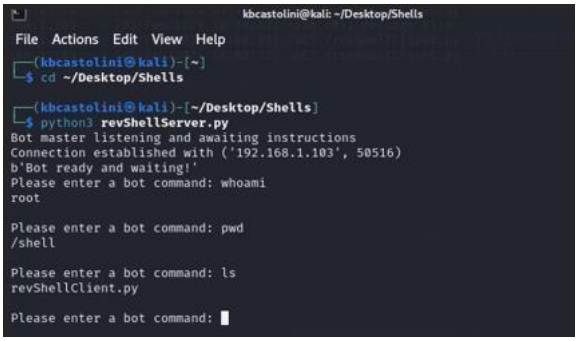


b

c

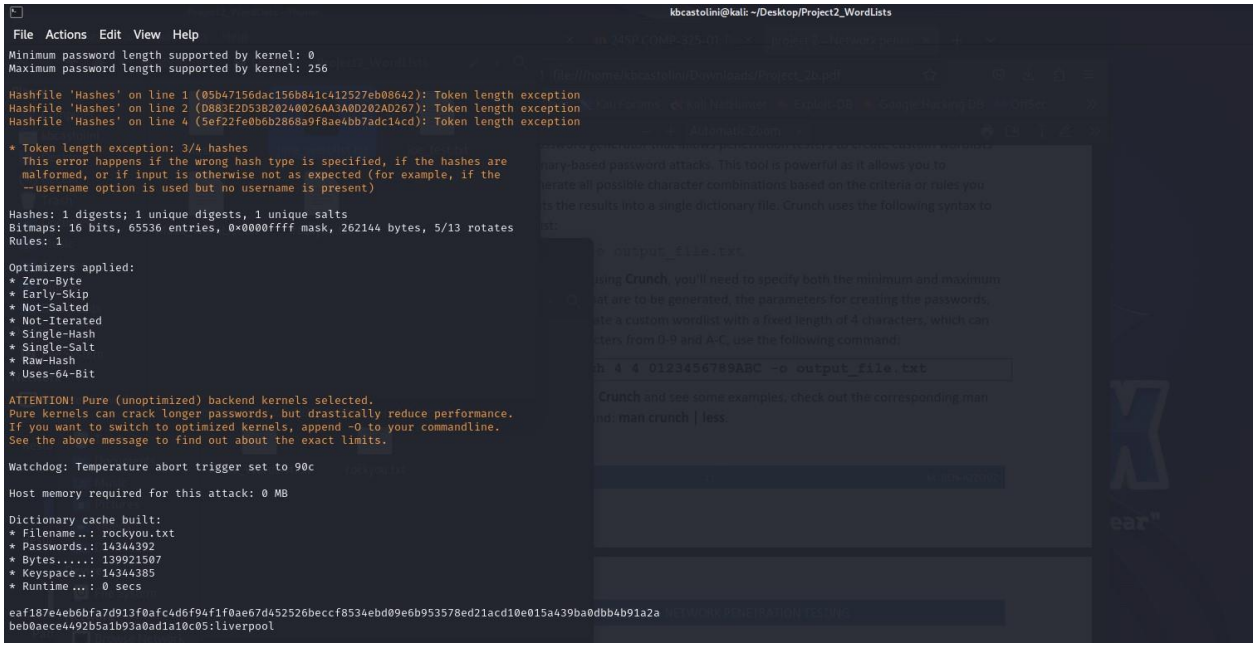


d



e

a) Get the server ready to go, await the client to connect to it
b) Start a local web server using netcat (nc) that will serve the reverse shell client that I created to the metasploitable virtual machine (compromised machine)
c) Establish an FTP connection from the kali terminal to the metasploitable machine (ip address 192.168.1.103 in my case as shown in screenshot) the login credentials used are that of the metasploitable machine
d) In order to create a working reverse shell, we are connecting to the vsftp backdoor shell on port 6200. A new directory is created on my metasploitable machine that we use to download the reverse shell python client from the kali box. “200 OK” lets me know that the download was successful
e) In this screenshot we can see we gained access to the metasploitable machine via reverse shell. All I had to do was call the reverse shell server and it is ready for me to execute commands as if I am in the terminal of the metasploitable machine.



At the bottom of this final screenshot, Zoe’s hash along with the now compromised password, “liverpool” is shown.