# [hackNos: Os-Bytesec](https://www.vulnhub.com/entry/hacknos-os-bytesec,393/)靶机练习实践报告

*下载地址:*

* <https://drive.google.com/open?id=1yBuih2CsBx45oTUDpFr4JldrzkaOTTeZ>
* <https://download.vulnhub.com/hacknos/Os-ByteSec.ova>
* <https://download.vulnhub.com/hacknos/Os-ByteSec.ova.torrent>     ([Magnet](magnet:?xt=urn:btih:4E52D43AF23CA19ED027B14654B2222CEFB6D01E&dn=Os-ByteSec.ova&tr=http://tracker.vulnhub.com:6969/announce&tr=udp://tracker.vulnhub.com:6969/announce&tr=udp://tracker.openbittorrent.com:80/announce&tr=udp://tracker.publicbt.com:80/announce&tr=udp://tracker.istole.it:6969))

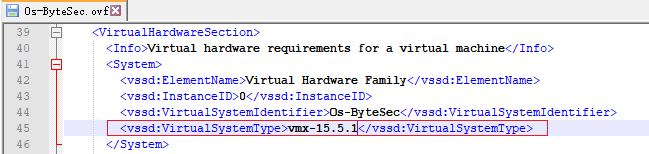
Flag : 2 Flag first user And second root

Learning : exploit | SMB | Enumration | Stenography | Privilege Escalation

## 安装靶机

靶机是.ova文件，需要用VirtualBox打开，但我习惯于使用VMWare,因此修改靶机文件，使其适用于VMWare打开。

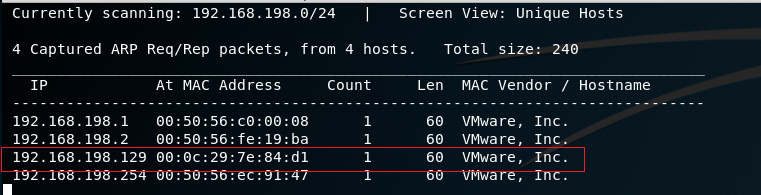
解压ova文件，得到.ovf文件和.vmdk文件。



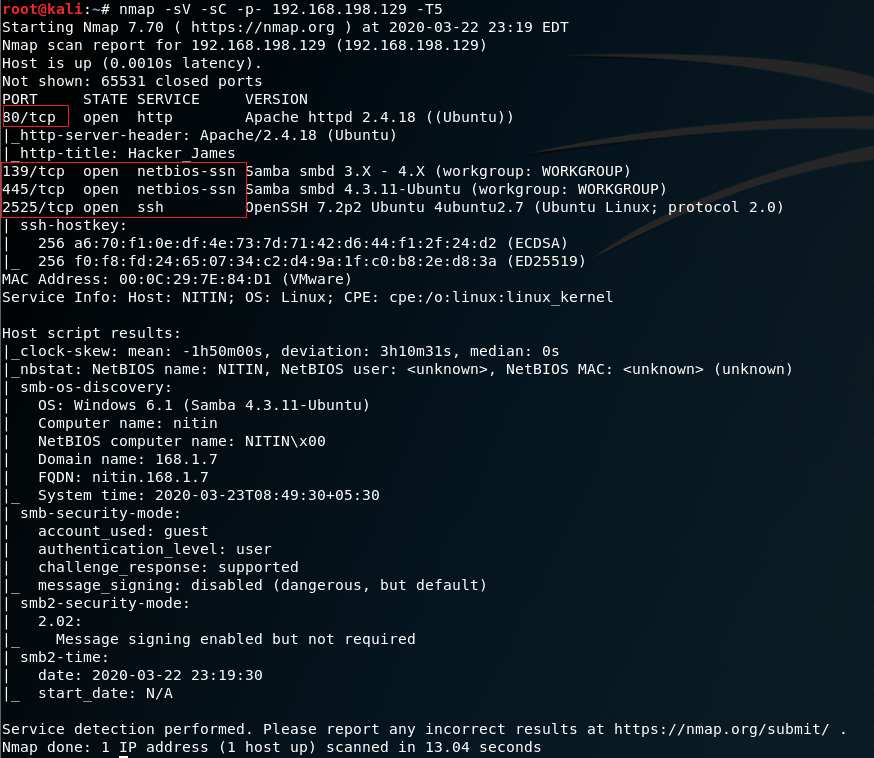
1. 修改虚拟使其可用vmware打开。虚拟运行后，通过netdiscover和nmap都无法扫描获取到ip地址。
2. 进入拯救模式查看情况。
3. 在开机时按下Shift键进入grub界面
4. 在grub页面按下e键进入配置界面，将ro 替换为 rw signie init=/bin/bash，然后按下Ctrl键+X键，即进入拯救模式
5. 查看当前网卡IP信息 “ip a”，查看网卡配置文件“/etc/network/interfacers”，发现网卡配置文件中网卡名同当前网卡名不一致，修改网卡配置文件重启即可。

## 夺旗步骤

第一步：IP扫描，端口扫描



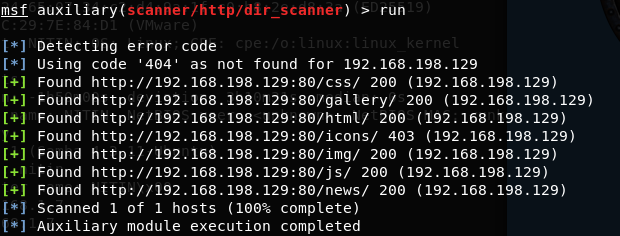
靶机的IP地址为192.168.198.129,nmap进行端口扫描，靶机开启了80端口、139端口、445端口和2525端口，其中2525端口是ssh端口。



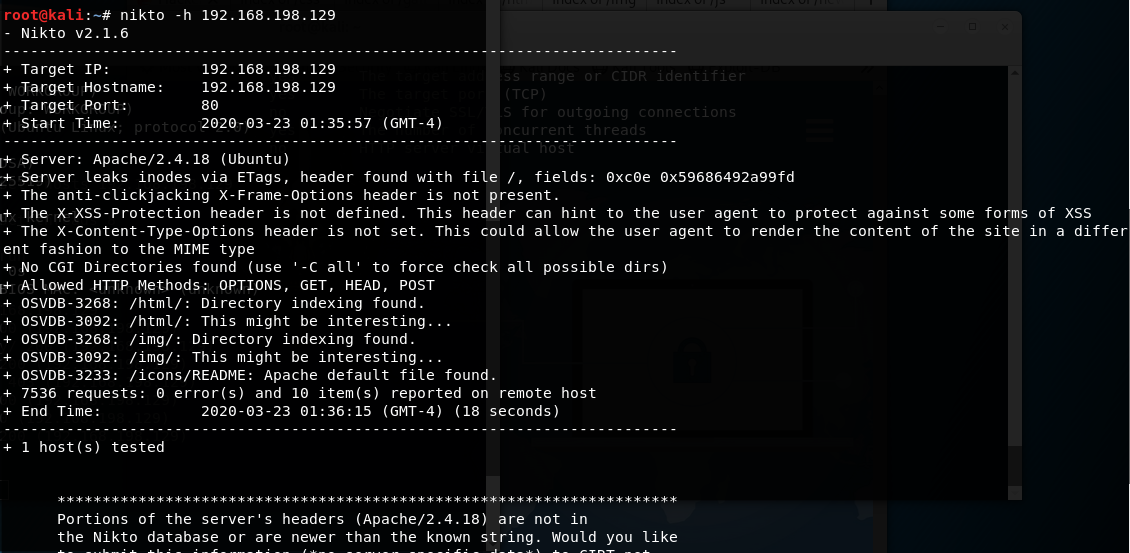
首先，打开http://192.168.198.129:80查看网站内容，发现页面底部有提示”GET###smb###free”。先放一放，smb同端口139、445相关。



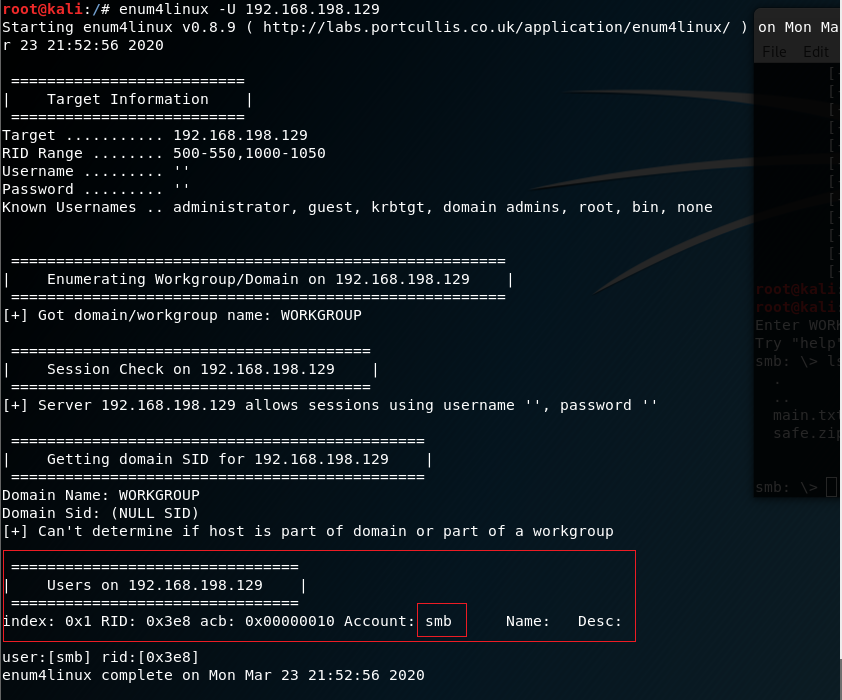
做目录扫描和网站漏扫。



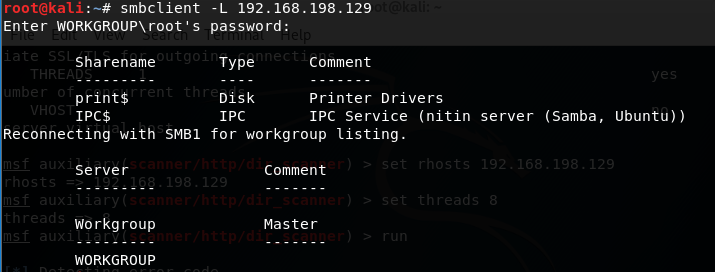
逐个打开地址查看，未发现有价值信息。



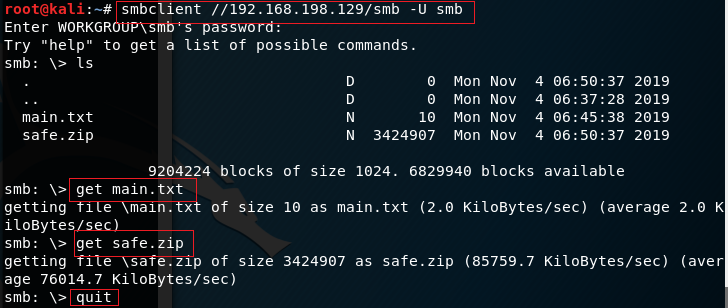
也没有有用信息。关注首页面的提示”GET smb free”。用kali自带的工具enum4linux进行信息收集，定位到用户名smb。



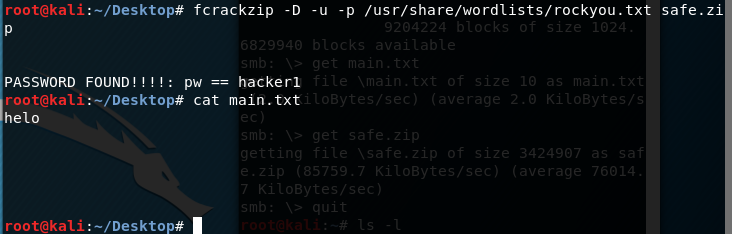
查看服务器端所分享出来的所有资源，并逐个尝试登陆，发现IPC$可登陆，但无任何可用信息。



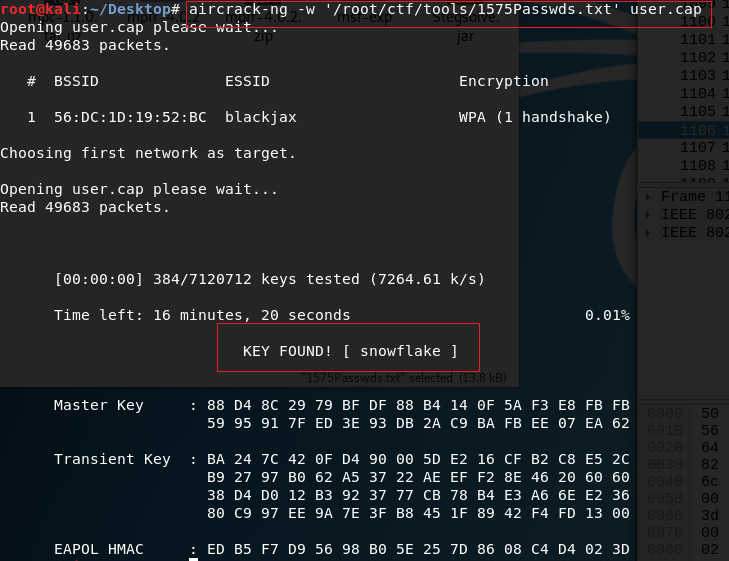
尝试是不是有同用户名同名的分享资源，并用空密码尝试登陆，果然有。



将main.txt和safe.zip下载，发现safe.zip是加密的压缩文件，暴力破解，得出解压密码”hacker1”。

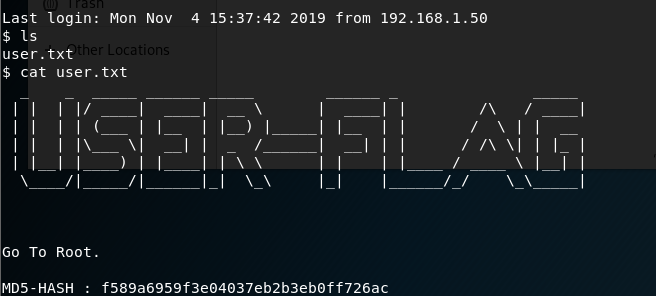


解压后是一张jpg图片和一个user.cap文件，wireshark打开user.cap文件，发现是IEEE 8011,看不到http，应该是需要找密码，同misc题目一样。用aircrack-ng爆破得到wifi的口令”blackjax:snowflake”。



仔细搜索user.cap解密后的内容，没发现有价值信息。题目有个提示考点有“stenography”，查资料发现它的意思是在其它信息内隐藏用户发送的信息，可什么也没找到。

转向ssh，尝试爆破ssh口令，用户名”root”、”admin”、”blackjx”，竟然爆破出来ssh登陆口令”blackjx:snowflake”,同wifi口令一致。难道它所有口令都是一个？登陆ssh，得到用户层flag。



题目告诉有两个flag，一个用户flag，一个root flag,而且考点有”Privilege Escalation”。常规操作，uname -a查看linux版本，用常见的linux提权exp.c尝试，都失败了,内核漏洞利用也不成功。继续查资料，发现suid提权方式，寻找有如下特点的文件：

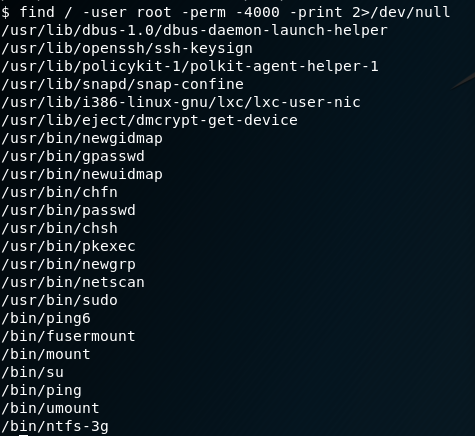
1. 有s标志；
2. 属主为root，那么我们运行这个程序就可以有了root的权限；
3. 程序还得能执行命令。

先找出有特点文件。

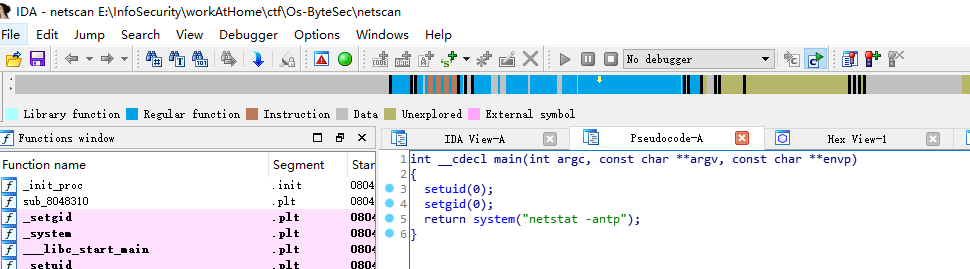
find / -user root -perm -4000 -print 2>/dev/null

find / -perm -u=s -type f 2>/dev/null

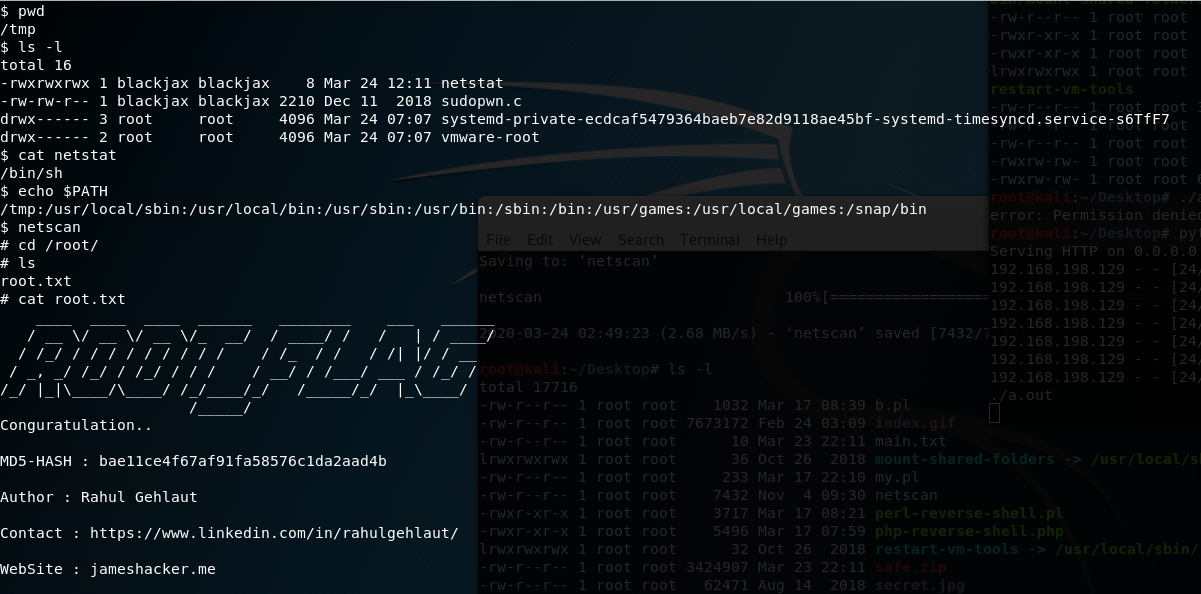
find / -user root -perm -4000 -exec ls -ldb {} \;



逐个排查，发现/usr/bin/netscan文件执行的效果同netstat一致，将文件拷贝下来用ida查看。



他果然只是包装了netstat命令。我们伪造一个netstat文件，并将其添加到环境变量的最开始，那么netscan执行的时候就会执行我们伪造的netstat,我们在netstat中写入“/bin/sh”,改命令被一个有S标志位的root属主的文件执行，该shell也就自动具有root权限。



得到root权限，拿到root下的flag。

## 总结

1. 之前只接触过windows下的smb漏洞，首次了linux下的smb的扫描和利用方式
2. 学习了suid的linux提权工具，多角度考虑提权方式，不要死磕一种方式