Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Implantación de una herramienta que permita desarrollar campañas de phising

Autor: Francisco Javier Jiménez Olmedo
Tutor: Fernando Cárdenas Fernández

Dpto. Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2020

Proyecto Fin de Grado
Ingeniería de las Tecnologías de Telecomunicación

Implantación de una herramienta que permita desarrollar campañas de phising

Autor:
Francisco Javier Jiménez Olmedo

Tutor:
Fernando Cárdenas Fernández
Profesor a tiempo parcial

Dpto. Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2020

Proyecto Fin de Grado: Implantación de una herramienta que permita desarrollar campañas de phising

Autor: Francisco Javier Jiménez Olmedo

Tutor: Fernando Cárdenas Fernández

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2020

El Secretario del Tribunal

A mi familia

A mis compañeros

A mis maestros

Agradecimientos

Durante todos estos años estudiando el grado de ingeniería en las tecnologías de telecomunicación me he rodeado de personas (tanto de la materia como no) que me han dado ánimos para alcanzar mis metas y así conseguir terminar esta etapa como estudiante.

Muy agradecido a mis padres por apoyarme en mis peores momentos y también a mi madrina Myriam, que fue la que me inspiró a entrar en este grado y esta preciosa profesión.

Por otro lado, también hacer mención a todos los profesores con los que he cursado las diversas materias del grado que me han transmitido sus conocimientos y sabios consejos para mi trayectoria profesional.

Por último y no menos importante, me llevo a unos compañeros increibles que durante estos años me han acompañado en muchas largas tardes (y noches) de estudio y se han convertido en una familia para mi.

Francisco Javier Jiménez Olmedo

Sevilla, 2020

Resumen

Hoy en día al hablar de *hacking* las personas se suelen imaginar enormes pantallas con gran cantidad de terminales y scripts interminables usados para penetrar sistemas, pero la realidad es otra, y es que hoy en día la mayoría de los ataques son iniciados mediante correo electrónico con una técnica denominada *phishing*.

A lo largo de este documento se explicará de forma teórica qué es este método, sus diferentes variantes, términos claves sobre técnicas utilizadas para ejecutarlo con éxito y lo más importante, como defenderte de un ataque de este tipo.

Existen diversas medidas a nivel técnico, pero actualmente la más importante implica al eslabón final de la cadena, el trabajador. Actualmente es tan importante o incluso más tener concienciados a los usuarios sobre este tipo de ataques que implantar mecanismos técnicos para evitar el *phishing*.

Para mejorar esto, se llevan a cabo las **campañas de concienciación**, las cuales son, como su nombre indica, campañas de *phishing* lanzadas a los trabajadores de forma controladar para revisar su nivel de conocimiento acerca de esto.

Existen diversas herramientas para realizar esto, por lo que se explicará como realizar la instalación desde cero de una en concreto para que una empresa sea capad de lanzar sus propias campañas, su nombre es *GoPhish.*

Abstract

Nowadays, when we talk about hacking, people usually imagine huge screens with a large number of terminals and endless scripts used to penetrate systems, but the reality is different, and today most attacks are initiated by mail electronic with a technique called phishing.

Throughout this document it will be explained in a theoretical way the method, its different variants, key terms about techniques that are used to execute it successfully and, most importantly, how to defend against an attack of this type.

There are multiple measures at a technical level, but currently the most important involves the final link in the chain, the worker. Currently, it is as important or even more important to make users aware of these types of attacks than to implement technical mechanisms to prevent phishing.

To improve this, so-called **awareness campaigns** are carried out, which are, as their name indicates, phishing campaigns launched at the workers in a controlled way to review their level of knowledge about this.

There are several tools to do this, so it will be explained how to install a specific one from scratch so that a company is able to launch its own campaigns, its name is GoPhish.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 PHISHING

Desde hace muchos años las técnicas existentes en el mundo del hacking han sido diversas, en este caso vamos a hablar sobre el phishing. Este término proviene de la palabra inglesa "*fishing*", que significa pesca y hace referencia a la labor de un phisher (atacante) de hacer que la víctima muerda el anzuelo para conseguir el objetivo que se busque como, por ejemplo, la obtención de credenciales.

1.1. Descripción

El phishing es hoy en día uno de los métodos más utilizados por los ciberdelincuentes para la sustracción de datos, información de sus víctimas y/o intrusión de los equipos mediante malware. Esta información suele tratarse de contraseñas o de datos bancarios.

El atacante utiliza ciertas técnicas para ganarse la confianza de la víctima y así conseguir su objetivo. Entre estas técnicas se encuentran la suplantación de identidad o *spoofing* mediante la cual, una persona se hace pasar por otra que no es, la ingeniería social que consiste en la manipulación psicológica de la misma para convencerla de que debe darnos sus datos y/o la suplantación de sitios web para la obtención de datos.

Como veremos posteriormente, el phishing, utiliza diversos medios de propagación que nos ayuda a dividirlo en varios tipos. El más común y el más conocido es mediante correo electrónico, pero también podemos verlo a través de SMS o de VoIP.

1.2. Tipos

Como ya se ha descrito en el apartado anterior, el phishing es uno de los ataques más utilizados hoy en día, incluso como principio de un vector de infección en caso de ataques a grandes empresas. Existen diversos tipos, cada uno con su medio de transmisión y sus caracteristicas. A continuación, se explicarán cada uno de ellos:

- **Phishing tradicional**

  Este tipo de phishing tiene como principal medio de propagación el correo electrónico. Normalmente suele estar relacionado con casos de *spam* o correo no deseado debido a que las campañas suelen enviarse de forma masiva a una gran cantidad de usuarios.

  En este caso, el objetivo suele ser la captura de credenciales o datos. Se puede dar de dos formas:

  - El atacante se hace pasar por otra persona y le solicita que le envíe su información directamente a la dirección de correo electrónico.
  - El objetivo recibe un correo electrónico haciéndose pasar por una empresa o persona de confianza. En este correo electrónico existen enlaces que apuntan hacia una web falsa que copia a la página de la que se quiere obtener informaciÓN.

- **Malware-Based Phishing**

  Al igual que el tipo anterior este se recibe por correo electrónico. Es muy similar al tradicional pero el objetivo no es conseguir directamente los datos del usuario. En el tipo Malware-Based se adjunta un fichero considerado malware en el correo o se añade un enlace que redirige a una web en la que se descarga.

El malware suele estar enfocado, por ejemplo, en la explotación de vulnerabilidades en servicio y software no actualizado para expandirse o en capturar en teclado de la víctima para robo de credenciales.

Este tipo de phishing suele verse en empresas, más que en particulares. Normalmente se le presenta a los usuarios un correo en el que se adjunta un fichero PDF, excel o word, y se indica que se trata de un comunicado, factura o un documento a rellenar.

- **Spear Phishing**

  El Spear phishing se trata de un tipo más enfocado a un grupo reducido de personas y no a un ataque lanzado de forma masiva. Debido a esto, los correos de las campañas de este tipo suelen estar más personificados para tener un porcentaje de éxito mayor.

  Los grupos objetivos suelen ser sectores o áreas con pocos conocimientos informáticos dentro de una empresa como, por ejemplo, departamentos financieros o recursos humanos.

  Este tipo suele estar ligado con un análisis de los objetivos y con técnicas de Ingeniería Social para conseguir convencer a las víctimas del engaño. En su mayoría estos ataques son lanzados mediante correo electrónico y redes sociales.

- **Smishing**

  Este tipo de phishing se caracteriza por enviarse a teléfonos móviles vía SMS o desde aplicaciones de mensajería gratuitas como Whatsapp o Telegram. Se le suele enviar a los usuarios un mensaje simulando ser una empresa real informándoles de que han ganado algún tipo de premio.

  Los objetivos de este ataque suelen ser uno de estos tres:

  1. Acceso a una URL.
  2. Solicitud de llamada a un número de teléfono.
  3. Envío de información mediante un mensaje de texto.

  Se suelen solicitar datos personales o incluso datos bancarios para conseguir un beneficio enconómico.

- **Vishing**

  Si el anterior tipo se basaba en el envío de SMS o mensajes desde aplicaciones de mensajería gratuitas, este se basa en el uso de centros de atención telefónica. El atacante intenta realizar un fraude al usuario objetivo haciéndose pasar por alguna empresa como, por ejemplo, una operadora o un banco.

  Este ataque normalente se asocia con otro para complementarlo y así conseguir mayor probabilidad de éxito.

- **Suplantación del CEO**

  La suplantación del CEO está basada en hacerse pasar por el CEO de una compañía. En estos casos, el atacante redacta un correo a personas muy concretas dentro de una empresa solicitándole algún tipo de información, o en algunos casos algún tipo de ingreso económico de forma urgente a cierta cuenta bancaria.

  Los atacantes en ocasiones analizan e investigan situaciones en las que el CEO de la empresa no está disponible para confirmar que están suplantando su identidad, por ejemplo, cuando se encuentra reunido o en algún tipo de viaje en avión.

1.3. SMTP

Ya explicado que es el phishing y los distintos tipos con sus respectivas características se pasará a explicar el protocolo de correo electrónico que resulta fundamental para conocer a un nivel más técnico el *phishing*, el protocolo SMTP. A parte se darán unas breves pinceladas sobre los protocolos IMAP y POP debido a que afectan al flujo de correo electrónico.

El protocolo de red SMTP o Simple Mail Transfer Protocol, definido en la RFC 5321, está por encima de la capa de transporte haciendo uso de los puertos 25, 587 y 2525 TCP y es utilizado para el envío y recepción de mensajes de correo electrónico. En la imagen siguiente se muestra una pila de protocolos en el uso de SMTP.

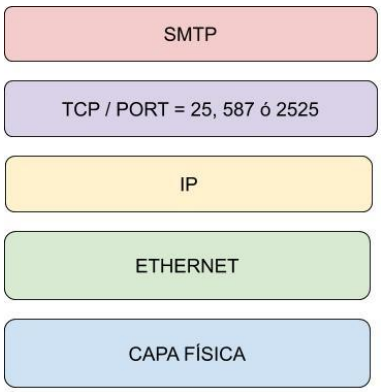


Figura 1-1 Pila del protocolo SMTP

Debido a sus limitaciones en cuanto a la recepción de correos ya que, por ejemplo, no tiene capacidad para almacenar en cola los mensajes en el receptor, se complementa con los protocolos IMAP o POP3, por lo que solo suele ser utilizado para el envío.

Gracias a SMTP, un cliente o un servidor puede comunicarse con otro servidor de correo para que este pueda hacer llegar el mensaje de correo. La estructura en la comunicación de este protocolo se puede ver en la siguiente imagen:

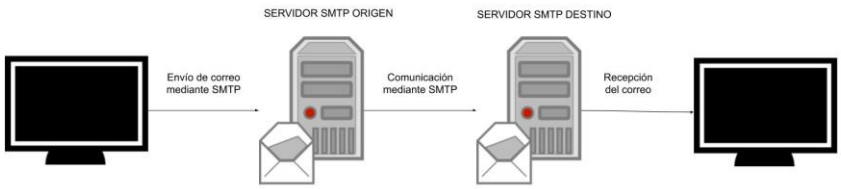


Figura 1-2. Flujo de mensajes SMTP

Para entender el diagrama mostrado anteriormente en profundidad, se necesitará conocer los diversos códigos de respuesta, comandos y cabeceras que componen el protocolo SMTP.

Cada comando engloba una serie de códigos de respuesta a este diferentes, debido a esto y a la gran cantidad de comandos que usa el protocolo, sólo se explicará cómo están estructurados los códigos y no se entrará en el significado de cada uno.

- **Estructura de los códigos de respuesta SMTP**

Los códigos usados en SMTP, o también conocidos como códigos de respuesta SMTP, están formados por 3 dígitos y se usan en el envío de correos electrónicos, cada uno con un significado diferente.

El primero de ellos indica si el comando usado funcionó correctamente o no. En la siguiente tabla se muestra el significado de cada dígito:

Dígito	**Definición**
1XX	Se aceptó el comando enviado, pero se está a la espera de algún comando de confirmación.
2XX	El comando ha finalizado de forma correcta.
3XX	Se ha aceptado el comando enviado, pero se está a la espera del envío de más información.
4XX	El comando se ha rechazado, pero se puede realizar un nuevo intento del uso de este.
5XX	Se rechazó el comando sin indicación de posibilidad de nuevo intento.

Tabla 1-1 Primer dígito de SMTP

El segundo de los dígitos del código de respuesta indica la categoría de la respuesta enviada. En la siguiente tabla se explica la categoría que indica cada uno:

Dígito	**Definición**
X0X	Sintaxis.
X1X	Información.
X2X	Conexión.
X5X	Sistema de correo.

Tabla 1-2 Segundo dígito de SMTP

El tercer dígito especifica el significado del código enviado y no sigue ninguna estructura específica en cuanto a dígitos.

- **Comandos SMTP**

Los comandos usados en el protocolo SMTP son varios, por lo que se definirá en la siguiente lista cada uno de ellos:

  - **DATA.** Este comando indica al servidor destino que el mensaje que se ha enviado es el contenido del correo electrónico que debe recibir el destinatario indicado en las cabeceras. Este texto tiene que cumplir el estandar del formato descrito en la RFC 822. El servidor origen envía el comando y espera que el servidor destino conteste con el código 354. Una vez sucedido esto, el origen envía el correo y el destino contesta con el código 250.

- **EXPN.** Comando utilizado para verificación de listas de correo. Se le introduce como parámetro el nombre de una lista y nos devuelve los nombres de usuario y direcciones de la lista introducida.
- **HELO.** Comando usado para inciar el diálogo SMTP. En este se utiliza como parámetro el nombre del cliente para indicar la identidad de este. El servidor destino tendrá que contestar con el código 250.
- **HELP.** Este comando es utilizado para solicitar información de ayuda sobre un comando específico o sobre todos los comandos existentes.
- **MAIL.** Se usa para indicar al servidor destino el inicio de un mensaje de correo y se indica en este el remitente del correo electrónico enviado.
- **NOOP.** Comando para comprobación de que la conexión con el servidor se mantiente. Se envía con la intención de que el servidor conteste con un OK.
- **QUIT.** Este comando se usa para cerrar la conexión SMTP con un servidor. Indica que no hay más operaciones a realizar, el destino inmediatamente cierra la conexión respondiendo con el código 221.
- **RCPT.** Comando utilizado para indicar el destinatario del correo que se está enviando. En caso de que el correo tenga que ser enviado a varios destinos se separarán por comas.
- **RSET.** Este es usado para descartar toda la información enviada, con esto se borran todos los estados guardados en la conexión.
- **SEND.** Este comando se utiliza para enviar un correo directamente a una terminal que tenga el destino del mensaje y no al buzón de correo. Normalmente se usa para mensajes críticos.
- **SOML.** Este es parecido al anterior, se diferencian en que si el destino no tiene una terminal disponible donde mostrar el mensaje, este se enviará directamente al buzón de correo electrónico.
- **SAML.** El comando SAML funciona de forma similar a SOML, solo que, aunque tenga una terminal disponible donde mostrar el mensaje el correo se enviará igualmente al buzón del destinatario.
- **TURN.** Comando usado para cambiar los servidores orígenes y destino. Esto se usa cuando el origen tiene también mensajes que enviar al destino y así evitar tener que establecer una nueva conexión SMTP.
- **VRFY.** Al enviar un correo electrónico a un servidor final se usa este comando para verificar que el destinatario del correo es válido y existe. Este se utiliza antes de iniciar el envío de un mensaje y así comprobar que es el servidor que le va a servir el correo al usuario final.

- **Cabeceras SMTP**

Una vez definidos los códigos de respuesta y los comandos usados por SMTP se pasará a describir las cabeceras más importantes en cuanto al *phishing* del protocolo. El significado de las que se van a describir a continuación es relevante de cara a realizar la labor de análisis de casos de *phishing*.

- **From.** Correo que ha enviado el mensaje. Esta línea resulta fácilmente modificable por un atacante.
- **Subject.** Breve descripción sobre lo que se va a redactar en el correo electrónico. Es lo que comunmente se conoce como "Asunto".
- **Date.** Fecha y hora del mensaje.
- **To.** Cabecera que indica a quién se envía el mensaje.
- **Return-Path.** Cuenta de correo a la que se le va a devolver el mensaje. Esto es similar al uso de "*Reply-To*:" en un correo electrónico.
- **Delivery Date.** Fecha en la que el correo fue recibido en tu cliente de correo electrónico.

- **Received.** Esta cabecera es sumamente importante de cara a un caso de *phishing* debido a que indica por qué servidores ha ido pasando el correo electrónico hasta llegar al destino final. La primera línea de correo muestra el servidor origen del correo, por lo tanto, gracias a esto podemos identificar desde donde se ha enviado.
- **Content-Type.** Formato del mensaje enviado.
- **X-Spam-Status.** Puntuación en cuanto a *spam* o correo no deseado asignada por el servidor del destinatario al correo recibido.
- **X-Spam-Level.** Puntuación que el servidor del destinatario suele asingar en cuanto a *spam* o correo no deseado.
- **Message-Body.** Contenido del correo electrónico redactado por el remitente.

Ya se han definido las diferentes partes del protocolo SMTP utilizado para enviar correos electrónicos y en este caso, correos de *phishing*. Aunque en el envío phishing se haga uso únicamente de SMTP, también se usan indirectamente los protocolos IMAP o POP para la recepción de los correos ya que tienen la capacidad de almacenar en cola los mensajes. Debido a esto, se definirán ambos para tener un breve conocimiento sobre el uso de cada uno.

- **IMAP.** El protocolo "Internet Message Access Protocol" te da la posibilidad de descargar y administrar tus correos electrónicos en tu servidor de correo. Con este protocolo se le mostrará al destinatario la lista con los diferentes mensajes recibidos y sus asuntos. Gracias a esto tenemos la posibilidad de acceder a nuestros correos desde cualquier dispositivo, ya que únicamente se realizará una sincronización con el servidor de correo donde estén almacenados.
- **POP.** Este protocolo se pone en contacto con el servidor de correo y descarga todos los mensajes nuevos en el equipo que realiza la conexión con el servidor. Debido a esto solo se pueden ver los correos electrónicos en el equipo donde se han descargado. Si se accede desde otro equipo, los mensajes ya descargados no estarán disponibles.

1.4. Ingeniería social

Una de las técnicas más importantes para realizar una buena campaña de *phishing* se basa en la utilización de la ingeniería social. Al hablar de vulnerabilidades, nos imaginamos la explotación de éstas en servidores y grandes redes de información, sin embargo, la ingeniería social busca explotarlas en el eslabón más débil de la cadena: el usuario final.

La ingeniería social se basa en un conjunto de técnicas que buscan manipular psicológicamente al usuario para la obtención de un beneficio para el atacante, ya sean datos personales, infección de un equipo por medio de un *malware* o la obtención de datos bancarios.

Las técnicas usadas para manipular a los usuarios se pueden resumir en las siguientes:

- **Respeto a la autoridad.** Suplantación de superiores dentro de nuestra empresa o de las autoridades del Estado. Aquí se aprovechan del respeto que solemos tener como ciudadanos o trabajadores a nuestros superiores.
- **Voluntad de ayudar.** Los atacantes se hacen pasar por compañeros de trabajo ofreciendo ayuda o por alguien del área de informática indicándole que tiene que instalar una herramienta para facilitarle ciertas tareas en el trabajo.
- **Temor a perder un servicio.** Este tipo de técnica es de las más utilizadas en los casos de phishing, debido a que se juega con necesidades como un cambio de contraseña o el iniciar sesión para aceptar un cambio de políticas. En estos tipos de correo se advierte que si el usario no realiza ciertas acciones puede llegar a perder un servicio.
- **Respeto social.** Los atacantes juegan con el estatus social de sus víctimas indicándoles que tienen vídeos privados suyos sensibles o que tienen cierta información suya que podría perjudicar a su reputación. Se

suelen enviar correos indicando esto y solicitando una cantidad monetaria importante para evitar la difusión de este tipo de información. Hoy en día se suelen pedir criptomonedas debido a la imposibilidad de rastrear transacciones y su anonimato.

- **Servicios o productos gratuitos.** Normalmente se ofrecen productos o servicios gratuitos que se consideran de necesidad del usuario por los cuales se obtiene información de todo tipo o credenciales de un usuario.

Y ahora llega la duda de cómo defenderse de la ingeniería social, y la respuesta es que no existe un método 100% eficaz. La única forma de defenderse de ésta es mediante la formación de los usuarios y la concienciación.

Esto último es muy importante de cara a los empleados de una empresa para evitar que caigan en ataques de *phishing* que puedan suponer filtraciones de información o la infección de equipos con *malware.*

1.5. Spoofing

La última técnica de la que se va a hablar y que está relacionada con el *phishing* es el *spoofing*. Existen diversas variantes de esta técnica, pero en concreto la que nos interesa y la que es usada en estos tipos de ataques se denomina *Email Spoofing.*

Esta técnica se basa en la suplantación de la persona que está enviando el correo electrónico, es decir, el atacante simula ser quien no es para ganarse la confianza de la víctima. Esto se consigue gracias a las modificaciones que puede realizar un atacante en la cabecera "From" del protocolo SMTP descrita anteriormente, ya que se puede falsificar fácilmente para que parezca que el correo ha sido enviado por otra persona. Debido a esto el *spoofing* es una técnica muy utilizada en las campañas de *phishing.*

Todo esto se consigue gracias a que el protocolo SMTP, utilizado en el envío de correos eletrónicos, no tiene ningún método de autenticación para que la persona que envía el correo electrónico pueda asegurar ser quien es. Los atacantes aprovechan esta debilidad en el protocolo para aumentar el éxito dentro de sus campañas de *phishing.*

A parte del *Email Spoofing* existen más variantes dentro de esta técnica. Otra muy utilizada en los ataques de *phishing* es el *Web Spoofing*. En esta técnica los atacantes crean una web falsa que intenta suplantar una real como, por ejemplo, el inicio de sesión de un proveedor de correo electrónico. Se suelen utilizar dominios que sean muy parecidos cambiando letras que se parecen y que visualmente engañan al usuario. Este tipo de suplantaciones suele tener como objetivo la obteción de credenciales de usuarios.

Para defenderse ante esto existen técnicas concretas, véase esto en puntos posteriores.

1.6. Medidas de seguridad

Se ha explicado como funciona el *phishing*, las técnicas que usa y los distintos tipos con sus características. Una vez conocido todo esto queda una de las partes más importantes, ¿cómo nos defendemos de esto? En los siguientes puntos se describirán diversos métodos que nos ayudarán a protegernos del *phishing*.

1.6.1. SPF

SPF o *Sender Policy Framework* es un registro DNS que es usado para evitar la suplantación de identidad o *spoofing*. Gracias a esto se pueden identificar los servidores que están autorizados a enviar correo saliente de un dominio específico. El sistema de correo electrónico verifica que la IP o host origen proceden de servidores de correo autorizados.

Si llega un correo que esté usando un dominio desde un servidor de correo no permitido, el sistema de correo lo mueve automáticamente a correo no deseado o lo elimina en función de la política a seguir en estos casos. Una regla SPF tiene la siguiente sintaxis:

```
v=spf1 <IP> <enforcement rule>
```

En esta sintaxis se diferencian dos apartados que son variables:

- <IP> → direcciones IP que están autorizadas a enviar correos electrónicos en nombre de un dominio.
- <enforcement rule> → regla de cumplimiento a seguir si dominio está siendo utilizado para enviar un correo electrónico desde una dirección IP no autorizada. Diferenciamos tres opciones dentro de este parámetro:
    - -all. Se denomina error grave, y es usado normalmente cuando se conocen todas las direcciones IP que están habilitadas para enviar correos en nombre de un dominio. Si el correo no es enviado desde una IP autorizada, una vez marcado como "error grave", se sigue la política configurada para correos con esta marca.
    - ~all. Usado cuando no se conoce toda la lista de direcciones IP autorizadas a enviar correo electrónico desde un dominio, esta opción se denomina error leve. Lo normal es que los clientes de correo tengan configurado marcar mensajes desde equipos no autorizados a enviar en nombre de un dominio como sospechosos.
    - ?all. Esta opción se llama "Neutra" y se suele usar para realizar pruebas con el registro SPF ya que no marca los correos ni hace nada con ellos.

1.6.2. DKIM

DKIM o *DomainKeys Identified Mail* se trata de una técnica utilizada para comprobar que el correo electrónico enviado es legítimo y que no ha sido modificado desde que se envió hasta que llegó al destinatario, esto al igual que SPF se utiliza para evitar técnicas de *spoofing* o suplantación de identidad y se recomienda usar ambas medidas en conjunto.

Esta técnica funciona añadiendo una cabecera al correo electrónico con una firma digital. Si se envía un correo electrónico y se tiene activo el registro DKIM se seguirían los siguientes pasos:

1. El usuario origen envía un correo electrónico en el que se añade una cabecera que contiene una firma creada con el resto de las cabeceras y el cuerpo del mensaje mediante una clave privada.
2. El servidor de correo del destinatario realiza una petición DNS al dominio del usuario que ha enviado el correo solicitando la clave pública del registro para descifrar la cabecera.
3. Se descifra la cabecera gracias a la clave pública del registro.
4. Una vez descifrada se recalcula la firma con el resto de las cabeceras y el cuerpo del mensaje, si los valores coinciden se confirma que el correo es legítimo y que no ha sido modificado.

Una de las grandes desventajas de esta técnica es el gran costo computacional que conlleva realizar labores de cifrado y descifrado por cada correo electrónico.

1.6.3. DMARC

DMARC o *Domain-based Message Authentication, Reporting and Conformance* es un registro TXT para unificar el uso de SPF y DKIM. Este se utiliza para establecer políticas en función de los resultados que se obtengan de los dos últimos registros mencionados para poder combatir eficazmente los casos de *phishing* evitando que lleguen a los buzones de correo.

El registro DMARC indica que hacer ante fallos en las validaciones SPF y DKIM, las acciones ha realizar se configuran en un registro dentro del servidor DNS que se use para el dominio de correo. Lo siguiente que se muestra es un ejemplo:

```
v=DMARC1; p=none; rua=mailto:correo@tudominio.com
```

Las etiquetas que se pueden utilizar son las siguientes:

- v → Versión del protocolo.
- p → Indicación sobre que tiene que se tiene que hacer si un correo no pasa la validación de DMARC, en este caso se distinguen tres valores:
    - reject. Se rechazan los correos electrónicos, el servidor devuelve los correos a los servidores que lo envían.
    - quarentine. Se marcan los correos como *spam* y se mandan a la carpeta de correo no deseado
    - none. No se hace nada con los correos electrónicos que no pasen la validación, pero aún así queda un registro de los correos que no lo han pasado.
- rua (Opcional) → Etiqueta con la que se puede enviar un correo electrónico informes de actividad de DMARC. La dirección de correo tiene que venir precedida de "mailto:".
- ptc (Opcional) → Porcentaje de mensajes sospechosos a los que se le va a llegar a aplicar la política configurada previamente.
- sp (Opcional) → Etiqueta para configurar de manera diferente en los subdominios de un dominio que hacer con los correos electrónicos que no superen la validación DMARC. Las opciones son las mismas que en la etiqueta "p".
- adkim → Grado de similitud que tiene que existir entre el mensaje recibido y las firmas que produce el tener activo el registro DKIM.
- aspf → Etiqueta similar a la enterior (adkim) pero relacionada con el registro SPF.

1.6.4. Antimalware

Se han descrito en el punto 1.2 los diferentes tipos de *phishing* en los que se ha podido ver que en ocasiones este tipo de ataque puede tener como objetivo la infección de un equipo con un malware adjunto. Para evitar que en caso de que un usuario sea afectado satisfactoriamente esto la medida más efectiva que se puede tomar es tener instalado un antimalware.

Por lo general los antimalware son conocidos comúnmente como antivirus, pero realmente no se tratan de lo mismo. Para conocer las diferencias nos podemos enfocar en lo que intenta evitar cada software, un virus o un *malware*.

Un virus informático tiene como objetivo provocar un malfuncionamiento del sistema como, por ejemplo, que el equipo del usuario afectado tenga un funcionamiento más lento. Sin embargo, el malware va más allá, ya que en primer lugar este está enfocado a todo tipo de software malicioso y, en segundo lugar, el malware está enfocado también en actividades como robo de credenciales o de información, o incluso llegar a encriptar un equipo.

Gracias a la computación en la nube, más conocido como *cloud computing*, se han desarrollado nuevos productos para hacer frente al *malware* de hoy en día, ya que este cada vez es más sofisticado y complicado de detectar. En concreto se pueden diferenciar dos:

- EPP o plataformas de protección endpoint, más conocido como antimalware de firmas tradicional. Este producto basa las detecciones en una lista de firmas que idenfican a cada clase de malware, las firmas son secuencias de bytes que permiten identificar cuando se está ante un software malicioso o no. Se considera que usar esto es insuficiente ya que solo llega a parar amenazas ya conocidas.
- EDR o detección y respuesta en endpoints. Gracias a esta tecnología se pueden parar las amenazas nuevas que son aún desconocidas, se hace uso de la nube para analizar, mediante diversas técnicas como por ejemplo el sandboxing, los ficheros desconocidos y así saber si estamos ante malware o no. Su función es evitar amenazas nuevas o vulnerabilidades del tipo Zero-Day, que aún no han sido corregidas.

Estas dos soluciones evitarian infecciones mediante archivos adjuntos en ataques de tipo *phishing*, ambas no son incompatibles entre sí todo lo contrario, normalmente suelen usarse en conjunto.

1.6.5. Proxy

Un servidor proxy es usado como punto intermedio entre un equipo y un destino específico. Este tiene diversas funcionalidades y no están enfocadas en detener ataques de *phishing*, pero si nos pueden ayudar a reducir casos de robo de credenciales de páginas web falsas o incluso reducir el impacto que pueda provocar la infección de un equipo.

En concreto, gracias al uso de servidores proxy podremos filtrar el acceso de los equipos que salen a través de el a ciertas direcciones IP o dominios que pueden considerarse maliciosos. Para ver lo útil que puede llegar a ser esto se van a explicar dos ejemplos que podrían ser casos reales:

- Un docente de la US recibe un correo suplantando a la Universidad de Sevilla. Se recibe un ataque de tipo phishing que simula ser un correo real de la universidad solicitando el reestablecimiento de la contraseña del objetivo por seguridad. En el correo electrónico existe un enlace a una página web que simula ser real con dominio unisevi1la.es. El usuario pincha en el enlace pensando ser real pero previamente han sido cortados todos los enlaces de dominios que puedan ser parecidos en cuanto a nombre a la universidad de sevilla, por lo que se ha evitado que el objetivo del ataque sufra un robo de credenciales.
- En este caso se lanza una campaña de *phishing* también a la US con objetivo de distribuir un malware que mande las pulsaciones de teclado a una dirección IP X.X.X.X. El archivo infectado se encuentra adjunto en el correo electrónico y el equipo se infecta debido a que el usuario lo ejecuta. Este se dedica a enviar las pulsaciones mencionadas con anterioridad a la dirección X.X.X.X, que se encuentra en listas negras, sin embargo, previamente han sido cortadas las direcciones IP de diversas listas negras para evitar que los usuarios que salgan por el proxy se conecten a estas. No se ha evitado la infección del equipo, pero gracias al proxy se ha evitado la captura de pulsaciones de teclado.

1.6.6. AntiSpam

Normalmente los filtros AntiSpam son soluciones más reactivas que proactivas, ya que estos permiten realizar un filtrado de los correos que queremos mandar a la carpeta de correo no deseado una vez llegan al destinatario.

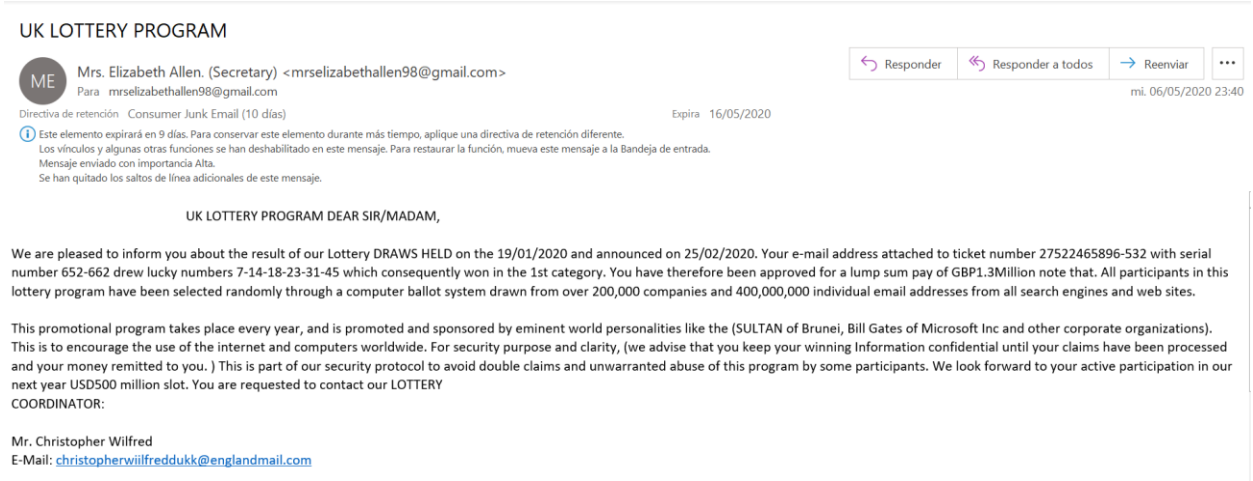
Lo usual es implementar reglas para evitar que puedan llegar correos de *phishing* que ya han llegado con anterioridad a los buzones de los usuarios, ya sea filtrando por dominio de correo o por contenido en el cuerpo del mensaje.

El problema es que el uso de reglas no configuradas correctamente puede llegar a producir que correos legítimos que si que se quieran recibir sean redirigidos a la carpeta de correo no deseado. Este es un precio a pagar para reducir en gran medida los correos fraudulentos. Las opciones de filtrados son varias y gracias a ellas algunos de los apartados de un correo que se pueden filtrar son los siguientes:

- Dominio de cuenta de correo.
- Palabras o frases que se encuentren en el cuerpo del mensaje o en el asunto.
- Por remitente.
- Por archivos adjuntos, por ejemplo, según el tamaño del fichero o la extensión.
- Se pueden aplicar de políticas de negar a todos los remitentes y tener una lista blanca que solo reconozca algunos como remitentes confiables.

2 ANÁLISIS DE UN CASO DE PHISHING

Una vez explicados los diversos puntos del *phishing* a nivel teórico, se procederá a analizar un caso real en el que se le anuncia a la víctima que le ha tocado la loteria y se solicita que se contacte con un tercero para reclamar el premio. Podemos ver el correo en la siguiente imagen.


UK LOTTERY PROGRAM

ME Mrs. Elizabeth Allen. (Secretary) <mrselizabethallen98@gmail.com>
Para mrselizabethallen98@gmail.com

Responder | Responder a todos | Reenviar | ...
mi. 06/05/2020 23:40

Directiva de retención Consumer Junk Email (10 días) Expira 16/05/2020

Este elemento expirará en 9 días. Para conservar este elemento durante más tiempo, aplique una directiva de retención diferente.
Los vínculos y algunas otras funciones se han deshabilitado en este mensaje. Para restaurar la función, mueva este mensaje a la Bandeja de entrada.
Mensaje enviado con importancia Alta.
Se han quitado los saltos de línea adicionales de este mensaje.

UK LOTTERY PROGRAM DEAR SIR/MADAM,

We are pleased to inform you about the result of our Lottery DRAWS HELD on the 19/01/2020 and announced on 25/02/2020. Your e-mail address attached to ticket number 27522465896-532 with serial number 652-662 drew lucky numbers 7-14-18-23-31-45 which consequently won in the 1st category. You have therefore been approved for a lump sum pay of GBP1.3Million note that. All participants in this lottery program have been selected randomly through a computer ballot system drawn from over 200,000 companies and 400,000,000 individual email addresses from all search engines and web sites.

This promotional program takes place every year, and is promoted and sponsored by eminent world personalities like the (SULTAN of Brunei, Bill Gates of Microsoft Inc and other corporate organizations). This is to encourage the use of the internet and computers worldwide. For security purpose and clarity, (we advise that you keep your winning Information confidential until your claims have been processed and your money remitted to you.) This is part of our security protocol to avoid double claims and unwarranted abuse of this program by some participants. We look forward to your active participation in our next year USD500 million slot. You are requested to contact our LOTTERY
COORDINATOR:

Mr. Christopher Wilfred
E-Mail: christopherwiilfreddukk@englandmail.com

Figura 2-1 Phishing real

Para analizar un caso de *phishing* primero tenemos que observar la fuente que se nos muestra de origen, sin pensar directamente que ha sido enviado por esa persona. Aún así el ver que una cuenta de correo con dominio gmail nos informa de que hemos ganado la lotería de UK resulta sospechoso.

Al ser un correo relacionado con lotería vemos que no se trata de un intento de sustracción de credenciales, ya que no se nos redirige a ninguna página que simula ser quien no es. A parte, tampoco contiene ningún adjunto que pueda resultar algún tipo de *malware.*

El correo electrónico no nos llama por nuestro nombre ni contiene ningún dato que sea personal nuestro por lo que todo esto indica que el correo ha sido enviado de forma masiva a una diversa cantidad de usuarios. Se puede deducir que nos encontramos ante un caso de *phishing* tradicional.

Una vez visto por encima el correo electrónico, observaremos las cabeceras. Dentro de las cabeceras se analizarán las posibles direcciones de correo electrónico que aparezcan, por si se encuentra otra diferente que indique que pertenece a la persona que ha lanzado la campaña. También se analizarán las diversas cabeceras “Recived” para encontrar el servidor de correo de origen. En la siguiente imagen se observan estas últimas y debajo se analizarán los siguientes apartados.

```
Received: from BN8NAM12HT036.eop-nam12.prod.protection.outlook.com
 (2603:10a6:20b:110::16) by AM7P191MB0710.EURP191.PROD.OUTLOOK.COM with HTTPS
 via AM7PR04CA0006.EURPRD04.PROD.OUTLOOK.COM; Wed, 6 May 2020 14:39:42 +0000

Received: from BN8NAM12FT036.eop-nam12.prod.protection.outlook.com
 (2a01:111:e400:fc66::4c) by
 BN8NAM12HT036.eop-nam12.prod.protection.outlook.com (2a01:111:e400:fc66::257)
 with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.2979.23; Wed, 6 May
 2020 14:39:42 +0000

Authentication-Results: spf=softfail (sender IP is 81.218.26.115)
 smtp.mailfrom=gmail.com; hotmail.com; dkim=none (message not signed)
 header.d=none;hotmail.com; dmarc=fail action=none
 header.from=gmail.com;compauth=fail reason=001
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 gmail.com discourages use of 81.218.26.115 as permitted sender)

Received: from ydi-dc.ydi.local (81.218.26.115) by
 BN8NAM12FT036.mail.protection.outlook.com (10.13.182.224) with Microsoft SMTP
 Server id 15.20.2979.23 via Frontend Transport; Wed, 6 May 2020 14:39:41
 +0000
```

Figura 2-2 Cabeceras SMTP

Una vez vistas las cabeceras, se puede ver que el correo electrónico ha seguido el siguiente recorrido:

ydi-dc.ydi.local (81.218.26.115) → BN8NAM12HT036.eop-nam12.prod.protection.outlook.com

Es decir, se observa que el correo ha sido mandado directamente desde el servidor con dirección IP 81.218.26.115 hacia un servidor de outlook que lo ha llevado a nuestra bandeja de correo electrónico.

Ya visto esto, podemos analizar la dirección IP con diversas herramientas gratuitas online. Primero se procederá a ver donde está geolocalizada la IP con la herramienta http://whois.domaintools.com/.

IP Location	Israel Petah Tikva Aspeka Diamonds Ltd Lan
ASN	AS8551 BEZEQ-INTERNATIONAL-AS Bezeqint Internet Backbone, IL (registered Nov 17, 1997)
Resolve Host	mail.ydiltd.com
Whois Server	whois.ripe.net
IP Address	81.218.26.115

Figura 2-3 Geolocalización del servidor de correo del phishing

Se ve que la dirección IP está geolocalizada en Israel, por lo que nos tiene que resultar extraño que se mande un correo informando de que se ha ganado la lotería de UK desde un servidor de Israel.

Por otro lado, se usará MxToolBox con URL https://mxtoolbox.com/blacklists.aspx ya que está enfocada a listas negras de direcciones IP de correo electrónico. Los usuarios comunes de Internet reportan direcciones que están realizando acciones no éticas y son incluidas en estas listas, por lo que de cara a un análisis es de interés saber si la IP se encuentra en alguna.

Como era de esperar, la dirección IP en cuestión se encuentra en 12 listas negras diferentes, algunas de ellas relacionadas con *spam*. Esto se ve en la siguiente imagen.

Checking **81.218.26.115** against **87** known blacklists...
Listed **12** times with **1** timeouts

	Blacklist	Reason	TTL	Res
LISTED	Abusix Mail Intelligence Blacklist	81.218.26.115 was listed Detail	60	
LISTED	BARRACUDA	81.218.26.115 was listed Detail	900	
LISTED	Hostkarma Black	81.218.26.115 was listed Detail	2100	
LISTED	ivmSIP	81.218.26.115 was listed Detail	2100	
LISTED	NIXSPAM	81.218.26.115 was listed Detail	60	
LISTED	Sender Score Reputation Network	81.218.26.115 was listed Detail	2100	
LISTED	SORBS NEW	81.218.26.115 was listed Detail	3600	
LISTED	SORBS SMTP	81.218.26.115 was listed Detail	3600	
LISTED	SORBS SPAM	81.218.26.115 was listed Detail	3600	
LISTED	SPAMCOP	81.218.26.115 was listed Detail	1	

Figura 2-4 Listas negras de la dirección IP del correo de phishing

Si seguimos usando herramientas para analizar el caso, otra interesante de cara al *phishing* es **Cisco Talos**. Esta herramienta desarrollada por Cisco te da la reputación en diversos puntos de la dirección IP, uno de los indicadores que te da resulta ser de correo electrónico. Esta herramienta se accede mediante la URL https://talosintelligence.com/reputation_center/, y si introducimos la dirección IP nos da la siguiente información:

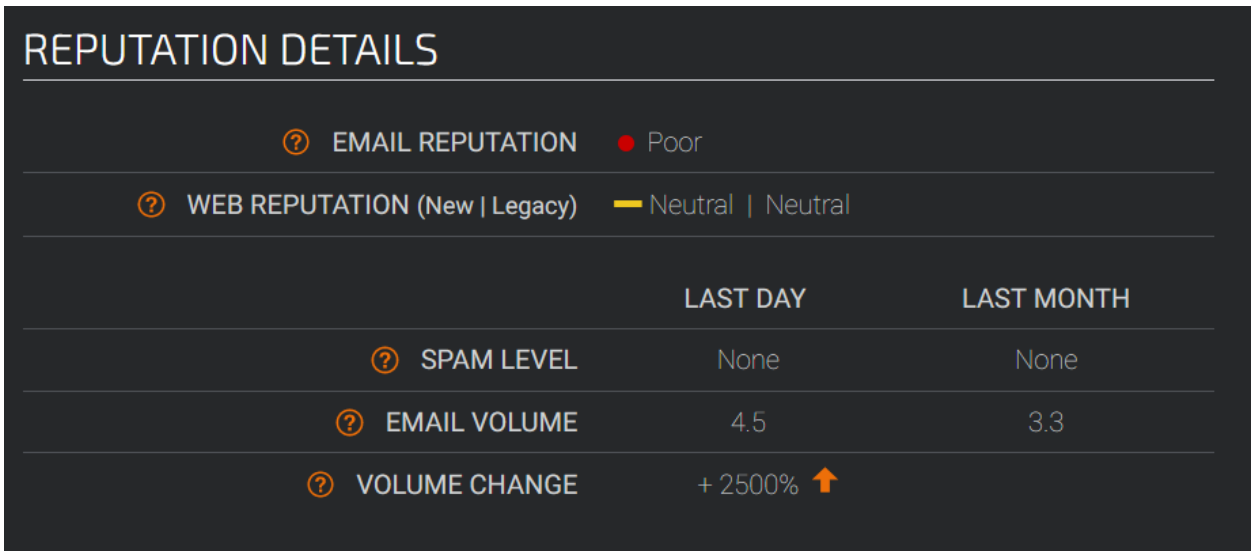


Figura 2-5 Reputación de la dirección IP que envía el phishing

En esta herramienta se destacan ciertas cosas. La primera es que a nivel de reputación Web le da una puntuación

neutral, sin embargo, a nivel de correo electrónico Cisco categoriza la IP como pobre. Finalmente vemos que el volumen de correos electrónicos se ha visto incrementado en un 2500%, esto será de interés posteriormente.

En la imagen de la herramienta domaintools, en el apartado "Resolved Host", se nos mostraba que la dirección del host SMTP resultaba ser smtp.ydiltd.com, es decir, esa es el dominio real del servidor de correo, pero, ¿contendrá también una página web alojada? Si introducimos el dominio nos encontramos con lo siguiente:

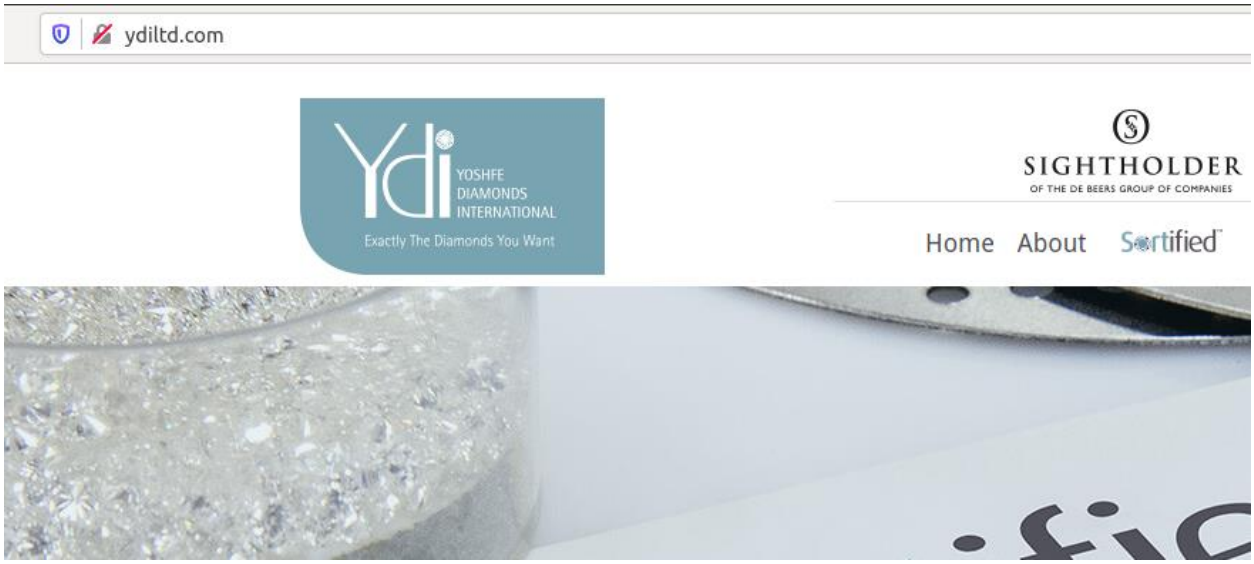


Figura 2-6 Página web de la IP del correo de phishing

Resulta ser una web de un comercio de venta de diamantes a nivel internacional, resulta un poco extraño que un comercio de estas características se dedique a realizar campañas de *phishing*.

Se procederá a usar una herramienta llamada **Shodan**. Esta herramienta es utilizada para conocer información sobre las direcciones IP públicas expuestas a Internet, se puede acceder a ella mediante www.shodan.io y si introducimos la IP de Israel se obtiene la siguiente información.

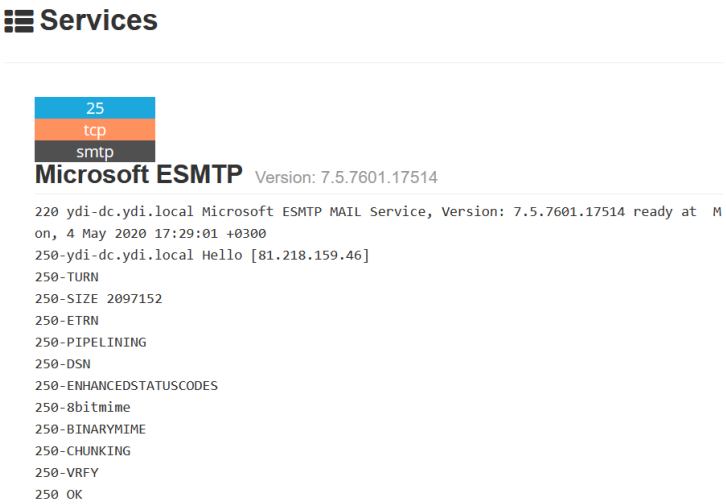


Figura 2-7 Servicios expuestos de la IP del phishing 1

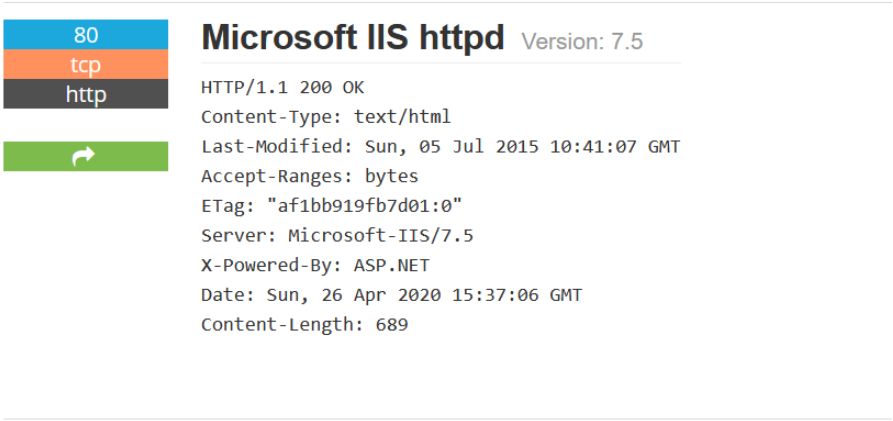


Figura 2-8 Servicios expuestos de la IP del phishing 2

De esta información podemos sacar dos conclusiones. En primer lugar, el servidor que tiene esa IP expuesta a internet tiene un servicio SMTP expuesto en el puerto 25 y un servicio web en el puerto 80. En segundo lugar, la última modificación de la web se realizó el 5 de Julio de 2015 por lo tanto, llevan 5 años sin cambiar nada de la web.

Por otro lado, Shodan nos muestra que la dirección IP contiene una gran cantidad de vulnerabilidades:

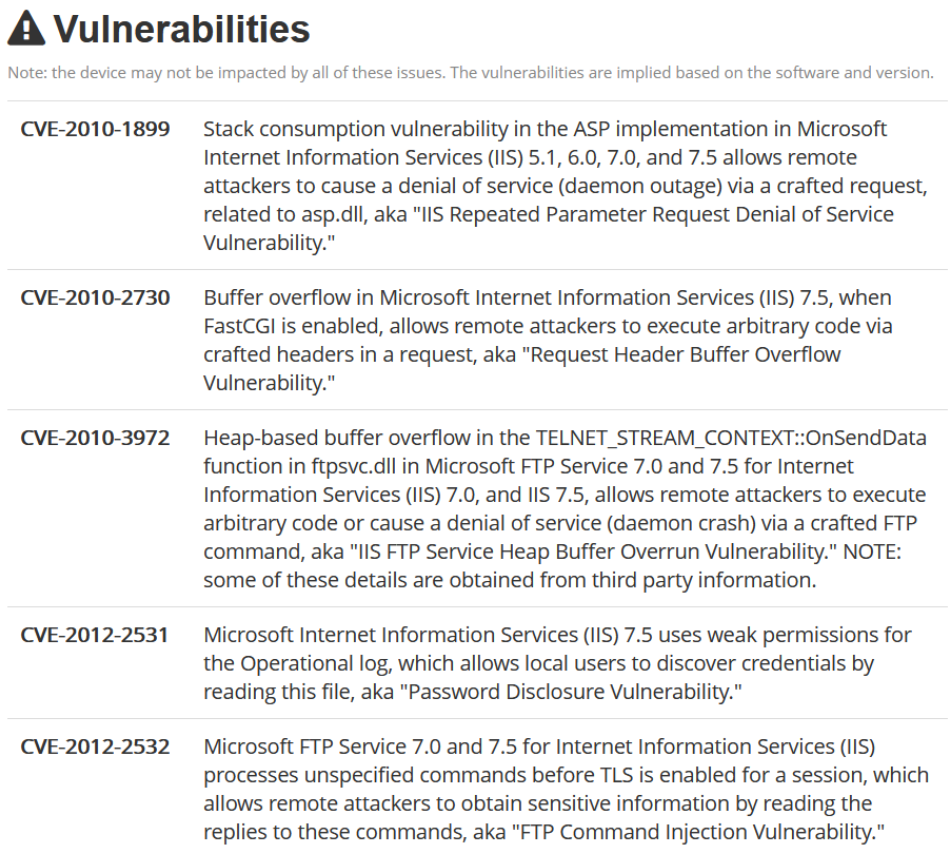


Figura 2-9 Vulnerabilidades existentes en los servicios expuestos por la IP

Por lo tanto, gracias a toda esta información se puede llegar a las siguientes conclusiones:

- El servidor con la dirección IP 81.218.26.115 ha sido hackeado, el atacante que ha realizado la campaña se ha aprovechado de las vulnerabilidades de este servidor para enviar campañas de *phishing* de correo electrónico.
- Esto demuestra el por qué una web enfocada a venta de diamantes iba a realizar campañas de *phishing* simulando que usuarios habían ganado la lotería de UK.
- En Cisco Talos se nos daba una puntuación web neutral y una puntuación de correo pobre, es decir, a nivel web la IP no tenía problema, pero en cuanto a correo electrónico sí.
- El hackeo ha sido reciente, esto concuerda con que la fecha de envío que se ve en el correo electrónico data del día 6 de mayo de 2020, y también con que en Cisco Talos se nos muestre un aumento de envío de correo electrónico del 2500%.

3. LAS CAMPAÑAS DE CONCIENCIACIÓN

Se han llegado a describir los diferentes tipos de medidas de seguridad que se pueden aplicar para combatir los ataques de *phishing* o al menos reducir su impacto, pero no se ha mencionado una de las más importantes, las campañas de concienciación a los usuarios.

3.1. Descripción

Todas las medidas de seguridad anteriormente mencionadas son implantaciones a nivel técnico, pero a parte de realizar todo lo mencionado a lo largo del punto 1.6. hay que reforzar también a los usuarios. Realmente los usuarios o los trabajadores de una empresa, que son los que suelen recibir campañas más personalizadas y por lo tanto con más probabilidades de éxito, son lo que se podría definir como el eslabón más débil de la cadena.

Debido a esto es importante conocer el grado de concienciación y de conocimiento que tienen los usuarios para implantar formación a las personas con poco conocimiento sobre los ataques de *phishing* para reducir la probabilidad de éxito de un posible atacante.

3.2. Objetivo

Ya que se considera de vital importancia la concienciación de los usuarios acerca del *phishing* se tendrá como objetivo el lanzamiento de una campaña de forma controlada para conocer el alcance de un posible ataque. Para esto se buscará una herramienta que sea capad de realizar esto de forma automática y personalizada, por lo que se lanzará un ataque de tipo *Spear Phishing*.

En el próximo apartado se analizarán diversas herramientas existentes para llegar a la conclusión de cual es mejor utilizar en base a nuestras necesidades, una vez hecho esto se implementará y se creará un piloto simulando una campaña enfocada a un grupo de usuarios.

3.3. Análisis de las posibles soluciones

Existen diversas herramientas que nos dan la posibilidad de realizar una campaña de phishing para conocer el grado de concienciación de los usuarios. Como se ha dicho anteriormente se van a analizar diversas soluciones y finalmente se seleccionará una en base a unos criterios para realizar un piloto. En la siguiente se va a proceder con el análisis indicado:

Nombre	Características
SecurityIQ PhishSim	El principal beneficio de este producto es que se trata de un SaaS o *Software As A Service* y no requiere de instalación ni configuración. Simplemente hay que registrarse y empezar a configurar las campañas que se quieran lanzar desde su web. El problema es que la versión gratuita tiene limitaciones en cuanto a número de opciones de configuración de las campañas.
GoPhish	GoPhish se trata de una plataforma *Open Source* compatible con gran cantidad de sistemas operativos y que requiere una sencilla instalación. No existen limitaciones en cuanto a campañas, usuarios o plantillas y se pueden generar informes de los resultados de las campañas.
LUCY	Este producto es gratuito únicamente en su versión comunitaria, pero se puede instalar facilmente con un simple script. Tiene incluidos módulos interactivos para la concienciación de los usuarios. El problema es que tiene grandes limitaciones para entornos empresariales y muchas opciones están limitadas en la versión comunitaria como, por ejemplo, añadir archivos adjuntos o exportar estadísticas.
Sophos Phish Threat	Sophos nos ofrece un buen producto con opciones como informes detallados, un dashboard interactivo o gran cantidad de plantillas. El problema es que la versión gratuita solo dura 30 días y está limitada a 100 usuarios.

Tabla 3 - 1 Comparativa de diversas herramientas para lanzamiento de campañas de concienciación

3.4. Determinación de la mejor solución

Después de presentar diversas soluciones existentes se ha llegado a la conclusión que la mejor herramienta para lo que se va a realizar es GoPhish. Esto se debe a que se va a buscar una instalación desde 0, es decir, instalar el servicio en una máquina y hacerlo funcionar a parte de que se trata de un producto *Open Source* por lo que no conllevará coste alguno.

A parte es muy flexible en cuanto a la creación de campañas porque podemos crear nuestros propios correos con código HTML evitando el uso o modificación de plantillas.

El único inconveniente es que no viene con herramientas de concienciación una vez que el usuario haya caido en el ataque controlado de phishing.

4. GoPhish

En este capítulo vamos a describir en diferentes apartados el funcionamiento de la herramienta para realizar campañas de phishing de forma ética como la securización del servidor donde está alojado, el funcionamiento de las diferentes características, diversas pruebas que se van a realizar y finalmente la explicación del piloto realizado para ponerla en funcionamiento.

4.1. Descripción

El software GoPhish se trata de una herramienta *open-source* enfocada a realizar campañas de *phishing* para exponer a una empresa o grupo a un ataque de *phishing*. Gracias a esto se puede llegar a comprobar el grado de concienciación de nuestros usuarios.

Esta herramienta destaca por su sencilla interfaz que nos permite en pocos pasos tener configurada una campaña sencilla para realizar pruebas.

A parte de la interfaz gráfica mencionada anteriormente, este software cuenta con una API REST que nos puede permitir generar informes con otra clase de software, como por ejemplo Microsoft Excel.

Finalmente también destacar que es compatible con las plataformas más comunes hoy en día. Estas son Linux, Mac OS y Windows.

4.2. Instalación y configuración

Al realizar la instalación se ha decidido alojar GoPhish en un VPS accesible mediante SSH con dirección IP 134.122.110.153. Las características del servidor son las siguientes:

- 1 GB de memoria RAM.
- 25 GB de almacenamiento SSD.
- Sistema Operativo: Ubuntu 18.04.3 LTS

Comenzando la instalación al ser un *software Open Source* se encuentra alojado en un repositorio de GitHub en el siguiente enlace: https://github.com/gophish/gophish/.

- El primer paso es el acceso al servidor por medio del servicio SSH, como se ha indicado anteriormente, para esto se utilizará PuTTY y se accederá con el usuario root:

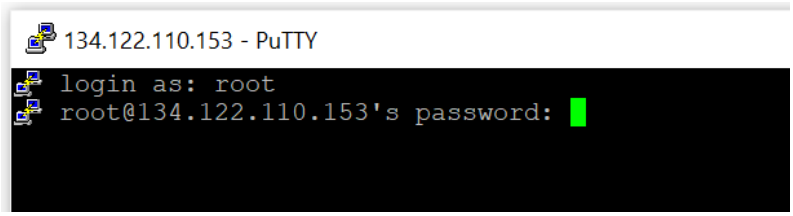


Figura 4-1 Inicio de sesión SSH

- En segundo lugar crearemos una carpeta donde alojar los archivos del *software*, hemos decidido que se llamará "gophish" y para ello se usa el siguiente comando:

  ```
  mkdir gophish
  ```

  Y posteriormente entramos en la carpeta creada con el commando:

  ```
  cd gophish
  ```

- Una vez dentro del directorio mencionado se procederá a descargar el software desde la URL: https://github.com/gophish/gophish/releases/download/v0.9.0/gophish-v0.9.0-linux-64bit.zip con el siguiente comando:

  ```
  wget https://github.com/gophish/gophish/releases/download/v0.9.0/gophish-v0.9.0-linux-64bit.zip
  ```

  Finalmente extraemos el fichero .zip que se descarga:

  ```
  unzip gophish-v0.9.0-linux-64bit.zip
  ```

- Una vez realizados los pasos anteriores tendremos que configurarlo. Esto se realiza mediante el fichero config.json dentro de la carpeta donde hemos descargado y extraido gophish. Para editar el fichero de configuración ejecutaremos el siguiente comando:

  ```
  nano config.json
  ```

  Ya en el fichero de configuración se nos mostrará algo como esto:

```
{
        "admin_server": {
                "listen_url": "127.0.0.1:3333",
                "use_tls": true,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key"
        },
        "phish_server": {
                "listen_url": "0.0.0.0:80",
                "use_tls": false,
                "cert_path": "example.crt",
                "key_path": "example.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}
```

Figura 4-2 Configuración por defecto de GoPhish

Dentro de la configuración, podemos destacar los siguientes apartados descritos en [1]:

- **admin_server.listen_url**: dirección IP y puerto a través de la cual se va a acceder al panel de administración de la herramienta. En caso de que se quiera acceder solo en local, no hará falta modificar esto, si se quiere exponer a internet se cambiará esto por 0.0.0.0:puerto.
- **admin_server.use_tls:** especificación con valores yes/no de si se va a utilizar una capa TLS para cifrado en la consola de administración o no.
- **admin_server.cert_path:** ruta donde se encuentra el certificado SSL que se va a utilizar si se tiene activada la configuración anterior en la consola del servidor. Al venir configurado con la capa TLS activa de forma predeterminada, gophish nos viene con un certificado firmado por sí mismo que los navegadores no lo marcan como de confianza.
- **admin_server.key_path:** ruta donde se encuentra la clave utilizada para descifrar los mensajes enviados al servidor. Como se indica en el apartado anterior al venir de forma predeterminada la capa TLS activa, gophish nos trae una clave predeterminada en la carpeta donde se ha descargado el mismo.

- **phish_server.listen_url:** dirección IP y puerto donde van a ser alojadas las páginas de phishing utilizadas en los ataques que se van a lanzar en las campañas. En este caso está de forma predeterminada en el valor 0.0.0.0:80 ya que las páginas webs estaran expuestas a internet. Está configurado el puerto 80 debido a que está configurado de forma predeterminada para que no se utilice TLS.
- **phish_server.use_tls:** especificación con valores yes/no de si se va a utilizar una capa TLS para cifrado en las páginas web utilizadas en las campañas de phishing o no. El valor predeterminado es no.
- **phish_server.cert_path:** carpeta donde se encuentra alojado el certificado usado para las páginas web de las campañas de phishing. En este caso al no estar marcado de forma predeterminada la capa TLS no nos vendrá un certificado firmado por gophish, en este caso tendremos que generarlo nosotros.
- **phish_server.key_path:** al igual que con el apartado del servidor de administración, aquí se indica la ruta en la que se encuentra la clave con la que el servidor cifra/descifra los mensaje. Al igual que con el certificado, al no estar configurada de forma predeterminada la capa TLS como activa no nos viene con una clave, por lo que tendremos que generarla nosotros.
- **db_name:** base de datos utilizada por gophish, en este caso se usa de forma predeterminada SQLite. Si queremos modificar el tipo de base de datos usada tendremos que modificar esta configuración, por ejemplo, en caso de querer usar MySQL tendremos que escribir aquí "mysql".
- **db_path:** ruta donde se encuentra la base de datos. GoPhish viene ya con una creada en el directorio donde se descargado con el nombre "gophish.db".

Una vez ya configurado GoPhish para su uso nos queda el siguiente archive de configuración:

```
{
        "admin_server": {
                "listen_url": "0.0.0.0:3380",
                "use_tls": true,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key"
        },
        "phish_server": {
                "listen_url": "0.0.0.0:80",
                "use_tls": false,
                "cert_path": "example.crt",
                "key_path": "example.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}
```

Figura 4-3 Nueva configuración de GoPhish

Se ha modificado el puerto predeterminado 3333 de la consola de administración por el 3380 para evitar usar puertos que ya vienen configurados a esto. Gracias a esto se evita que sea fácil de encontrar el panel de inicio de sesión de la consola de administración.

- Ya finalizada la configuración podemos arrancar GoPhish. Para esto tendremos que acceder al directorio donde ha sido descargado y ejecutar el siguiente comando:

  ```
  ./gophish
  ```

- Si hemos configurado todo correctamente podríamos acceder a través del navegador. Si usaramos la configuración predeterminada accederíamos a través de la dirección https://localhost:3333. En este caso al usar una configuración diferente accederemos a través de https://134.122.110.153:3380/. La pantalla que se nos mostrará es la siguiente:

Figura 4-4 Inicio de sesión de GoPhish

GoPhish viene con un usuario por defecto, este se llama “admin” y tiene como contraseña “gophish”. Esto se ha modificado para evitar problemas de seguridad. En apartados posteriores se explicará como realizar esto.

4.3. Estructura

En este apartado se dará una descripción de cada una de las secciones que nos da GoPhish, qué nos aporta cada una y como utilizarla. Primero se describirán los apartados de administración de la herramienta, es decir, las secciones que únicamente podrán usar los usuarios con permisos de administrador. Después pasaremos a describir el resto en el orden en el que se usan para crear una campaña de *phishing*. Los distintas secciones que tenemos en nuestra herramienta son las siguientes:

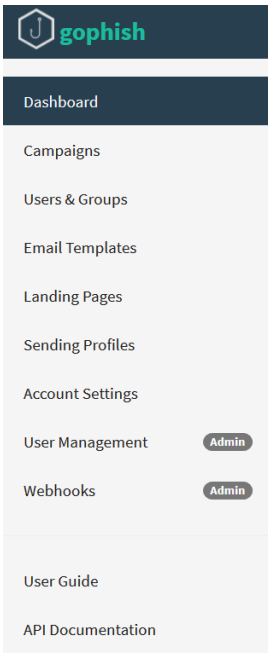


Figura 4-5 Menú de GoPhish

4.3.1. Zonas de administración

Como su título lo índica empezaremos explicando las secciones que solo pueden ver usuarios con rol de administrador, estas son las siguientes:

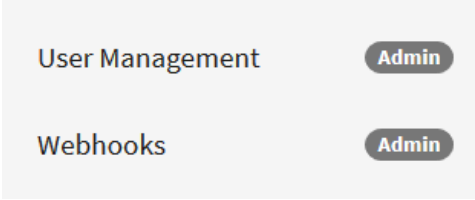


Figura 4-6 Panel de administración

- User Management

En esta sección se nos permitirá gestionar los usuarios que tienen acceso a la herramienta. Al realizar clic aquí se nos mostrará un menú similar al siguiente en el que se nos mostrará una lista de los usuarios actualmente creados y su rol:

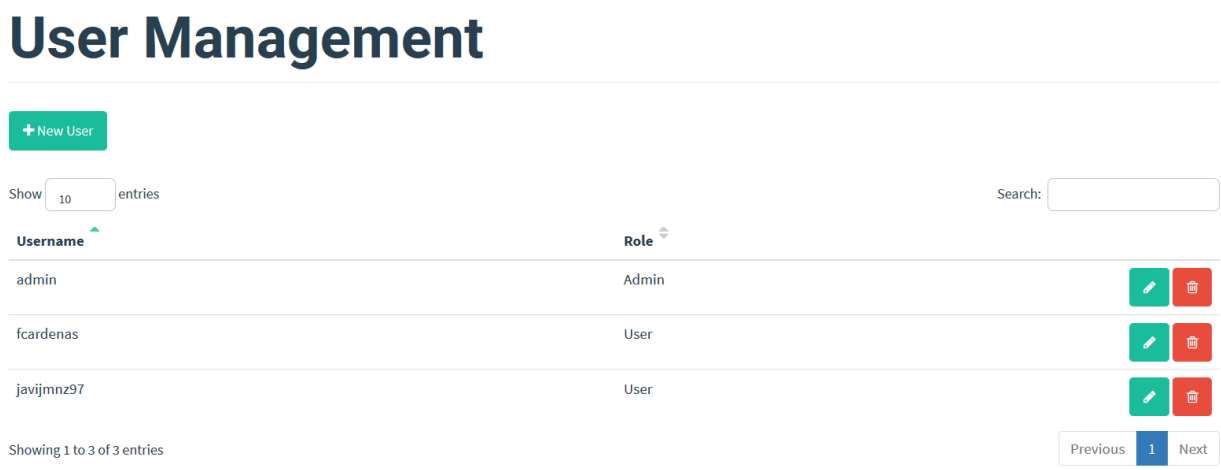


Figura 4-7 Lista de usuarios

Como podemos observar tenemos las siguientes opciones:

- Crear nuevos usuarios con la opción New User.
- Editar usuarios ya existentes.
- Borrar usuarios.

Al realizar clic en el botón de New User se nos mostrará un recuadro como el siguiente:

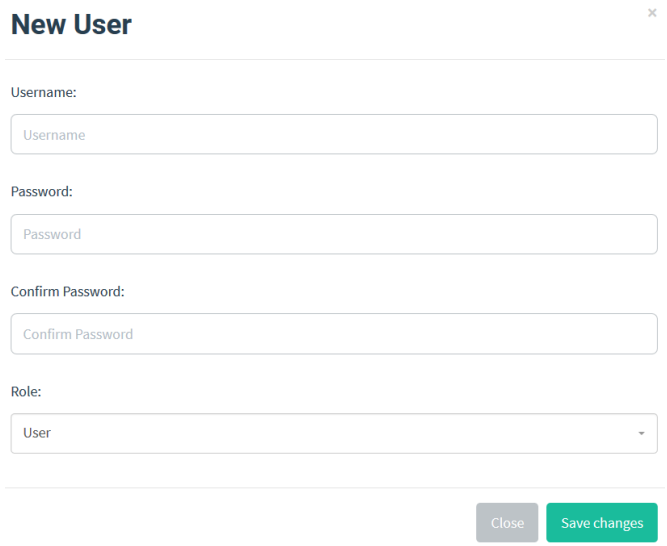


Figura 4-8 Creación de un nuevo usuario 1

Como se puede ver te da la opción de elegir un nombre de usuario ya existente, su contraseña y su rol. Dentro de los roles tenemos dos opciones: User y Admin. Las opciones que diferencian a cada uno son muy sencillas. Los usuarios Admin tendrán acceso a las secciones con el siguiente recuadro  y los que no lo son no.

Por otro lado podremos editar los usuarios existentes dándole clic al botón  que aparece a la derecha de cada uno. Aquí se nos mostrará un menú similar al visto con anterioridad al crear un usuario nuevo, pero con el campo Username y Role rellenos. En la siguiente imágen podemos ver un ejemplo:

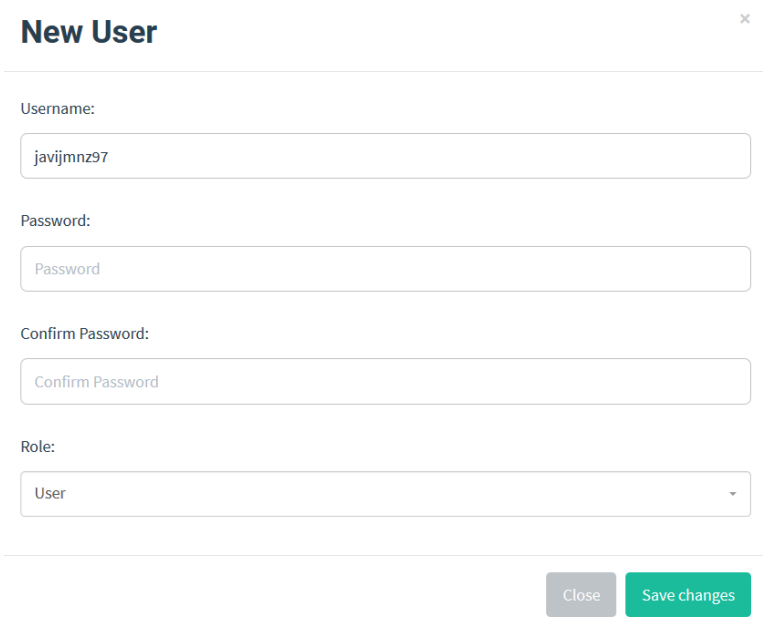


Figura 4-9 Creación de un nuevo usuario 2

Como se ha podido observar, tenemos también la opción de editar la contraseña de cada uno de los usuarios.

Finalmente, realizándo clic en el botón  conseguiremos borrar un usuario en concreto.

- Webhooks

Un *webhook* no es más que una acción que se realizar al suceder cierto evento, esto es útil para programar ciertas actividades dentro de nuestras campañas de *phishing*, esto se implementa mediante el protocolo HTTP con mensajes del tipo POST y suele utilizarse para conectar aplicaciones. *GoPhish* tiene la capacidad de programarlos dentro de su interfaz. Este trabajo no usará esto, aún así se realizará una breve descripción de este apartado.

Estos funcionan siendo asignados a una URL concreta que es la que manda un mensaje desde *GoPhish* a una aplicación denominémosla "B". Es decir, pongamos el ejemplo de que se tiene una aplicación para monitorizar mediante correos electrónicos en tiempo real una campaña de phishing. La persona que lanza las campañas asigna un *webhook* a la URL de su campaña de *phishing* para que al ser accedida se mande un mensaje a la aplicación B para que mande un correo electrónico avisando de esto.

Al hacer clic en "Webhooks" se nos mostrará un menú en el que se ve un listado de los que están creados actualmente, la URL que tiene asignada y si está actualmente activado. Esto se puede ver en la siguiente imagen:

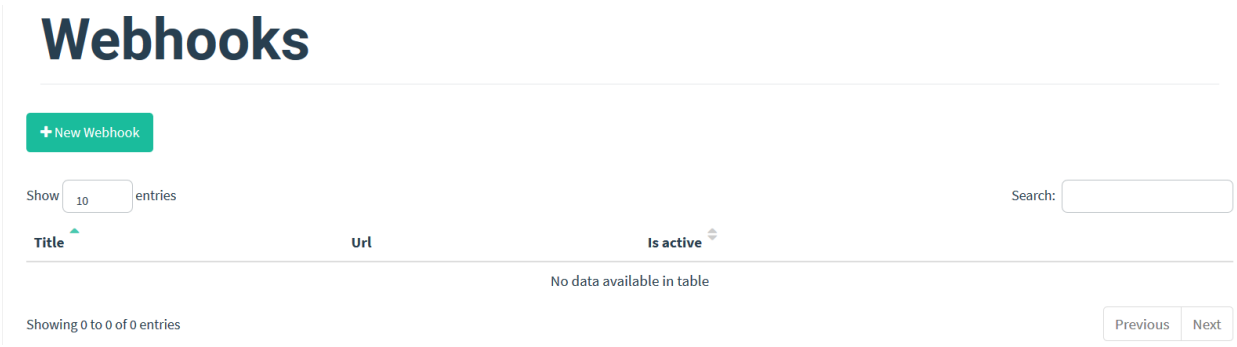


Figura 4-10 Lista de Webhooks

Al seleccionar el botón de "New Webhook" se mostrará un menú similar al siguiente:

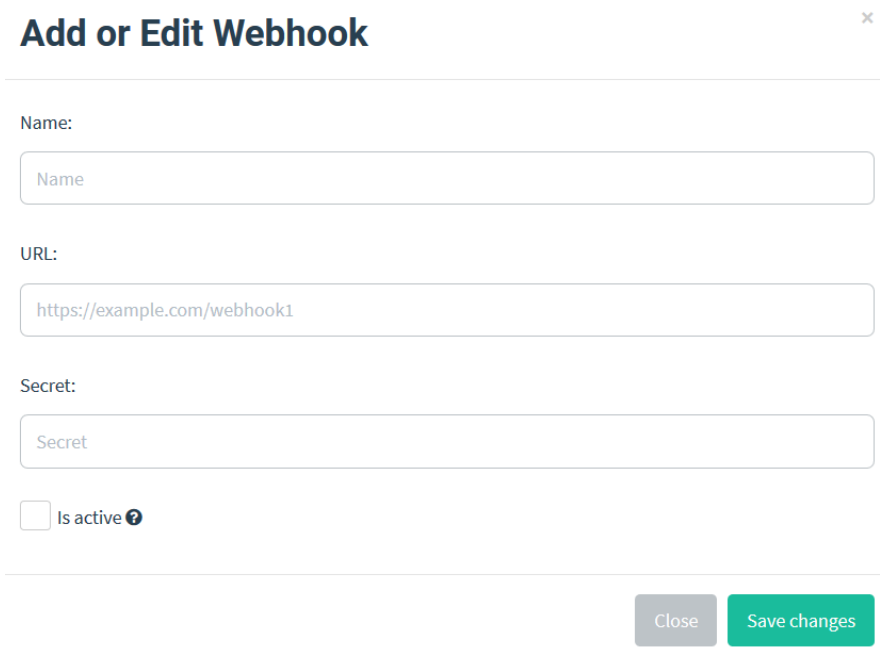


Figura 4-11 Creación de un nuevo Webhook

En este podremos seleccionar el nombre que identificará el webhook, la URL asignada y el secreto, como denomina gophish, con el que se firmarán los mensajes POST con el protocolo HTTP para que otro usuario no sea capaz de ver la información que se envía si consigue capturar los paquetes. Con la casilla "Is active" podremos seleccionar si actualmente está en uso o no.

Los *webhooks* en *GoPhish* son usados para enviar los eventos en formato JSON a un destino final y así poder procesarlo como el usuario desee. No se va a usar esto como se indicó, aún así la web de GoPhish nos aporta un ejemplo en el que se muestra un aviso de que un email del usuario foo.bar@example.com ha sido abierto:

```
{
    "email": "foo.bar@example.com",
    "time": "2020-01-20T17:33:55.553906Z",
    "message": "Email Opened",
    "details": ""
}
```


Figura 4-12 JSON enviado por un Webhook

4.3.2. Opciones de cuenta

Antes de explicar los diferentes apartados para crear desde cero una campaña de *phishing* empezaremos configurando correctamente un usuario recién creado desde el que se van a empezar a crear estas campañas.

Un dato importante sobre las cuentas de usuario es que un usuario no tiene acceso a los diferentes objetos creados por otro en una sección concreta. Por ejemplo, el usuario **Juan** crea un Sending Profile para enviar correos y el usuario **Manuel** crea una plantilla de Email Templates para una futura campaña que quiere lanzar, pues ni Manuel podrá usar el perfil para enviar correos de Juan, ni la plantilla de correo creada de Juan podrá ser usada por Manuel. Esto es similar para las campañas que lanza cada usuario y sus estadísticas.

Una vez en el apartado de configuración de la cuenta de usuario nos aparecerá una pantalla similar a la siguiente:

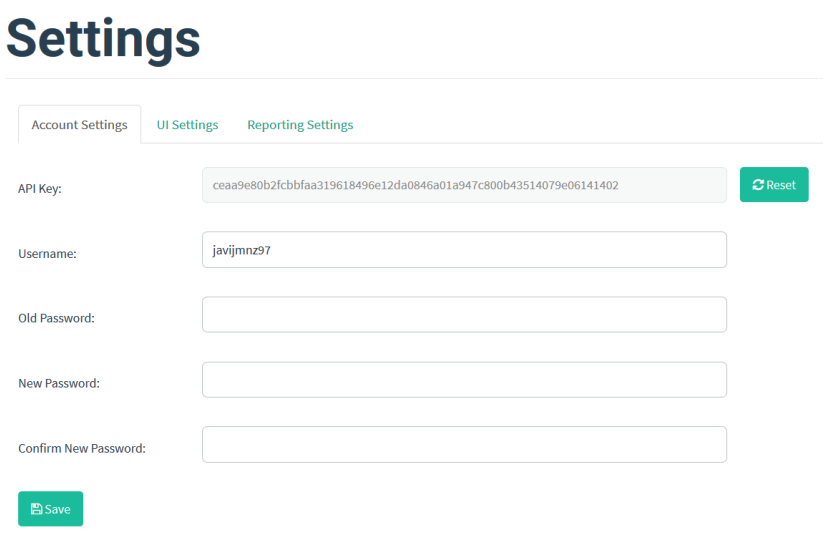


Figura 4-13 Configuración de la cuenta de un usuario

En esta sección podremos conseguir el API Key que tendrá nuestro usuario para hacer uso de la API REST que nos ofrece GoPhish. También podremos modificar nuestra contraseña de usuario.

Si entramos en el apartado de UI Settings únicamente podremos marcar/desmarcar la opción de que se nos muestre un mapa con información en los resultados de nuestra campaña de *phishing*, esto viene desactivado por defecto.

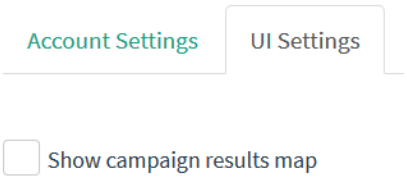


Figura 4-14 Activación de la visualización de un mapa en los resultados de una campaña

Si lo activamos se nos mostrará en los resultados un mapa similar al siguiente:

Figura 4-15 Mapa que se muestra en los resultados de una camapaña

Finalmente, para acabar con este apartado describiremos la sección de Reporting Settings. Esta es muy importante de cara a si la herramienta GoPhish está pensanda únicamente para lanzar campañas dentro de nuestra empresa y no a clientes externos.

Aquí podremos configurar una cuenta de correo electrónico para monitorizar los usuarios que están reportando a la empresa o a un destino en concreto que han recibido un *phishing*. Esto se realiza mediante IMAP.

Al acceder a esta sección se nos mostrará el siguiente menú:

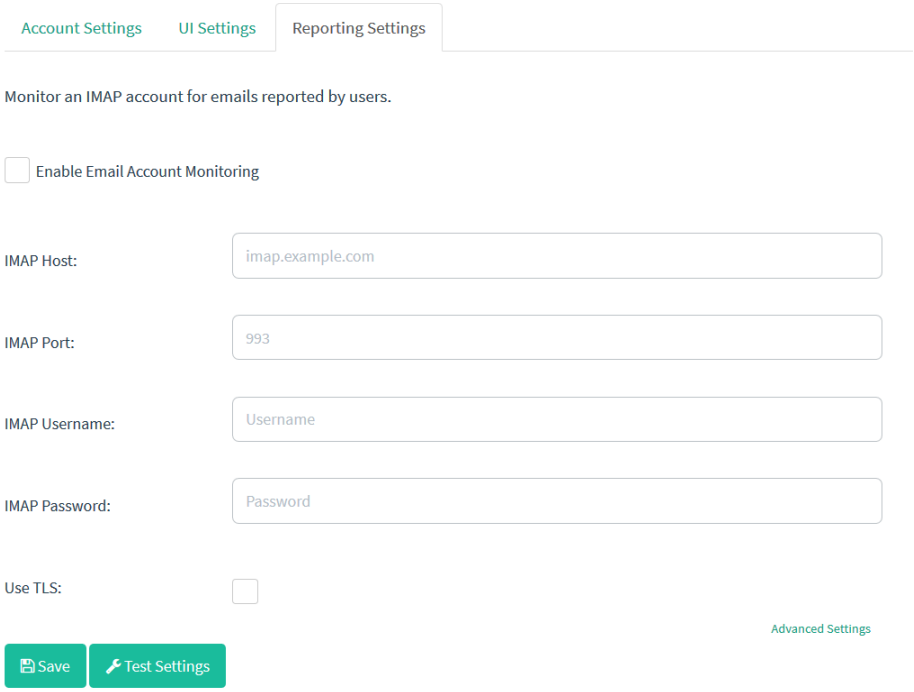


Figura 4-16 Configuración de IMAP

Como se ha dicho anteriormente, esta configuración es utilizada para monitorizar los usuarios que están

reportando recibir un *phishing*. Tal y como se muestra en la imagen, tendremos que indicar un Host IMAP y un puerto donde esté el servicio activo, un usuario y una contraseña para realizar las peticiones y por último si se va a utilizar TLS para encriptar la información.

A continuación, se explicará cómo funciona esto dentro de GoPhish, y cómo se hace para identificar cuando un usuario concreto ha reportado el recibir un phishing.

Para poder explicar esto se usarán conceptos descritos posteriormente en este documento referentes a los enlaces generados para realizar el *phishing*, aún así se definirá brevemente para poder detallar el funcionamiento de como GoPhish detecta los reportes.

El servidor de *phishing* de GoPhish (configurado como se ha explicado en el apartado 3.2) genera enlaces individuales para cada usuario. Por ejemplo, llamemos a la URL o IP que está asignada al servidor de *phishing* direccion_server_phishing. Cuando se envía un email a una dirección de correo objetivo de una campaña, si se va a redirigir a una página falsa que copie a otra, se genera un enlace similar al siguiente:

```
https://direccion_server_phishing/?rid=223344
```

Como podemos ver, direccion_server_phishing es lo indicado anteriormente. Sin embargo, lo importante es el apartado rid, ya que con este se identifica al enlace individual generado a un usuario concreto.

Imaginemos que el correo configurado para que los usuarios reporten haber recibido un *phishing* dentro de la empresa donde se lanza la campaña es seguridad@miempresa.com. Cuando un usuario denuncie que ha recibido un correo que está intentando suplantar a otra para capturar sus credenciales con URL https://direccion_server_phishing/?rid=223344, gracias al identificador 223344, GoPhish puede saber qué usuario es el que ha reportado esto si se ha configurado correctamente el apartado de IMAP.

4.3.3 Perfiles de envío de correos

Una vez detallada las configuraciones de una cuenta de usuario se pasará a explicar el apartado "Sending Profiles". En esta sección se detalla la configuración de la cuenta de correo que procederá a enviar los distintos *phishing* a los objetivos de la campaña. En este apartado cuando se mencione la palabra "perfil" o "perfiles" se hará referencia a un Sending Profile

Como en el anterior apartado, al realizar clic en el apartado que se va a describir se mostrará una lista con los diferentes perfiles configurados, en esta se puede editar, copiar la configuración del perfil o eliminarlo.

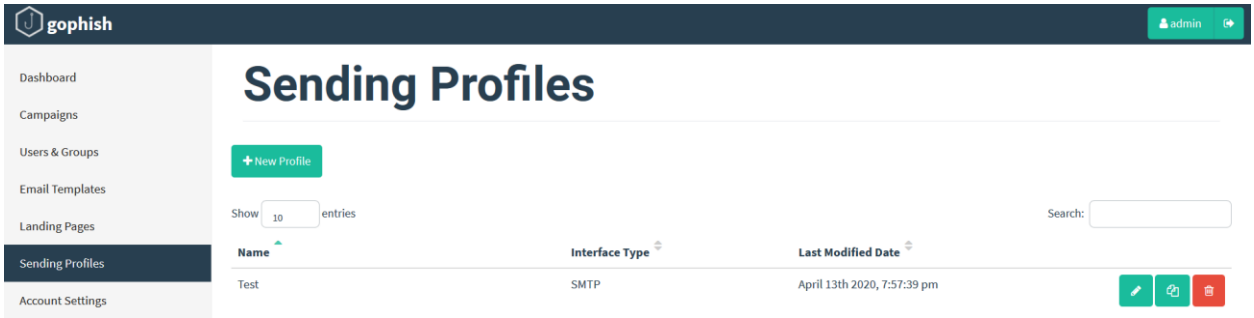


Figura 4-17 Lista de perfiles de envío

Dentro de la lista, en cada perfil se mostrará el nombre, el tipo de interfaz configurada y la última vez que se ha modificado.

Supongamos que se va a crear un nuevo perfil, al hacer clic en "New Profile" se desplegará el menú para esto que es el siguiente:

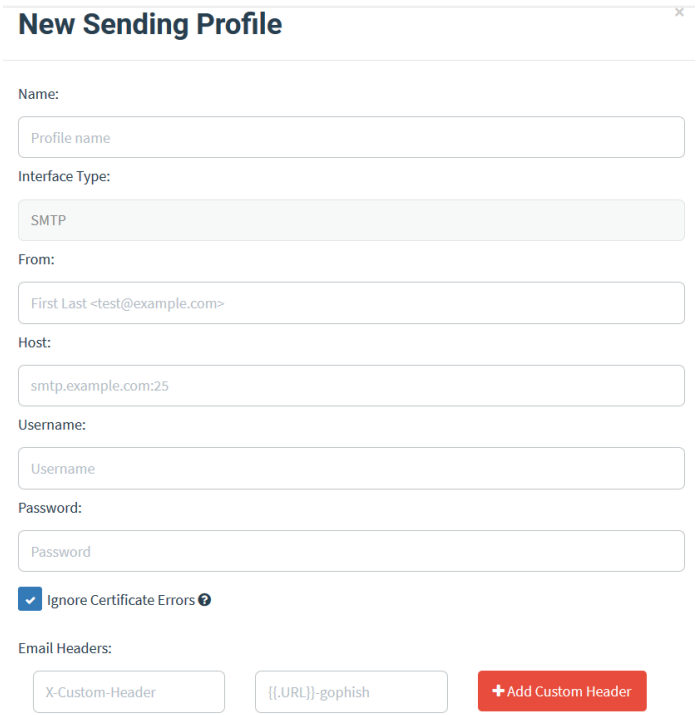


Figura 4-18 Configuración de un perfil de envío

Los diferentes apartados a rellenar para configurar un perfil en la campaña son los siguientes:

- **Name:** nombre con el que se va a identificar al perfil dentro de la lista de los perfiles creados.
- **Interface Type:** actualmente GoPhish únicamente permite el uso de SMTP, por lo que esta será la configuración por defecto y la única que se admite.
- **From:** este dato es muy importante ya que esto es lo que aparece en la cabecera From de los mensajes SMTP que se enviaran con este perfil.

  La estructura es, "First Last <test@example.com>. Es decir, en "First Last" se escribirá el nombre de la persona a la que se quiere suplantar tal y como venga usualmente en los correos que envíe, en test@example.com se colocará el correo electrónico de la persona a suplantar. Es muy importante rellenar esto correctamente debido a que sino puede ser que la campaña de *phishing* no tenga éxito.
- **Host:** servidor correo a el que GoPhish enviará los mensajes de *phishing* para que, a su vez, este lo envíe a los destinatarios. Aquí podemos usar servidores de correos gratuitos que usamos usualmente como Outlook o Gmail, o podemos usar nuestro propio servidor de correo.
- **Username:** cuenta de correo electrónico desde la que se enviarán los correos de phishing.
- **Password:** contraseña de la cuenta de correo electrónico usada para lanzar las campañas y que se ha introducido en el apartado Username.
- **Email Headers:** este campo es muy interesante debido a que podemos rellenar las cabeceras del protocolo SMTP con la información que se quiera En caso de ya existir la cabecera se sustituye el valor que tenía por el que introducimos en este apartado.

  Esta parte es muy interesante de cara a mejorar nuestro *phishing*, ya que GoPhish rellena la cabecera X-Mailer con el valor gophish como se muestra en la siguiente imagen.

```
X-Mailer: gophish
```

Figura 4-19 Valor de X-Mailer por defecto

De cara a una empresa que filtre sus correos por este apartado o que tenga usuarios objetivos de la campaña con conocimientos de análisis de *phishing* esto hace que pierda efectividad. Gracias a este

apartado se puede evitar esto, modificando su valor. En este caso se ha modificado por “none”. En la siguiente imagen un ejemplo.

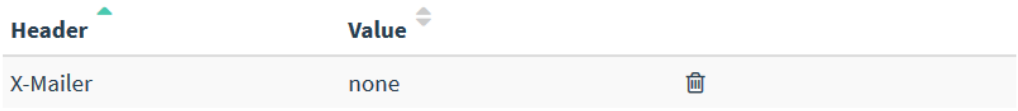


Figura 4-20 Lista de cabeceras modificadas

Y como se puede ver en las cabeceras, este valor está modificado.

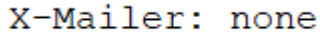


Figura 4-21 Nuevo valor de X-Mailer

Ya configurado todo esto, GoPhish da la opción de enviar un correo electrónico de prueba a una cuenta seleccionada en un botón que aparece más abajo como en el de la imagen que viene a continuación.

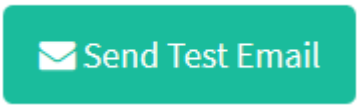


Figura 4-22 Botón de envío de correo de prueba

Al hacer clic, se solicitará el nombre, los apellidos, el correo electrónico y la posición dentro de la empresa de la víctima.

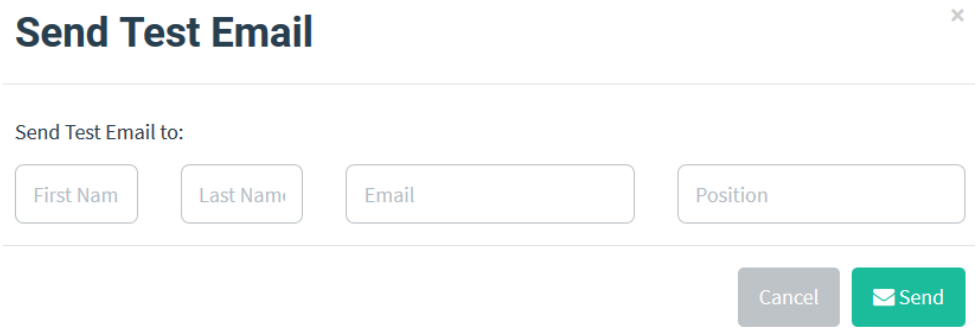


Figura 4-23 Valores para el envío de un correo de prueba

Si todo funciona correctamente, debería llegar un email parecido al siguiente en la bandeja de entrada de la cuenta que se ha elegido de prueba.

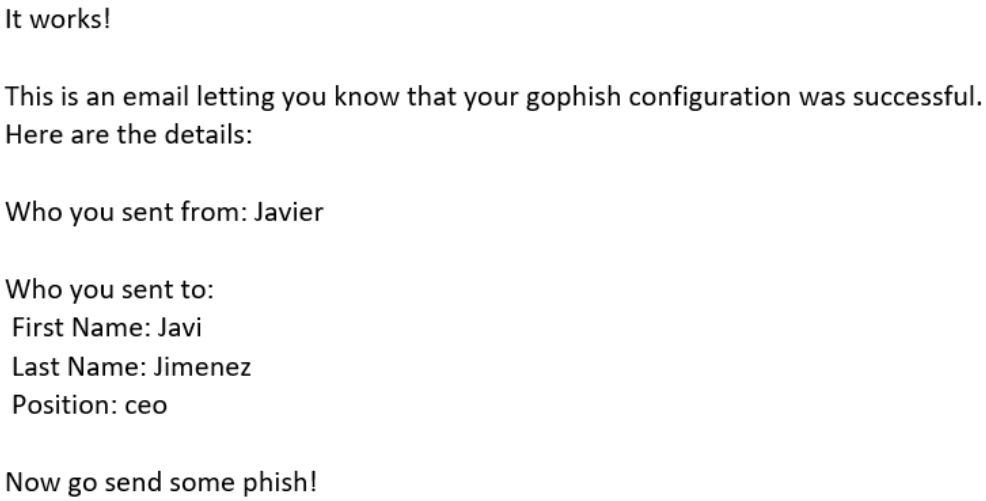


Figura 4-24 Correo de prueba recibido

4.3.4. Páginas web

En esta sección se verá la creación de las paáginas web que suplantarán a una original para realizar un ataque de *phishing*, estas son denominadas por *GoPhish* como "*Landing Pages*". Como siempre al principio se muestra una lista con las que actualmente están creadas para crear, editar, copiar o eliminar una página. Se muestra una lista similar a la siguiente:

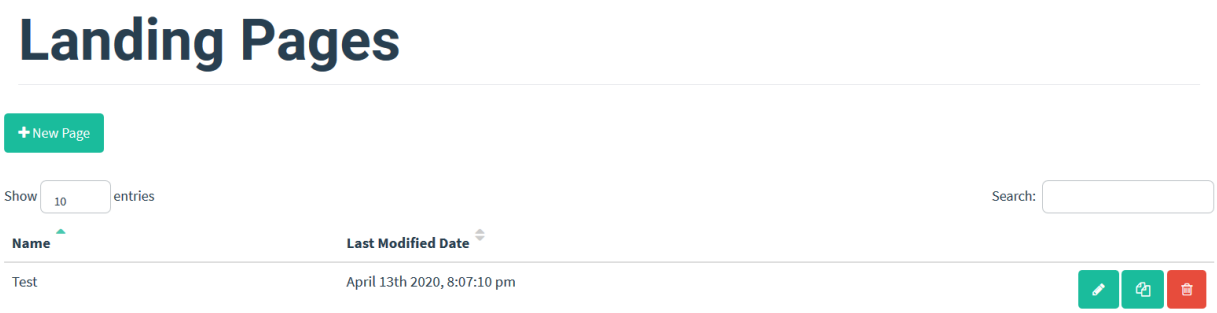


Figura 4-25 Lista de páginas web de phishing

Al igual que en apartados anteriores, se describirá la creación de una *Landing Page* desde cero. Para esto tendremos que realizar clic en el botón "*New Page*", con el que se nos mostrarán las siguientes opciones.

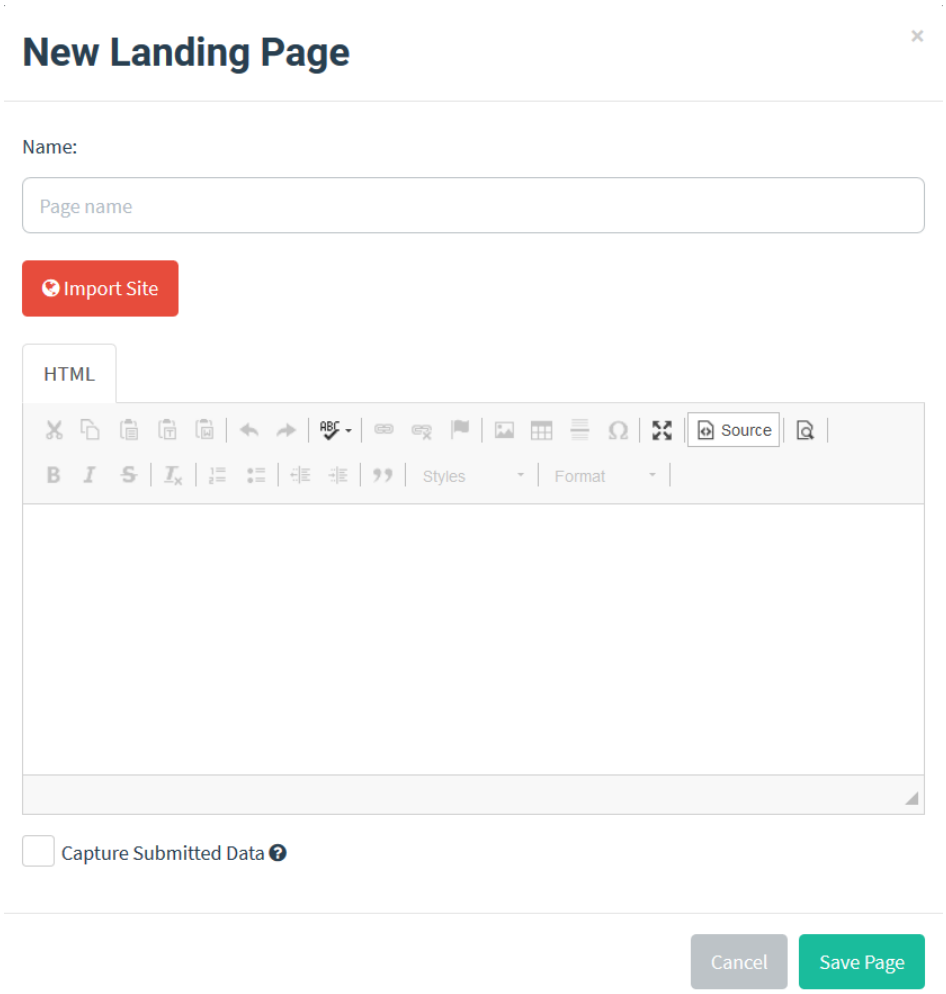


Figura 4-26 Creación de una nueva página web de phishing

Los puntos que configurar son los siguientes:

- **Name:** nombre que identifica a nuestra *Landing Page*.
- **Import Site:** con este botón se puede exportar el diseño de una web que se vaya a suplantar. Imaginemos que se desea suplantar el inicio de sesión de la enseñanza virtual de la Universidad de Sevilla, al realizar clic nos aparecerá un campo para completarlo con la URL que se quiere suplantar.

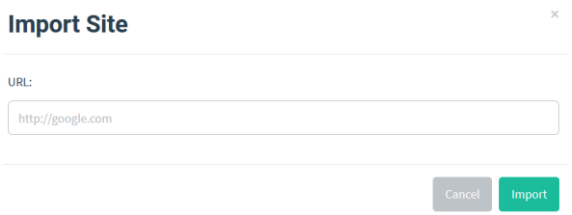


Figura 4-27 Apartado para copiar una página web real

Ya con en este punto tendremos que rellenar el anterior apartado con al URL completa de un inicio de sesión de la US. Es decir, lo siguiente:

Figura 4-28 URL de la página web de ejemplo

Una vez se haga esto y se le de clic al botón Import se generará en el apartado HTML la página que suplanta a la seleccionada anteriormente.

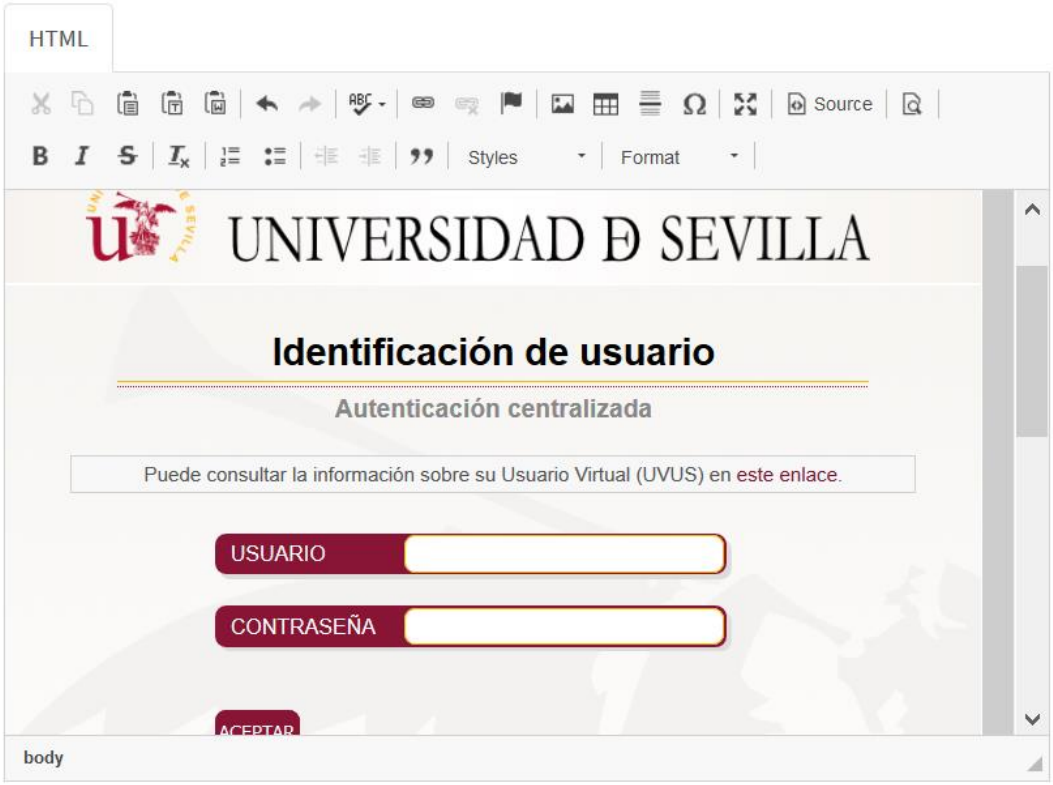


Figura 4-29 Resultado de la copia

- **HTML:** como es obvio, aquí se introducirá el código html de las páginas web que aparecerán suplantando a la deseada.
- **Capture Submitted Data:** se eligirá aquí si se quieren capturar los datos de los formularios existentes en nuestra página web suplantadora o no. Marcar esta opción no significa que capturemos las contraseñas de los objetivos.
- **Capture Password:** si se marca la opción anterior se dará una adicional para elegir si se desea capturar también las contraseñas de los usuarios. Habrá que tener cuidado con esta opción y estar seguros de que se tiene el GoPhish alojado de forma segura ya que las contraseñas se almacenarán en claro, se mostrará un mensaje advirtiendo de esto último.

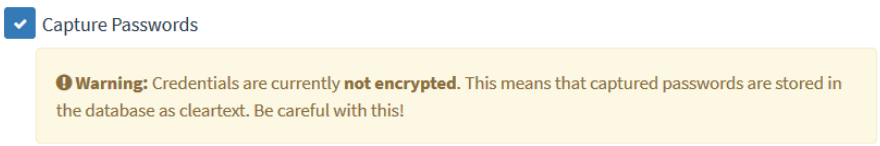


Figura 4-30 Opción de captura de contraseñas

- **Redirect to:** por último, se dispone de otra nueva opción a parte de la anterior al marcar que se quiere capturar la información de los formularios. Esto es aconsejable rellenarlo con la página web que se ha suplantado, para una vez que los usuarios caigan en la página de phishing se les rediriga a la original.

Figura 4-31 Opción de reedirección de la página web de phishing

4.3.5. Usuarios y grupos

En la explicación de este punto se va ha hablar de cómo crear los grupos de usuarios que van a ser objetivo de una campaña y las diferentes formas de realizarlo.

Una vez en la sección Users & Groups vamos a crear un grupo nuevo para pasar a la explicación.

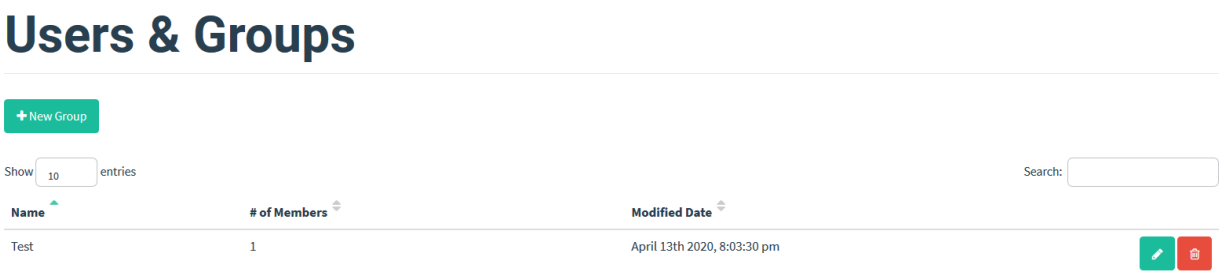


Figura 4-32 Lista de usuarios y grupos

Si se realiza clic en "New Group" se mostrará una ventana como en la siguiente imagen

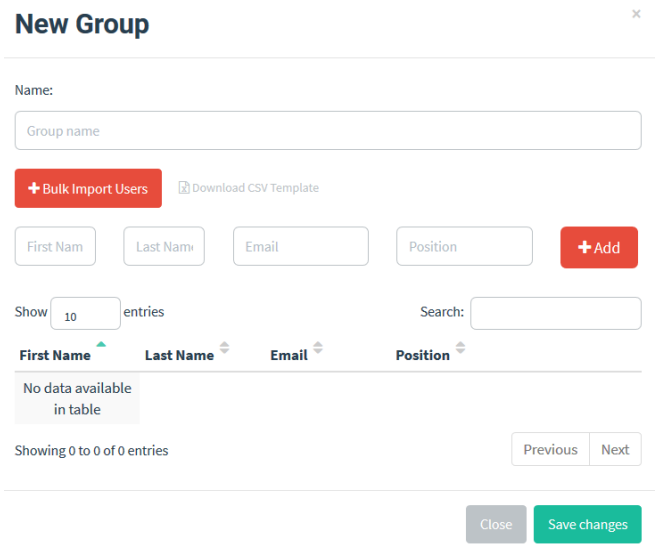


Figura 4-33 Configuración de un nuevo grupo

En este apartado se dividirá la sección en dos formas de configurar grupos de manera diferente:

- **Configuración mediante CSV**

Para realizar esto habrá que dar clic en "Bulk Import Users", una vez hecho esto se mostrará una ventana en la que se tiene que seleccionar un fichero CSV. Aquí se obviará la explicación de que es un fichero .csv y se supondrá que el usuario tiene conocimientos sobre esto.

GoPhish da la opción de descargarnos un fichero CSV de ejemplo para ver la estructura de este. Para esto se tiene que dar clic en "Download CSV Template" que aparece a la derecha de "Bulk Import Users". El fichero de prueba es el siguiente.

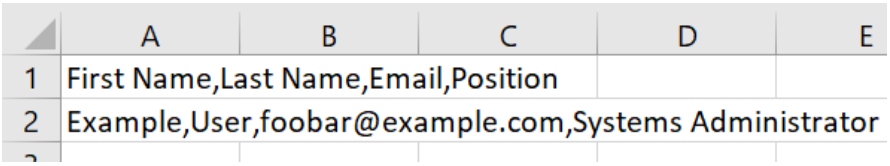


Figura 4-34 CSV de ejemplo

Vemos que en la primera fila tenemos la estructura que tiene que seguir nuestro .csv.

Nombre, Apellidos, Correo electrónico, Posición empresarial

En la segunda fila se muestra un ejemplo de un usuario con correo foobar@example.com que se trata de un administrador de sistemas.

- **Configuración mediante la pestaña de New Group**

Este método es más sencillo si no se tiene una lista previa en un fichero .csv o no se puede generar con alguna clase de automatísmo, es más lento ya que se introduce de uno en uno.

Simplemente se rellena el siguiente apartado para cada usuario.

Figura 4-35 Creación de un usuario dentro de un grupo

Aquí solamente se tiene que introducir el nombre, apellidos, correo electrónico y posición en los diferentes campos y en este orden mencionado. Cuando esté relleno se le da al botón "Add" y se añadirá a la lista que aparece debajo. Se ha añadido un ejemplo a la lista para mostrarla.

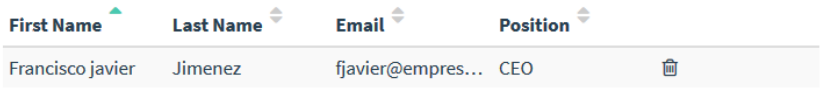


Figura 4-36 Lista de usuarios de un grupo

4.3.6. Plantillas de correo

Ahora se pasará a crear las plantillas de los correos electrónicos que se enviarán a los objetivos de la campaña de *phishing*. Una vez en la lista de plantillas creadas para explicar este apartado se realizará clic en "New Template" para crear una nueva.

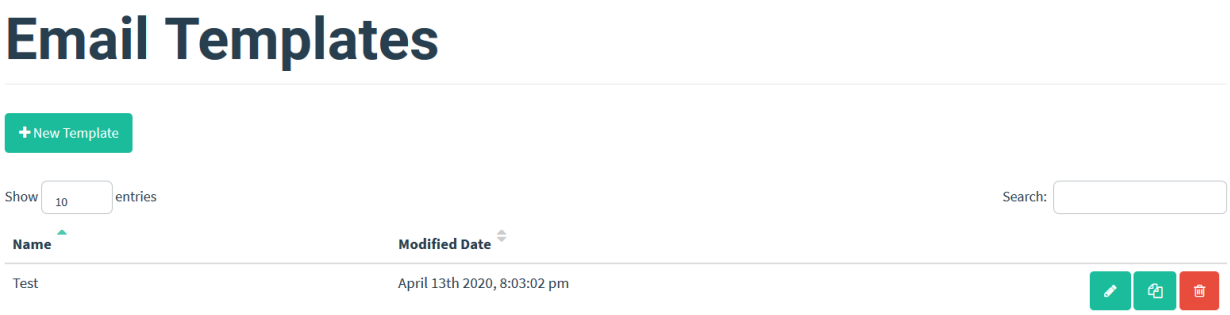


Figura 4-37 Lista de plantillas de correo

Dentro de la plantilla hay una serie de opciones que se muestran en la siguiente imagen y se describen después de esta.

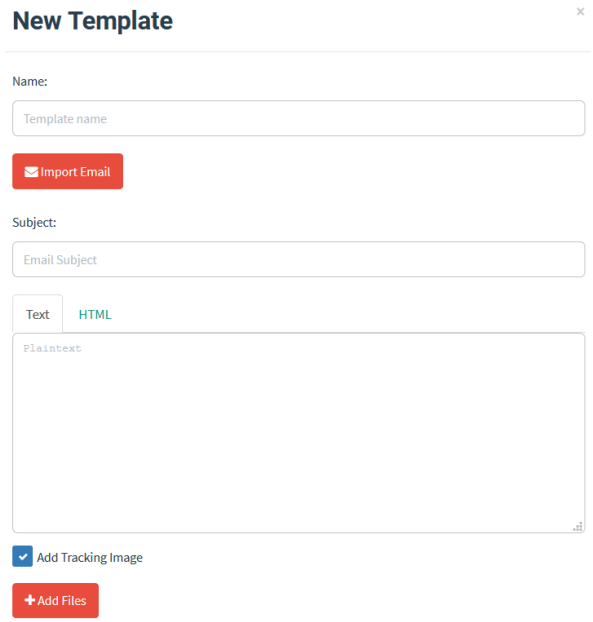


Figura 4-38 Configuración de una nueva plantilla

- **Name:** nombre de la plantilla creada.
- **Import Email:** gracias a esto se podrá importar un email si se tiene su contenido en crudo. Si se le da clic se muestra lo siguiente.

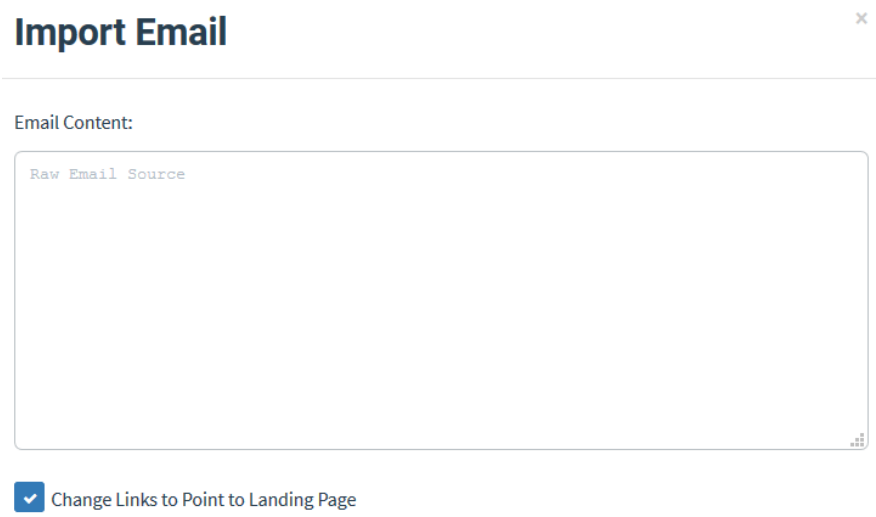


Figura 4-39 Opción de copiar un correo ya existente

Aquí simplemente habrá que introducir el contenido del correo electrónico en crudo que se quiere importar. Por defecto está marcada la opción para cambiar todos los enlaces que aparezcan por enlaces a la Landing Page que se asignará a la campaña como se describirá más adelante.

- **Subject:** asunto que aparecerá en el correo electrónico que se mandará a los usuarios.
- **Text/HTML:** si no se elige la opción de importar el correo electrónico aquí se escribirá el email que será enviado a los objetivos de la campaña. Para que los correos sean individuales y personalizados para cada usuario, *GoPhish* define una variable que cambiarán en función del correo. Todas tendrán el formato {{.$NombreVarable}}. Estas como se muestran en [2] son las siguientes:
    - {{.RId}} → Identificador del usuario.
    - {{.FirstName}} → Nombre del usuario, definido en el apartado de *Users & Groups*.
    - {{.LastName}} → Apellidos del usuario, definido en el apartado de *Users & Groups*.
    - {{.Position}} → Posición del usuario dentro de la empresa, , definido en el apartado de *Users & Groups*.
    - {{.Email}} → Correo electrónico del usuario, , definido en el apartado de *Users & Groups*.
    - {{.From}} → Persona que queremos suplantar en la campaña de phishing.
    - {{.TrackingURL}} → URL utilizada para el *tracking* al usuario.
    - {{.Tracker}} → Imagen utilizada en el correo para conocer si el usuario abrió o no.
    - {{.URL}} → URL desde la que se realiza el *phishing*.
    - {{.BaseURL}} → URL del servidor de *phishing* pero sin el identificador (rid) de la URL específica del usuario. Como se ha explicado anteriormente, cada dirección web de *phishing* enviada a cada usuario lleva un parámetro en la petición GET a nuestro servidor denominado rid que identifica unívocamente a un objetivo.

      Esta función es útil si se tiene algún tipo de fichero alojado en nuestro servidor de *phishing* y se quiere incluir su URL en el correo electrónico para que, por ejemplo, el usuario lo descargue desde ahí.

- **Add Files:** por último, se tiene la opción de añadir un adjunto a la plantilla de correo electrónico. De cara a una campaña para una empresa creada desde el lado del hacking ético se podría añadir un documento informativo sobre lo peligroso que hubiese sido abrir un fichero infectado en un correo electrónico que realizase un ataque real. Si se piensa como un hacker no ético, aquí podríamos incluir cualquier tipo de *malware* como por ejemplo, un troyano.

4.3.7. Campañas

Ya teniendo configurado todo lo anterior se llega a la sección donde se muestran todas las campañas y podemos crear una nueva. De forma predeterminada se nos mostrarán las campañas actualmente activas, sin embargo, también podemos visualizar las finalizadas.

En este caso, vamos a crear una nueva campaña y a explicar sus diversas opciones. Para esto daremos clic en en "New Campaing" mostrado en la siguiente imagen.

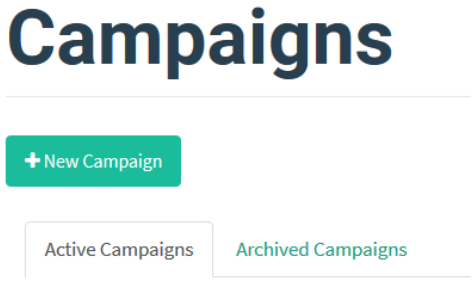


Figura 4-40 Sección para la creación de una nueva campaña

Se mostrará la siguiente ventana, posterior a la imagen se describirá el funcionamiento de cada campo.

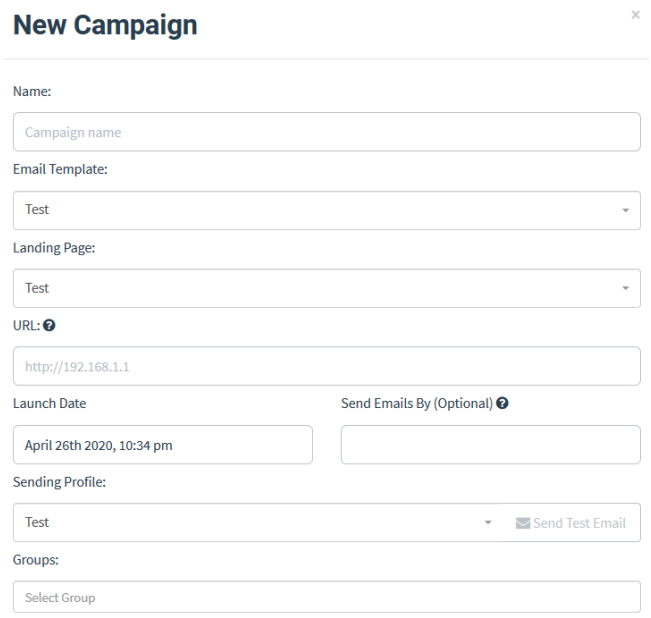


Figura 4-41 Configuración de una nueva campaña

- **Name:** nombre con el que identificará la campaña.
- **Email template:** correo electrónico que será enviado a los objetivos de la campaña.
- **Landing Page:** página web a la que apuntarán los diferentes enlaces (no necesariamente todos) del correo.
- **URL:** valor que tomará la variable {{.URL}} descrita en el punto 3.3.5. Esta es utilizada en las plantillas de correo electrónico y es recomendable rellenarla con la dirección IP del servidor de GoPhish.
- **Launch Date:** fecha en la que se lanzará la campaña.
- **Send Emails By:** GoPhish da la opción de enviar los correos de manera distribuida en el tiempo. Para esto se configura una fecha en este apartado y se mandarán de forma espaciada y de manera equitativa entre la fecha de "Launch Date" y esta.
- **Sending Profile:** configuración de la cuenta que enviará los correos de *phishing* en la campaña. Nuevamente desde aquí se podrá enviar un correo de prueba con la opción "Send Test Email".
- **Groups:** grupos de objetivos para la campaña creada, se pueden seleccionar varios.

Una vez creada se añadirá a la lista de campañas, y desde ahí podremos ver los resultados en tiempo real dando clic en el botón  que hay a la derecha como en la siguiente imagen.

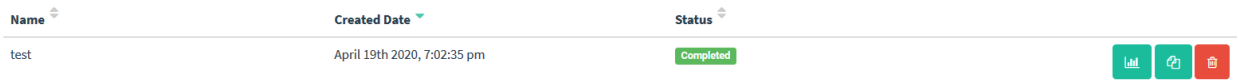


Figura 4-42 Lista de campañas creadas y su estado

Ya en la sección de resultados se mostrarán diferentes gráficas con las estadísticas actuales de la campaña y un timelime de esta. Se muestra a continuación, una imagen de ejemplo.

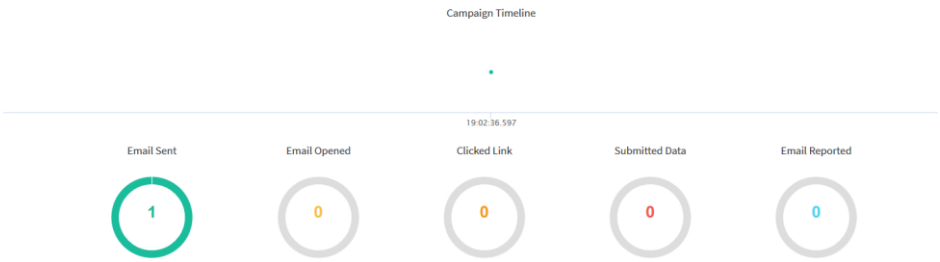


Figura 4-43 Estadísticas de la campaña

Cada estadística describe lo siguiente:

- **Email Sent.** Correo enviado.
- **Email Opened.** Correo enviado, esto se sabrá gracias al Tracker.
- **Clicked Link.** Si el usuario ha abierto alguno de los enlaces que apuntan a la URL de phishing. Esto se sabe gracias al parámetro rid.
- **Submitted Data.** En caso de que se haya marcado la opción en la plantilla del correo, si se han capturado datos de formularios.
- **Email Reported.** Si se le ha configurado a nuestro usuario un monitor IMAP, podremos saber si los usuarios han reportado el phishing enviado o no.

Debajo de esto se muestra con detalle usuario por usuario las acciones realizadas. En la siguiente imagen se encuentra un ejemplo en el que al usuario únicamente se le ha enviado el correo.

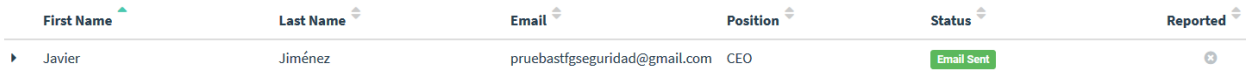


Figura 4-44 Estado de un correo de la campaña enviado

En la parte que se muestra arriba cuando vemos los usuarios se nos da diferentes opciones a realizar en nuestra campaña, estas son las siguientes.

- **Back.** Volver a la lista de campañas.
- **Export CSV.** Exportar los resultados actuales a un fichero de formato .csv.
- **Complete.** Dar por finalizada la campaña.
- **Delete.** Eliminar la campaña.
- **Refresh.** Refrescar los resultados mostrados en ese momento, gracias a esto evitaremos tener que referescar la página en el navegador.

Se muestra una imagen con las opciones mencionadas anteriormente.

Figura 4-45 Opciones de una campaña existente

4.4. Configuración del dominio

Una vez explicada la estructura de la herramienta *GoPhish*, se procederá ha adquirir un dominio tanto para la campaña de phishing que se vaya a realizar como para las "Páginas web falsas". En este caso se ha comprado el dominio *cibersecurityhunter.com.*

Al no tener el dominio contratado en la misma plataforma que el servicio VPS, se tendrán que configurar los servidores DNS para que apunten a DigitalOcean, que es el proveedor utilizado para alojar *GoPhish*. En este caso, se configuran los siguientes servidores DNS.

SERVIDORES DNS	TIPO
ns1.digitalocean.com	Personalizado
ns2.digitalocean.com	Personalizado
ns3.digitalocean.com	Personalizado

Figura 4-46 Servidores DNS del dominio

Ya realizado lo anterior se procederá a configurar un registro A en el servidor DNS, este usa para enlazar una dirección IP con un dominio, es decir, se asociará la dirección IP 134.122.110.153 a *cibersecurityhunter.com*. Este quedaría de la siguiente forma.

A	cibersecurityhunter.com	directs to 134.122.110.153	3600

Figura 4-47 Registro A

Una vez creado el registro ya podremos acceder a *GoPhish* directamente desde el dominio. Como el servicio estaba asociado al puerto 3380 al introducir *https://cibersecurityhunter.com:3380* se puede apreciar el inicio de sesión de la herramienta de lanzamiento de campañas de *phishing*.

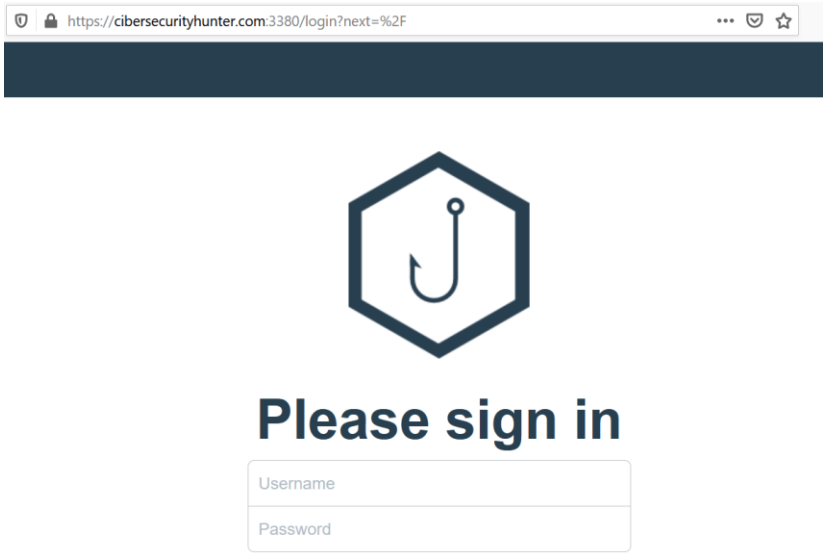


Figura 4-48 Inicio de sesión desde el dominio

4.5. Instalación del certificado para GoPhish

Para añadirle fiabilidad a las páginas de phishing, en primer lugar, después de configurar el dominio y para evitar que aparezca una dirección IP en el navegador al realizar clic en las webs falsas, hay que instalar un certificado SSL de una entidad fiable para el navegador.

Esto sirve para evitar el mensaje que se muestra cuando accedemos a una página no fiable para el navegador, como la siguiente.

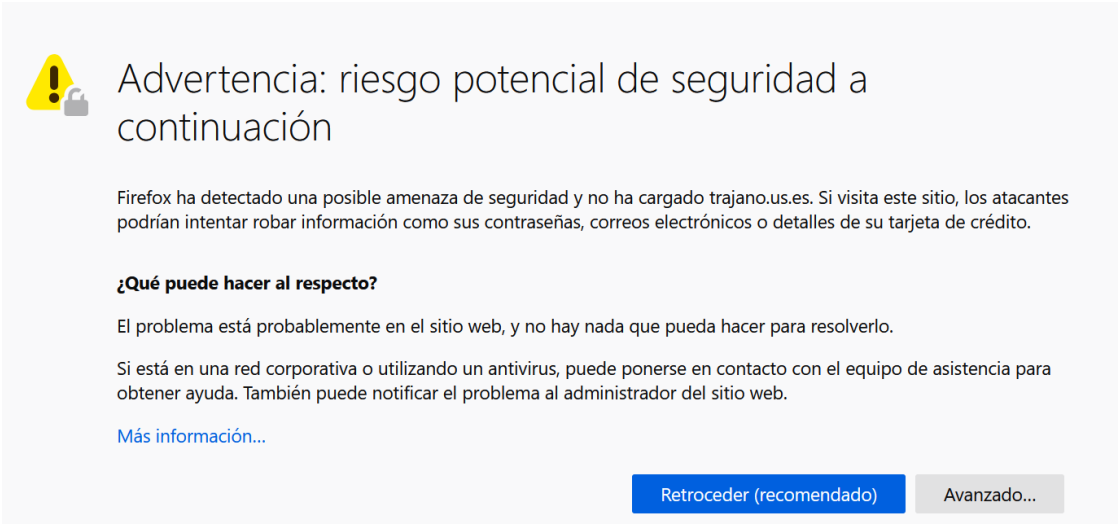


Figura 4-49 Alerta de seguridad del navegador

El que aparezca un aviso como el anterior hace desconfiar al usuario sobre si es real o no la página web a la que esta accediendo. Debido a esto se adquirirá un certificado de la web ZeroSSL, ya que son gratuitos los primeros 3 meses y son confiables para diversos navegadores.

Una vez realizado el proceso de registro y la creación del certificado, se descargará un **.zip** que contendrá tanto el certificado como la clave privada usada en el protocolo SSL/TLS.

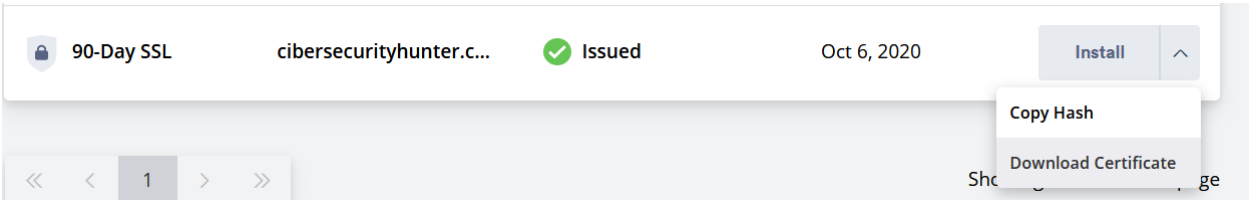


Figura 4-50 Certificado SSL del dominio

Una vez descargado, este contendrá los ficheros certificate.crt, private.key y ca_bundle.crt. En este punto solo serán de interés los dos primeros, que tendrán que ser copiados dentro de la carpeta donde se encuentra *GoPhish* en el servidor con los nombres *cibersecurity.crt* y *cibersecurity.key*. Esto último se aprecia en la siguiente imagen gracias al comando "ls" que muestra los ficheros que se encuentran dentro de un directorio.

```
root@cibersecurityhunter:~# ls gophish/ | grep "cibersecurity"
cibersecurity.crt
cibersecurity.key
```

Figura 4-51 Certificado y clave privada dentro del servidor

Ya copiados se cambiará la configuración de GoPhish en el fichero *config.json* (descrito en el punto 4.2). En concreto se modificarán los apartados *cert_path* y *key_path* dentro de *admin_server* y *phish_server*. Con esto se usará el certificado tanto para el panel de gestión de *GoPhish* como para las páginas web falsas de las futuras campañas de "*phishing*".

```
"admin_server": {
        "listen_url": "0.0.0.0:3380",
        "use_tls": true,
        "cert_path": "cibersecurity.crt",
        "key_path": "cibersecurity.key"
},
"phish_server": {
        "listen_url": "0.0.0.0:443",
        "use_tls": true,
        "cert_path": "cibersecurity.crt",
        "key_path": "cibersecurity.key"
},
```

Figura 4-52 Nueva configuración de config.json de GoPhish

Después de configurar lo indicado anteriormente se puede comprobar, gracias al navegador, que hay instalado un certificado de confianza de ZeroSSL y que no se muestra el mensaje de la Figura 4-53.

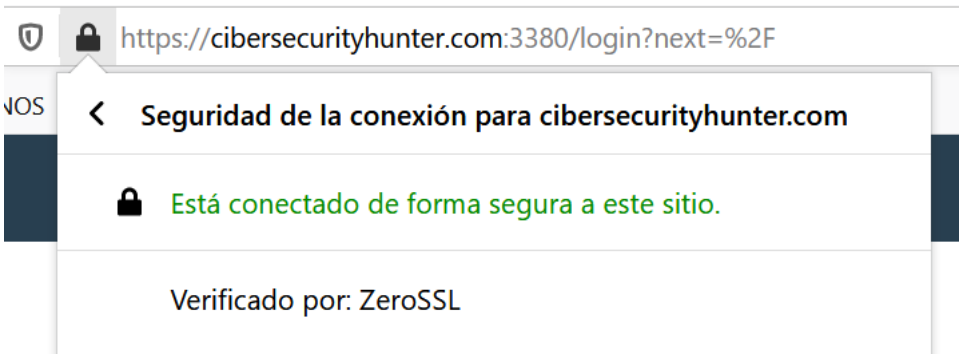


Figura 4-54 Comprobación de que el certificado pertenece a la entidad que hemos usado

4.6. Servidor de correo Postfix

Para manejar las direcciones de correo electrónico del dominio *cibersecurityhunter.com* se instalará un servidor de correo propio que usará *GoPhish* para enviar todos los mails de *phishing* en las campañas. Posteriormente se instalará un certificado para que los correos vayan cifrados y así aumentar el grado de confianza de los diferentes proveedores de correo electrónico. Finalmente se instalarán y configurarán los registros SPF, DKIM, y DMARC descritos en el apartado 1.6. para evitar que los correos vayan a la carpeta de *spam* o correo no deseado y para proteger nuestro dominio de correo de posibles ataques de "*spoofing*".

4.6.1. Instalación y configuración

Para la instalación del servidor de correo únicamente habrá que lanza el siguiente comando en una terminal.

```
apt install postfix
```

Una vez hecho esto se mostrará una pantalla para iniciar la configuración de postfix, esta se podrá realizar posteriormente en los ficheros del mismo servicio, aún así la pantalla mostrada es la siguiente.

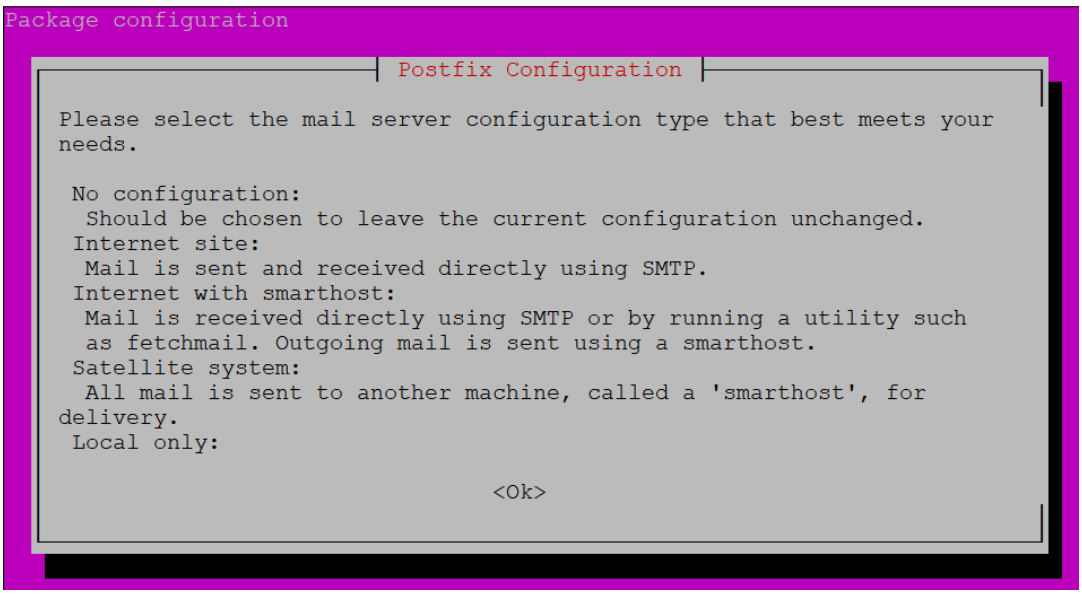


Figura 4-55 Imagen de configuración de postfix

Al darle a "*Ok*" hay que seleccionar la configuración "*Internet site*" debido a que el servicio se va a usar, como bien dice la imagen anterior, para enviar correos usando el protocolo SMTP.

En la siguiente pantalla se pregunta por el nombre del sistema de mail, es decir, el dominio que identifica a las direcciones de correo, por lo que su valor será *cibersecurityhunter.com*.

Figura 4-56 Configuración del dominio de las cuentas de correo electrónico

En el resto de configuraciones se dejará el valor por defecto debido a que se modificarán posteriormente los ficheros de configuración, en concreto el archivo /etc/postfix/main.cf. Para editarlo se lanzará el siguiente comando.

```
nano /etc/postfix/main.cf
```

Ahora se describirán los valores modificados y su significado.

- `mydomain = cibersecurityhunter.com`

Atributo que identifica al dominio de las direcciones de correo electrónico, al usar el dominio *cibersecurityhunter.com* se usará esto como valor.

- `myhostname = smtp.cibersecurityhunter.com`

Aquí se define el nombre del servidor en la red, al ser un servidor de salida que usa el protocolo SMTP se le ha asignado el subdomino *smtp.cibersecurituhunter.com*. Para que esto funcione se tiene que registrar el subdominio en el proveedor que nos lo ha facilitado y crear un registro tipo A en el servidor DNS que indique que el subdominio mencionado anteriormente apunta a la dirección IP 134.122.110.153.

Esto último se ve en la plataforma de la siguiente manera.

Figura 4-57 Registro A del servidor de correo

- `mynetworks = mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24 134.122.110.153/32`

Finalmente este parámentro definirá las direcciones IP que tienen permitido usar este servidor para enviar correo electrónico. A la configuración por defecto (direcciones IP privadas y locales) se le añadirá al final la dirección en donde esté funcionando "*GoPhish"*, que en este caso es la misma que la de "*postfix"*.

Una vez configurado todo lo anterior solo habrá que recargar el servicio con el siguiente comando.

```
postfix reload
```

Si todo ha sido configurado correctamente se mostrará una respuesta como la siguiente.

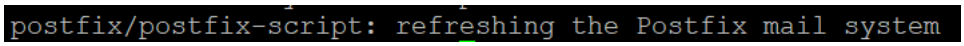


Figura 4-58 Actualización de la configuración de postfix

4.6.2. Pruebas de funcionamiento

Para comprobar que el servicio "*postfix"* está funcionando correctamente se utilizará el comando **mail** de la librería **mailutils**. Para esto se usará una cuenta de correo temporal, que en este caso es wimajo5048@stevefotos.com, lanzando el siguiente comando.

```
echo "Prueba del trabajo sobre GoPhish" | mail -s "Prueba US" wimajo5048@stevefotos.com
```

Si todo está funcionando correctamente se debería recibir el correo de la dirección mencionada anteriormente. Esto se puede apreciar en la imagen que se muestra a continuación.

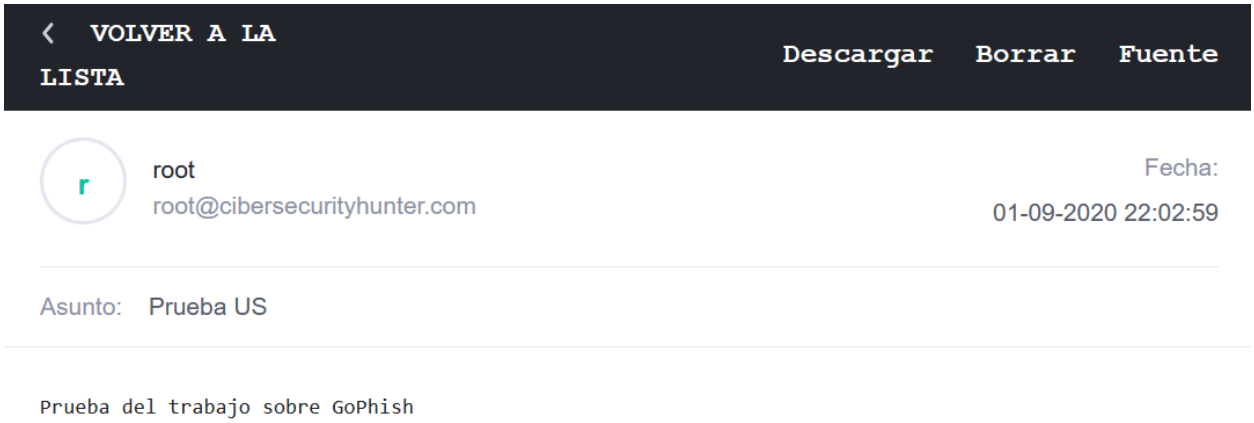


Figura 4-59 Prueba usando postfix

4.6.3. Configuración de la capa TLS

Si se quiere realizar una campaña de "*phishing*" efectiva, tendrán que cumplirse ciertos factores para evitar que el proveedor de correo electrónico del objetivo marque los emails enviados como *spam* o correo no deseado. El envío de correos cifrados es uno de los requisitos necesarios.

Para conseguir esto se tiene que activar y configurar correctamente la capa TLS para el servicio "*postfix*". A continuación, se mostrarán los pasos a seguir para realizar esto correctamente.

1. Activación de la capa TLS en postfix.

En primer lugar, se modificará el fichero /etc/postfix/master.cf quitando los símbolos # de las filas marcadas en la siguiente imagen.

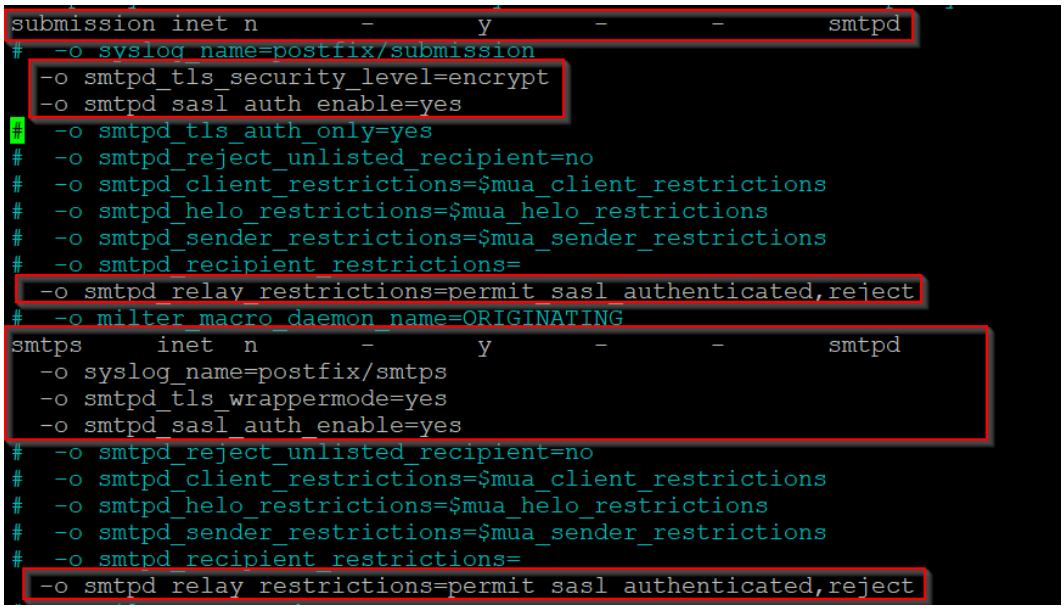


Figura 4-60 Configuracion en master.cf para activar la capa TSL

El fichero en cuestión define qué servicios dentro de postfix están habilitados. La configuración que se ha activado es la siguiente.

- smtpd_tls_security_level=encrypt → Nivel de seguridad en postfix. El valor "*encrypt*" sirve para indicarle a los demás servidores que los correos han de ir cifrados.
- smtpd_sasl_auth_enable=yes → Activación de la autenticación SASL (*Simple Authentication and Security Layer)*, que como su nombre indica se usa para la autenticación y autorización dentro del servidor postfix para enviar y recibir correos electrónicos.
- smtpd_relay_restrictions=permit_sasl_authenticated,reject → Reestricciones en la autenticación dentro del servidor de correo, en este caso el valor *"reject*" indica que se rechacen las conexiones con autenticaciones no exitosas.
- syslog_name=postfix/smtps → Directorio donde se guardarán los logs de un servicio de postfix en concreto.
- smtpd_tls_wrappermode=yes → Activación de la capa TLS, el valor "*yes*" indica que esta está activada.

Después de configurar el fichero *master.cf* se pasará a editar y añadir parámetros en /etc/postfix/main.cf el cual ha sido editado antes. Este sirve para definir el valor de ciertos parámetros del servicio postfix en sí. Como se ha hecho anteriormente la siguiente figura mostrará el atributos a modificar en el archivo mencionado.

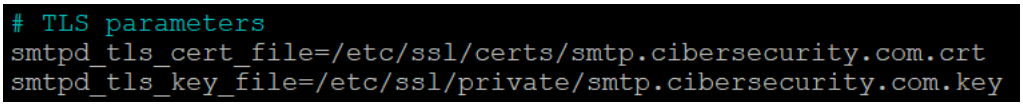


Figura 4-61 Configuración en main.cf para activar la capa TLS

Los parámetros mostrados configuran lo siguiente:

- smtpd_tls_cert_file → Ruta del certificado utilizado por el servidor para cifrar los correos electrónicos.
- smtpd_tls_key_file → Directorio donde se encuentra la clave privada usada por el certificado mencionado en el atributo anterior.

2. Instalación del certificado para el servidor de correo.

Para este paso se crearán y descargarán tanto el certificado como la clave privada de la misma forma que se hizo en el punto 4.5. añadiendo la instalación del certificado raíz llamado *ca_bundle.crt* que se encuentra en el fichero comprimido que aporta ZeroSSL. El proceso se explicará posteriormente.

En primer lugar, se copiará el certificado *certificate.crt* con el nombre *smtp.cibersecurity.com.crt* en la ruta /etc/ssl/certs/ que se configuró en el paso anterior.

Posteriormente se realizará lo mismo con el fichero *private.key* con el nombre *smtp.cibersecurity.com.key* en el directorio /etc/ssl/private.

Finalmente habrá que instalar el certificado raíz para que el servicio postfix reconozca a la entidad certificadora que gestiona los certificados que se usarán. Para esto se empleará el fichero *ca_bundle.crt* mencionado anteriormente.

Los certificados raíz se encuentran en el sistema operativo Ubuntu dentro del directorio /usr/share/ca-certificates. Para esta ocasión se creará una carpeta llamada "smtp" donde se copiará el fichero antes mencionado. En la siguiente captura se aprecia que el archivo ha sido copiado en el directorio mencionado.

```
root@cibersecurityhunter:~# ls /usr/share/ca-certificates/smtp/
ca_bundle.crt
```

Figura 4-62 Certificado raiz en el directorio de Ubuntu

Después de copiarlo se editará el fichero /etc/ca-certificates.conf donde se encuentran registrados todos los certificados raíz guardados en el equipo dentro del directorio /usr/share/ca-certificates. Debido a esto se tendrá que añadir al final del fichero la línea smtp/ca_bundle.crt. Esto se puede apreciar en la siguiente figura.

```
root@cibersecurityhunter:~# cat /etc/ca-certificates.conf | grep "smtp/"
smtp/ca_bundle.crt
```

Figura 4-63 Ruta del certificado raíz en la configuración de Ubuntu

Para terminar, se tendrá que ejecutar el siguiente comando para actualizar la lista de certificados raíz.

```
update-ca-certificates
```

Ya configurado todo lo anterior se puede comprobar que funciona correctamente enviando un correo con el comando `mail` a una dirección de correo electrónico existente. Si se realiza esto se puede comprobar como en la siguiente imagen que los correos son enviados cifrados con TLS.

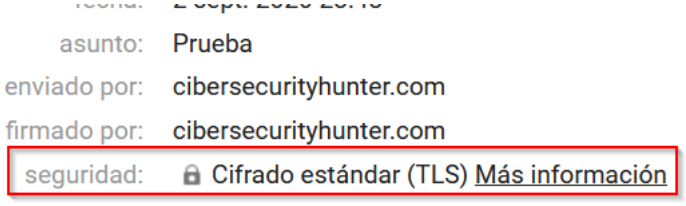


Figura 4-64 Prueba de la correcta configuración de TLS

4.6.4. Medidas de seguridad

Como se ha mencionado en el punto 1 existen diversas medidas de seguridad para evitar técnicas de *spoofing*, para esto se usa SPF, DKIM y DMARC.

El último paso para evitar que los proovedores de correo electrónico manden las campañas de phishing lanzadas con el dominio usado a la carpeta de correo no deseado es tener correctamente configurado estos registros. A lo largo de este apartado se va a mostrar como configurar correctamente estas medidas de seguridad que sirven tanto como para lanzar una campaña de *phishing* más exitosa, como para reforzar nuestro dominio frente a técnicas de *spoofing*.

4.6.4.1. Configuración SPF

El registro SPF tiene como finalidad el definir que direcciones IP o que equipos están autorizados para enviar correo en nombre del dominio configurado, en este caso *cibersecurityhunter.com*. Para implantarlo se tendrá que crear un registro TXT en el servidor DNS del dominio, estos se utilizan para crear recursos y administrarlos.

Para este caso se ha creado el siguiente registro TXT.

```
@ IN TXT ("v=spf1 ip4:134.122.110.153/32 ~all")
```

Este indica lo siguiente:

- `v=spf1` → Indica que el registro es para spf.
- `ip4:134.122.110.153/32` → Sirve para mostrar que direcciones Ipv4 o que rangos están habilitados para enviar correo electrónico en nombre del dominio. En este caso se ha añadido la dirección IP del servidor de correo *postfix*.
- `~all` → Política a seguir en caso de no ser una dirección IP o equipo autorizado para mandar correo electrónico con el dominio. Esta opción marca como sospechosos los mensajes que estén enviados desde equipos no permitidos.

Ya configurado todo si se prueba a enviar un correo electrónico desde el servidor de correo ha otra dirección existente se puede ver en el mensaje original si se ha cumplido con la condición del registro SPF satisfactoriamente. Esto se puede apreciar en la siguiente figura.

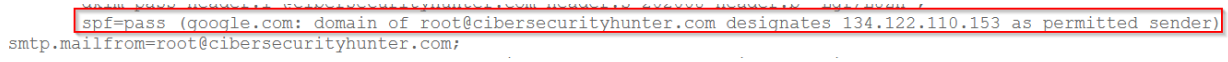


Figura 4-65 Prueba de la correcta configuración de SPF

4.6.4.2. Configuración DKIM

En este apartado se realizará la configuración del registro DKIM, que es utilizado como se ha explicado en apartados anteriores, para verificar que el correo electrónico no ha sido modificado desde que fue enviado por el origen y por lo tanto ha sido enviado por el mismo. Para realizar la configuración se utilizará el servicio *opendkim* y solo hay que manzar el siguiente comando para empezar la instalación.

```
apt install opendkim
```

A la hora de configurarlo se deberá editar el fichero /etc/opendkim.conf de tal forma que los siguientes atributos tengan el valor que se indica a continuación:

- `Syslog = yes` → Activación de registro de logs.
- `UMask = 022` → Permisos asignados para la creación de archivos. Este indica que los ficheros solo pueden ser modificados por el mismo servicio o por el grupo al que pertenezca el servicio.

- `Domain = cibersecurityhunter.com` → Dominios que van a ser fimados.
- `Canonicalization = relaxed/relaxed` → Los servidores de correo que atraviesa un correo electrónico suelen hacer cambios leves en el correo, estos pueden provocar problemas con la firma de DKIM. Este atributo marca lo estricto que se será con los cambios realizados en nodos intermedios, el método *simple* es el más estrictro y el valor *relaxed* el que menos. Para este caso se ha utilizado el último ya que el objetivo es que el *phishing* atraviese el filtro antispam, por lo que nos interesa que se pase el registro DKIM fácilmente. En este se han indicado dos valores separados por "/", el primero indica el método de la cabecera y el segundo el del cuerpo del mensaje.
- `Socket = inet:8891@localhost` → Puerto que se usará para poner en marcha el servicio, en este caso se usará el 8891.
- `UserID = opendkim:opendkim` → Configuración del usuario y grupo respectivamente separados por el caracter ":" que usará el servicio *opendkim*.
- `ExternalIgnoreList = refile:/etc/opendkim/TrustedHosts` → Lista de *hosts* que podrán enviar correos electrónicos a nombre del dominio configurado.
- `InternalHosts = refile:/etc/opendkim/TrustedHosts` → Indica la lista de *hosts* los cuales si envían mensajes han de ser firmados. Lleva el mismo valor que el anterior debido a que solo se maneja únicamente el servidor con dirección IP 134.122.110.153.
- `KeyTable = refile:/etc/opendkim/KeyTable` → Archivo donde se indica el directorio donde se encuentra la clave para firmar un dominio en concreto.
- `SendReports = yes` → Gracias a esta configuración se nos enviará un reporte a una dirección de correo indicada en el registro DNS del servidor DNS en caso de que haya fallado la verificación de una firma en un correo electrónico. Realmente no afecta al funcionamiento del servicio, pero es útil tenerlo activado.

El resto de las configuraciones que no aparecen en esta lista no se modificarán y se dejarán los valores por defecto. Ya terminada la edición del fichero habrá que crear los ficheros necesarios para el funcionamiento correcto de *openkim*.

En primer lugar, se creará la carpeta donde se alojará la clave privada que firmará los correos electrónicos del dominio *cibersecurityhunter.com* que en este caso se guardará en el directorio /etc/opendkim/keys/cibersecurityhunter.com/. Esto se realiza con el siguiente comando.

```
mkdir /etc/opendkim/keys/cibersecurityhunter.com/
```

Después tendremos que generar la clave privada que firmará los correos, para esto usaremos el comando **opendkim-genkey** que sigue la siguiente estructura.

```
opendkim-genkey -s <identificador> -d <dominio> -D <ruta donde almacenar la clave privada>
```

Como el identificador ha de ser numérico se utilizará una combinación de números usando el año y el mes actual por lo que el comando a lanzar quedaría de la siguiente forma.

```
opendkim-genkey -s 202008 -d cibersecurityhunter.com -D /etc/opendkim/keys/cibersecurityhunter.com/
```

Ya hecho esto solo hay que cambiar los permisos de la carpeta creada para almacenar la clave privada para que pertenezca al usuario de *opendkim*. Para esto se usará el siguiente comando.

```
chown -R opendkim:opendkim /etc/opendkim/keys/cibersecurityhunter.com/
```

Una vez lanzado los comandos anteriores tocará crear y editar 3 ficheros que se describen a continuación:

1. /etc/opendkim/KeyTable

Fichero que configura la clave privada usada para un dominio y su *hostname* usado en el registro DNS que se explicará posteriormente. La estructura es la siguiente.

```
<identificador>._domainkey.<dominio> <dominio>:<identificador>:<ruta de la clave><identificador>.private
```

Según la estructura mostrada anteriormente el fichero quedaría de la siguiente manera.

```
202008._domainkey.cibersecurityhunter.com cibersecurityhunter.com:202008:/etc/opendkim/keys/cibersecurityhunter.com/202008.private
```

2. /etc/opendkim/SigningTable

Archivo que indica que cuentas serán necesario encriptar, en este caso cada fila seguirá el formato <cuentas> <registro del dominio> por lo que el archivo quedará de la siguiente forma.

```
*@cibersecurityhunter.com 202008._domainkey.cibersecurityhunter.com
```

3. /etc/opendkim/TrustedHosts

Equipos que podrán hacer uso de DKIM, que en este caso serán el servidor de correo y *GoPhish*, por lo que se añadiran a la lista tanto la dirección IP de ambos como el subdominio de *postfix.* El fichero quedará de la siguiente forma.

```
127.0.0.1

::1

134.122.110.153

cibersecurityhunter.com

smtp.cibersecurityhunter.com
```

Cuando se realice todo lo mencionado ya se tendrá configurado correctamente la parte del servicio *opendkim*, por lo que ahora se tendrá que realizar una pequeña modificación en el fichero de configuración de *postfix* llamado *main.cf* editado anteriormente. Los atributos por editar son los siguientes. →

- `smtpd_milters = inet:127.0.0.1:8891` → Lista de servicios usados para el filtrado de correos salidos del mismo servidor que no pertenecen a *postfix*. Como se ha mencionado anteriormente, *opendkim* iba a usar el puerto 8891 con la dirección IP local, debido a esto la configuración de este atributo.
- `non_smtpd_milters = inet:127.0.0.1:8891` → Ídem descripción anterior, pero con correos llegados de servidores externos.
- `milter_protocol = 6` → Versión del protocolo del filtrado de correos usado. Por defecto se usa la 2, para no tener problemas con *opendkim* se usará la 6.

Ya realizado esto estará terminada toda la configuración a realizar dentro del servidor y únicamente quedará por introducir el registro DNS para que todo funcione correctamente. Este se puede ver en el fichero /etc/opendkim/keys/<dominio>/<identificador>.txt, que en este caso los datos a rellenar tendrán el valor "cibersecurityhunter.com" y "202008" respectivamente. En la siguiente figura se aprecia el contenido de este.

```
202008._domainkey       IN      TXT     ( "v=DKIM1; h=sha256; k=rsa; "
          "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsQs3uXroYB2QOXjnaz/L24f
KCu+GHfR8dgC7d6MFXJcwXwE3D4yQN33A6Y7vE82gfX8GZNTVIu21FJmVUfv6UzrI2nAFw9vPZ8zBPg6
```

Figura 4-66 Registro DKIM resultante

Solo quedará introducir este registro dentro del servidor DNS como se muestra en la imagen a continuación.

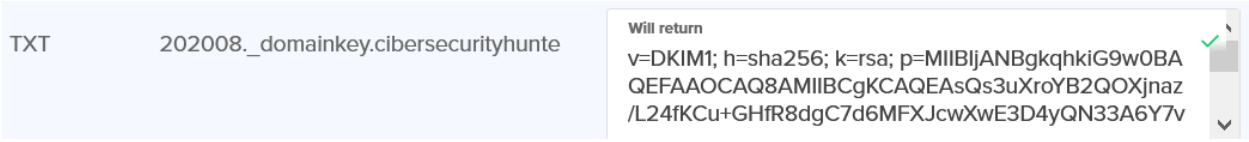


Figura 4-67 Registro DKIM en el servidor DNS

Para comprobar que está todo configurado correctamente se puede usar la herramienta gratuita online "dmarcanalyzer" con la siguiente URL únicamente introduciendo el dominio y su respectivo identificador.

https://www.dmarcanalyzer.com/es/dkim-3/dkim-record-check/

Gracias a esto se puede ver que DKIM se ha instalado y configurado correctamente.

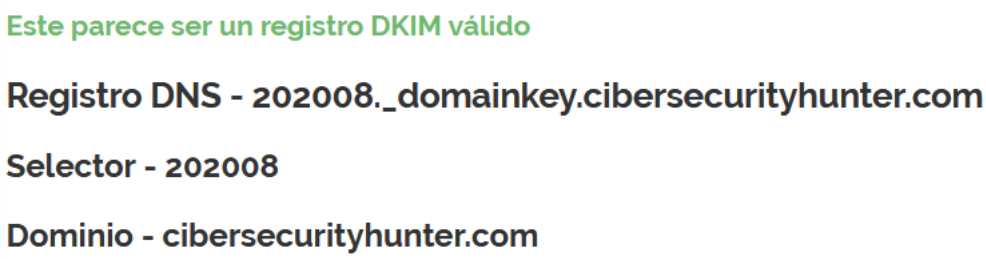


Figura 4-68 Validación del regitro DKIM

4.6.4.3. Configuración DMARC

Finalmente se realizará la configuración del registro DMARC que se utiliza para establecer políticas en función de los resultados obtenidos de DKIM y SPF. Solo habrá que introducir un nuevo registro TXT en el servidor DNS con *hostname* _dmarc.<dominio> con los valores de las políticas establecidos. El resultado sería el siguiente.

```
_dmarc IN ("v=DMARC1; p=quarantine; rua=mailto:admin@cibersecurityhunter.com")
```

En este caso el valor "p" como se ha explicado anteriormente selecciona la política establecida, siendo la elegida *quarantine* con la que se mandan a la carpeta de correo no deseado los correos que no pasen la validación de DMARC. El valor de "rua" es opcional por lo que podría omitirse, se ha añadido una dirección del dominio para el caso en el que se quiera monitorizar los registros configurados en estos últimos apartados.

Al igual que para DKIM la herramienta mencionada anteriormente "dmarcanalyzer" puede comprobar que se ha configurado sin errores el registro DMARC. La URL para esto es la siguiente.

https://www.dmarcanalyzer.com/es/dmarc-3/dmarc-record-check/

Ya configurados todos los registros se puede ver enviando un correo que si se envía un correo desde la dirreción IP 134.122.110.153 pasa todas las validaciones correctamente.

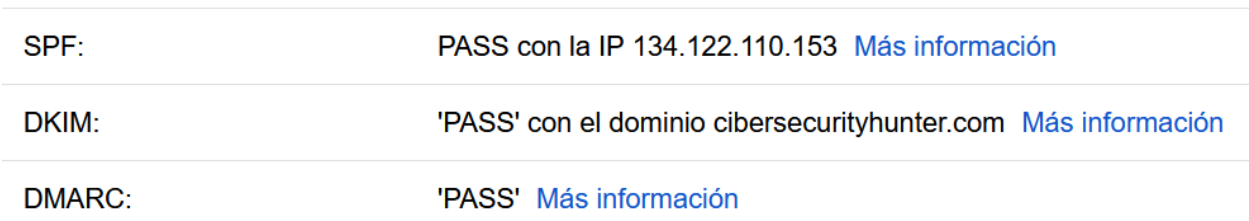


Figura 4-69 Validación de los registros SPF, DKIM y DMARC

4.7. Campaña piloto.

Para probar todo el sistema montado a lo largo del trabajo desarrollado se preparará una campaña de *phishing* a modo de piloto para la empresa Sandetel que pertenece a la Junta de Andalucía. En los siguientes apartados se desarrollarán las diversas configuraciones creadas dentro de *GoPhish*.

4.7.1. Perfil de envío de correos

En primer lugar, hay que configurar el llamado *Sending Profile* dentro de *GoPhish* o perfil de envío para la campaña de phishing que se va a crear. Se han rellenado los campos según la siguiente figura.

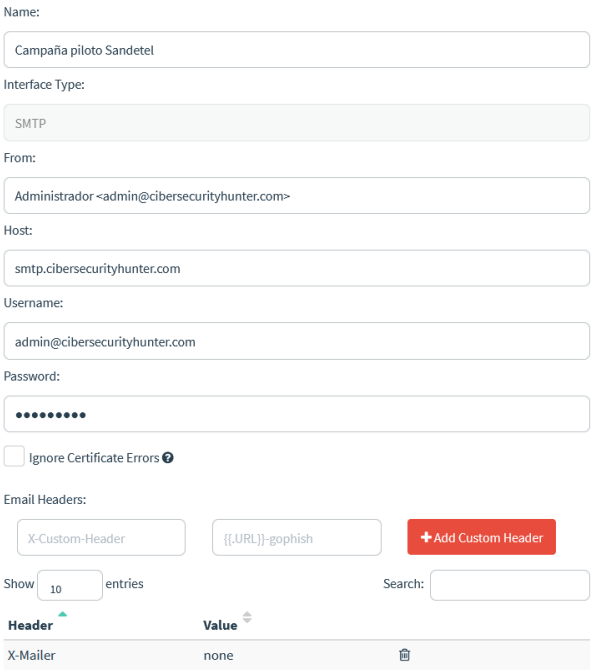


Figura 4-70 Perfil de envío en la campaña piloto

La descripción de cada uno de los apartados mostrados anteriormente es la siguiente:

- Name → Nombre identificativo para la campaña, en este caso "Campaña piloto sandetel".
- From: → Desde donde aparecerá que se va a enviar el correo, se podría realizar una técnica de *spoofing* para suplantar el correo real de la empresa, pero seguramente no pasaría el filtro antispam. Debido a esto se usará una dirección de correo perteneciente al dominio usado durante el documento, admin@cibersecurityhunter.com
- Host → Servidor de correo que lanzará la campaña de phishing, en este caso el configurado en apartados anteriores. A este se le asigno el subdominio "smtp.cibersecurityhunter.com".
- Username → Cuenta usada para enviar los correos electrónicos.
- Password → Contraseña de la cuenta del apartado anterior.
- Email Headers → En este caso únicamente se ha modificado el valor de la cabecera "X-Mailer" ya que *GoPhish* por defecto añade el valor "gophish" a esta. Como esto puede ocasionar problemas de cara a pasar el filtro anti-spam se cambia su valor a "none".

4.7.2. Página Web

En este apartado se hará uso de la facilidad que da *GoPhish* para suplantar inicios de sesión de páginas webs únicamente teniendo su URL, que en este caso es la siguiente.

https://ssoweb.juntadeandalucia.es/opensso/UI/Login?realm=correo

Entrando en el apartado "*Landing Pages*" se configura esta parte y para crear la suplantación solo habrá que pulsar sobre "*New Page*" y posteriormente copiar la URL antes mencionada en el recuadro que aparece al realizar clic sobre "*Import Site*". En la siguiente imagen se aprecia el resultado final al rellenar este apartado.

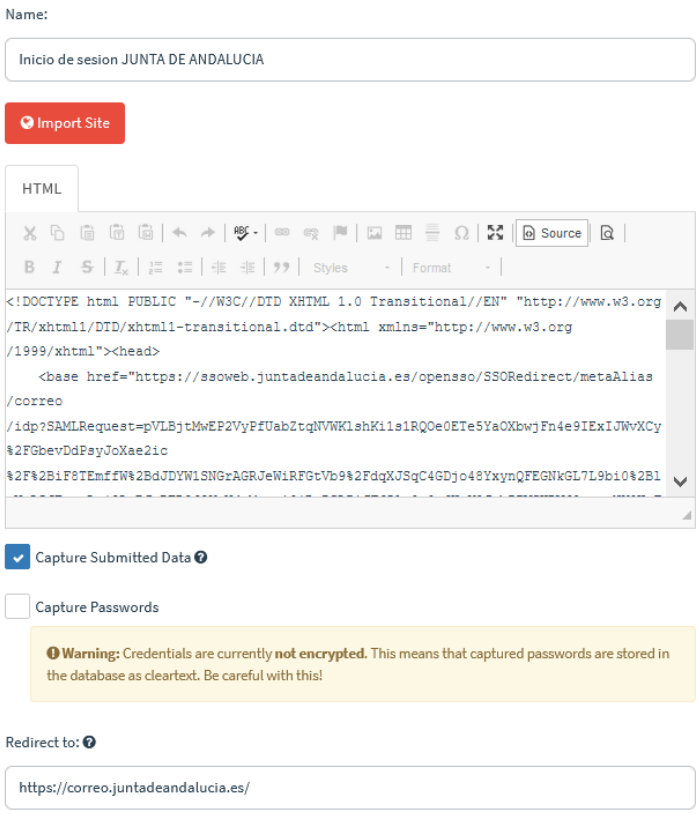


Figura 4-71 Configuración de la página web de phishing en la campaña piloto

Los apartados existentes se han completado de la siguiente manera:

- Name → Nombre identificativo para la página web de *phishing*.
- HTML → Resultado de copiar la web real con la opción "*Import Site*" en código HTML.
- Capture Submitted Data → Opción marcada para capturar los datos introducidos en el formulario de inicio de sesión. Si solo se marca esta opción **no** se capturará el valor de la contraseña.
- Capture Password → Opción desmarcada de captura de contraseñas dentro de un formulario debido a que se guardan dentro del servidor en texto claro. Como la campaña tiene como objetivo únicamente conocer el grado de concienciación de los trabajadores el saber sus contraseñas carece de interés.
- Redirect to: → Web a la que se redirecciona al intentar iniciar sesión desde la web de *phishing*. En este caso se ha introducido la dirección del portal previo al portal de login.

Finalmente se puede observar que la página web de *phishing* ha sido creada satisfactoriamente en el dominio cibersecurityhunter.com.

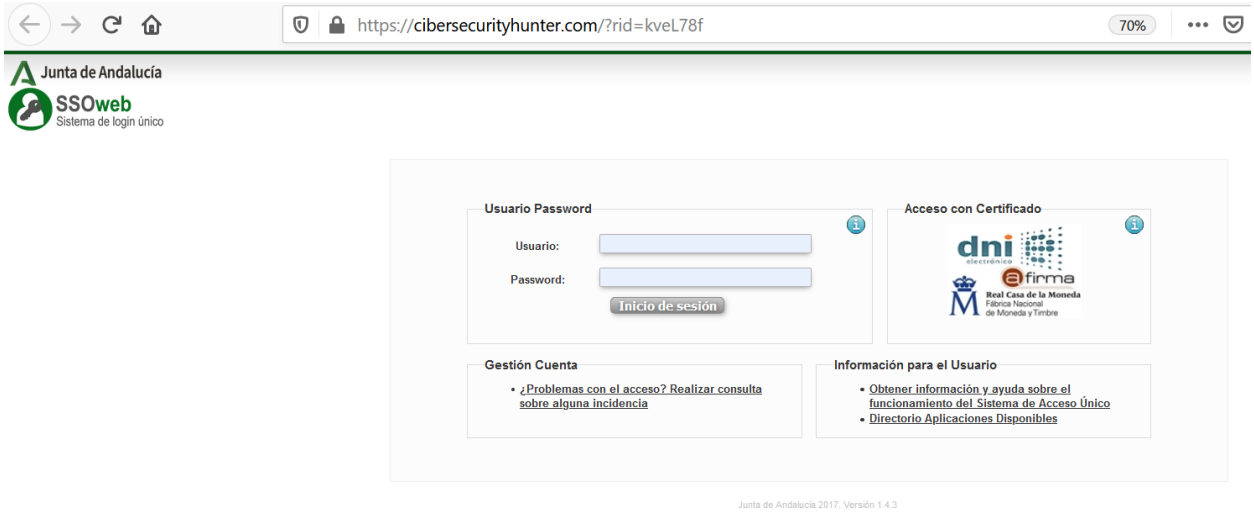


Tabla 4-71 Página web de phishing

4.7.3. Correo electrónico

Para esta campaña se ha decidido usar un correo electrónico que le indique al usuario objetivo de la campaña que la contraseña caducará al día siguiente de enviar el email y que tiene que cambiarla para no tener problemas en el acceso a su cuenta.

Después se le pondrá al final un enlace que reediriga a la página web creada en el punto anterior más un *tracker* que detectará si el empleado ha abierto el correo.

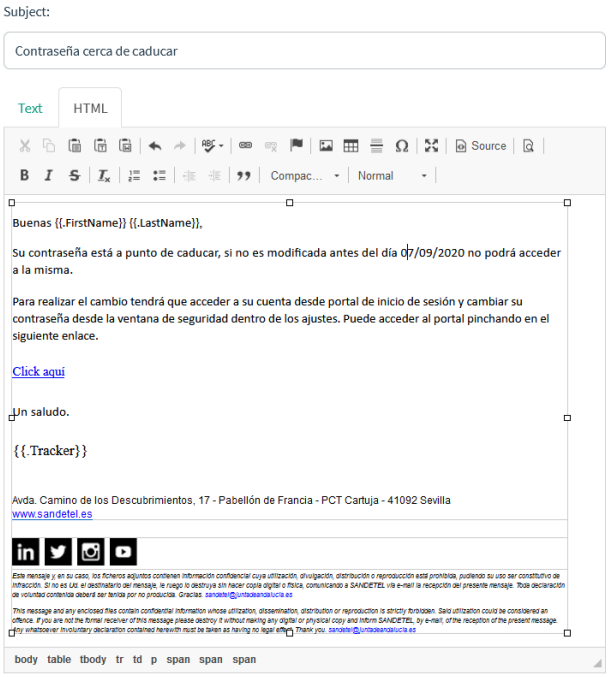


Tabla 4-72 Correo electrónico para la campaña piloto

Al final del correo se puede observar que se ha añadido la firma que se utiliza dentro de la empresa para aportarle fiabilidad, a parte se ha estructurado el mensaje para que parezca que está generado automáticamente por el sistema.

En este se han usado las variables {{.FirstName}} para personalizar el nombre en cada correo enviado, {{.LastName}} para los apellidos, dentro del enlace "Click aquí" se encuentra {{.URL}} para que este redirija a la página web de *phishing* y finalmente {{.Tracker}} para que se incluya este y se pueda saber cuando el usuario abre el correo electrónico.

4.7.4. Creación de la campaña

Una vez configurado todo lo mencionado anteriormente, y la lista de usuarios que recibirán los correos de *phishing* no siendo esta mostrada, solo queda configurar los parámetros de la campaña. Estos se muestran en la siguiente foto.

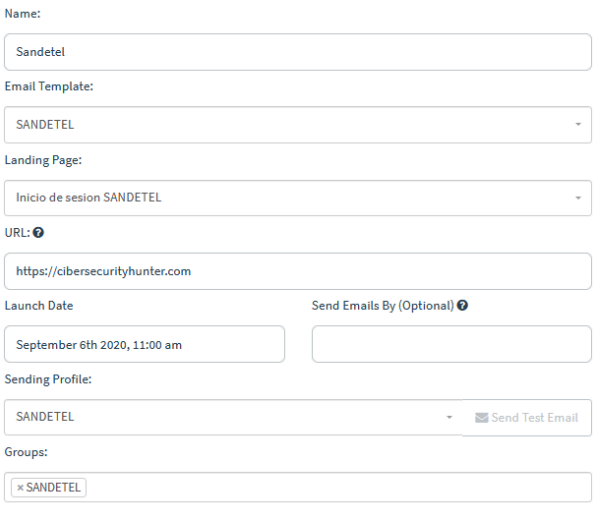


Tabla 4-73 Configuración de la campaña piloto

Los parámetros configurados corresponden a los creados con anterioridad con sus respectivos nombres representativos. Únicamente ha dos parámetros de interés:

- URL → URL o dirección IP del servidor web utilizado para mostrar las páginas web del ataque de phishing, en este caso se ha usado el mismo dominio tanto para el servidor de *GoPhish* como para el servidor web que trae la herramienta.
- Launch Date → Fecha y hora en la que se lanzará la campaña de *phishing*. Se pueden enviar de forma escalonada con la opción "*Send Emails By*", pero no ha procedido en este caso.

Ya con todo configurado únicamente habrá que pulsar el botón "*Launch Campaign*" para que se programe la campaña de *phishing*, después de esto solo hay que esperar los resultados.

4.7.5. Resultados

Una vez explicado todo lo anterior se lanzará la campaña dentro de la empresa y se recolectarán los resultados. En total han sido enviado los correos electrónicos de *phishing* a 180 personas, finalizando la campaña pasados dos días (09/09/2020) desde que se lanzó, siendo los resultados los siguientes:

- 167 personas llegaron a abrir el correo electrónico.
- 47 personas hicieron clic en el enlace.
- 7 personas introdujeron sus datos.

Una vez observados estos resultados, en primer lugar, el que hayan abierto el correo no resulta relevante a la hora de sacar conclusiones, porque si no se hace es muy difícil comprobar que resulta un correo de *phishing*. En consecuencia, las 13 personas que no lo han abierto se considera que lo han visto después de los dos días del lanzamiento de la campaña (cuando finalizó).

Por otro lado, se ha observado que 47 personas (un 26,1%) han realizado clic en el enlace, y solo 7 (el 3,9% del total) de esas 47 han llegado a introducir sus datos en la web de *phishing*. Esto es buena señal, debido a que 40 empleados han sabido identificar que no resultaba ser un inicio de sesión real.

Este buen resultado es fruto de que en la empresa Sandetel se han realizado campañas de concienciación con anterioridad. Esto ha ayudado a los usuarios a no caer en este tipo de engaños. Sin embargo, no hay que descuidar a los 7 empleados que sí han introducido sus datos, por lo que para habrá que realizar una formación para ellos en la que se les indique como evitar este tipo de ataques y así no sufrir un robo de credenciales.

5 BIBLIOGRAFÍA

[1] https://www.infospyware.com/articulos/que-es-el-phishing/

[2] https://www.pandasecurity.com/es/security-info/phishing/

[3] https://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/

[4] https://randed.com/tipos-de-phishing/

[5] https://www.muyseguridad.net/2019/02/15/ataques-phishing-riesgo-seguridad/

[6] https://tools.ietf.org/html/rfc5321

[7] https://www.dsi.uclm.es/personal/miguelfgraciani/mikicurri/Docencia/LenguajesInternet0910/web_LI/Teoria/Protocolos%20de%20nivel%20de%20aplicacion/Material/Comandos%20del%20protocolo%20SMTP.htm

[8] https://clouding.io/hc/es/articles/360011403640-Entender-una-cabecera-de-correo

[9] https://support.office.com/es-es/article/%C2%BFqu%C3%A9-son-imap-y-pop-ca2c5799-49f9-4079-aefe-ddca85d5b1c9

[10] https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

[11] https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide

[12] https://www.nerion.es/soporte/todo-sobre-dkim/

[13] https://es.mailjet.com/blog/news/spf-dkim-dmarc-como-configurar/#dmarc

[14] https://support.google.com/a/answer/2466563?hl=es

[15] https://www.kaspersky.es/blog/epp-edr-importance/16154/

[16] https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

[17] https://www.osi.es/es/actualidad/blog/2018/09/26/filtros-de-correo-antispam-para-que-sirven-y-como-configurarlos

[18] https://elblogdebillgate.blogspot.com/2018/10/top-9-simuladores-de-phishing-gratis.html

[19] https://www.sophos.com/es-es/medialibrary/pdfs/factsheets/sophos-phish-threat-datasheet.pdf

[20] https://docs.getgophish.com/user-guide/installation

[21] https://docs.getgophish.com/user-guide/template-reference

[22] http://www.postfix.org/documentation.html

[23] http://opendkim.org/

GLOSARIO