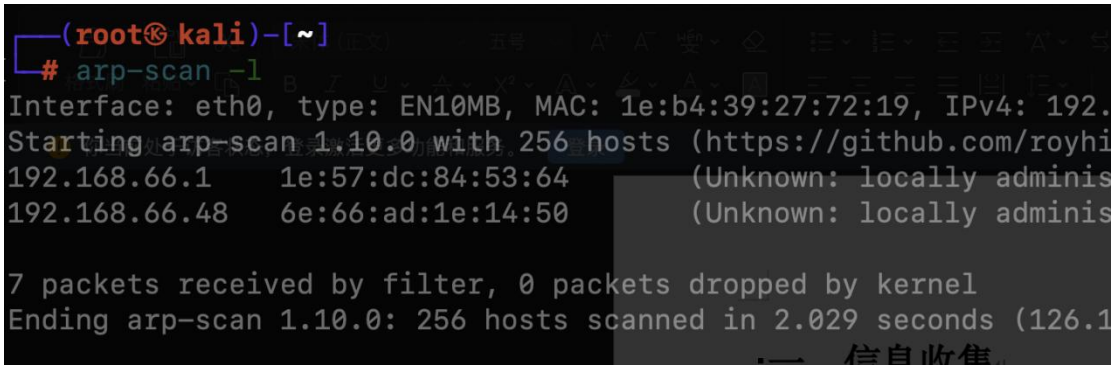
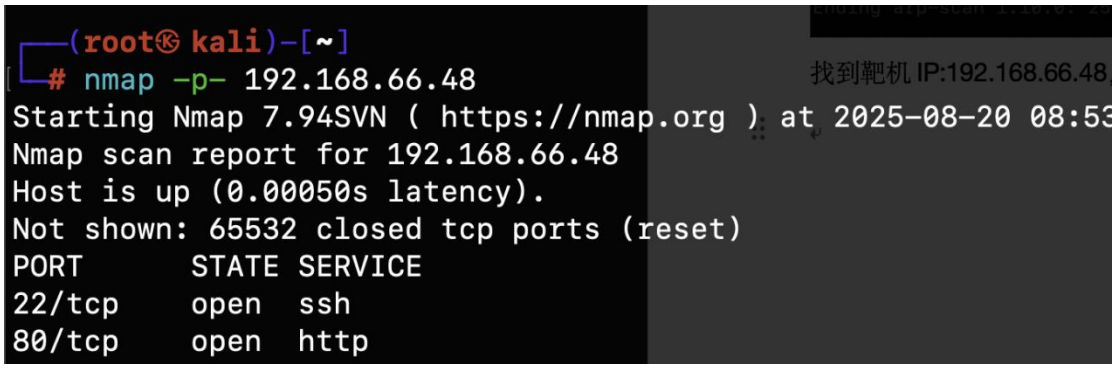
一. 信息收集

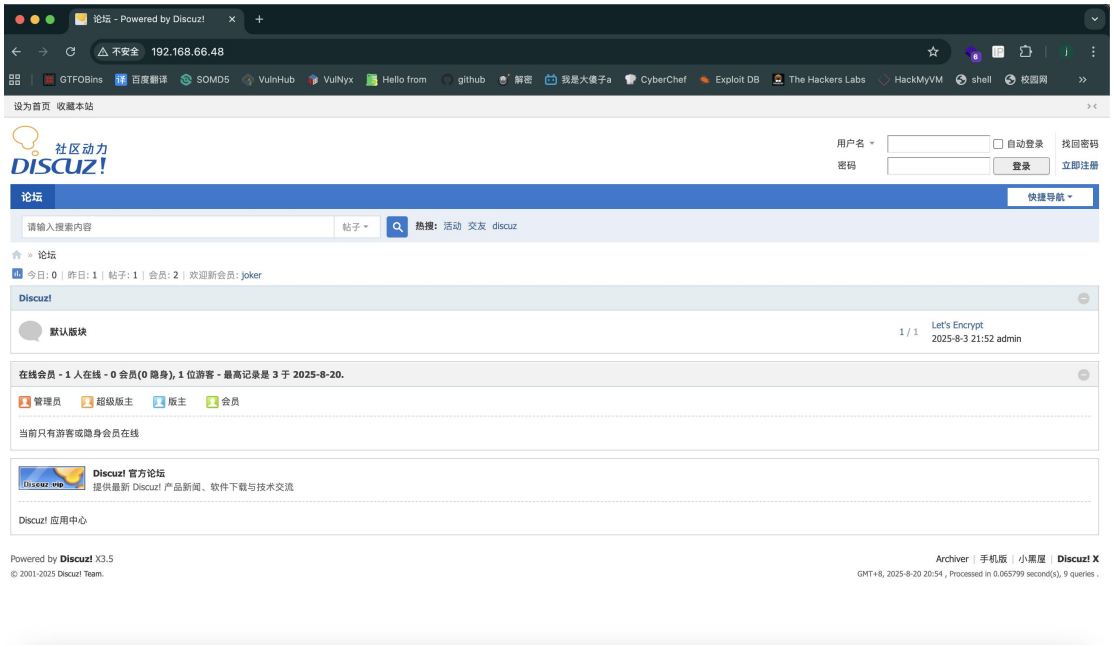
先用 arp-scan-l 进行内网扫描确认靶机 IP。



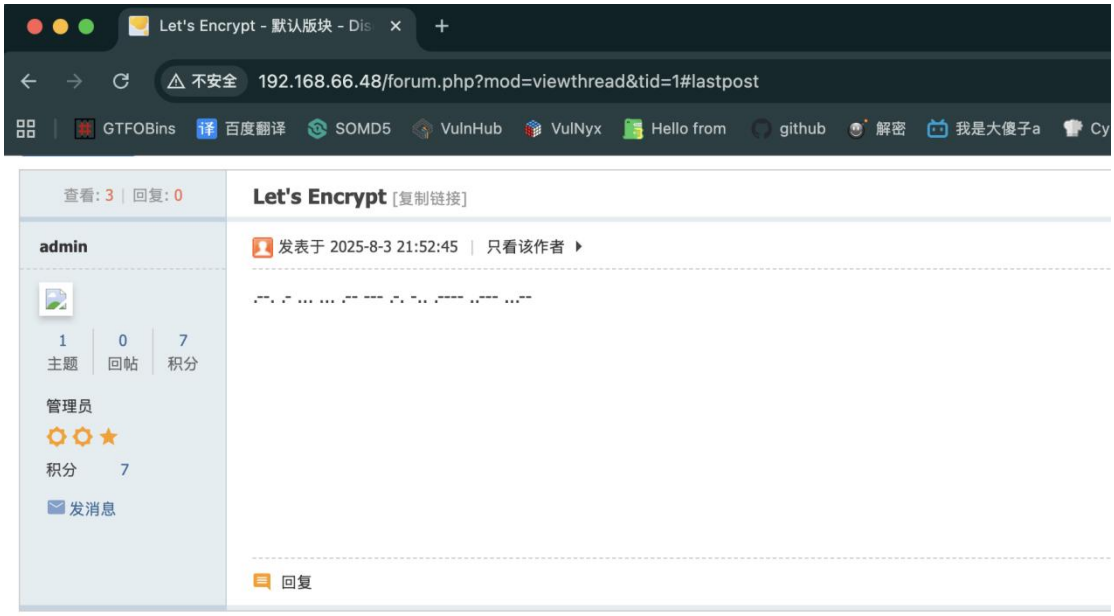
找到靶机 IP:192.168.66.48，对 IP 进行全端口扫描。



发现开通了 22，80 端口。上 80 端口看看。



发现是一个社区论坛，里面有一条帖子是 admin 发布的进去看看。



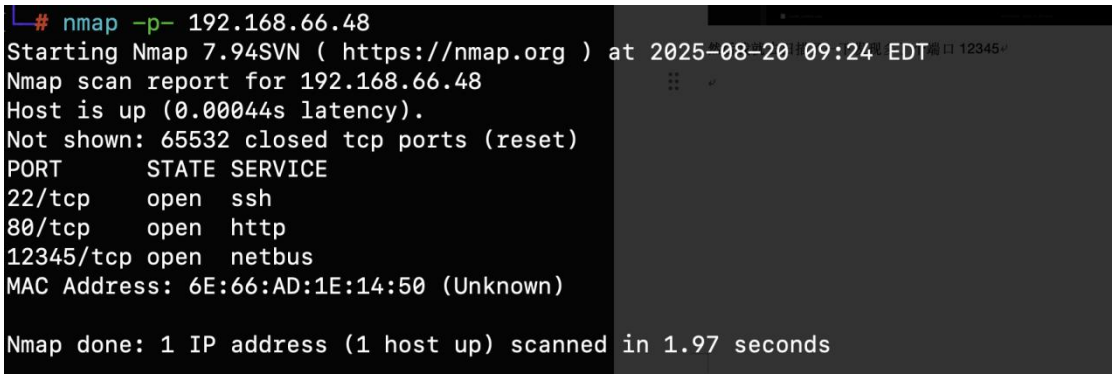
发现是一段摩斯密码对他进行解密。发现密码 password123 再寻找后台登入界面用 dirsearch 对 http://192.168.66.48/进行扫描。

发现 admin.php 进去发现要登入前端，输入账号 admin 密码 password123

进入到后台管理系统，再工具——计划任务里面发现有个名字叫 shell 的计划任务可以执行，我们点击执行

执行完工具里面有个有文件校验点击开始校验发现有文件被修改了

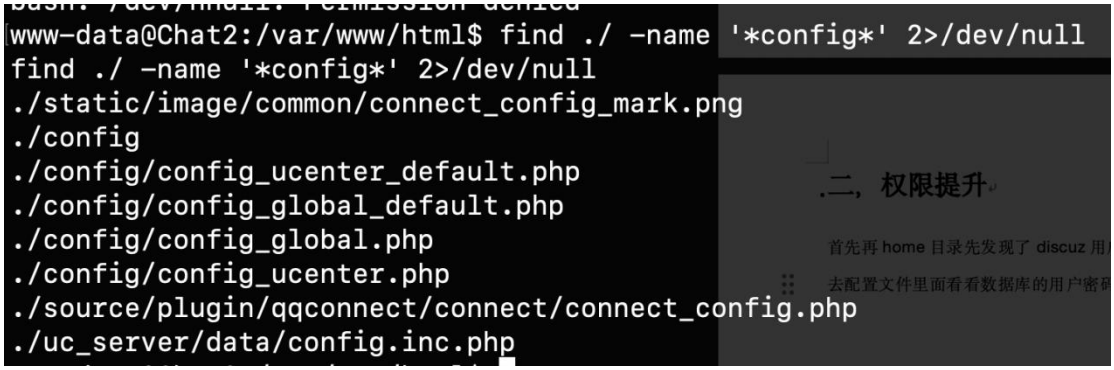
然后我就去扫描了一下发现多了个端口 12345



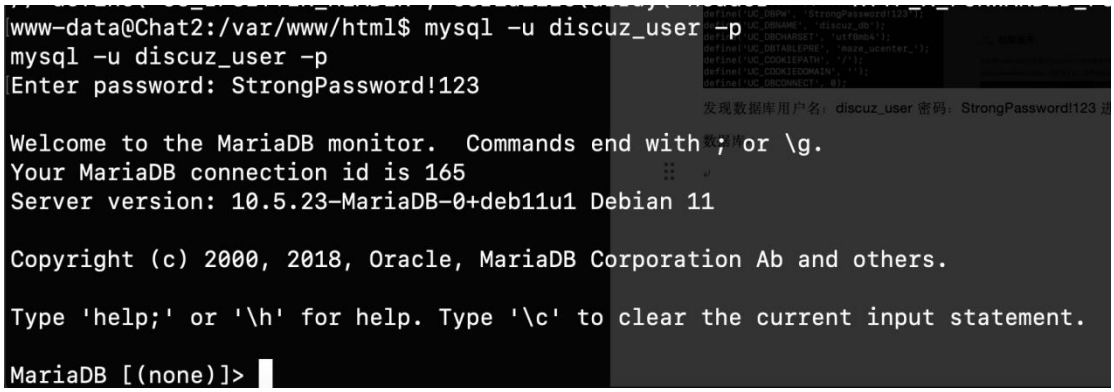
我们 nc 连去看看发现拿到了 www-data 用户

二，权限提升

首先再 home 目录先发现了 discuz 用户想办法拿到他的 shell，我们去/var/www/html 下面找一下配置文件，看看数据库的用户密码



发现数据库用户名：discuz_user 密码：StrongPassword!123 进入数据库



去数据库里面找 user 数据表里面的 user 和 pass

```
MariaDB [mysql]> select User,Password from user;
select User,Password from user;
+-------------+-------------------------------------------+
| User        | Password                                  |
+-------------+-------------------------------------------+
| mariadb.sys |                                           |
| root        | invalid                                   |
| mysql       | invalid                                   |
| discuz_user | *CF0058A6F9B624591DDA643E26A401BEBAD3DFD8 |
| hackme      | *FAAFFE644E901CFAFAEC7562415E5FAEC243B8B2 |
+-------------+-------------------------------------------+
5 rows in set (0.017 sec)
```

发现账号和密码密码是由 md5 加密的在 cmd5.com 上解密，

dirscu_user 的密码没解密出来 hackme 的密码解密出来是 root123

我们尝试 su 一下 discuz 发现 root123 就是他的密码

```
www-data@Chat2:/var/www/html$ su discuz
su discuz
Password: root123

discuz@Chat2:/var/www/html$
```

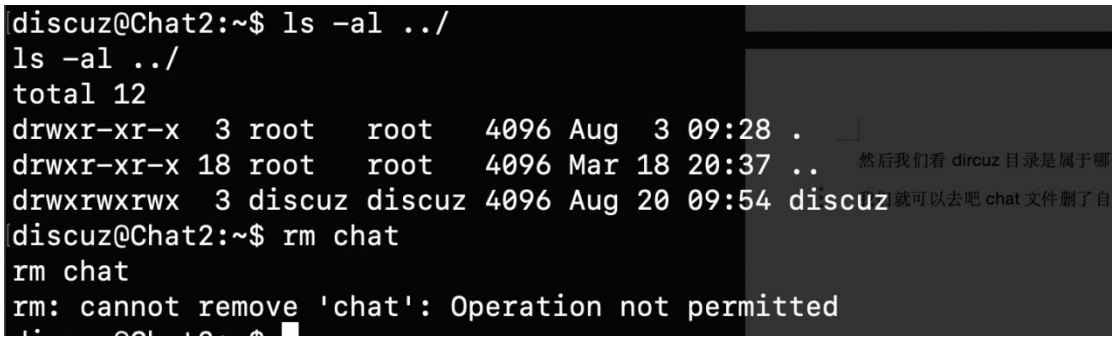
三，获取 root 权限

sudo -l 一下发现 root 不需要密码就能执行/root/dircuz/chat

```
discuz@Chat2:/var/www/html$ sudo -l
sudo -l
Matching Defaults entries for discuz on Chat2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User discuz may run the following commands on Chat2:
    (ALL) NOPASSWD: /home/discuz/chat
```

然后我们看 dircuz 目录是属于哪个用户的发现是 dircuz 这个用户，我们就可以去吧 chat 文件删了自己创个文件但是发现删不了



这里其实是用了 chattr 命令我也是第一次了解这个命令，我做的时候是上传了个 linpeas.sh 脚本发现了 chattr 这个命令又 suid 权限，然后才去了解的它。

这个命令其实就是可以改变文件或文件夹的属性，让用户不能删除、重命名、修改它或者是只能追加内容等。

格式：chattr [选项] <操作符><属性> 文件或目录...

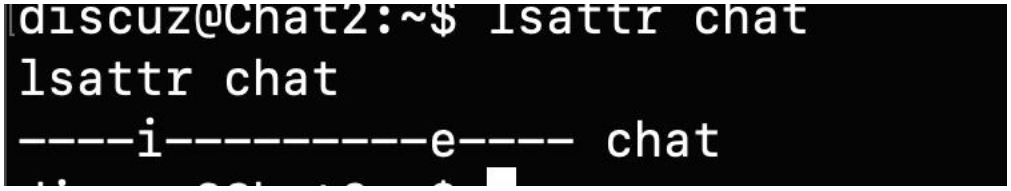
+：增加一个属性

-：移除一个属性

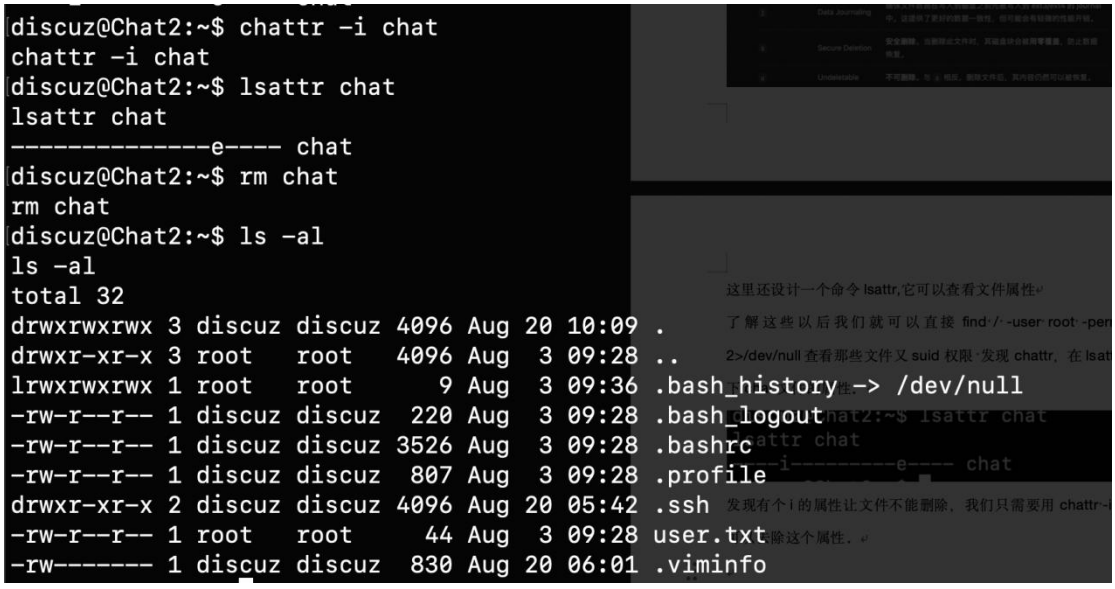
a	Append Only	**仅允许追加**。文件内容只能被追加（例如用 `>>`），不能删除、覆盖或修改已有内容。对于日志文件非常有用。
i	Immutable	**不可变更**。这是最强大的锁。文件不能被删除、重命名、修改；不能创建指向它的链接；不能向文件追加数据。**即使是 root 用户也无法操作**，除非先移除此属性。
A	No Atime Update	告诉系统**不要更新**这个文件的**访问时间（atime）**。这可以提高性能，减少对固态硬盘的写入。
c	Compressed	文件在磁盘上会自动被**压缩**（需要文件系统支持）。
d	No Dump	在使用 `dump` 命令进行备份时，**排除**此文件。
j	Data Journaling	确保文件数据在写入到磁盘之前先被写入到 **ext3/ext4 的 journal** 中。这提供了更好的数据一致性，但可能会有轻微的性能开销。
s	Secure Deletion	**安全删除**。当删除此文件时，其磁盘块会被**用零覆盖**，防止数据恢复。
u	Undeletable	**不可删除**。与 `s` 相反，删除文件后，其内容仍然可以被恢复。

这里还涉及一个命令 lsattr,它可以查看文件属性

了解这些以后我们就可以直接 find / -user root -perm -4000 2>/dev/null 查看那些文件又 suid 权限 发现 chattr，在 lsattr 查看一下 chat 文件的属性。



发现有个 i 的属性让文件不能删除，我们只需要用 chattr -i chat 就可以去除这个属性，然后就能删除 chat 文件了。



然后我们只需要自己创建了 chat 里面写入/bin/bash 加入可执行权限，再用 root 运行就能拿到 root 权限了