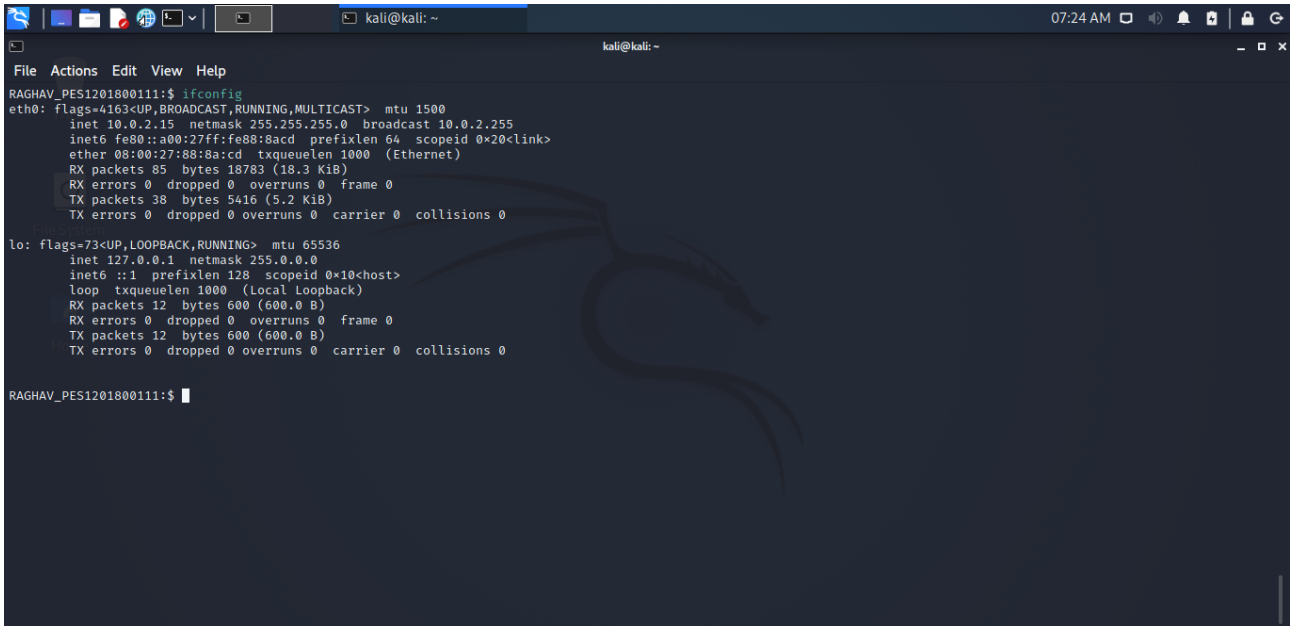
Ethical Hacking
Assigment-1

By:
Raghav Goyal,
PES1201800111,
Section-D,
Roll No: 7

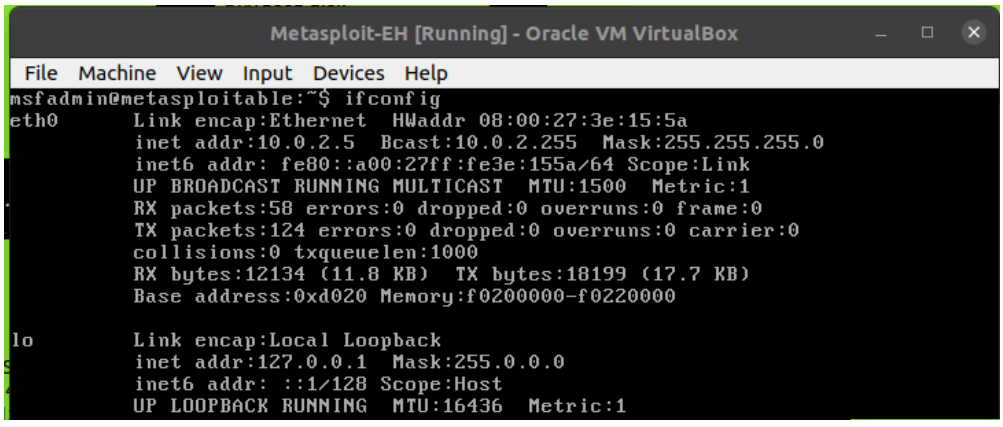
Configuration:

Kali OS System (Attacker): 10.0.2.15



Terminal prompt: RAGHAV_PES1201800111:$

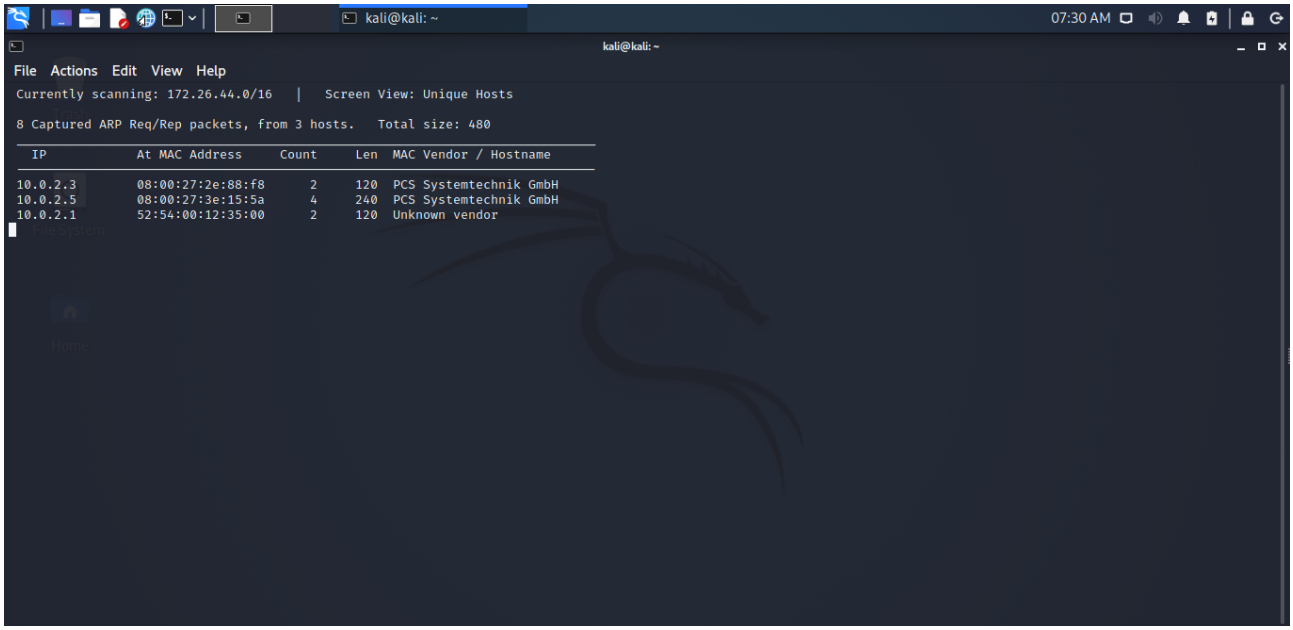
Metasploitable (Victim): 10.0.2.5



Initial Scannings:

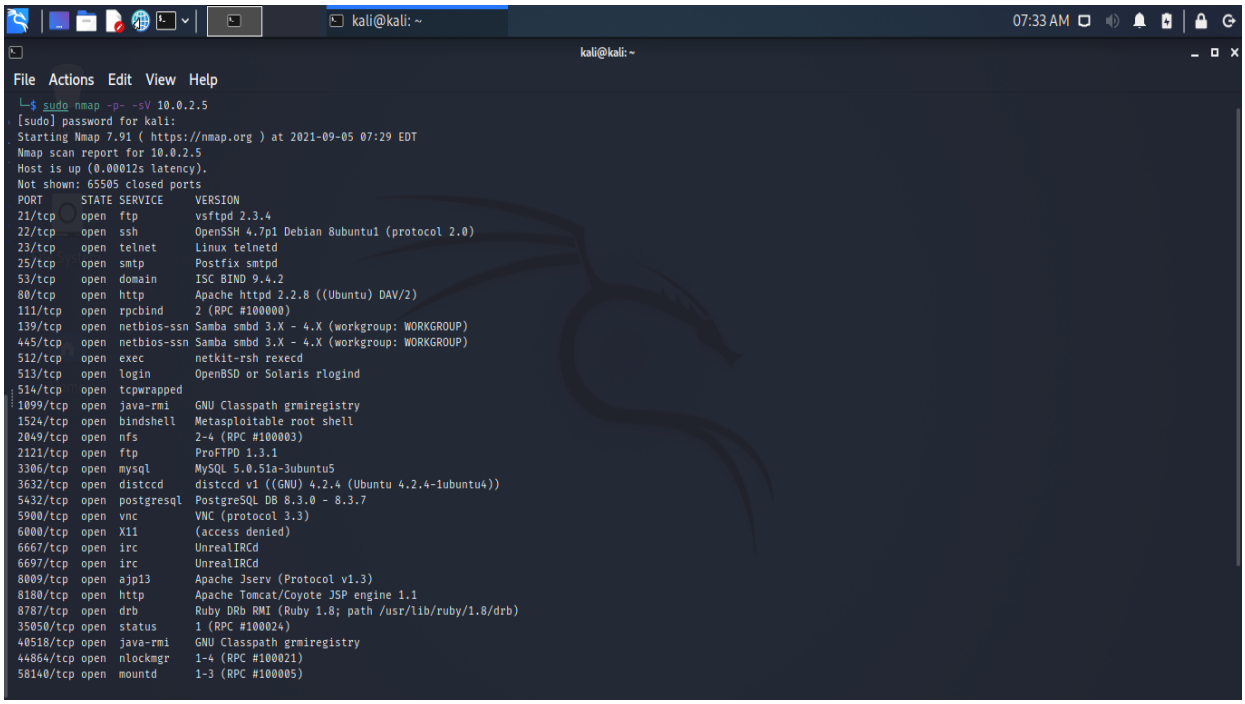
1. Discovering victim's IP:

$ sudo netdiscover



We see that victim's IP ==10.0.2.5 has been discovered.

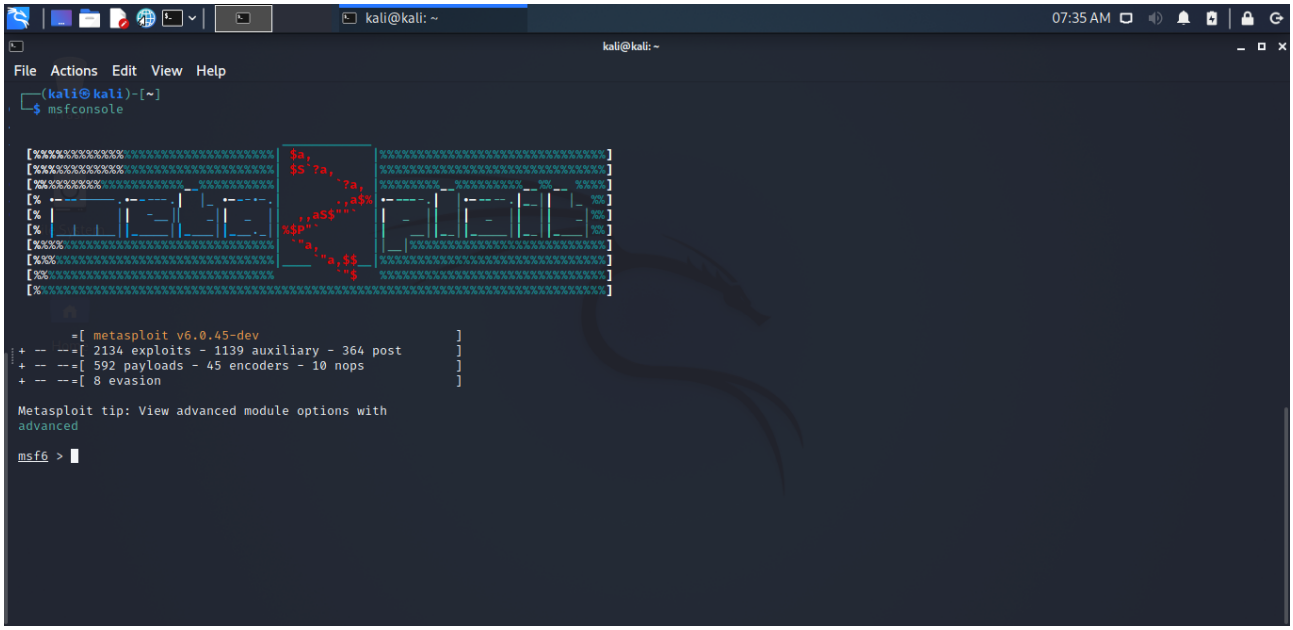
2. Scan the victim for vulnerable services on all the ports:



List of all vulnerable open services with their ports used is outputed.

Out of these services, I will be exploiting following services:
i. distccd v1
ii. UnrealIRCd

3. Open msfconsole



msfconsole provides efficient access to all options available in Metaspoitable Framework.

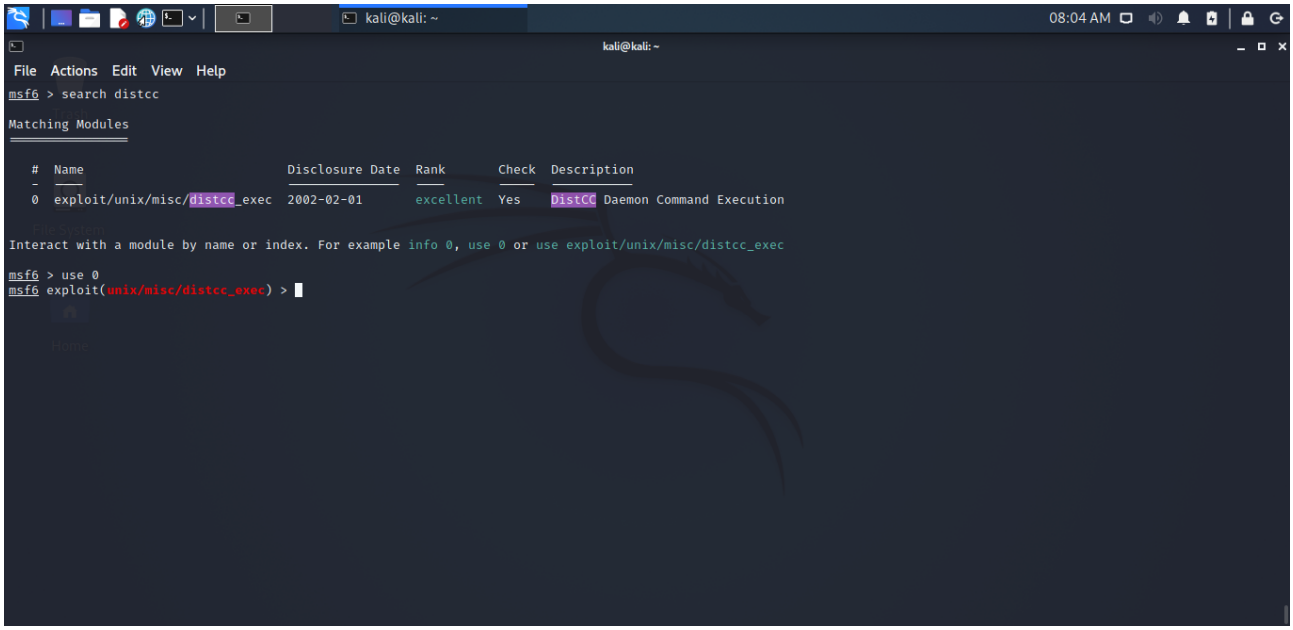
Exploits:

Exploit 1: distccd v1

Info:

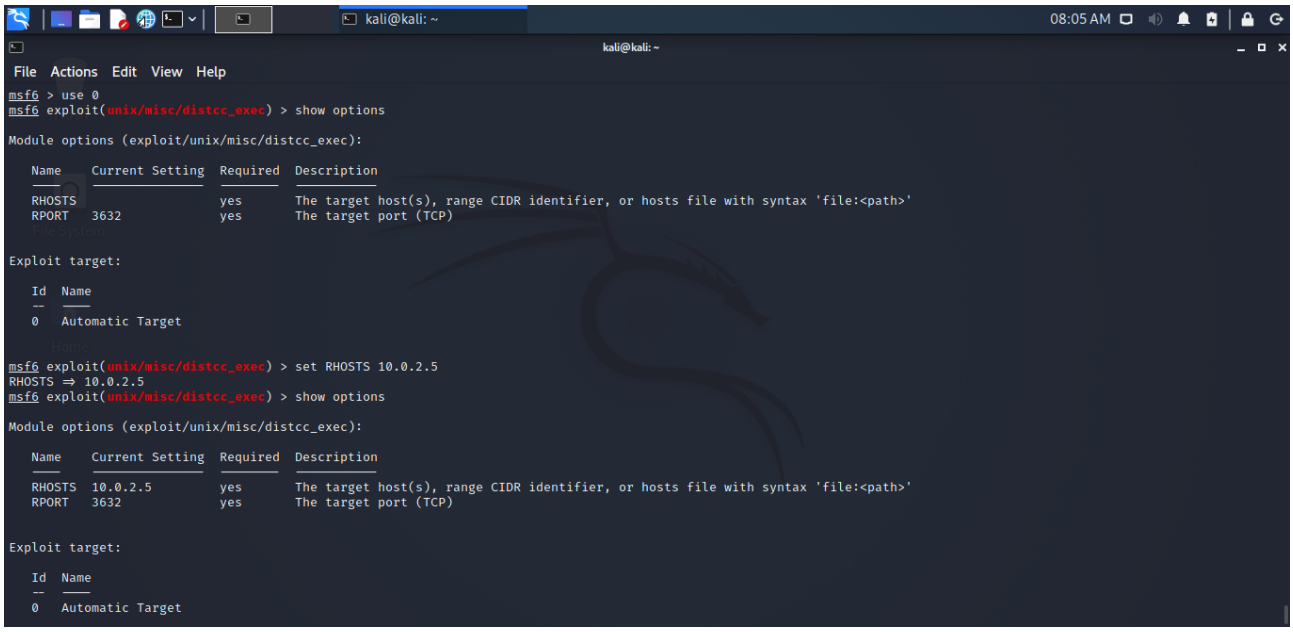
distcc is a tool for speeding up compilation of source code by using distributed computing over a computer network. Distccd is the daemon which has to run in all the participating machines of the cluster.

1. Search for exploit



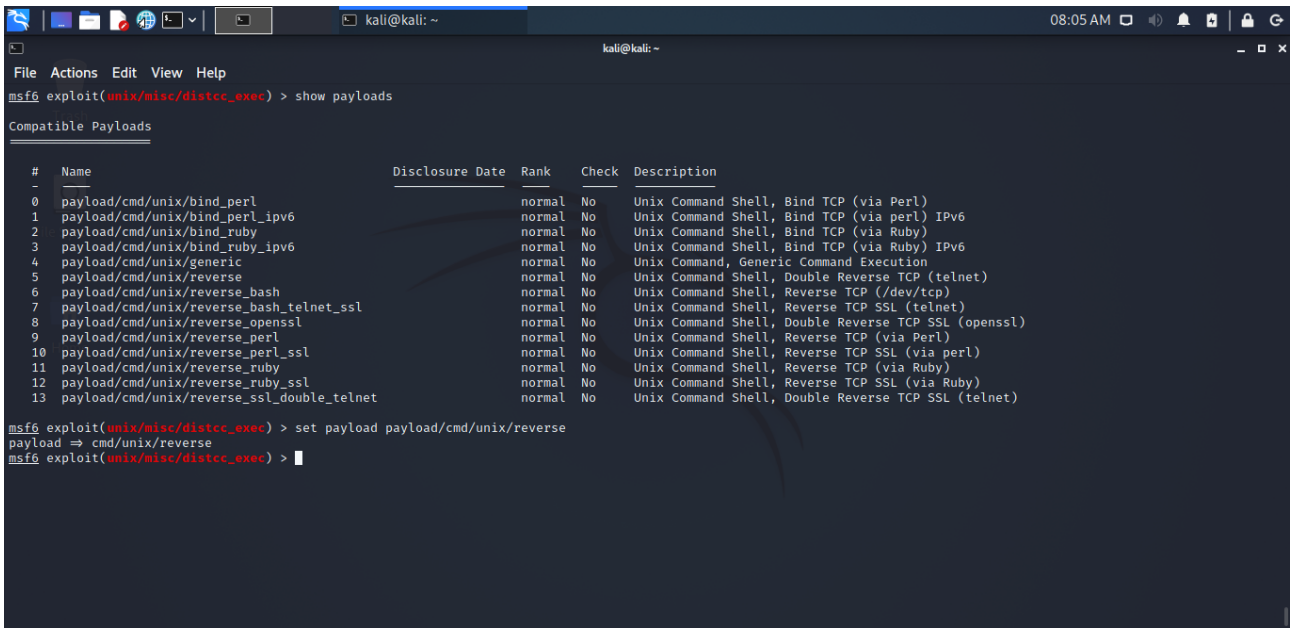
We find one exploit for distccd service and use it.

2. See options and set RHOSTS



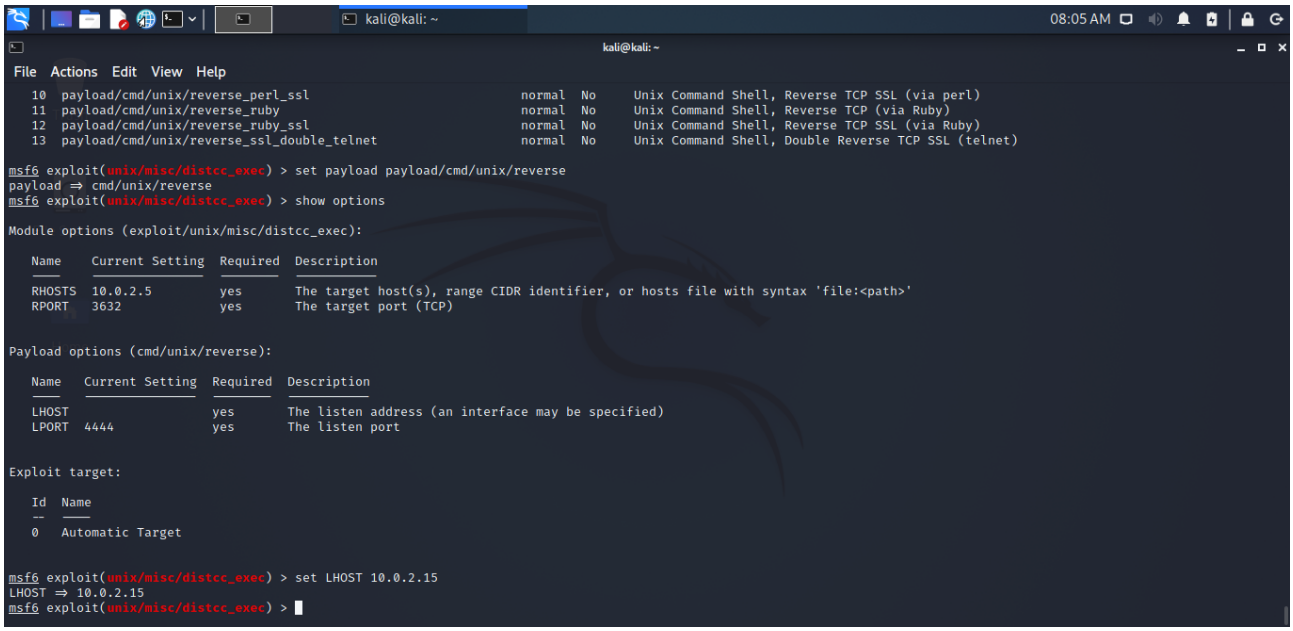
RHOSTS is the remote host machine which has to be exploited. Add victim's IP as RHOSTS value.

3. Set a payload



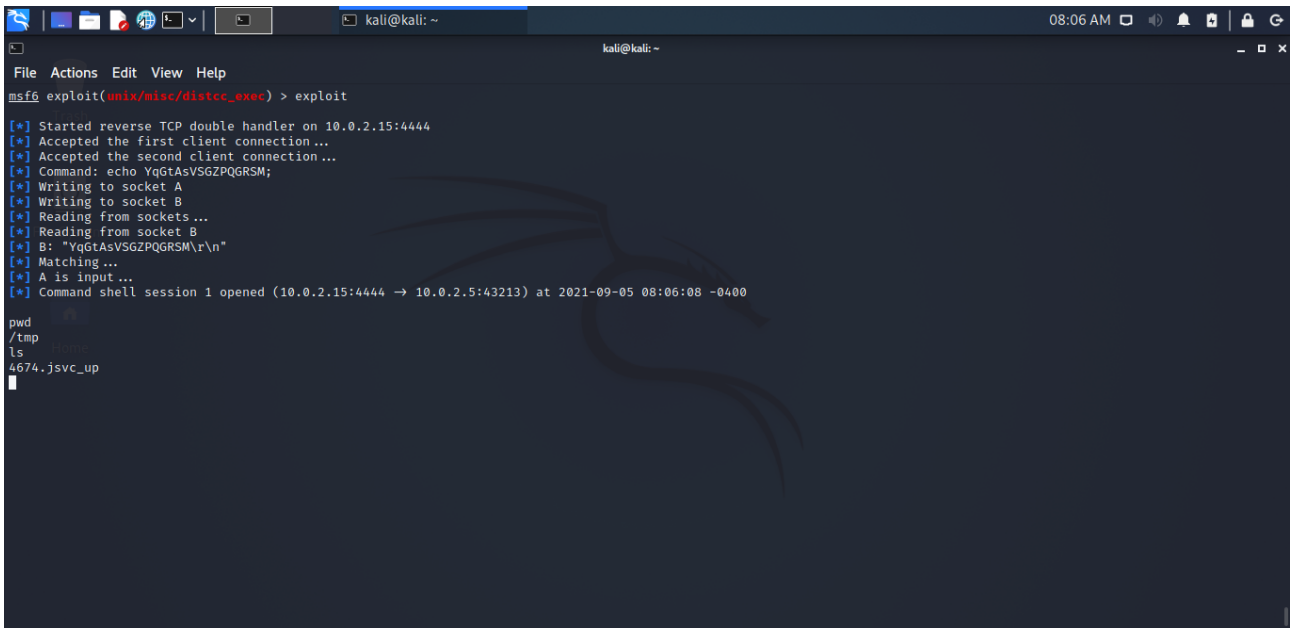
Payload is the data/code that will be executed in the victim's machine for exploitation.

4. Set LHOST



LHOST is the local machine that is attacking other machine. So Kali machine's IP will be added to LHOST.

5. Run exploit



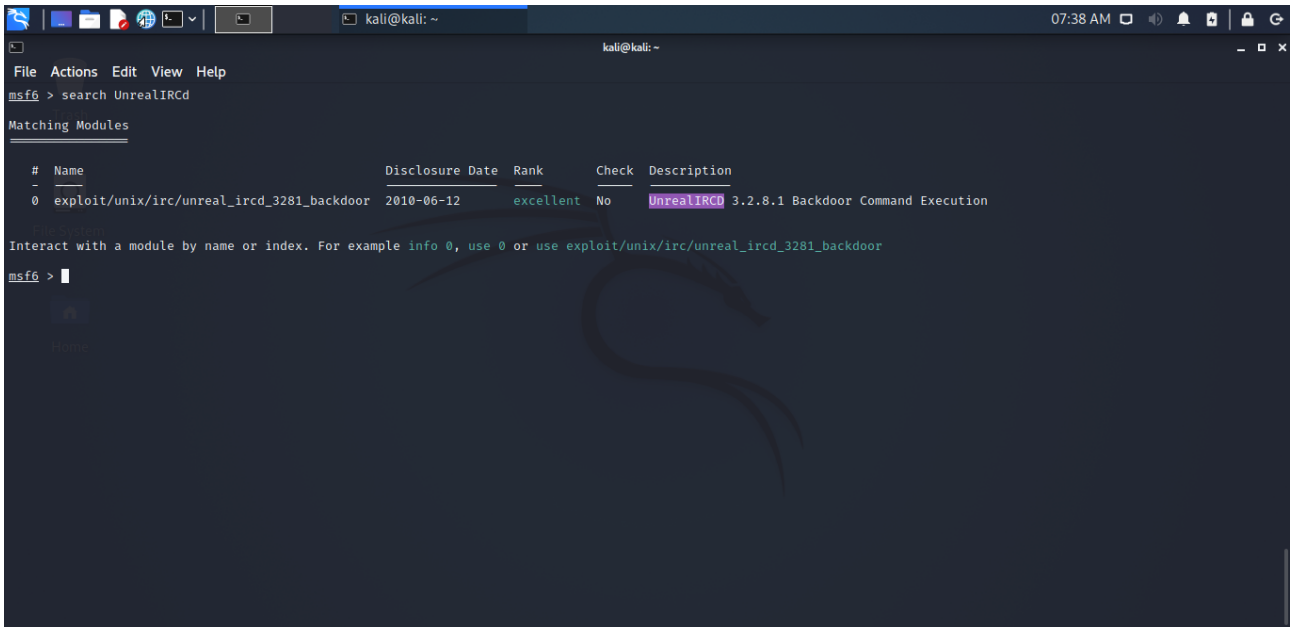
Exploit runs successfully as we have access to the victim machine.

Exploit 2: UnrealIRCd

Info:

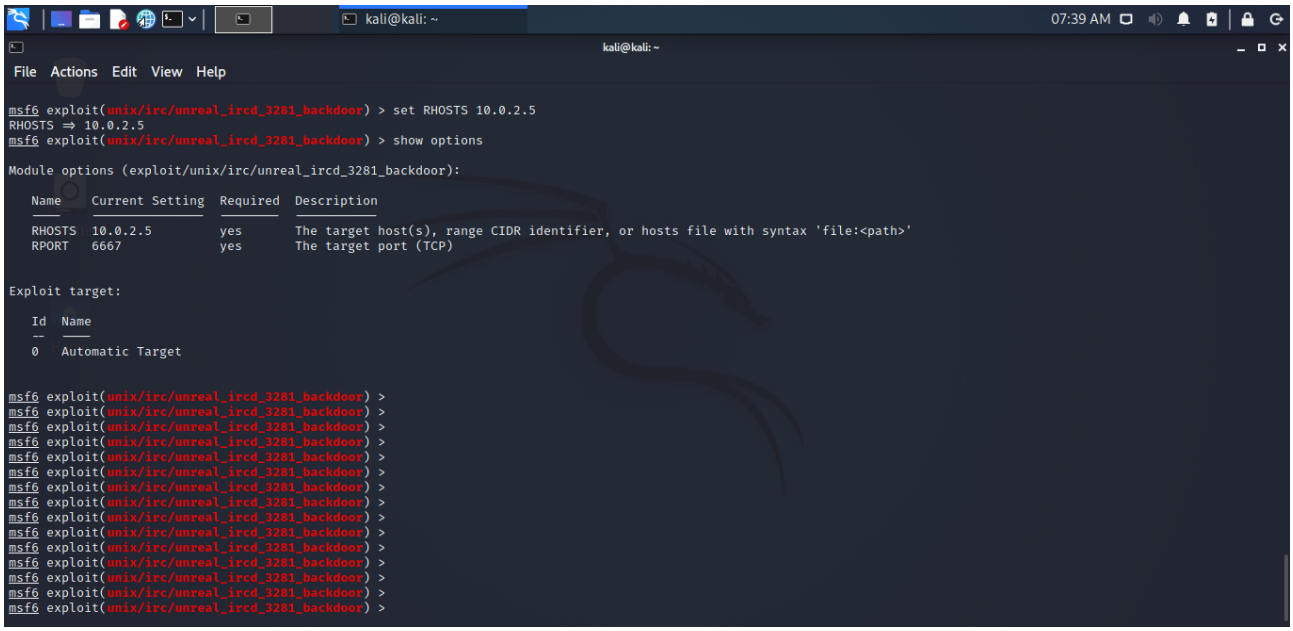
UnrealIRCd is an open source IRC daemon used since 1999.

1. Search for exploit



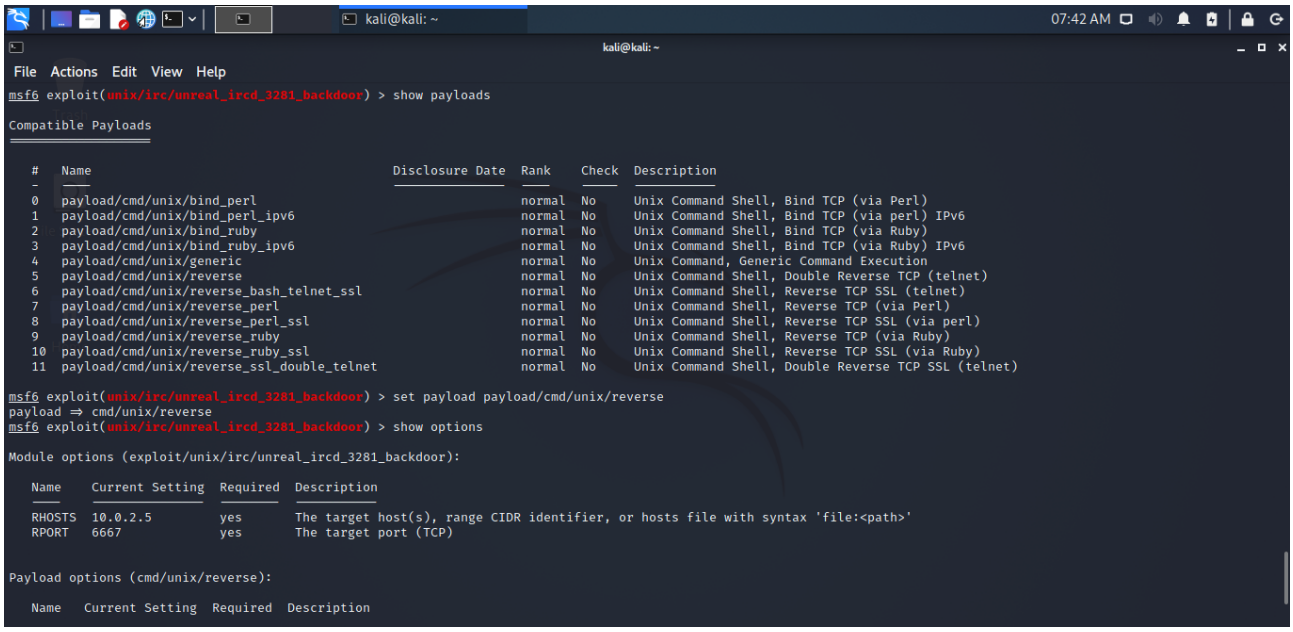
One exploit is available for unrealircd service.

2. Use the exploit and set the options

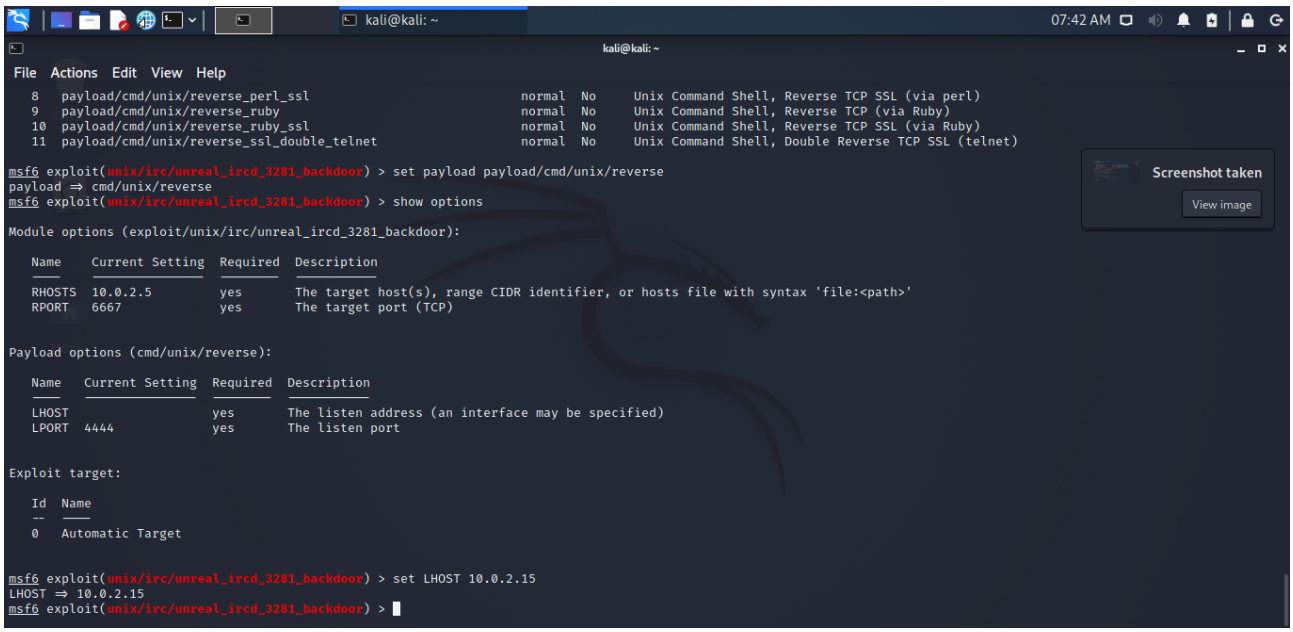


Since the RHOSTS is empty, we set its value to victim's IP address.

3. Set payload

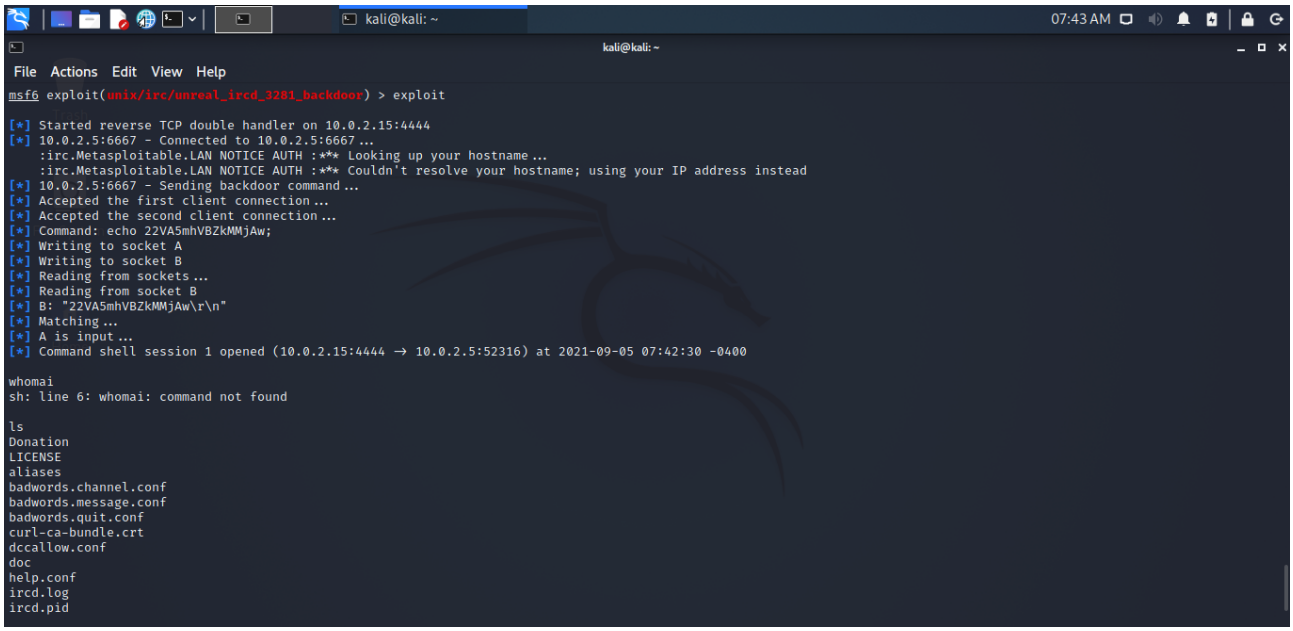


4. Set LHOST



LHOST is the local machine that is attacking other machine. So Kali machine's IP will be added to LHOST.

5. Run exploit



Access to victim’s machine is achieved.

========== END ==========