Defining tools for phishing campaigns

A Degree Thesis

Submitted to the Faculty of the

Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

by

Youssef El Houas Ghouddana

In partial fulfilment

of the requirements for the degree in

Telecommunications **ENGINEERING**

Advisor: Alfonso Rojas

Barcelona, January 2022

Abstract

The objective of this project is to carry out a real phishing campaign in order to assess the impact on a company and its employees, to be affected by these malicious practices, to raise awareness and train workers to detect possible malicious emails and to create an action plan that can be used to teach employees how to act in case of detecting these emails or being a victim of them.

The project will cover all the essential points to carry out a successful phishing campaign, from the creation of a social engineering plan to make the employees of the company fall into the campaign, the creation and configuration of all the technical infrastructure for this, this point includes the realization of a mail server (SMTP), the use of tools to automate and track the phishing campaign as the creation of emails and web pages necessary to carry out such practice.

Resum

L'objectiu d'aquest projecte és dur a terme una campanya real de phishing amb la finalitat d'avaluar l'impacte en una empresa i els seus empleats en veure's afectats per aquestes pràctiques malicioses, conscienciar i formar als treballadors per a detectar possibles correus electrònics maliciosos i crear un pla d'acció que pugui servir per a ensenyar als empleats com actuar en cas de detectar aquests correus electrònics o ser víctima d'ells.

El projecte abastarà tots els punts essencials per a dur a terme una reeixida campanya de phishing, des de la creació d'un pla d'enginyeria social per a fer que els empleats de l'empresa caiguin en la campanya, la creació i configuració de tota la infraestructura tècnica per a això, aquest punt inclou la realització d'un servidor de correu (SMTP), l'ús d'eines per a automatitzar i rastrejar la campanya de phishing com la creació de correus electrònics i pàgines web necessàries per a dur a terme aquesta pràctica.

Resumen

El objetivo de este proyecto es llevar a cabo una campaña real de phishing con el fin de evaluar el impacto en una empresa y sus empleados al verse afectados por estas prácticas maliciosas, concienciar y formar a los trabajadores para detectar posibles correos electrónicos maliciosos y crear un plan de acción que pueda servir para enseñar a los empleados cómo actuar en caso de detectar estos correos electrónicos o ser víctima de ellos.

El proyecto abarcará todos los puntos esenciales para llevar a cabo una exitosa campaña de phishing, desde la creación de un plan de ingeniería social para hacer que los empleados de la empresa caigan en la campaña, la creación y configuración de toda la infraestructura técnica para ello, este punto incluye la realización de un servidor de correo (SMTP), el uso de herramientas para automatizar y rastrear la campaña de phishing como la creación de correos electrónicos y páginas web necesarias para llevar a cabo dicha práctica.

Dedication:

I would like to dedicate this project to my whole family who have been supporting me in this university stage.

Make special mention to my brother who has always been the person who has encouraged me to study technological studies and thanks to him I am finishing this degree.

Acknowledgements

In this section I would like to thank all the EY employees who have made possible the realization of this project, these are the members of the cybersecurity department, who have guided me and helped me when I have needed it. Also mention the help received by my supervisors, who have been guiding me and commenting on what factors could change or improve the project.

Revision history and approval record

Revision	Date	Purpose
0	15/12/2021	Document creation
1	21/01/2022	Document revision

DOCUMENT DISTRIBUTION LIST

Name	e-mail
Youssef El Houas Ghouddana	
Alfonso Rojas	
Noel Castillo	

Written by:		Reviewed and approved by:	
Date	15/12/2021	Date	21/01/2022
Name	Youssef El Houas Ghouddana	Name	Alfonso Rojas
Position	Project Author	Position	Project Supervisor

Table of contents

List of Figures

1. Introduction

The objective of this project is to carry out a real phishing campaign in order to assess the impact on a company and its employees, to be affected by these malicious practices, to raise awareness and train workers to detect possible malicious emails and to create an action plan that can be used to teach employees how to act in case of detecting these emails or being a victim of them.

The project will combine social engineering techniques to create malicious emails and free and proprietary software to carry out phishing campaigns.

First, it will be explained why it is so important to take preventive measures against these practices and to be alert so as not to be a potential victim of phishing. It will also include the procedure to be followed in order to create an awareness campaign from scratch, so that employees of an organisation can be trained to detect possible scams.

The project will cover all the essential points to carry out a successful phishing campaign, from the creation of a social engineering plan to make the employees of the company fall into the campaign, the creation and configuration of all the technical infrastructure for this, this point includes the realization of a mail server (SMTP), the use of tools to automate and track the phishing campaign as the creation of emails and web pages necessary to carry out such practice.

As a main hypothesis we want to check how harmful it can be for a real company to being a victim of one of these practices and being able to know if a company can be vulnerable to a phishing attack.

It would be considered already critical, that a single employee disseminated personal or corporate data to the attacker. In this project, the statistics of how employees have been affected, those who have fallen into the trap, how many have ignored the mail and those who have had the ability to report the emails as possible phishing.

As a complement to the phishing campaign, a tool will be developed throughout the project to support future phishing campaigns making the task of phishing easier, this tool will be detailed in the technical sections of this report.

The requirements and specifications that need to be met in order to complete this project are listed below:

Project requirements:

- To be able to develop a phishing campaign which uses emails that make users fall into the "trap".
- Create a mail server in which we are able to send such mails using a domain similar to the affected company domain name.
- Develop an application capable of making easier to carry out phishing campaigns.
- Develop a step-by-step guide on how to conduct phishing campaigns for corporate awareness purposes.

Project specifications:

- The campaign will be considered a success when we see the statistics of users who have interacted with the campaign.
- The SMTP server will be tested to check that it is able to send emails without any problems.
- To carry out a phishing campaign using the developed application.
- EY should review the guidelines for the creation of campaigns

This project is carried out in EY's cybersecurity department, which provides cybersecurity consultancy services to companies of all types.

My project will be part of one of these consultancies and will serve to advise on phishing attacks to a real company.

The project will be supported by the tutor in the company and also by employees who have participated in previous phishing campaigns.

In addition, we will use free software focused on the creation of these campaigns, you can find more information about the program used here: Gophish - Open Source Phishing Framework (getgophish.com)

The project has been worked on by separating it into the following Work Packages which have been sorted in time as shown in the Gantt chart:

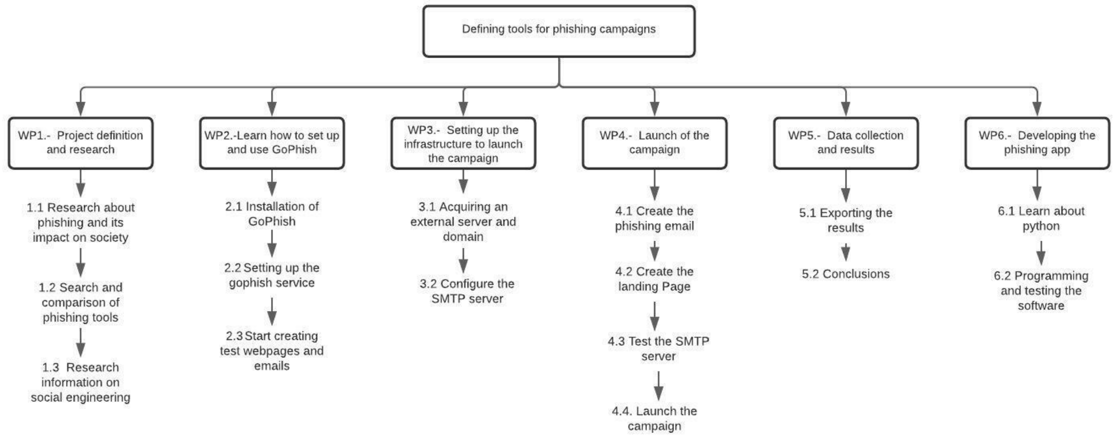

Defining tools for phishing campaigns
WP1.- Project definition and research
WP2.-Learn how to set up and use GoPhish
WP3.- Setting up the infrastructure to launch the campaign
WP4.- Launch of the campaign
WP5.- Data collection and results
WP6.- Developing the phishing app
1.1 Research about phishing and its impact on society
1.2 Search and comparison of phishing tools
1.3 Research information on social engineering
2.1 Installation of GoPhish
2.2 Setting up the gophish service
2.3 Start creating test webpages and emails
3.1 Acquiring an external server and domain
3.2 Configure the SMTP server
4.1 Create the phishing email
4.2 Create the landing Page
4.3 Test the SMTP server
4.4. Launch the campaign
5.1 Exporting the results
5.2 Conclusions
6.1 Learn about python
6.2 Programming and testing the software

Figure 1: Work Packages

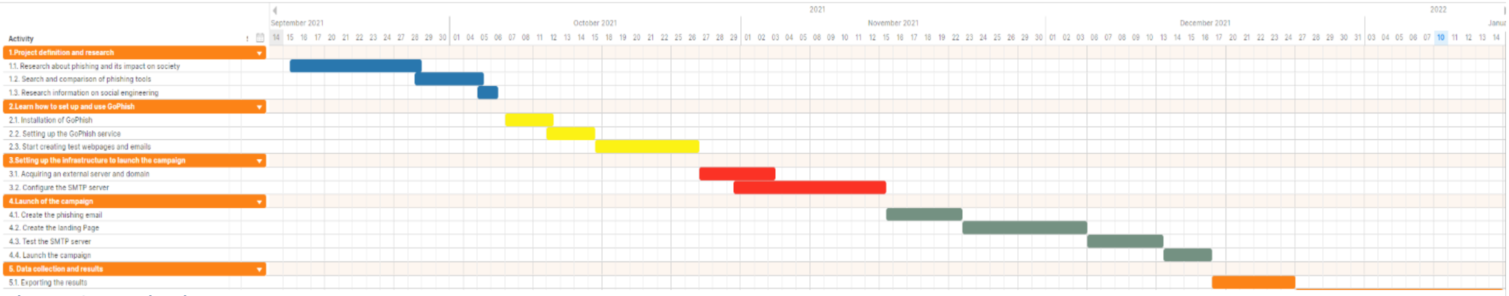


Figure 2: Work Plan

2. State of the art of the technology used or applied in this thesis:

Phishing is the crime of tricking people into sharing sensitive information such as passwords and credit card numbers. There is more than one way to carry out phishing campaigns, but one phishing tactic is the most common.

Victims receive an email or text message that mimics (or "impersonates") a trusted person or organization, such as a co-worker, bank or government office. When the victim opens the email or text message, he or she encounters a message designed to scare him or her, with the intent to undermine his or her judgment by instilling fear. The message demands that the victim go to a website and act immediately or face some consequence.

If a user takes the bait and clicks on the link, they are sent to a website that is an imitation of the legitimate one. From there, he is prompted to log in with his username and password credentials. If you do, the login information gets to the attacker, who uses it to steal identities, loot bank accounts, and sell personal information on the black market.

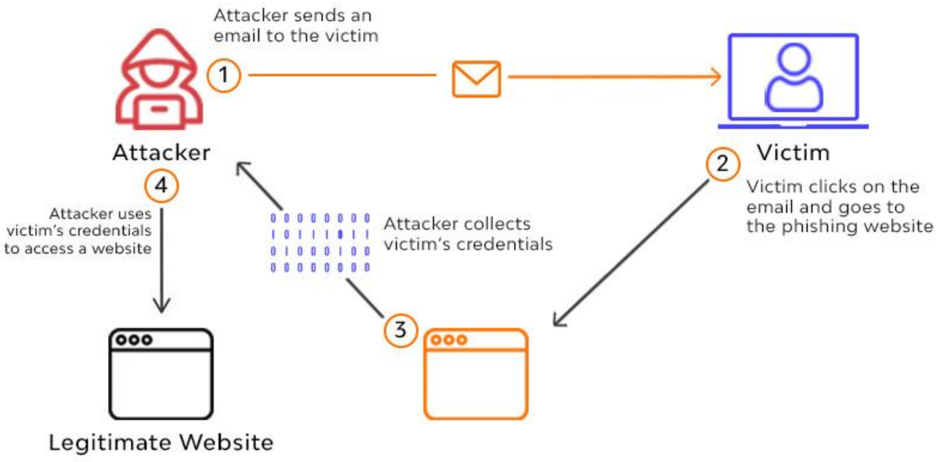

Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Legitimate Website

Figure 3: Phishing basic scheme

2.1. Origins of phishing

The word phishing was coined around 1996 by hackers stealing America Online accounts and passwords. By analogy with the sport of angling, these Internet scammers were using e-mail lures, setting out hooks to "fish" for passwords and financial data from the "sea" of Internet users. They knew that although most users wouldn't take the bait, a few likely would. The term was mentioned on the alt.2600 hacker newsgroup in January 1996, but it may have been used earlier in the print journal 2600, The Hacker Quarterly.

Hackers commonly replace the letter f with ph, a nod to the original form of hacking known as phone phreaking. By 1996, hacked accounts were called phish, and by 1997, phish were being traded among hackers as a form of currency.

2.2. Types of Phishing Attacks :

There are different types of phishing attacks, which are characterised by using different social engineering techniques or different ways by which the attacker interacts with the victim. The most common types of attacks will be listed but more types of attacks can be found.

2.2.1. Email phishing

Most phishing attacks are sent via email. Attackers will register fake domains impersonating real organizations and will send thousands of generic requests. Links usually lead to malicious websites that steal credentials or install malicious code, known as malware, on users' devices. Or, they might use the organization's name in the local part of the email address (such as amazon@fakedomain.com) in the hope that the sender's name will only appear as "Amazon" in the recipient's inbox.

2.2.2. Whaling

Attackers use social media or company websites to find the names of the organization's CEO or other members of senior management. Then they impersonate the person using a similar email address. Emails may require a money transfer or require the recipient to review documents. A whaling attack is also known as CEO fraud. Scams involving fake tax returns are an increasingly common type of whaling.

2.2.3. Vishing

Vishing is short for "voice phishing", which consists of tricking people on the phone, persuading them to divulge sensitive information. In this type of attack, the attacker tries to steal the victim's data and use it to his advantage.

2.2.4. Smishing

Smishing is sending a message that requires someone to take action. This is the next evolution of vishing. Often the text includes a link that, when clicked, installs malware on the user's device.

2.2.5. Angler phishing

Social media has become another popular place for phishing attacks. Angler phishing occurs when cybercriminals use notification features or direct messages in social media applications to trick someone into taking action.

2.2.6. Spear phishing

This type of phishing attack uses email but with a specific targeted approach. The attackers use open-source intelligence (OSINT) to gather information about a particular company through social media or the company's website. Then, they make specific individuals from the company as their target using real names, job roles to make the recipient think the email has arrived from a known, legitimate source.

2.2.7. HTTPS Phishing

Nowadays cybercriminals are using HTTPS in the links that they use to perform phishing attacks. Even though HTTPS is a secure protocol, attackers are now making use of HTTPS links.

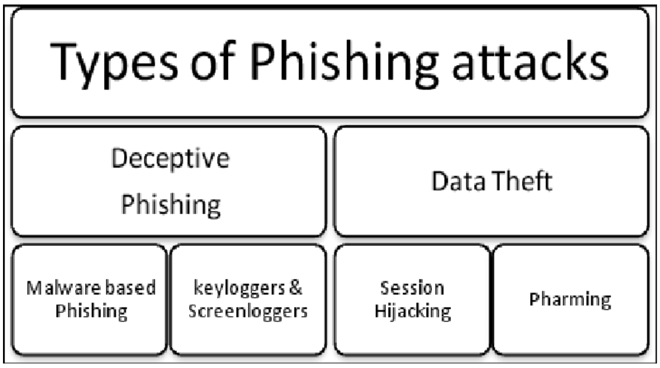


Figure 4: Types of Phishing attacks

2.2.8. Malware-Based Phishing

Refers to scams that involve running malicious software on user's PCs. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities

2.2.8.1. Keyloggers and Screenloggers

Are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started.

2.2.8.2. Session Hijacking

Describes an attack where users' activities are monitored until they sign into a target account or transaction and establish their credentials.

2.2.8.3. Web Trojans

Pop up invisibly when users are attempting to log in. They collect the user's credentials locally and transmit them to the phisher.

2.2.8.4. DNS-Based Phishing (“Pharming”)

Pharming is the term given to hosts file modification or Domain Name System (DNS)-based phishing.With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site

2.3. <u>Why is phishing a real problem in the business world?</u>

We consider that phishing is a real problem in the business world because it directly attacks the part of the company considered most vulnerable, its employees, in this way this attack bypasses all anti-malware measures that companies can apply against cyber-attacks and cybercriminals get access to confidential information or inject malicious code in companies around the world.

According to the FBI, phishing was the most common type of cybercrime in 2020—and phishing incidents nearly doubled in frequency, from 114,702 incidents in 2019, to 241,324 incidents in 2020.

The FBI said there were more than 11 times as many phishing complaints in 2020 compared to 2016.

It is estimated 75% of organizations around the world experienced some kind of phishing attack in 2020. Another 35% experienced spear phishing, and 65\% faced BEC attacks.

This has a considerable impact on a company:

2.4. Impacts on a Business

2.4.1. Loss of money

From every phishing incident that has ever taken place in history, one constant effect is financial loss. First is the direct loss from transferred funds by employees who were fooled by the hackers. Second is the fines for non-compliance imposed by regulatory bodies.

Finally, there are costs of investigating the breach and compensating the affected customers, which would further compound the company's financial losses.

A 2018 Internet Crimes Report by the FBI revealed that Business Email Compromise (BEC) attacks cost US businesses over 1.2 billion dollar.

2.4.2. Loss of intellectual Property

Financial losses are not the only thing businesses have to worry about in the event of a phishing attack. Even more devastating is the loss of customer data, trade secrets, project research, and blueprints.

When the company at stake is in the tech, pharmaceutical, a stolen patent would mean millions of research expenditures.

While it is relatively easy to recover from direct monetary losses, it is more difficult to make up for the loss of sensitive business information.

2.4.3. Damage Reputation

Businesses often try to hide the fact that they have suffered any phishing attacks. The major reason for this is the damage to reputation. Customers often patronize brands they consider to be reliable and trustworthy. Not only will the disclosure of a breach taint the brand image, but it will also break that established trust. Regaining customers' confidence is no easy feat, and the value of a brand is directly related to its customer base.

An exposed breach attack will also damage the company's reputation in the eyes of investors.

With combined damage to customer and investor confidence, a successful phishing attack could potentially sabotage hundreds of millions in market capitalization.

2.4.4. Business Disruption

It is nearly impossible for a business to run exactly as it used to after suffering a phishing attack, especially one involving malicious bugs. Attacks involving malware usually take a while to rectify. Systems will have to be taken offline or shut down, and this could result in a substantial decrease in productivity.

Interruption to businesses providing services like transportation, technology, waste disposal, and other critical infrastructure could cripple the economy significantly.

Figure 5: Phishing example picture

2.5. Common characteristics of phishing attacks

After analysing phishing emails sent across the internet, a list of the most characteristic aspects of phishing emails can be obtained:

- They usually contain content that gives a sense of urgency.
- They try to get you to interact with the mail by requesting an action from the recipient of the mail.
- The emails are often classified as important, pretending to be from an official organisation.
- Malicious emails could contain links to pages that ask for payment or some other type of transaction to obtain the victims' bank details.
- They have components that demand the attention of those affected.

We have also obtained a list of the organizations that are most often supplanted in this type of mailings as well as the actions that are demanded from the users:

- IT: Annual Asset Inventory.
- Changes to your health benefits.
- Twitter: Security alert: new or unusual Twitter login.
- Amazon: Action Required - Your Amazon Prime Membership has been declined.
- Zoom: Scheduled Meeting Error.
- Google Pay: Payment sent.
- Stimulus Cancellation Request Approved.
- Microsoft 365: Action needed: update the address for your Xbox Game Pass for Console subscription.
- Workday: Reminder: Important Security Upgrade Required.

Figure 6: Phishing example picture 2

3. Methodology / project development:

In this section we will detail step by step the procedures carried out for the realisation of the project. It will detail how the phishing campaign has been created from scratch taking into account all the necessary parts, that includes the creation and configuration of the SMTP server, the use of GoPhish which is the software used to create the campaign, the creation of emails and web pages and also the part of dealing with the companies antispam and what factors are key to avoid your emails being rejected.

The following diagram shows the experiment and all the components involved:

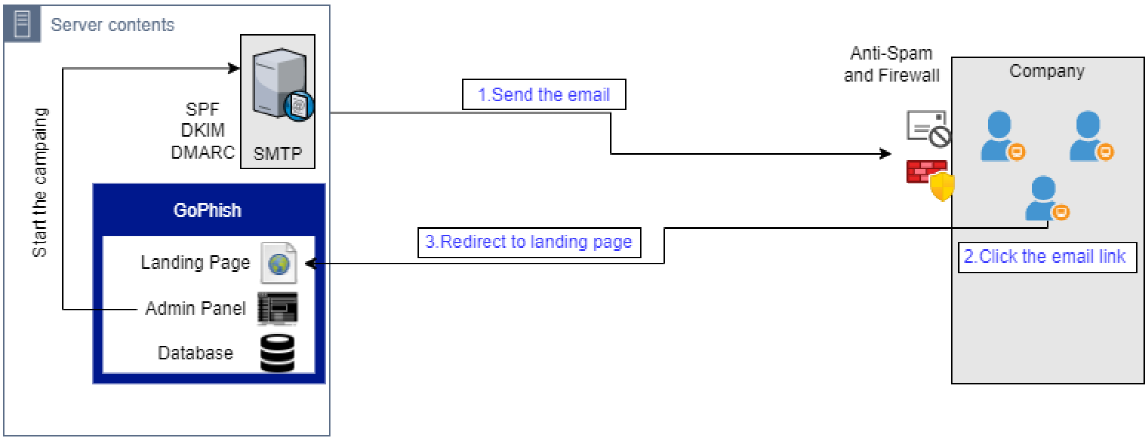


Figure 7: Project Diagram

For the correct execution of the phishing campaign, we will start by setting up the infrastructure known as server contents, this will be an external server with internet access which will host our mail server, the application to execute the phishing campaigns (GoPhish) and the web pages to which the victims of our experiment will be directed after clicking on the link in the malicious email.

After having set up the infrastructure, to start the campaign we need to have created the email and the web pages that will be used in the campaign, for that we can use GoPhish, from this software we launch the campaign and then the SMTP server will be in charge of sending the mail to the corresponding destinations of the target company. Before the mails reach the employees, they must pass the anti-spam filters of the respective company, the best configuration practices will be explained and discussed in order to have a better chance of passing these filters. When employees receive the email, we will monitor what actions they have taken, and we will know how many users saw the email and did not click on it, who reported the email as a possible phishing email and then those who were tricked and clicked on the link, which would be directed back to our server where the web pages are displayed for them to enter their credentials. All events and data entered by the users will be recorded in the databases created when deploying GoPhish and can be further processed to show the results in the most convenient and appropriate way for the purposes of the company performing the phishing simulation.

During the development of the phishing campaign, it was proposed by me the programming of a tool that facilitates the task of conducting these campaigns for use in conducting awareness campaigns to employees, this tool is characterized by using the own API of GoPhish and launching campaigns using email templates and web pages already preset, so the task of launching the campaign can be done in a few clicks.

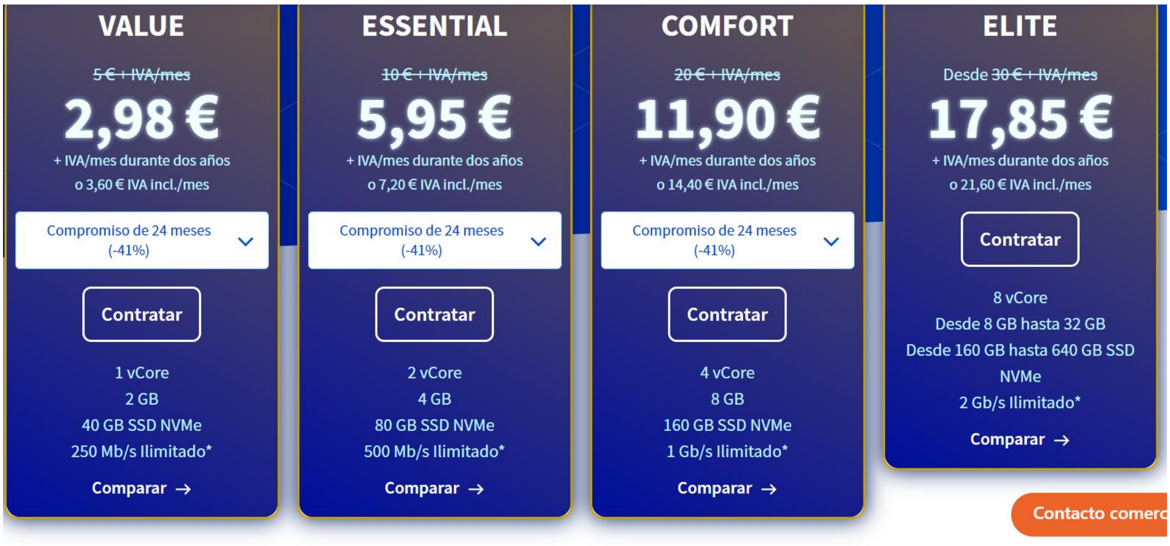
Below, we detail how the entire infrastructure has been set up so that it can be used as a guide for future phishing campaigns and how it could be used in the future.

3.1. Prerequisites

3.1.1. VPS with internet access and Static IP

In order to carry out the phishing campaign we need to have a machine on which to have all the necessary software installed and the necessary servers running. To do this we will start by acquiring and configuring a VPS (Virtual Private Server) with internet access (static public IP), this server can be one of our own internal servers which can be taken out to the internet or it can be acquired from different providers, the second option being more recommendable.

There are different platforms to hire a VPS, one of the most recommended is OVH, on this website (VPS de OVHcloud: sus servidores privados virtuales en la nube | OVHcloud) they offer different types of features for your VPS:



VALUE
~~5 € + IVA/mes~~
2,98 €
+ IVA/mes durante dos años
o 3,60 € IVA incl./mes
Compromiso de 24 meses (-41%)
Contratar
1 vCore
2 GB
40 GB SSD NVMe
250 Mb/s Ilimitado*
Comparar →

ESSENTIAL
~~10 € + IVA/mes~~
5,95 €
+ IVA/mes durante dos años
o 7,20 € IVA incl./mes
Compromiso de 24 meses (-41%)
Contratar
2 vCore
4 GB
80 GB SSD NVMe
500 Mb/s Ilimitado*
Comparar →

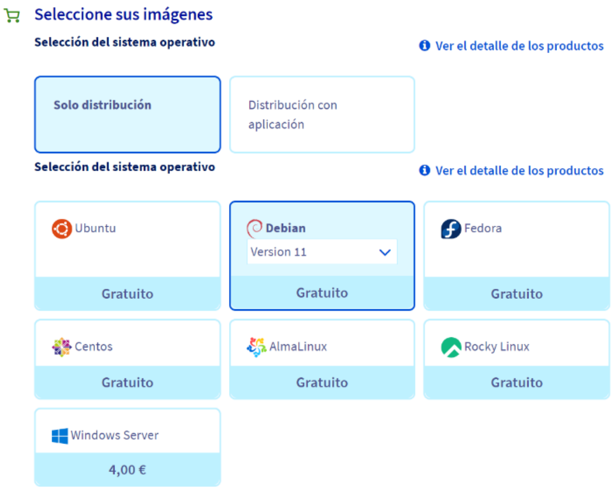
COMFORT
~~20 € + IVA/mes~~
11,90 €
+ IVA/mes durante dos años
o 14,40 € IVA incl./mes
Compromiso de 24 meses (-41%)
Contratar
4 vCore
8 GB
160 GB SSD NVMe
1 Gb/s Ilimitado*
Comparar →

ELITE
Desde ~~30 € + IVA/mes~~
17,85 €
+ IVA/mes durante dos años
o 21,60 € IVA incl./mes
Contratar
8 vCore
Desde 8 GB hasta 32 GB
Desde 160 GB hasta 640 GB SSD NVMe
2 Gb/s Ilimitado*
Comparar →

Contacto comerc

Figure 8: Selecting VPS option

We see that there are different types of prices and characteristics, for our practice we recommend any option, we will choose the one that best suits the price.



Seleccione sus imágenes

Selección del sistema operativo — Ver el detalle de los productos

- Solo distribución
- Distribución con aplicación

Selección del sistema operativo — Ver el detalle de los productos

Ubuntu Gratuito	Debian Version 11 Gratuito	Fedora Gratuito
Centos Gratuito	AlmaLinux Gratuito	Rocky Linux Gratuito
Windows Server 4,00 €		

Figure 9: VPS Operating System

Then we will be given the option to choose the operating system of our server, the most recommended is to use Ubuntu or Debian, due to the lightness of these and the simplicity to create servers on these operating systems.

When installing the VPS for the first time or reinstalling it from the client area, a user with full rights will be created and you will receive an email with the access data. The username will be generated depending on the operating system, e.g. "ubuntu" or "debian".

3.1.2. Configure VPS Access

3.1.3. SSH access

The connection to our remote server will be via ssh, a protocol used to establish secure point-to-point connections. If you have a VPS, we will receive the credentials to be able to connect to our server, however if we deploy the server ourselves we must ensure that we can connect using this protocol, then we will briefly explain how to configure the ssh service:

Configure SSH (only in case it is not installed)

We start by using the following command after logging into the system:

```
$ sudo apt install ssh
```

This command allows you to install ssh on Ubuntu, remember that in order to perform this action you must have a static ip configured with an internet connection.

Check that the SSH service is installed and activated with the following command:

```
$ systemctl status ssh
```

In case the service is not active you can activate it with the following command:

```
$ sudo systemctl start ssh
```

or deactivate it with the following:

```
$ sudo systemctl stop ssh
```

Connect via ssh

To connect remotely, we can do it by using a terminal or by using applications such as mobaXterm or Putty.

The connection via terminal would be made in the following way (by default it will establish a connection with port 22):

```
ssh nombre_de_usuario@IPv4_de_su_VPS
```

As you are now logged in with high privileges (sudo user), you can enter commands to perform administrative tasks. We recommend that you change your password first:

```
~$ sudo passwd

New password:

Retype new password:

passwd: password updated successfully
```

Note that passwords are not displayed. Change to the root user and set your admin password:

```
~$ sudo su -

~# passwd

New password:

Retype new password:

passwd: password updated successfully
```

3.1.4. SSH Tunneling

To be able to browse the server's internal web pages via a local browser, we can use ssh tunnels to redirect traffic to the VPS's internal ports, for which we can use applications such as MobaXterm, Putty or the terminal itself.

3.2. Domain purchase

A fundamental part of phishing campaigns is the correct choice and configuration of the domain that will be associated with the elements used in phishing, such as email addresses and landing pages. There are different platforms where you can get these domains, all of them working in a very similar way, from previous experiences we recommend the use of Namecheap, a website where you can register domains at different prices but in general very cheap, besides having a very simple configuration section and with a very intuitive interface. Buy a domain name - Register cheap domain names from $0.99 - Namecheap

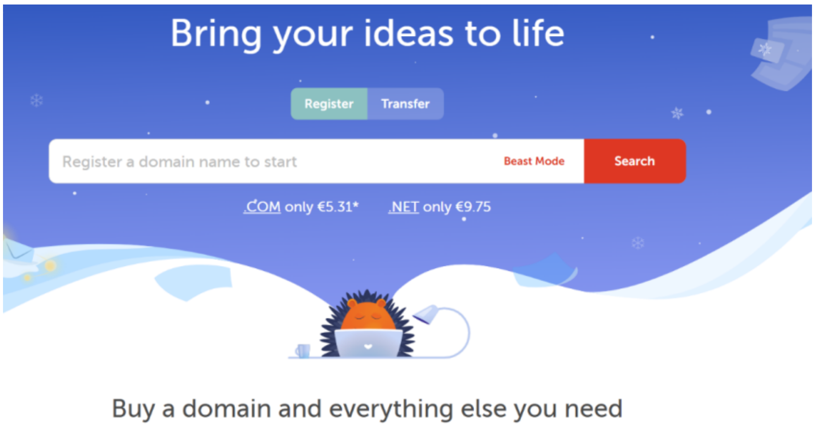
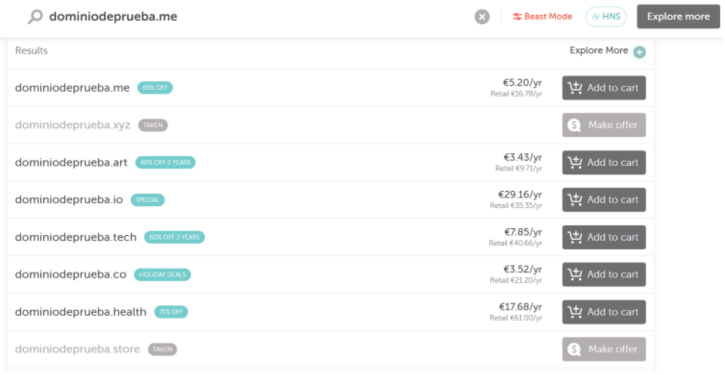


Figure 10: Domain purchase

Entering the Namecheap portal you have the possibility to search for the domain name you want to buy, if it is not available, similar domains will appear. For example, when searching for the domain dominiodeprueba.me, the following options appear:



Results		
dominiodeprueba.me 69% OFF	€5.20/yr Retail €16.78/yr	Add to cart
dominiodeprueba.xyz TAKEN		Make offer
dominiodeprueba.art 40% OFF 2 YEARS	€3.43/yr Retail €9.71/yr	Add to cart
dominiodeprueba.io SPECIAL	€29.16/yr Retail €35.35/yr	Add to cart
dominiodeprueba.tech 60% OFF 2 YEARS	€7.85/yr Retail €40.66/yr	Add to cart
dominiodeprueba.co HOLIDAY DEALS	€3.52/yr Retail €21.20/yr	Add to cart
dominiodeprueba.health 71% OFF	€17.68/yr Retail €61.00/yr	Add to cart
dominiodeprueba.store TAKEN		Make offer

Explore More

Figure 11: Selecting Domain

We see the possibility of choosing different domains related to our search with their respective prices, we will select the option that best fits with the phishing campaign to perform and add it to the shopping cart, once there we will be asked for an existing user or the creation of one and then proceed to make the payment and get our domain.

In later sections we will explain how to configure our server to use the domain purchased.

3.3. Infrastructure configuration

3.3.1. SMTP Server

Once we have our server with ssh access, we will proceed to set up a mail server, for this we will use IRedMail, free software that covers all the points to create our mail server in the easiest way possible. With IredMail you can deploy an "open source" mail server, in several minutes, for free, iRedMail - Free, Open Source Mail Server Solution for more information on this free software.

We will now proceed to explain how we have configured our mail server step by step.

First, we will make sure that we have the host name of the server well established, which has to be associated to the domain name we want to use for our campaign (we assume mail.domainname.com). To do this we perform the following actions and commands:

- Establish a Fully Qualified Domain Name (FQDN) for your server

```
sudo hostnamectl set-hostname mail.nombredominio.com
```

- Update the ***/etc/hosts*** file (you can use any text editor)

```
sudo nano /etc/hosts
```

- Edit the file as follows

```
127.0.0.1       mail.nombredominio.com localhost
```

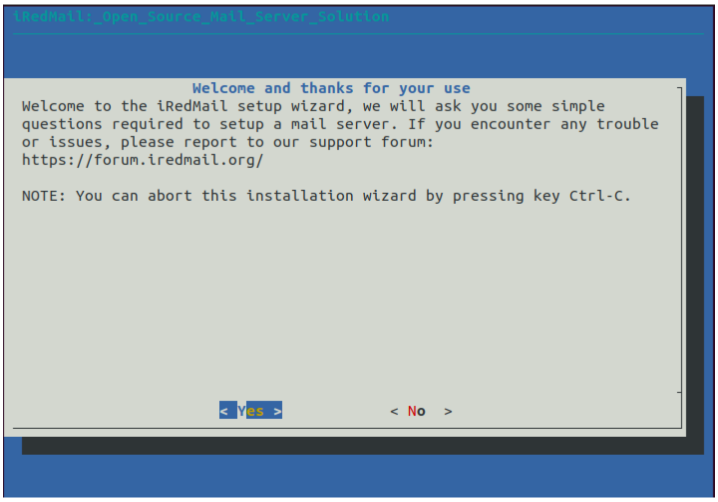
- To view the changes, log back in and run the following command to view your hostname

```
hostname -f
```

Next, we will proceed to install IRedMail and configure it as we are most interested in, the download and execution of the application will be carried out by executing the following commands in order (download the latest version available):

```
wget https://github.com/iredmail/iRedMail/archive/1.4.2.tar.gz

tar xvf 1.4.2.tar.gz

cd iRedMail-1.4.2/

chmod +x iRedMail.sh

sudo bash iRedMail.sh
```

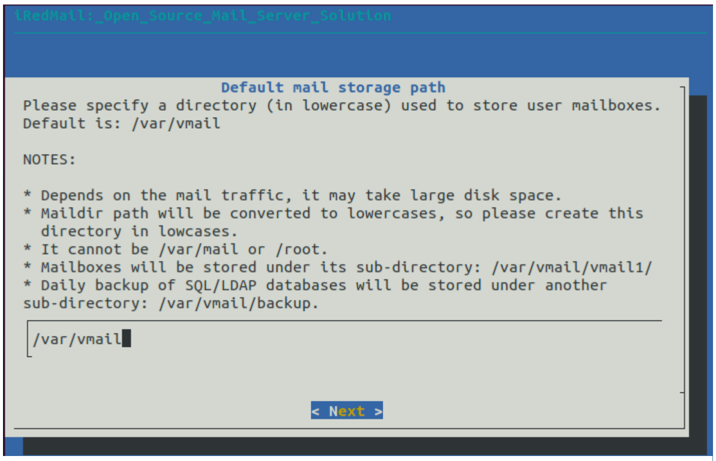
The mail server configuration wizard appears. Use the Tab key to select Yes and press Enter.



```
iRedMail: Open Source Mail Server Solution

                         Welcome and thanks for your use
  Welcome to the iRedMail setup wizard, we will ask you some simple
  questions required to setup a mail server. If you encounter any trouble
  or issues, please report to our support forum:
  https://forum.iredmail.org/

  NOTE: You can abort this installation wizard by pressing key Ctrl-C.
```

Figure 12: IRedMail first screen

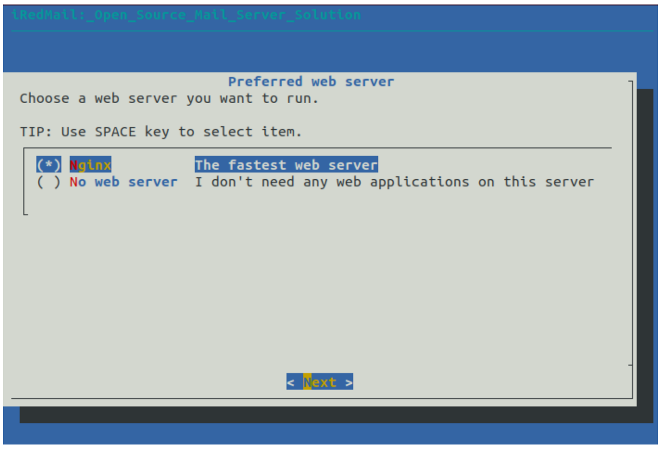
The next screen will ask you to select the mail storage path. You can use the default***,*** ***/var/vmail***, so just press Enter.



```
iRedMail: Open Source Mail Server Solution

                         Default mail storage path
  Please specify a directory (in lowercase) used to store user mailboxes.
  Default is: /var/vmail

  NOTES:

  * Depends on the mail traffic, it may take large disk space.
  * Maildir path will be converted to lowercases, so please create this
    directory in lowcases.
  * It cannot be /var/mail or /root.
  * Mailboxes will be stored under its sub-directory: /var/vmail/vmail1/
  * Daily backup of SQL/LDAP databases will be stored under another
  sub-directory: /var/vmail/backup.

   /var/vmail
```

Figure 13:IRedMail path

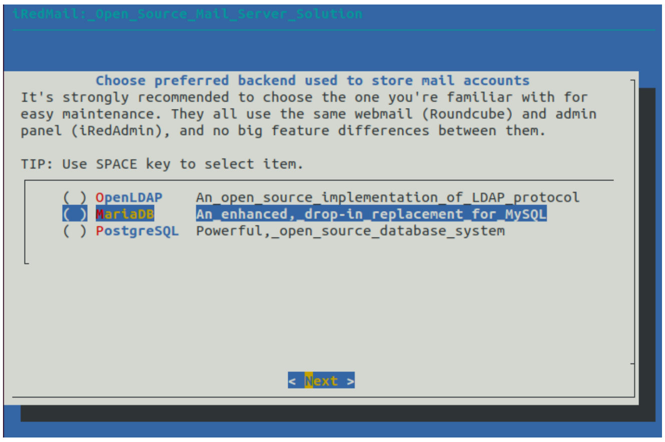
Next, choose whether you want to run a web server. It is highly recommended that you choose
to run a web server because it will later allow us to add email accounts by accessing the web admin panel.
Additionally, enabling the web server will allow you to access the Roundcube webmail. By default, the Nginx web server is selected, so you can simply press Enter.



```
iRedMail:_Open_Source_Mail_Server_Solution

                    Preferred web server
Choose a web server you want to run.

TIP: Use SPACE key to select item.

 (*) Nginx          The fastest web server
 ( ) No web server  I don't need any web applications on this server

                          < Next >
```

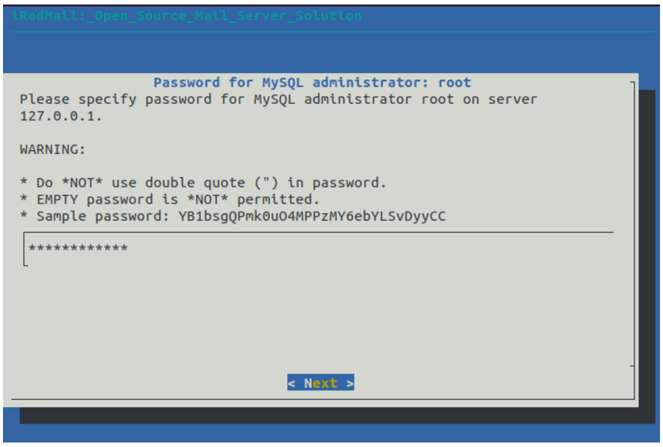
Figure 14:IRedMail server

Next, select the storage backend for the email accounts, in the campaign we used MariaDB which is highly recommended, then we will be asked to set a password to access the database.



```
iRedMail:_Open_Source_Mail_Server_Solution

         Choose preferred backend used to store mail accounts
It's strongly recommended to choose the one you're familiar with for
easy maintenance. They all use the same webmail (Roundcube) and admin
panel (iRedAdmin), and no big feature differences between them.

TIP: Use SPACE key to select item.

    ( ) OpenLDAP     An_open_source_implementation_of_LDAP_protocol
    ( ) MariaDB      An_enhanced,_drop-in_replacement_for_MySQL
    ( ) PostgreSQL   Powerful,_open_source_database_system

                          < Next >
```

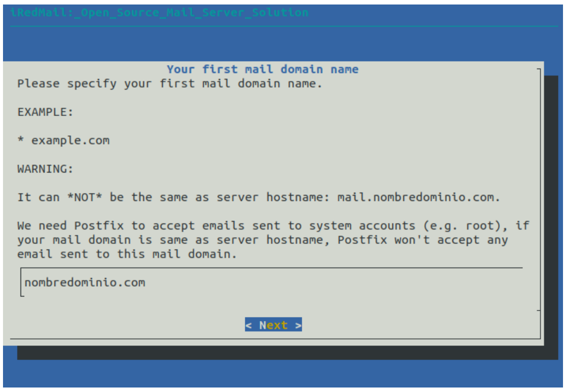
Figure 16:IRedMail DataBase



```
iRedMail:_Open_Source_Mail_Server_Solution

             Password for MySQL administrator: root
Please specify password for MySQL administrator root on server
127.0.0.1.

WARNING:

* Do *NOT* use double quote (") in password.
* EMPTY password is *NOT* permitted.
* Sample password: YB1bsgQPmk0uO4MPPzMY6ebYLSvDyyCC

 ************

                          < Next >
```

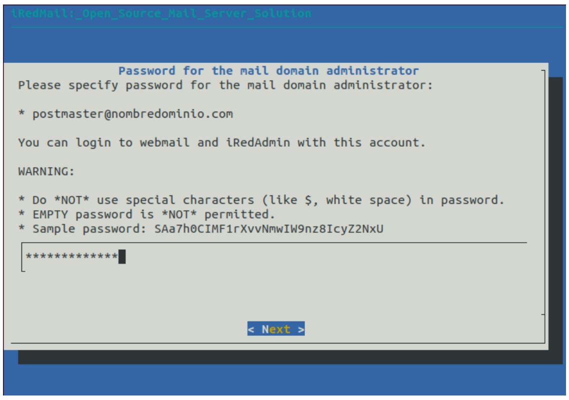
Figure 15:IRedMail DataBase password

After selecting the database type, enter your first mail domain. You can add additional mail domains later in the administration panel.
As the goal is to eventually use ***ejemplo@nombredominio.com*** style email addresses we will add ***nombredominio.com*** in the configuration panel.
Next we will be asked to add a password for our mail administrator account, this account will be ***postmaster@nombredominio.com*** style and you will need to add a password following the conditions specified by the IRedMail installer.



```
iRedMail:_Open_Source_Mail_Server_Solution

                    Your first mail domain name
Please specify your first mail domain name.

EXAMPLE:

* example.com

WARNING:

It can *NOT* be the same as server hostname: mail.nombredominio.com.

We need Postfix to accept emails sent to system accounts (e.g. root), if
your mail domain is same as server hostname, Postfix won't accept any
email sent to this mail domain.

 nombredominio.com

                              < Next >
```

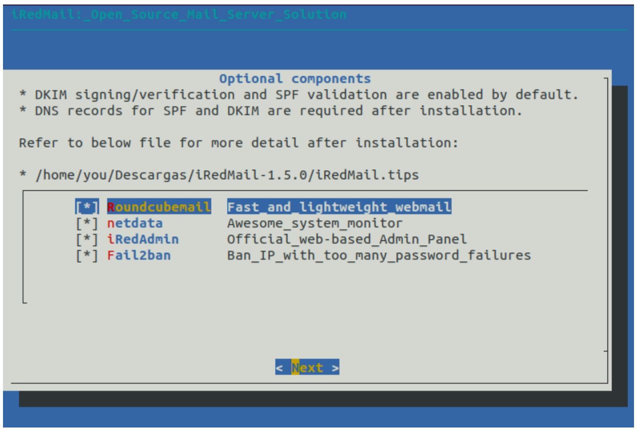
Figure 18:IredMail Domain



```
iRedMail:_Open_Source_Mail_Server_Solution

               Password for the mail domain administrator
Please specify password for the mail domain administrator:

* postmaster@nombredominio.com

You can login to webmail and iRedAdmin with this account.

WARNING:

* Do *NOT* use special characters (like $, white space) in password.
* EMPTY password is *NOT* permitted.
* Sample password: SAa7h0CIMF1rXvvNmwIW9nz8IcyZ2NxU

 *************

                              < Next >
```

Figure 17:IredMail Domain password

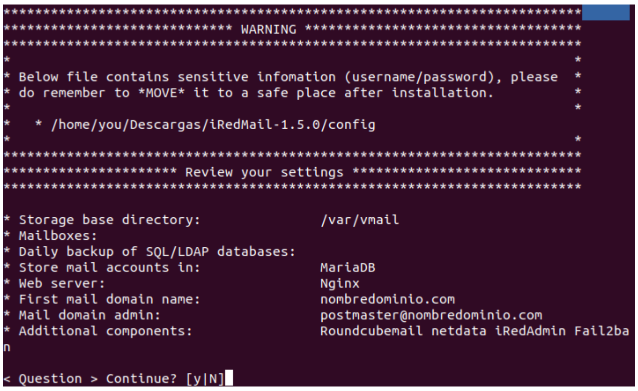
Finally, we select the optional components for our mail server, check all the available boxes:



```
iRedMail:_Open_Source_Mail_Server_Solution

                        Optional components
* DKIM signing/verification and SPF validation are enabled by default.
* DNS records for SPF and DKIM are required after installation.

Refer to below file for more detail after installation:

* /home/you/Descargas/iRedMail-1.5.0/iRedMail.tips

       [*] Roundcubemail  Fast_and_lightweight_webmail
       [*] netdata        Awesome_system_monitor
       [*] iRedAdmin      Official_web-based_Admin_Panel
       [*] Fail2ban       Ban_IP_with_too_many_password_failures

                              < Next >
```

Figure 19:IredMail extra components

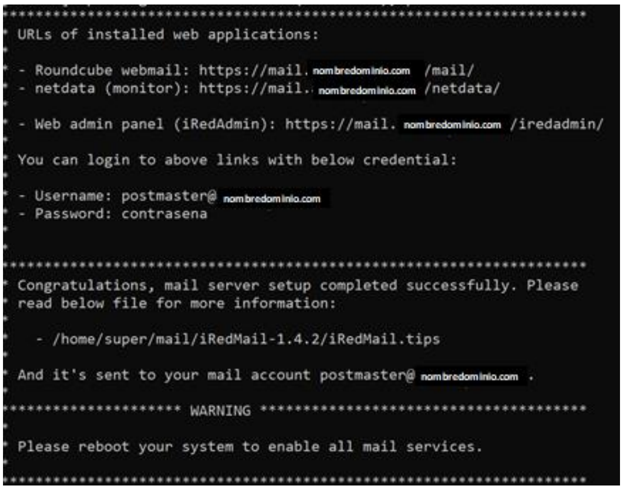
When we have all the parameters configured, we will have at our disposal a panel to check all the server configurations, we select continue if we are satisfied with the configuration (we also give to continue to the other options that appear later).



```
*************************************************************************
***************************** WARNING ***********************************
*************************************************************************
*                                                                       *
* Below file contains sensitive infomation (username/password), please  *
* do remember to *MOVE* it to a safe place after installation.          *
*                                                                       *
*   * /home/you/Descargas/iRedMail-1.5.0/config
*                                                                       *
*************************************************************************
********************** Review your settings *****************************
*************************************************************************

* Storage base directory:               /var/vmail
* Mailboxes:
* Daily backup of SQL/LDAP databases:
* Store mail accounts in:               MariaDB
* Web server:                           Nginx
* First mail domain name:               nombredominio.com
* Mail domain admin:                    postmaster@nombredominio.com
* Additional components:                Roundcubemail netdata iRedAdmin Fail2ba
n

< Question > Continue? [y|N]
```

Figure 20:Configuration Resume

The iRedMail installation is now complete. You will be notified of the webmail URL and the web administration panel, as well as the login credentials.



```
********************************************************************
* URLs of installed web applications:
*
* - Roundcube webmail: https://mail.nombredominio.com /mail/
* - netdata (monitor): https://mail.nombredominio.com /netdata/
*
* - Web admin panel (iRedAdmin): https://mail.nombredominio.com /iredadmin/
*
* You can login to above links with below credential:
*
* - Username: postmaster@nombredominio.com
* - Password: contrasena
*
*
********************************************************************
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
*
*   - /home/super/mail/iRedMail-1.4.2/iRedMail.tips
*
* And it's sent to your mail account postmaster@nombredominio.com .
*
******************** WARNING **************************************
*
* Please reboot your system to enable all mail services.
*
********************************************************************
```

Figure 21:IredMail installation confirmation

After configuring our server, we will restart our machine for the changes to take effect. We can access the administration website by accessing the following web address:

```
https://mail.nombredominio.com/iredadmin/
```

3.3.2. Gopish

For the creation and monitoring of our phishing campaign we will use the Gophish service, free software which has many utilities that will help us to carry out the complete campaign. This application consists of an administration server which we can access locally and also gives us the possibility of hosting the pages dedicated to phishing.

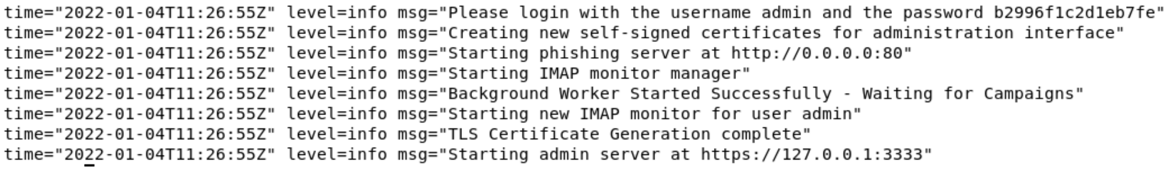
(For more information -> Gophish - Open Source Phishing Framework (getgophish.com)).

The steps to use this tool will be explained below:

To install GoPhish and start using GoPhish, download the latest version via command console, then unzip the zip file and run the binary:

```
wget https://github.com/gophish/gophish/releases/download/v0.11.0/gophish-v0.11
.0-linux-64bit.zip/


unzip gophish-v0.11.0-linux-64bit.zip


chmod +x gophish


./gophish
```

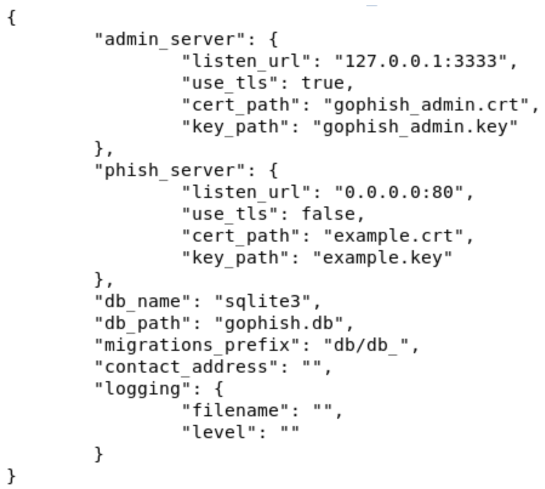
Once the program is running, the terminal will display the credentials to access the administrator panel for the first time, and the URL addresses where the administration client has been set up and where the users affected by the campaign will access.



```
time="2022-01-04T11:26:55Z" level=info msg="Please login with the username admin and the password b2996f1c2d1eb7fe"
time="2022-01-04T11:26:55Z" level=info msg="Creating new self-signed certificates for administration interface"
time="2022-01-04T11:26:55Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2022-01-04T11:26:55Z" level=info msg="Starting IMAP monitor manager"
time="2022-01-04T11:26:55Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2022-01-04T11:26:55Z" level=info msg="Starting new IMAP monitor for user admin"
time="2022-01-04T11:26:55Z" level=info msg="TLS Certificate Generation complete"
time="2022-01-04T11:26:55Z" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

Figure 22:First time GoPhish

These addresses can be changed in the config.json configuration file that you will find with the other files that come with the GoPhish download. In this file we can also add the TLS certificates to use on our web pages, which is discussed later.



```
{
        "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": ""
        }
}
```

Figure 23:GoPhish config.json

We can see that the landing page will be accessible by any petition to the port 80 of the machine, can be to the local ip address or the external ip address. The admin server is only running in the local host interface.

Access the administration url (127.0.0.1) and change the default password:

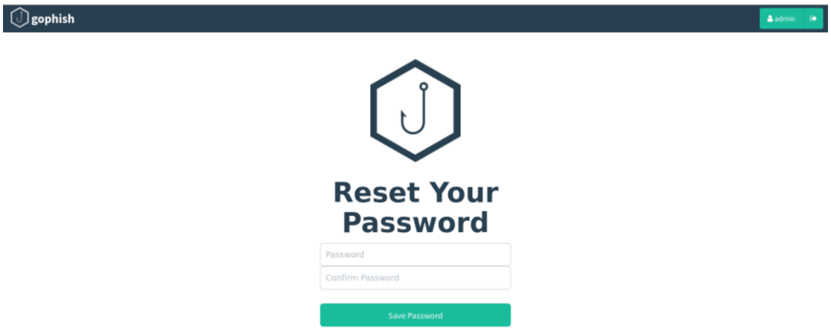
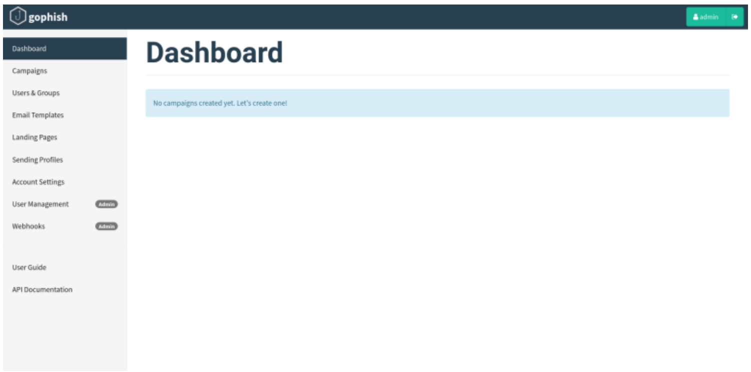


Figure 24:GoPhish reset password



Dashboard

No campaigns created yet. Let's create one!

Figure 25:GoPhish acces

3.3.3. Configuration of the necessary protocols

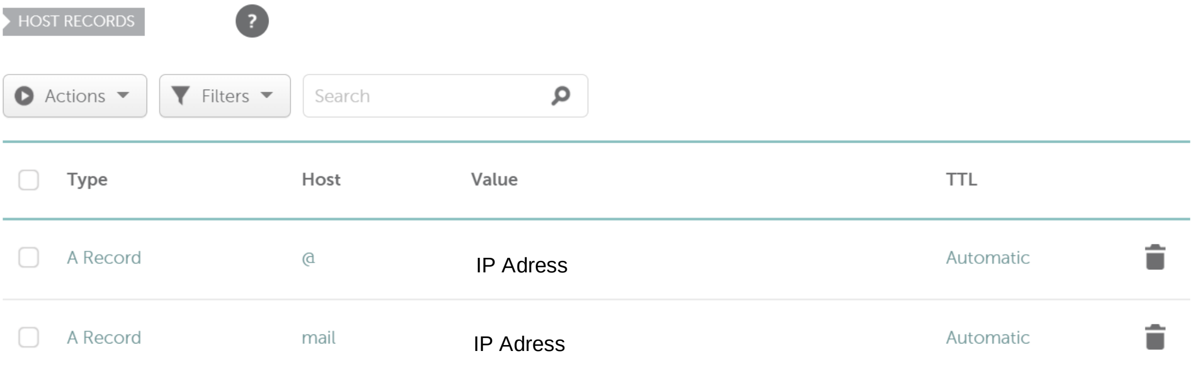
Once an SMTP server has been created and has access to the internet, we will proceed to correctly configure all the necessary protocols to be able to use our server to send emails, and that these can pass most of the requirements imposed by the anti-spam filters used by companies to avoid possible malicious emails.

The corresponding DNS records must be added to the acquired domain so that they relate the IP of the server with the domain address.

Then the reverse DNS resolution, DMARC protocol, SPF and DKIM have to be configured. In the process that the anti-spam services follow, the first thing they check is that the reverse resolution of the ip that the mail domain has is the same as the one that sends the mail. Then they check the reputation of the domain sending the mail, if they are signed by the DKIM public key and if they have a TLS certificate. All this is covered by the aforementioned protocols.

3.3.4. Basic configuration (A, MX, Reverse DNS)

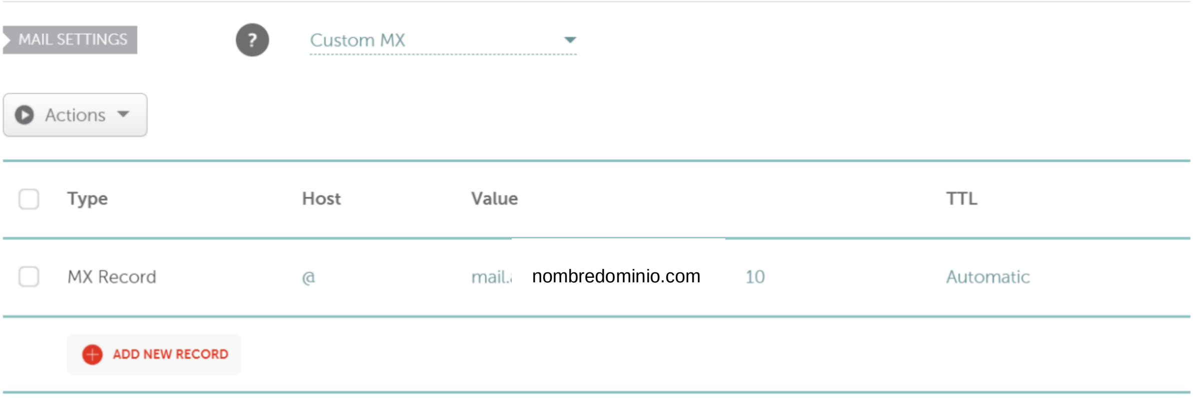
First, we will have to make a basic configuration of the DNS of our domain to be able to associate the ip address of our server with the domain name, for that we add A record with host (@) which indicates that we associate the address ***nombredominio.com*** with the ip indicated and we add a record for mail, so you can access the smtp server using the address ***mail@nombredominio.com***.



□	Type	Host	Value	TTL	
□	A Record	@	IP Adress	Automatic	🗑
□	A Record	mail	IP Adress	Automatic	🗑

Figure 26:Basic DNS Records

The MX record is a special type of DNS record that serves only for e-mail communication. MX stands for "Mail Exchanger" and is a prerequisite when setting up the mail server. In other words, if the goal is to host an email server, then your DNS server must have an MX record pointing to that email server. So we will add an MX record to our DNS, this will point to the address ***mail.nombredominio.com***, with the host value @.



MAIL SETTINGS ? Custom MX

□ Type	Host	Value		TTL
□ MX Record	@	mail.nombredominio.com	10	Automatic

Figure 27:Adding MX record

After configuring our DNS records for the domain, we would have to set up the reverse DNS to avoid some of the techniques used by anti-spam services to block emails.

A reverse DNS lookup, sometimes also known as a reverse IP lookup is a type of DNS lookup request which does the opposite of the much more common forward lookup. A forward lookup will convert a domain name like www.example.com into an IP address like 192.0.2.1, while a reverse lookup will convert an IP address back into a domain name.

Reverse DNS records are not required to be configured for DNS to function correctly, and forward and reverse DNS records do not even have to agree with each other - but if they do, then this is referred to as a forward-confirmed reverse DNS.

Reverse DNS records are not stored with other DNS records for the domain name they are for, but instead are stored on the special .arpa domain name. The DNS record type used for reverse DNS is known as a PTR record, short for a Pointer record.

A records live under the .in-addr.arpa. An example PTR record for our domain may look like the following:

1.2.168.192.in-addr.arpa.   PTR   nombredominio.com   3600

3.3.5. SPF

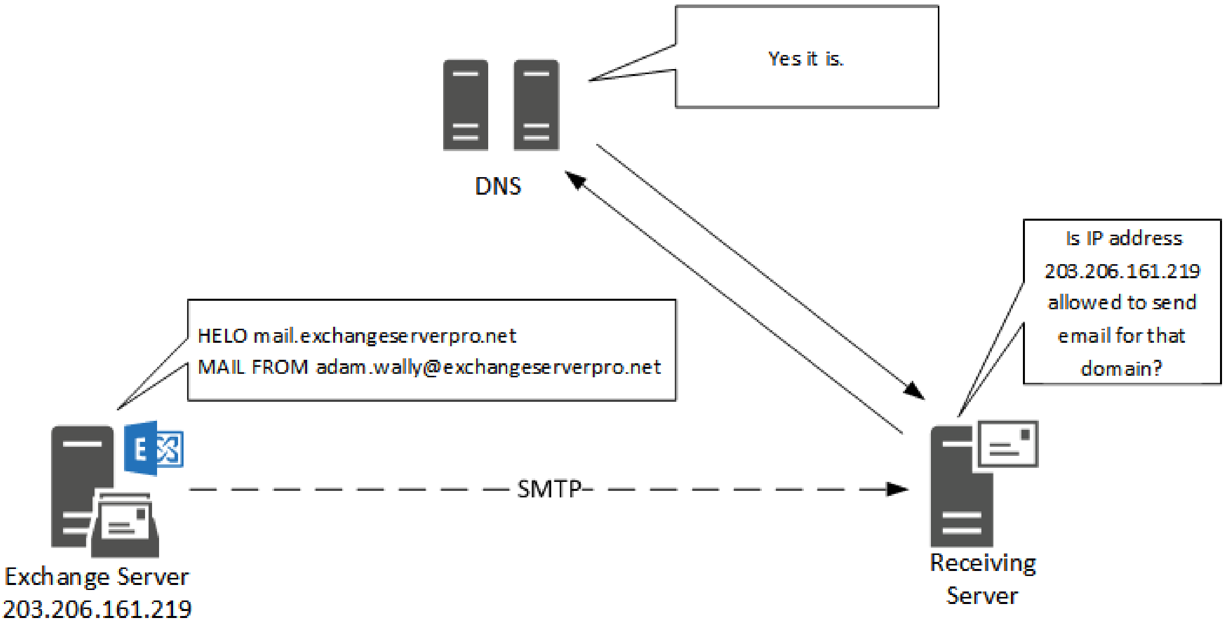

Yes it is.
DNS
Is IP address 203.206.161.219 allowed to send email for that domain?
HELO mail.exchangeserverpro.net
MAIL FROM adam.wally@exchangeserverpro.net
SMTP
Exchange Server
203.206.161.219
Receiving Server

Figure 28:SMTP diagram

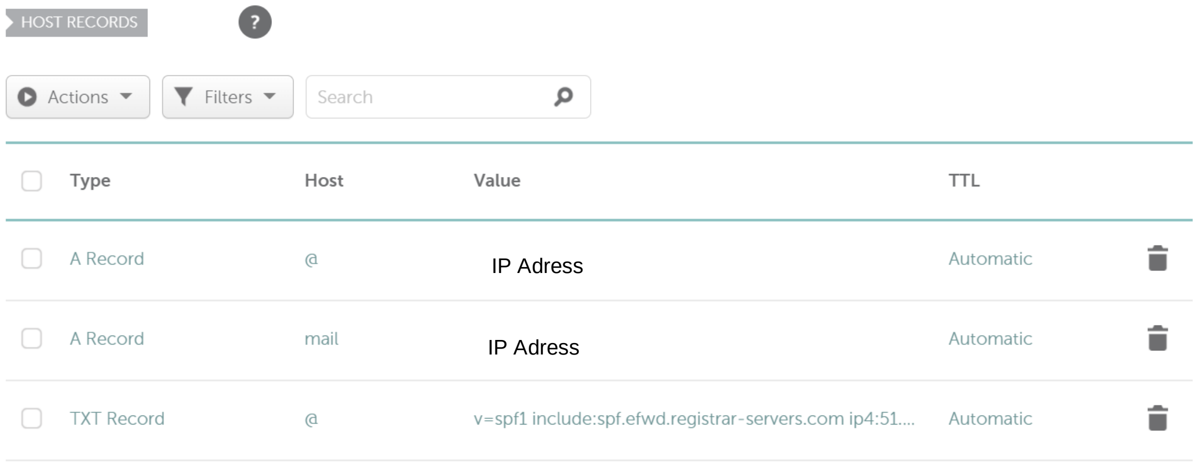
SPF is an acronym for Sender Policy Framework. It describes a method of verifying whether a sender is valid when accepting mail from a remote mail server or email client. An SPF check involves verifying the email address the sender is using to send from, and the IP address they connect to the SMTP service with. SPF uses the sender's domain to retrieve a TXT DNS record (basically a small text snippet) that describes which IP addresses the domain sends on. The retrieved record is then compared against the connecting IP address and if it matches then the sender is determined to be valid; otherwise it indicates that the sender is impersonating the sending domain.

In basic terms, Sender Policy Framework (SPF) is a method of detecting when an email sender is forging their sender address. It does this by confirming with the senders alleged domain (via DNS lookups) as to whether the connecting IP address, or other details, are valid. For example, if a spammer was sending emails as greatdeals@hotmail.com, a lookup is done for SPF details against the hotmail.com domain. Information returned from this lookup could determine that since the IP address of the spammer is not Hotmail IP address then it is likely to be spam. Email can then be marked as likely spam, or not accepted.

In order to configure SPF in our SMTP server we will have to add a TXT record with the following information in our DNS configuration, this will make that only the hosts defined in the SPF record are the ones enabled to send email, that is to say, the only hosts allowed are the ones that come from the server's ip.

To authorize Namecheap Email Forwarding to send emails on your behalf you will have to include it in your SPF record. The SPF record mechanism used is shown below.

v=spf1 include:spf.efwd.registrar-servers.com ip4:51.254.199.123 ~all



HOST RECORDS ?

Actions ▾ | Filters ▾ | Search

□	Type	Host	Value	TTL	
□	A Record	@	IP Adress	Automatic	🗑
□	A Record	mail	IP Adress	Automatic	🗑
□	TXT Record	@	v=spf1 include:spf.efwd.registrar-servers.com ip4:51....	Automatic	🗑

Figure 29:Adding SMTP

3.3.6. DKIM

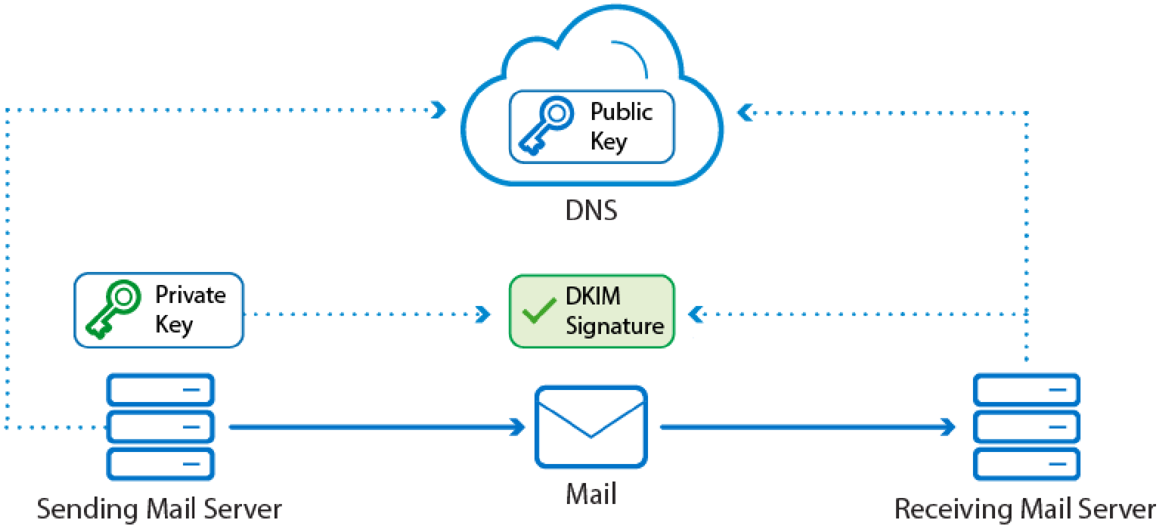


Figure 30:DKIM Diagram

DKIM allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. It achieves this by affixing a digital signature, linked to a domain name, to each outgoing email message. The recipient system can verify this by looking up the sender's public key published in the DNS. A valid signature also guarantees that some parts of the email (possibly including attachments) have not been modified since the signature was affixed.

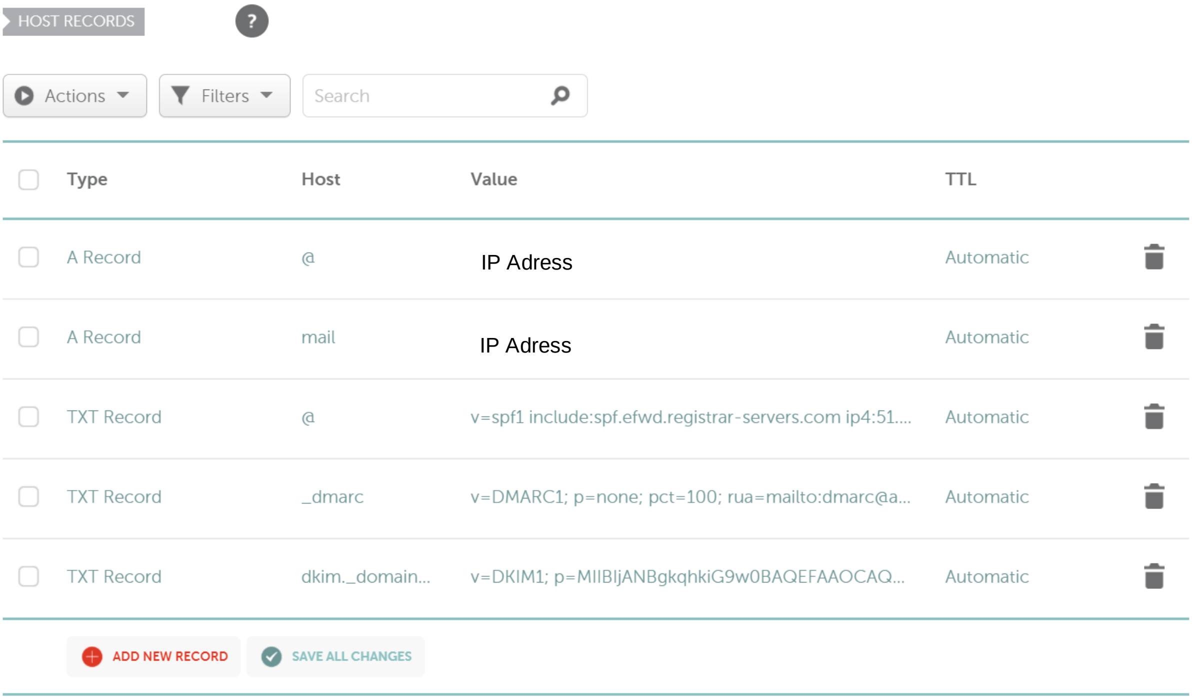
Thanks to IRedMail, the DKIM authentication has been done automatically on our server. The only thing left to do is to create the DKIM record in the DNS manager. Run the following command to display the DKIM public key:

```
sudo amavisd-new showkeys
```

The public key will appear between double quotes, which we will have to add in our DNS by using a text record.

Example of a DKIM public key:

***“v=DKIM1;
p=MIIBIjBBBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuLClvnWkfV1aRgzzA
MKXUQIo8drG54rah+ZwuYvOXWyREqwD5Ab2GgGMUJqt81rUb4dhpCF42DtKwsb5
ty0ioRh7H7q0beBdremZRzbK7Ame9+FlIGDRnjObzDsDbLENvQ7/EvR2yLo/NXtzwD
1x64dyAMEuwMEvoxPkUl755MR1/dPV35m50XZ5Hq67bhjr4ZQr/aonr5jxKTkXsctcy
DtNWpPXIyCky6/SDZJAV6fmabGbBDfsuK4XoJX3+BMh07XViBK3LhdGkajI3aW9yjP
wqzLnC2GYIinD3DTv1W9FlWDkHtbFjao0qsV+9P8rXuhYWBJvJfnALoFH+moKdwID
AQAB”***



☐ Type	Host	Value	TTL	
☐ A Record	@	IP Adress	Automatic	🗑
☐ A Record	mail	IP Adress	Automatic	🗑
☐ TXT Record	@	v=spf1 include:spf.efwd.registrar-servers.com ip4:51....	Automatic	🗑
☐ TXT Record	_dmarc	v=DMARC1; p=none; pct=100; rua=mailto:dmarc@a...	Automatic	🗑
☐ TXT Record	dkim._domain...	v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ...	Automatic	🗑

Figure 31:Adding DKIM

3.3.7. DMARC

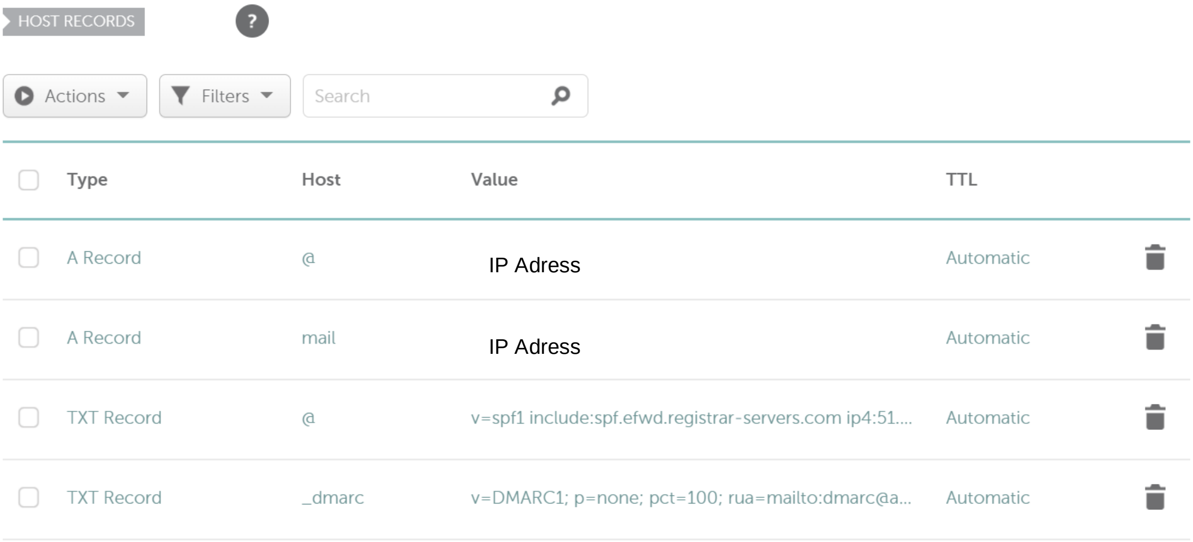
DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing.

The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails, email scams and other cyber threat activities.

For the same reason, our SMTP server must have correctly configured DMARC authentication in order to be able to pass the companies' anti-spam systems, which would discard our mail because they interpret that the domain nombredominio.com has been used in an unauthorized manner.

To correctly configure the DMARC protocol on our server, we must add a text record with the following information in our DNS:

v=DMARC1; p=none; pct=100; rua=mailto:dmarc@nombredominio.me



□	Type	Host	Value	TTL
□	A Record	@	IP Adress	Automatic
□	A Record	mail	IP Adress	Automatic
□	TXT Record	@	v=spf1 include:spf.efwd.registrar-servers.com ip4:51....	Automatic
□	TXT Record	_dmarc	v=DMARC1; p=none; pct=100; rua=mailto:dmarc@a...	Automatic

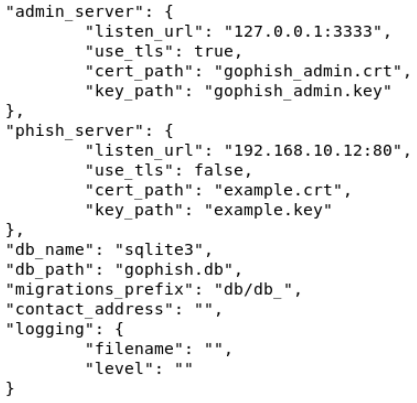
Figure 32:Adding DMARC

3.4. Publishing HTTP Service

When publishing our website and the different services of the external server, we must differentiate the case of when our server has a firewall that acts as an intermediary for the requests we receive and when it does not. It is recommended to have this because we do not want to have services such as GoPhish exposed directly to the Internet, which could be the target of attacks by third persons.

1 – With Firewall

As good configuration practices it is recommended to have an intermediary proxy which receives requests from the internet and redirects the traffic to the internal ports of the server where the servers are up, for example redirecting the traffic of users trying to access port 443, to the internal port of the server.



```
"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": "192.168.10.12:80",
        "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": ""
}
```

Figure 33:GoPhish config.json 2

The interesting thing is to redirect the incoming traffic destined to users who want to access the landing page to the internal port 80 of the server which is the one set in the GoPhish configuration (example in the picture). The same would be done for requests to the mail server.

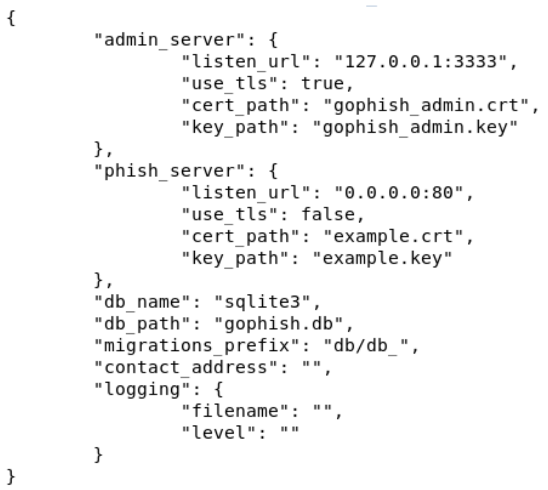
To redirect the traffic, we can use the ***iptables*** firewall rules, an example of this would be the following:

# All traffic that comes from the outside and goes to port 80 (if we use https for our website the port will be 443) we redirect it to an internal machine, in this case to the address of our server (for this example suppose that the internal ip of the sever is 192.168.10.12).

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.10
.12:80
```

2 – Without firewall

In the case of not having any traffic filtering system our server will expose its servers to the internet, so in the configuration shown the landing page will be accessible by any user who makes a request to the public ip by port 80 of our server.



```
{
        "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": ""
        }
}
```

Figure 34:GoPhish config.json 3

3.5. <u>TLS Certificate</u>

A key point to ensure greater success in our phishing campaign would be to provide our website and our mail server with a valid TLS certificate. If we do not configure it, a self-signed certificate would be used which would make the alarms go off by the browsers making users see that they are about to enter an insecure page.

For that reason, we will request a valid certificate to add to our server, this we will do through **Let's Encrypt TLS certificate**. The first thing we must do is install the Let's Encrypt client using the following commands:

```
sudo apt install software-properties-common

sudo add-apt-repository ppa:certbot/certbot -y

sudo apt install certbot -y
```

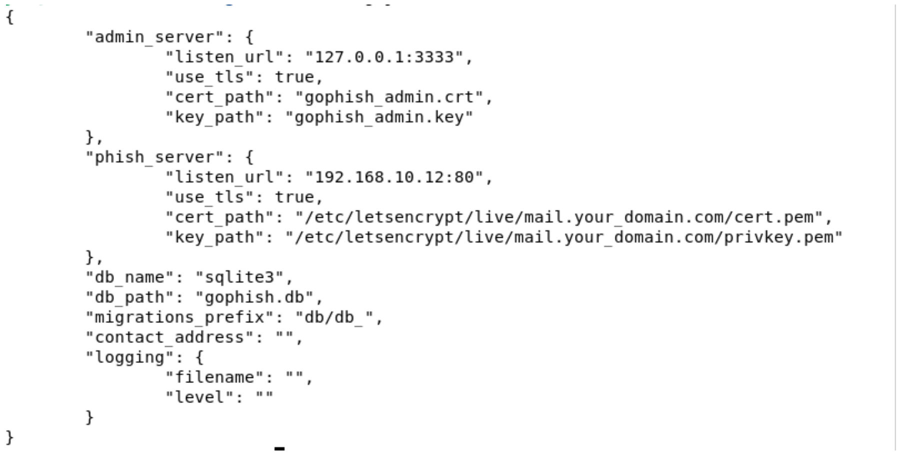
Once we have installed the client on our server, we will request the certificate using the following command:

```
sudo certbot certonly --webroot --agree-tos --email postmaster@example.com -d
mail.nombredominio.com -w /var/www/html/
```

If the commands have been executed without any error, we should find what is necessary to use TLS certificate in the path ***/etc/letsencrypt/live/mail.your-domain.com/***

3.5.1. Putt TLS certificate in GoPhish web server

To use the TLS certificate in the web pages deployed for the phishing campaign we will have to edit the config.json file, adding the paths from where our certificates are hosted, and change the value of the variable "use_tls" to true, with this we will specify in GoPhish where to obtain the TLS certificate to use.



```
{
        "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": "192.168.10.12:80",
                "use_tls": true,
                "cert_path": "/etc/letsencrypt/live/mail.your_domain.com/cert.pem",
                "key_path": "/etc/letsencrypt/live/mail.your_domain.com/privkey.pem"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}
```

Figure 35:GoPhish config.json 4

3.6. Dealing with companies antispam

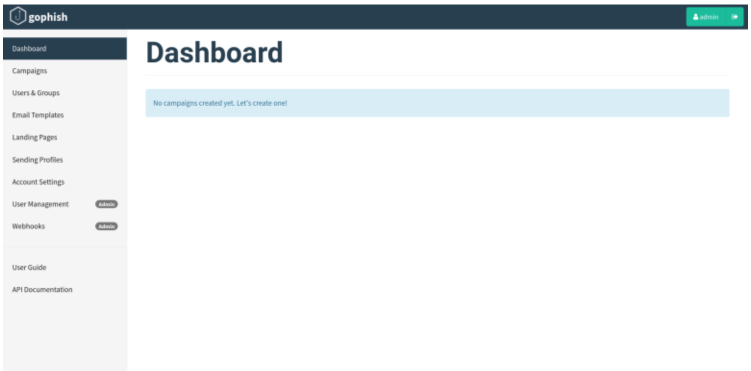
During the course of the project, we carried out different tests of sending emails to the targets of the company, and we had a number of problems, these were solved by communicating with those in charge of managing the anti-spam services of the company, we asked them to add our created domain to domains allowed to send emails, so that it was not rejected. The service managers told us that the emails were being rejected mainly for two reasons. The first was the reputation of the domain, being this newly created its score was low, therefore this factor will have to be taken into account in future campaigns and try that the domain is acquired prior to the campaign and go making periodic shipments to go up to the reputation of this (you can use this website to check the reputation of your domain Domain Reputation Check Tool | IPVoid.).

Another point that they stressed to us was that it was not possible to perform reverse DNS resolution of the emails that were being received due to a bad configuration of the DNS reverse resolution, we can use this page to check that we have correctly configured all the previously defined protocols. https://www.mail-tester.com/

During the campaign we spent weeks commenting with those responsible for the anti-spam the situation, and after many tests and the aggregation of different rules in the anti-spam services, it was possible to send emails and that these were received by the employees.

3.7. Creation of the phishing campaign

After having configured the entire infrastructure we will proceed to explain how to use GoPhish to create and monitor our campaign.



Dashboard

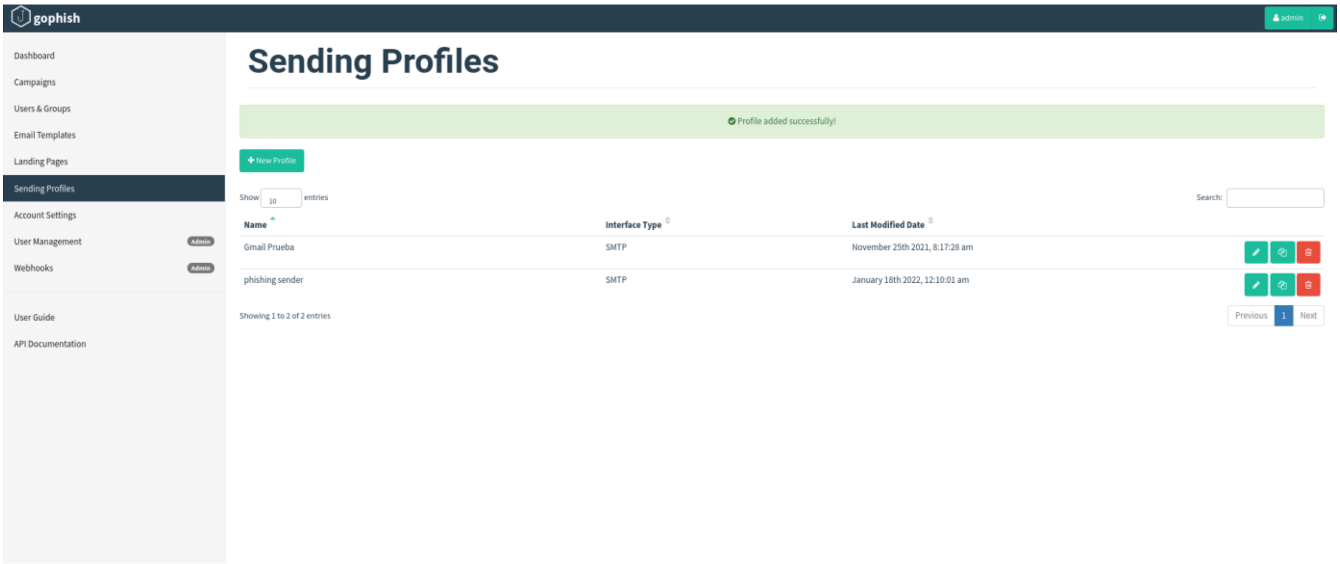
No campaigns created yet. Let's create one!

Figure 36:GoPhish Dashboard

In the image the control panel is shown, we will have to create the different sections to use them as parameters of our phishing campaign.

3.7.1. Domain

To make GoPhish use the created mail server you will have to configure the Sending Profile section, in this the email address that will send the email will be added (the address should be of this style ***example@nombredominio.com***) and you will also have to add who is the host of the SMPT server that will be in charge of managing the shipment (the address should be of this style ***mail.nombredominio.com***), once we have this profile created, we save it and we can use it in the campaign. We will also have the opportunity to send a test email to test that the SMTP server works correctly.



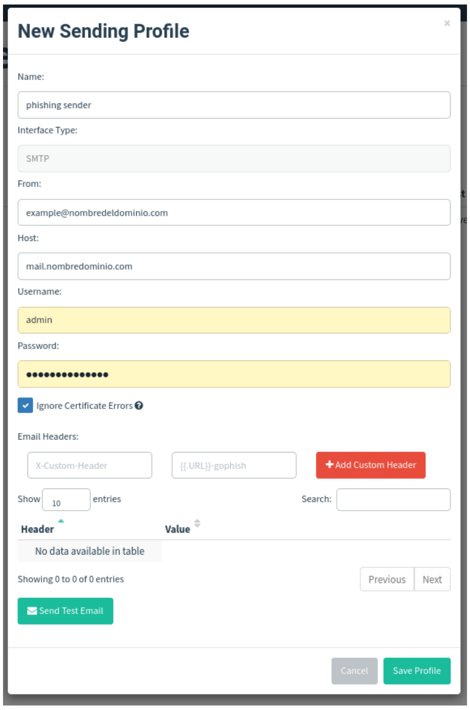
Sending Profiles

Profile added successfully!

Name	Interface Type	Last Modified Date
Gmail Prueba	SMTP	November 25th 2021, 8:17:28 am
phishing sender	SMTP	January 18th 2022, 12:10:01 am

Showing 1 to 2 of 2 entries

Figure 37:GoPhish Sending Profiles



New Sending Profile

Name: phishing sender

Interface Type: SMTP

From: example@nombredeldominio.com

Host: mail.nombredominio.com

Username: admin

Password: ••••••••••••••

☑ Ignore Certificate Errors

Email Headers: X-Custom-Header {{.URL}}-gophish

Header	Value
No data available in table	

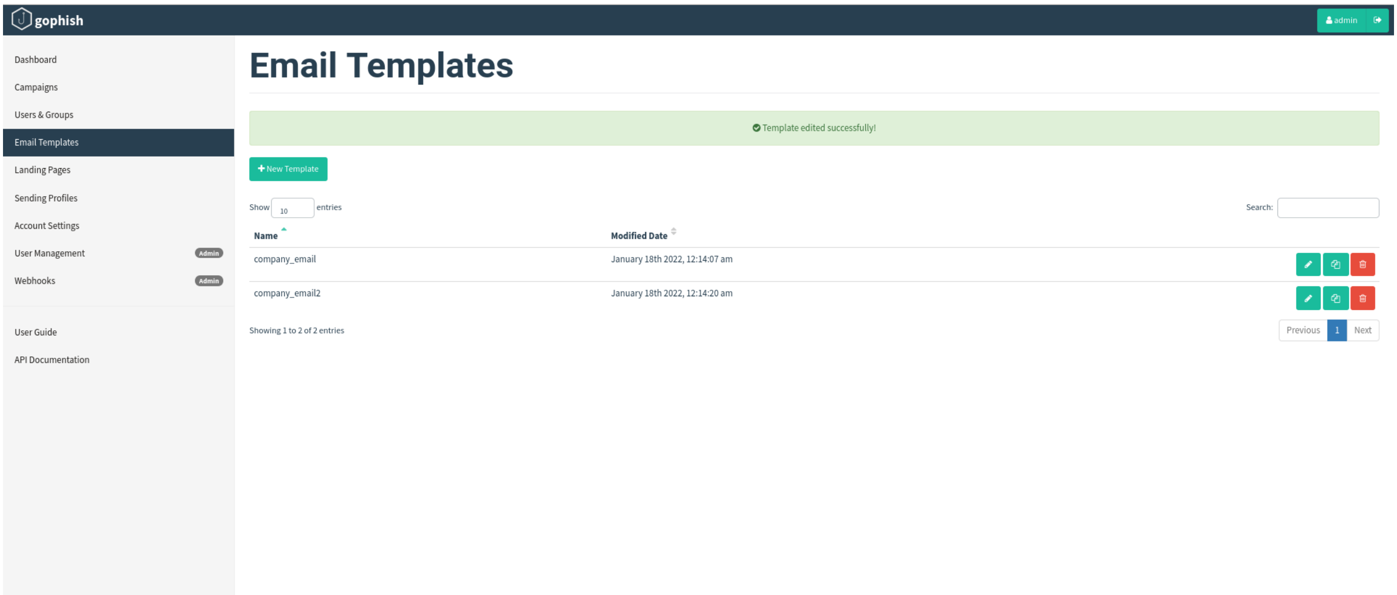
Showing 0 to 0 of 0 entries

Figure 38:New Sending Profile

3.7.2. Email Address

In the section of mail templates, we can add the mail that will be used for the realization of the campaign, it is recommended to use the mail in an html format, we can use the GoPhish code editor which will show us a preview of the added html code. Keep in mind that to add the address of the web page to which users will be redirected we can use the variable {. URL}, the program will understand that in that variable is necessary to add the web address which is specified in the section of the Landing Page. Another interesting utility that is advisable to activate is the image tracker, selecting that box you can have a control of the users who have opened the mail. It will also have some other extra functionalities, such as uploading files and being able to write which is the subject of the mail.

Once the template is created, we can save it and it will be available to use in our campaign.



Email Templates

Template edited successfully!

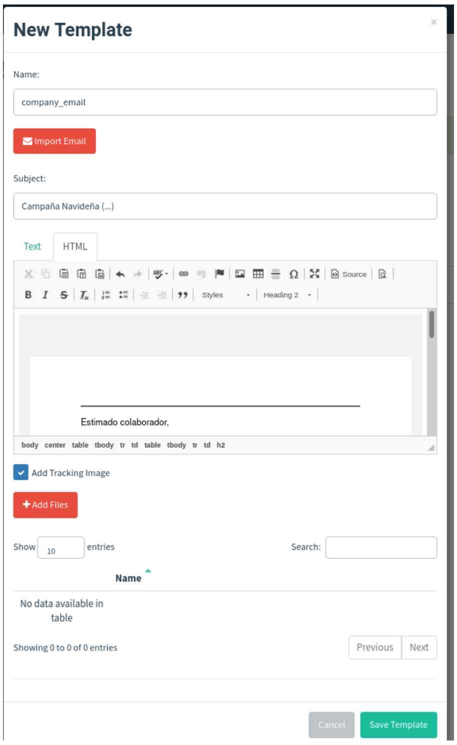
Show 10 entries

Search:

Name	Modified Date
company_email	January 18th 2022, 12:14:07 am
company_email2	January 18th 2022, 12:14:20 am

Showing 1 to 2 of 2 entries

Figure 39:GoPhish Email Templates



New Template

Name: company_email

Subject: Campaña Navideña (...)

Estimado colaborador,

☑ Add Tracking Image

Show 10 entries

Search:

Name
No data available in table

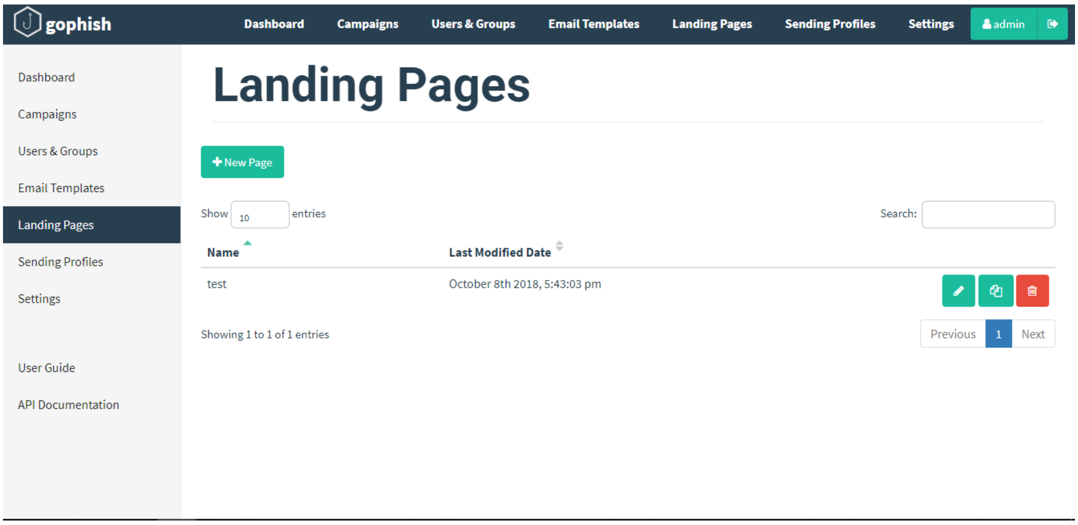
Showing 0 to 0 of 0 entries

Figure 40: New Template

3.7.3. Landing pages

In the landing pages section, we will be given the possibility to create the web pages that we consider necessary for the campaign. Similar to the editor used to create the mail template, we can create our website using html code, the GoPhish editor allows us to add basic elements and modify its characteristics, this will interpret our code and we can preview it. A highly recommended utility to use is to import web pages, this option replicates the web page you want, simply by putting the URL of this when you click on the Import Site option. Then with the code editor you can modify the page in the most convenient way you consider.

Next, the Capture Submitted Data and Capture Password check boxes will be selected to store the data that users enter on the created web page. As a complement you can select which web page users will redirect to after entering credentials, this web page may be the most convenient for the campaign, if you decide to redirect to another web page hosted by our server, we should put the Html resource under the ***static/endpoint*** directory. You can then reference them using the URL ***http[s]://phishing_server/static/filename.***



Landing Pages

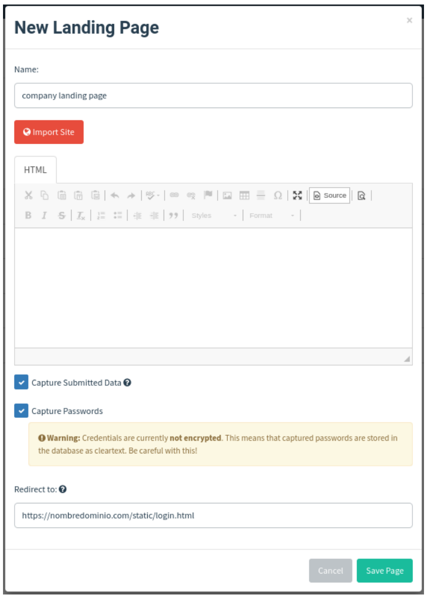
Show 10 entries

Search:

Name	Last Modified Date
test	October 8th 2018, 5:43:03 pm

Showing 1 to 1 of 1 entries

Figure 41:GoPhish Landing Page



New Landing Page

Name:

company landing page

☑ Capture Submitted Data

☑ Capture Passwords

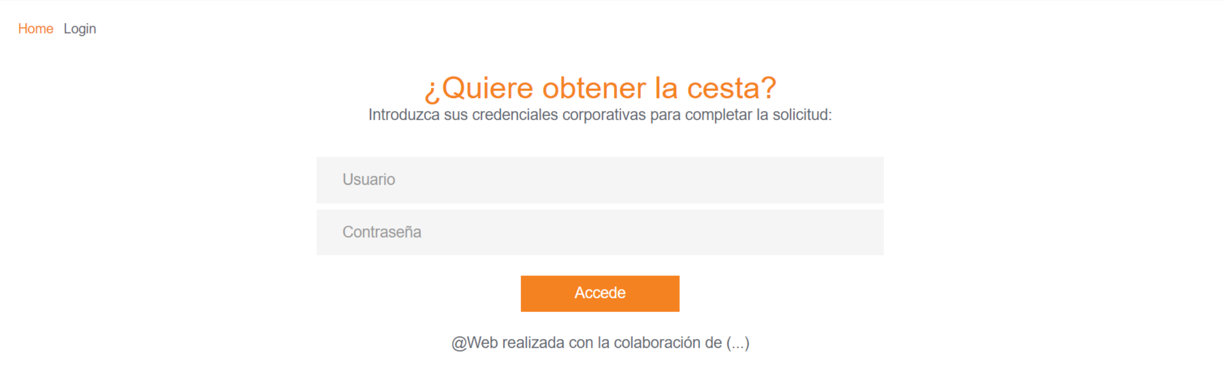
Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

https://nombredominio.com/static/login.html

Figure 42:Landing Page

In the campaign carried out, 2 web pages were created, both simulating the appearance of the company for which the drill was being carried out. The first is the main page, in this there is a login section where the victims will be encouraged to put their credentials and then a page where users who decide to put the credentials will be redirected which will simulate that the request, they have believed they have requested is being processed.

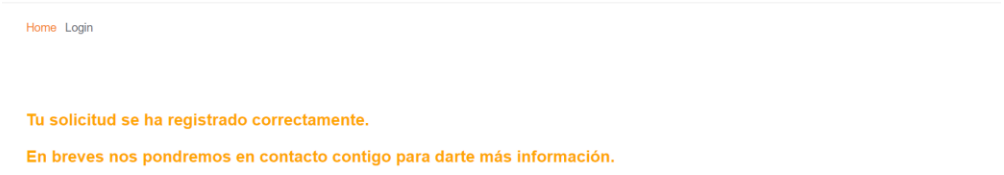


¿Quiere obtener la cesta?

Introduzca sus credenciales corporativas para completar la solicitud:

@Web realizada con la colaboración de (...)

Figure 43:Campaign Landing Page



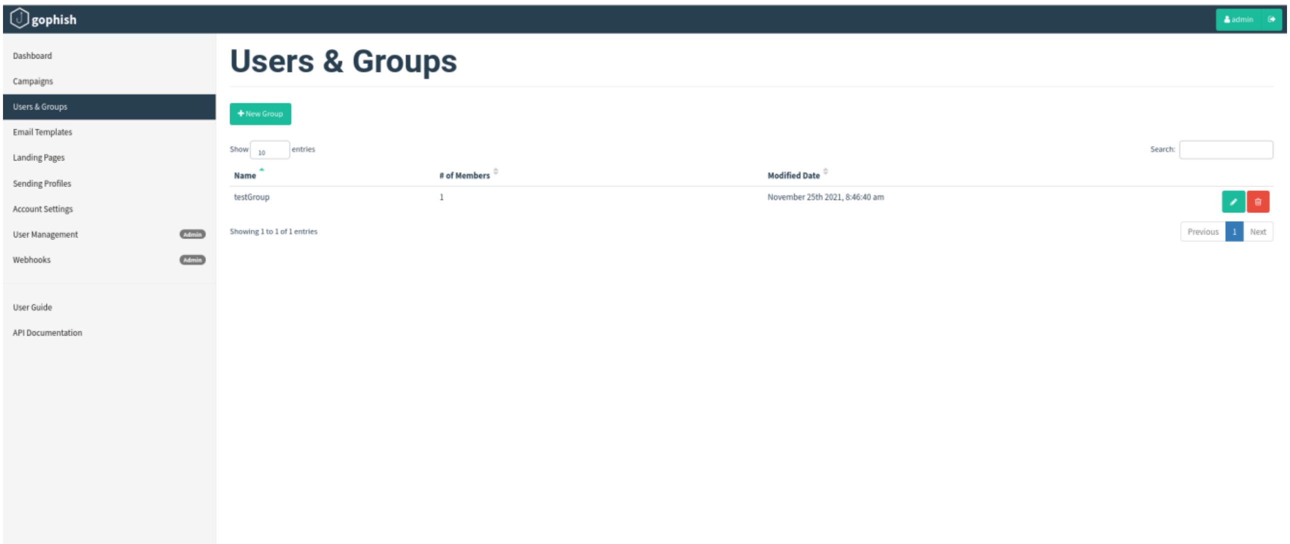
Tu solicitud se ha registrado correctamente.

En breves nos pondremos en contacto contigo para darte más información.

Figure 44:Campaign Redirect Page

3.8. Launch of the campaign

Once we have the parameters of the campaign, it will be necessary to add the objectives to which the campaign will be destined, as it is an awareness campaign the objectives will be the employees of the company that carries out the campaign, therefore it should provide a file .csv to be able to import the users affected by the campaign. This will be added in the User Groups tab.



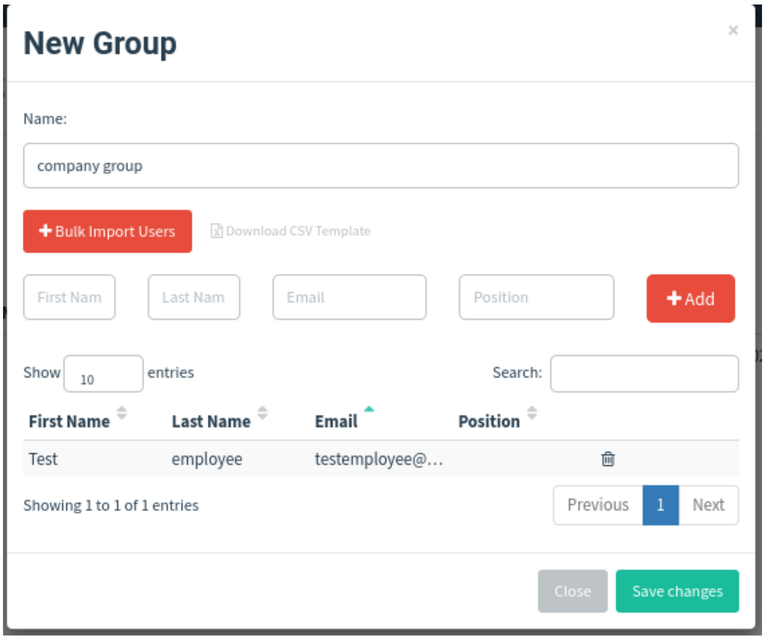
Users & Groups

Show 10 entries

Name	# of Members	Modified Date
testGroup	1	November 25th 2021, 8:46:40 am

Showing 1 to 1 of 1 entries

Figure 45:GoPhish Users&Groups



New Group

Name: company group

Show 10 entries

Search:

First Name	Last Name	Email	Position
Test	employee	testemployee@…	

Showing 1 to 1 of 1 entries

Figure 46:New Group

After having the targets of the campaign, we will proceed to create and launching the campaign.

3.8.1. How to launch the campaign

Now we will be able to launch the campaign, this is done from the Campaigns tab. In the new campaign section, we will be displayed a tab in which we can create our campaign, we will be asked to select the previously defined sections, the only section to add would be the URL, in this you have to put the address of the GoPhish listener, that is, where the phishing server is deployed as seen in the ***config.json*** file, this address must be accessible by affected users who decide to click on the link in the email. For example, if we are using TLS certificate and we have well configured the DNS of our server, we would add as an address ***https://nombredominio.com***, this would be the address added to the mail and where users would access.

First it would be recommended to launch a test campaign with a small number of users and test that everything is configured correctly and once it works launch the campaign with all users

3.8.2. How to track the campaign

Once the campaign has been launched, we can monitor the different events carried out by the users. In the Campaigns tab there is an Active Campaigns section, in this we will be shown our active campaign and if we select the statistics section, we will be told what status each user of the campaign is in:

- Email Sent: The user has received the mail
- Email Opened: The user has opened the received mail
- Clicked Link: The user has clicked on the link of the open mail

- Submitted Data: The user has entered credentials on the Landing Page (these credentials will be displayed in plain text)
- Email Reported: The user has reported as spam or possible phishing attempt the mail (for this functionality an additional configuration is needed which has not been realized for this project)

We will also have a timeline in which it will show us in a visual way at what moment each action has occurred. Once we consider that the campaign is finished, we can close it and the results of this will be archived in the Archived campaigns tab, in addition to being able to export the results of the events produced in .csv format and edit them and show the information in the way that is considered most appropriate.

With this it could be considered that the campaign has already been completed, and then the results should be analyzed.

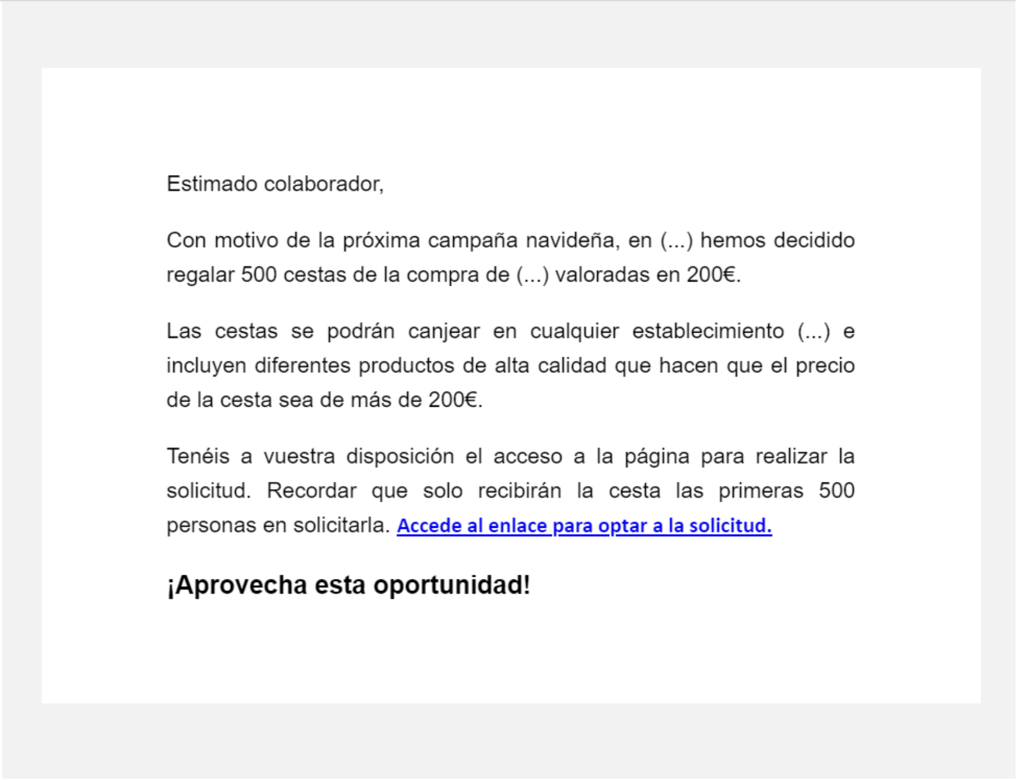
4. Results

After explaining how a phishing campaign would be carried out from scratch, we will proceed to comment on the results of the campaign carried out for this experiment, to put context the campaign has been carried out for an external company which has requested the company in which I am carrying out the project an awareness campaign for its employees.

This campaign has been used practicing the techniques described above, an external server associated with the domain ***nombreempresadelacampaña.me*** was raised, simulating that we are interacting with the real domain of the company in order to have more possibilities of tricking the employees.

The launch of the campaign was on Christmas dates, on December 14, for that reason the mail is related to these holidays, and includes common features of phishing emails (urgency, some type of gift or benefit for which you receive the mail etc).

These are the email and the pages used for this campaign**, all the data referring to the companies involved in the campaign have been anonymized, removing logos and names.**



Estimado colaborador,

Con motivo de la próxima campaña navideña, en (...) hemos decidido regalar 500 cestas de la compra de (...) valoradas en 200€.

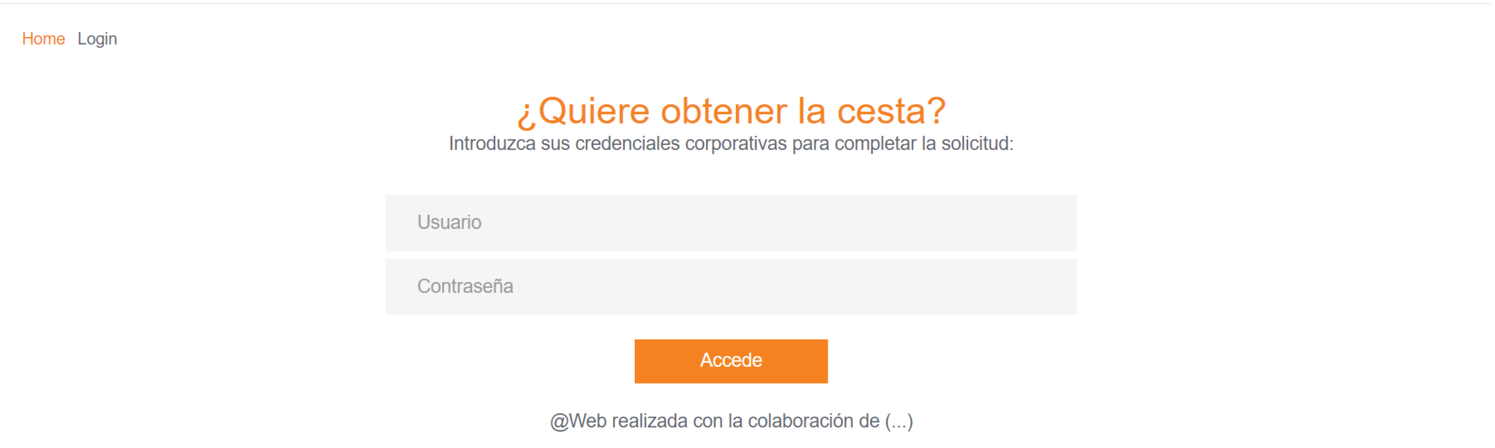
Las cestas se podrán canjear en cualquier establecimiento (...) e incluyen diferentes productos de alta calidad que hacen que el precio de la cesta sea de más de 200€.

Tenéis a vuestra disposición el acceso a la página para realizar la solicitud. Recordar que solo recibirán la cesta las primeras 500 personas en solicitarla. Accede al enlace para optar a la solicitud.

¡Aprovecha esta oportunidad!

Figure 47:Campaign Email

The sender email used on the campaign was ***navidad@nombreempresadelacampaña.me*** and the subject of the email was “Campaña navideña en (…)”.



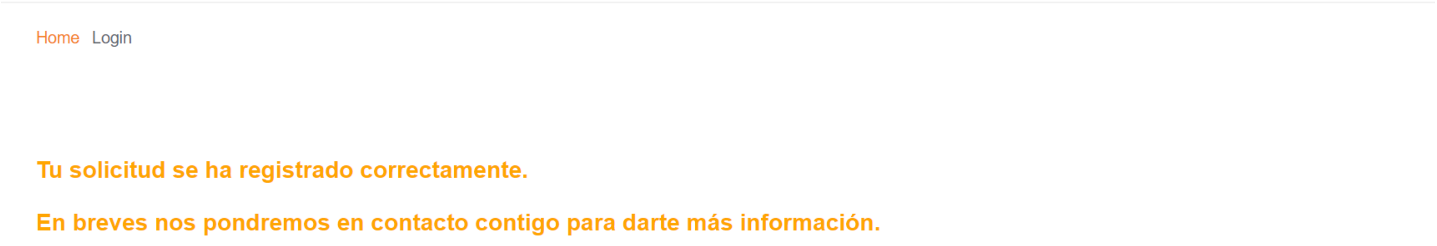
Home Login

¿Quiere obtener la cesta?

Introduzca sus credenciales corporativas para completar la solicitud:

@Web realizada con la colaboración de (...)

Figure 49:Campaign Landing Page



Home Login

Tu solicitud se ha registrado correctamente.

En breves nos pondremos en contacto contigo para darte más información.

Figure 48: Campaign Redirect Page

The campaign was active 3 days (from Tuesday to Thursday), was deployed in all departments of the company covering a total of 770 employees. Here we have the statistics obtained directly from the GoPhish application (We considered the sample to be 770 employees because one of the target emails was mine to make sure everything was working ok):

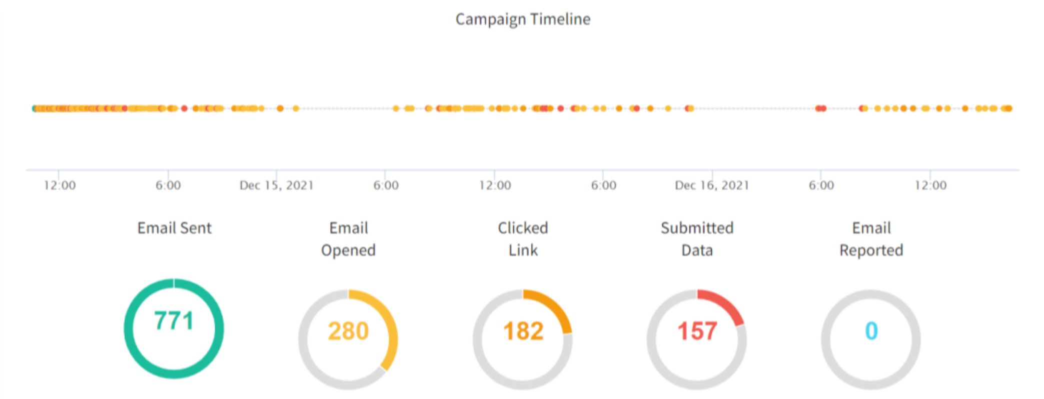
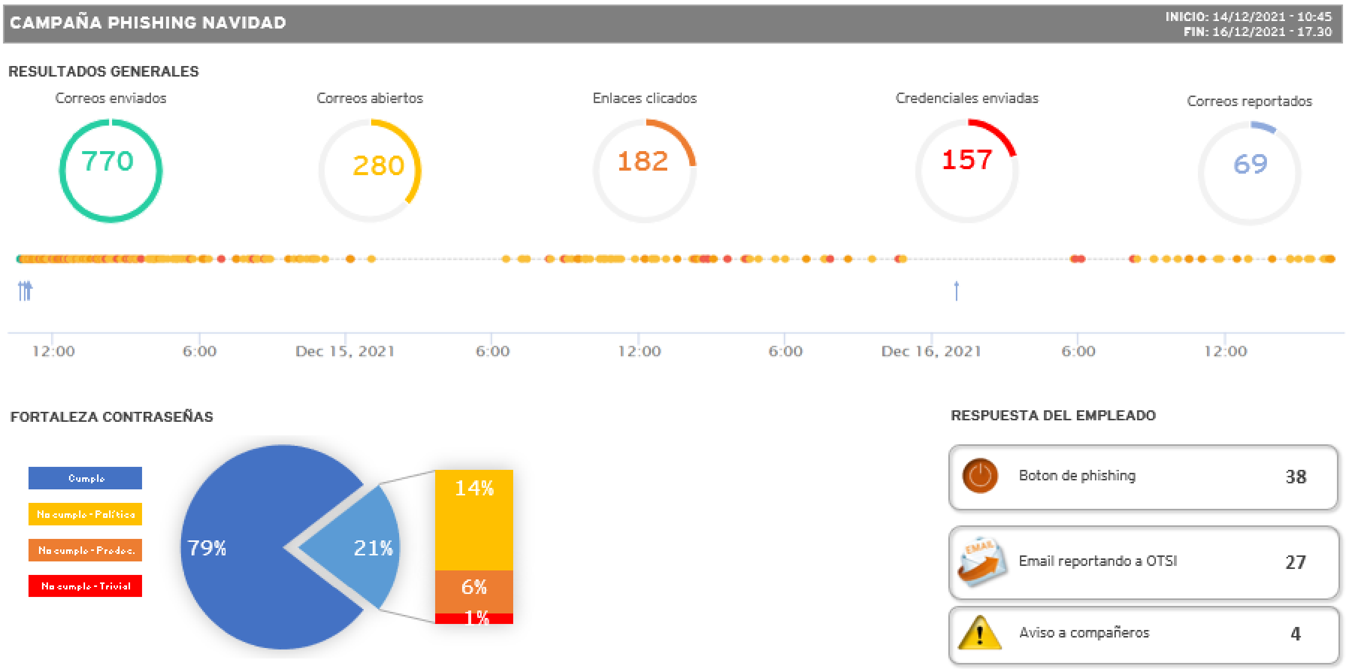


Figure 50:GoPhish Campaign Results

We can see the great impact of the campaign in the employees, where more than 20% have entered real credentials in our login portal. In addition, 36% of employees have interacted with our email, and 24% have clicked on the link in the email.

A surprising fact is that 56% of the people who have opened the mail, have ended up putting credentials, confirming the impact that an email that transmits immediacy and urgency can have.



Boton de phishing	38
Email reportando a OTSI	27
Aviso a compañeros	4

Figure 51:Campaign Final Results

Here we have the data after having treated the .csv files exported when completing the campaign. In these the strengths of the passwords are analyzed and the sections of reporting the emails as possible phishing are added, the latter was done by analyzing one by one the emails that reported as phishing within the company itself, so it is not reflected in the GoPhish statistics and were taken out manually. These show us that 69 employees were able to report the email received as suspicious, using the different methods provided by the company to report them.

Reporting suspicious emails can help prevent the impact of a phishing campaign. It's recommended to build a culture that rewards the users who report emails. Even something small like an email to that employee and their manager thanking them for their vigilance can go a long way. This gives positive feedback that will encourage users to report more emails in the future.

As a result of the realization of this phishing campaign, it was proposed for me the creation of a desktop application made with Python to get the most out of GoPhish since this software has an API to which you can make requests. This will help us to continue using the GoPhish utilities but being able to customize the interaction with it.

The main objective of the application is to be able to create campaigns in a simple way, using a previously created infrastructure as already shown in this project. This tool will save the creator of the campaign having to devise the phishing emails and pages, because this app will include generic templates that are valid for any awareness campaign, and it is scalable, the templates can be added and changed and the proposal is a first version, to which new functionalities can be proposed taking full advantage of the possibilities offered by the GoPhish API (for more information → Introduction - Python API Client (getgophish.com)).

To be able to use the application previously you will have to download Python, and some libraries used. To do this we execute the following commands:

```
sudo apt install python3.8


pip3 install gophish
```

Then we can run the application and we will be shown the first screen:

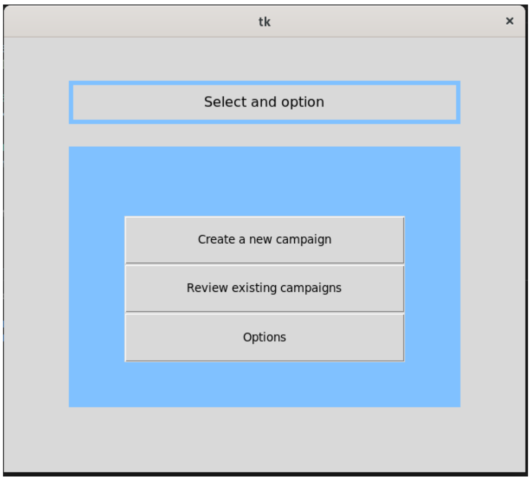
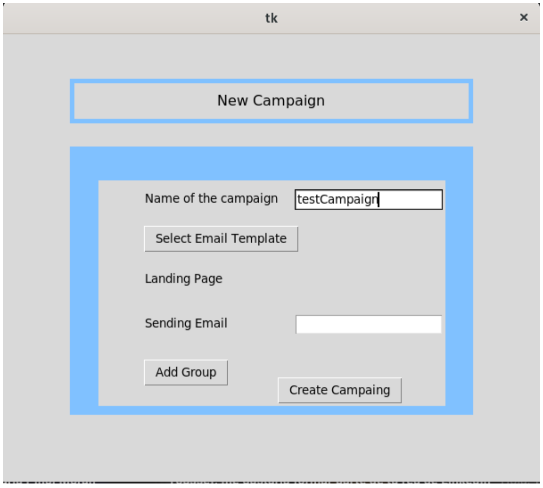


Figure 52:Phishing App First Screen

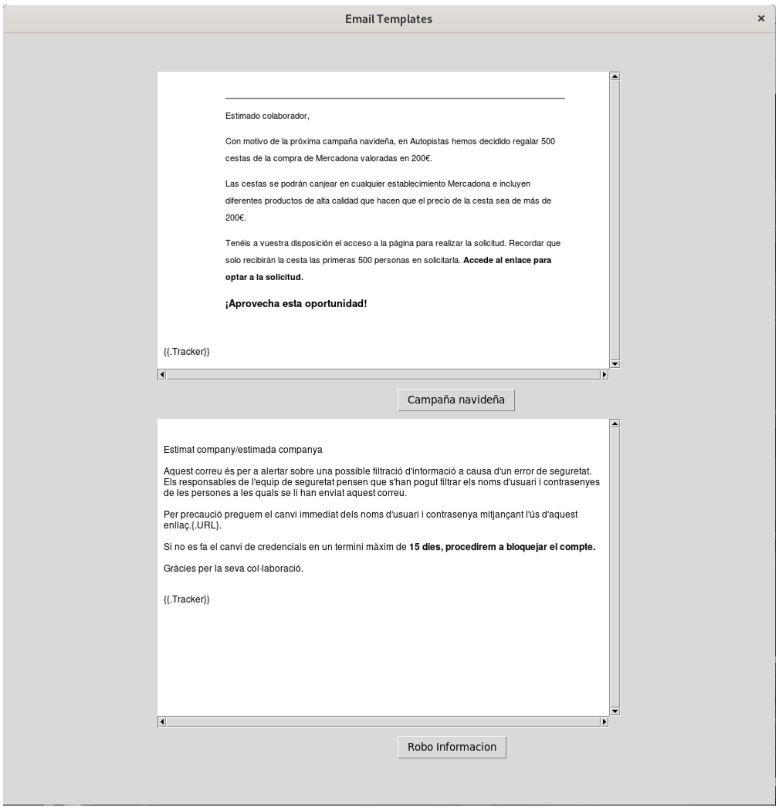
In this we can choose the option to create a new campaign, and we will be shown the option to choose the parameters of our campaign:

As you can see, we are given the option to name the campaign, choose an email template, which will automatically assign a landing page associated with said email:



Name of the campaign: testCampaign

Figure 53:Phishing App New Campaign Screen



Estimado colaborador,

Con motivo de la próxima campaña navideña, en Autopistas hemos decidido regalar 500 cestas de la compra de Mercadona valoradas en 200€.

Las cestas se podrán canjear en cualquier establecimiento Mercadona e incluyen diferentes productos de alta calidad que hacen que el precio de la cesta sea de más de 200€.

Tenéis a vuestra disposición el acceso a la página para realizar la solicitud. Recordar que solo recibirán la cesta las primeras 500 personas en solicitarla. **Accede al enlace para optar a la solicitud.**

¡Aprovecha esta oportunidad!

{{.Tracker}}

Estimat company/estimada companya

Aquest correu és per a alertar sobre una possible filtració d'informació a causa d'un error de seguretat. Els responsables de l'equip de seguretat pensen que s'han pogut filtrar els noms d'usuari i contrasenyes de les persones a les quals se li han enviat aquest correu.

Per precaució preguem el canvi immediat dels noms d'usuari i contrasenya mitjançant l'ús d'aquest enllaç.{.URL}.

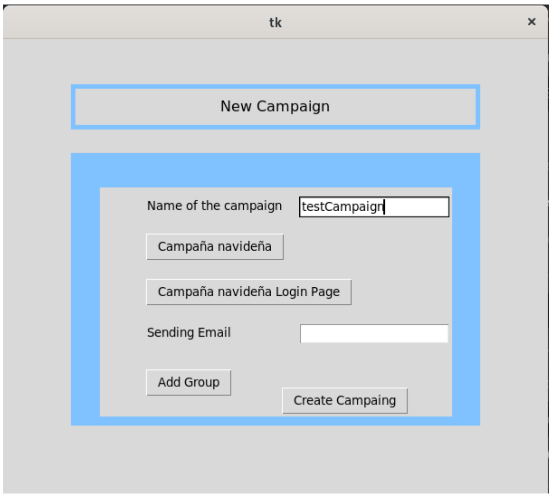
Si no es fa el canvi de credencials en un termini màxim de **15 dies, procedirem a bloquejar el compte.**

Gràcies per la seva col·laboració.

{{.Tracker}}

Figure 54:Phishing App Select Email Template

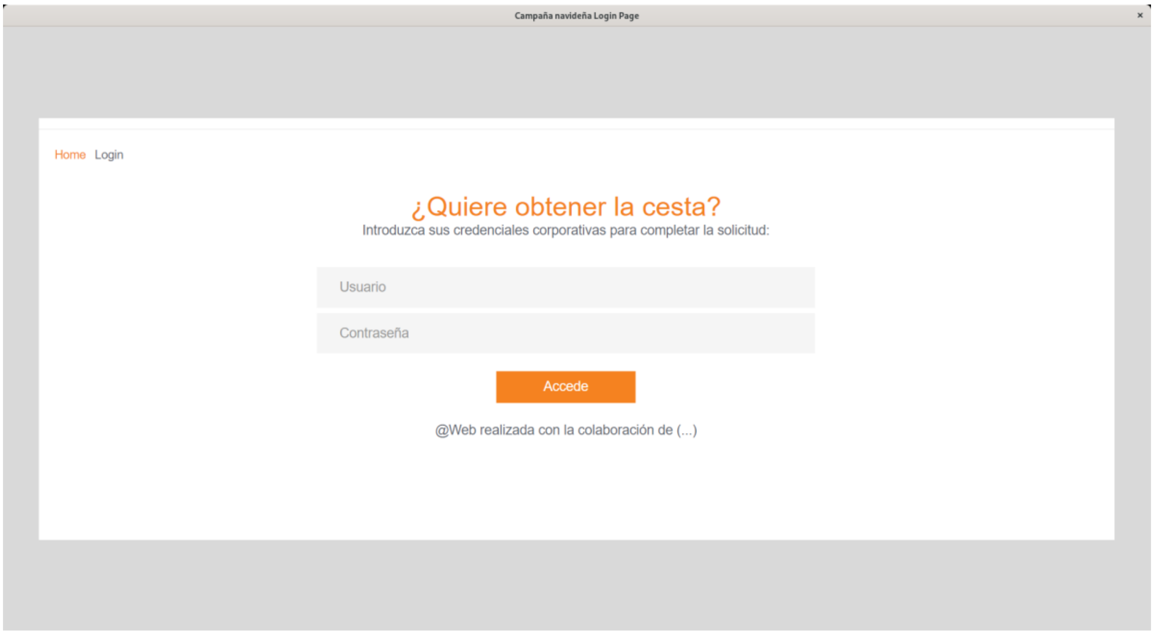
We can preview these templates by clicking on the different buttons



Name of the campaign testCampaign

Sending Email

Figure 55:Phishing App with selected templates



Campaña navideña Login Page

Home Login

¿Quiere obtener la cesta?

Introduzca sus credenciales corporativas para completar la solicitud:

Usuario

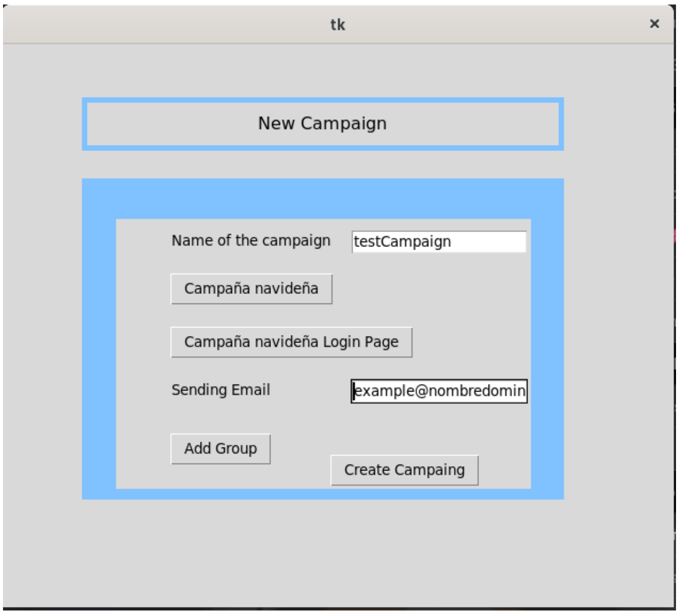
Contraseña

Accede

@Web realizada con la colaboración de (...)

Figure 56:Phishing App Show Landing Page Template

Then we can select the email address with which the mail will be sent (example@nombredominio.com), and automatically associate a domain with smtp server of the mail.nombredominio.com style, facilitating the use of this. Finally, before clicking on the campaign creation button, we will select a group to which the campaign will be directed, this must be added through a .csv file, which we can select by clicking on the Add Group button:



tk

New Campaign

Name of the campaign: testCampaign

Campaña navideña

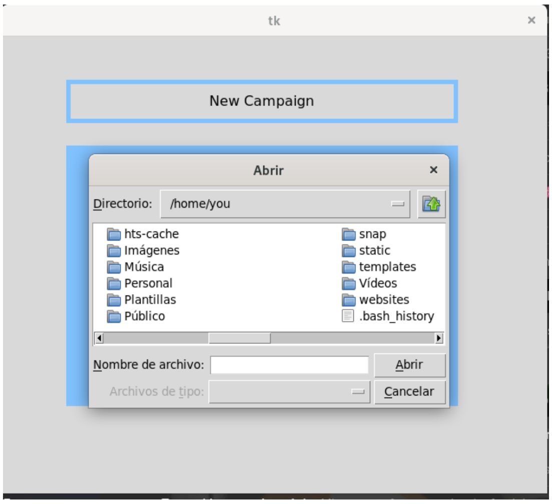
Campaña navideña Login Page

Sending Email: example@nombredomin

Add Group

Create Campaing

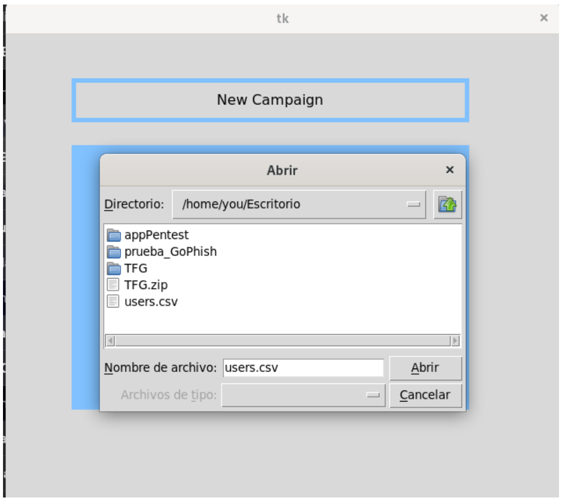
Figure 57:Phishing App Sending Email



Directorio: /home/you

Nombre de archivo:

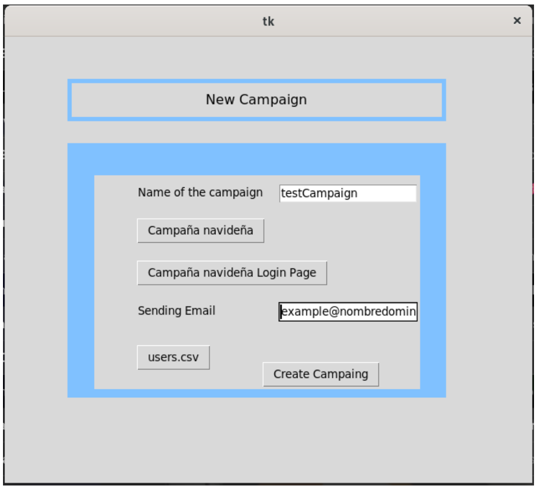
Figure 59:Phishing App Add Group



Directorio: /home/you/Escritorio

Nombre de archivo: users.csv

Figure 58::Phishing App Add Group 2



Name of the campaign testCampaign

Sending Email example@nombredomin

Figure 60:Phishing App Final Configuration

Once we have everything configured, the next thing will be to give Create Campaign, and it will automatically connect to your GoPhish server and carry out the campaign with the established parameters. (all the code will be added in the annex of this project and it shows how the API calls are made)

5. Budget

The costs of this project would be focused following the guidelines of any software development project, we will not have raw material or any type of electronic component, it will be all via software.

To calculate the total cost of the development of this project, the salary of the person in charge of carrying out this campaign will be considered, the cost of acquiring a domain on the specified page and that of having an external server deployed to mount the described infrastructure, we will consider the duration of the project that has been 4 months. The software used is free code, so we have been able to use it without any cost, and we consider that the computers used are part of the company's office material, which is included in the salary.

	Total Hours	Price (Brute salary)	Social Cost	Total Cost
Junior Software engineer	20h x week x 16 weeks= 320 h	9€ x hour	1,30 x worker	3744€
Domain (Namecheap)	-	-	-	7€
VPS (OVH essential plan)	4 months	6€ x month	-	24€
Total cost of the project				**3775€**

6. Conclusions and future development:

In conclusion, this essay has covered everything that refers to phishing campaigns, from a more theoretical part, what they consist of and how they can affect companies, and from a more technical part providing a guide to create these campaigns from scratch complementing it with a real awareness campaign in a company and with a tool to facilitate the realization of these campaigns, in order to be able to make periodic campaigns and raise awareness among employees to be alert to these practices.

We have been able to demonstrate in a real case how many employees would be affected by these practices, was a generic phishing attack and even so it has had great repercussions on the company. Imagine the impact that a more focused attack could have, that uses more sophisticated tools and using social engineering techniques more focused on the objective, managing to steal more credentials from employees and also from high position employees of the companies. The latter could lead to other types of attacks and compromise the affected company in a critical way.

As digitalization evolves, part of our identity and information, is more exposed on the Internet increases in value and the reliability on the part of attackers to carry out this type of attacks.

In this way, cybersecurity and its specialists should be part of any type of public or private organization and there should be a disclosure so that ordinary people can defend themselves against these practices.

The employee is the weakest part of the company, no matter how much technical security there is in the work infrastructure if there are no courses and awareness policies these end up resulting in vain since the attacker finds a security breach, which cannot be solved with security patches or technical updates, therefore we must try to protect the worker as much as possible by giving him the tools to be alert to these possible attacks.

If an employee is a victim of this type of email and comes to put their credentials, download some type of dangerous file or some other action that may compromise the company, it must immediately notify the cybersecurity team of the company or the team responsible for dealing with these incidents, you should never shut it up for fear of possible repercussions, the most sensible thing is to notify and warn other colleagues that the company is being victim of an attack.

As a future development, it could be possible to try to carry out a phishing attack on another company using more individualized techniques to try to obtain credentials from a senior official of that company in addition to having a greater number of affected employees and trying to use more sophisticated emails and pages for the campaign.

In addition to these possible ideas for future development, you could also spend time improving the tool created, adding functionalities, such as being able to import preconfigured settings already in the GoPhish application, being able to add logos and characteristics of the company that wants to perform the simulation, obtain the results of campaigns via API calls and represent these in a different way than GoPhish does, add campaign automation to be able to periodically carry out awareness campaigns and collect results from how many employees have improved and have learned to differentiate malicious emails from those that are not.

These are just some ideas to implement but many related ones could be investigated.

Bibliography:

[1] Available: 5 Common Types of Phishing Attacks — How to Recognize & Avoid Them - InfoSec Insights (sectigostore.com).

[2] Available: Phishing - Wikipedia, la enciclopedia libre.

[3] Available: Types of Phishing Attacks and How to Identify them – GeeksforGeeks.

[4] Available: IPTABLES manual practico, tutorial de iptables con ejemplos (umh.es).

[5] Available: (PDF) Phishing Defense Mechanism (researchgate.net).

[6] Available: How to Easily Set Up a Full-Featured Mail Server on Ubuntu 18.04 with iRedMail (linuxbabe.com).

[7] Available: https://sectigostore.com/blog/common-types-of-phishing-attacks-how-to-recognize-avoid-them/.

[8] Available: Introduction - Gophish User Guide (getgophish.com)

[9] Available: https - In what path I can find the .crt file for Let's Encrypt SSL? - Webmasters Stack Exchange.

[10] Available: 7 Effective Tips to Stop Your Emails Being Marked as Spam – LinuxBabe.

[11] Available: How Does Phishing Affect a Business? | First Citizens Bank

[12] Available: Domain Name System - Wikipedia

[13] Available: What is the business impact of a Phishing Attack? - Packetlabs

[14] Available: Phishing Statistics (Updated 2022) - 50+ Important Phishing Stats - Tessian

[15] Available: DKIM: What is it and should you configure it? (securitytrails.com)

[16] Available: 37+ Scary Phishing Statistics - An Growing Threat in 2021 (hostingtribunal.com)

[17] Available: Modern Email Security Enhancements (SPF,DKIM,DMARC) — SNOWCAP TECHNOLOGIES

[18] Available: Phishing statistics and facts for 2019–2021 | Comparitech

[19] Available: Sender Policy Framework (SPF) for Exchange Administrators (practical365.com)

[20] Available: dmarc.org – Domain Message Authentication Reporting & Conformance