**🎯 Goal**

To simulate a phishing attack campaign and then analyze the network and host-based evidence left behind to detect the threat.

**🧰 Tools & Setup**

* **Ubuntu VM:** Your attacker machine.
* **Windows VM:** Your victim machine.
* **GoPhish:** An open-source phishing framework (this will run on your Ubuntu VM).
* **Wireshark:** For network packet analysis on the Windows VM.
* **Windows Event Viewer:** For host-level log analysis on the Windows VM.
* **A simple email account:** You'll need an email account (like a free Gmail or Outlook account) to act as your sending server.

That's an excellent idea. Simulating an email-based attack is a core exercise that highlights skills in social engineering, network traffic analysis, and host-level detection. A phishing attack is the perfect scenario for your existing lab setup.

Here is a step-by-step plan to guide you through a practical email-based attack home lab using your Ubuntu and Windows VMs.

# 🎯 Goal

To simulate a phishing attack campaign and then analyze the network and host-based evidence left behind to detect the threat.

# 🧰 Tools & Setup

* **Ubuntu VM:** Your attacker machine.
* **Windows VM:** Your victim machine.
* **GoPhish:** An open-source phishing framework (this will run on your Ubuntu VM).
* **Wireshark:** For network packet analysis on the Windows VM.
* **Windows Event Viewer:** For host-level log analysis on the Windows VM.
* **A simple email account:** You'll need an email account (like a free Gmail or Outlook account) to act as your sending server.

# 🛠️ The Lab Plan: Phishing Simulation & Detection

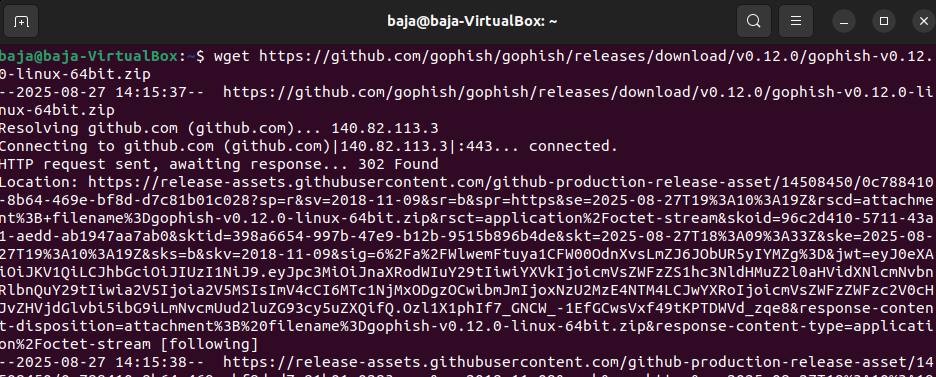
## Step 1: The Red Team (Attacker) Setup

1. **Install GoPhish on Ubuntu:**
   * Download the GoPhish executable from the official GitHub repository.
   * Run the executable. By default, GoPhish listens on http://127.0.0.1:3333 for its administrative panel.
   * Configure the config.json file to allow access from your Windows VM.

### 1.1. Download and Install GoPhish

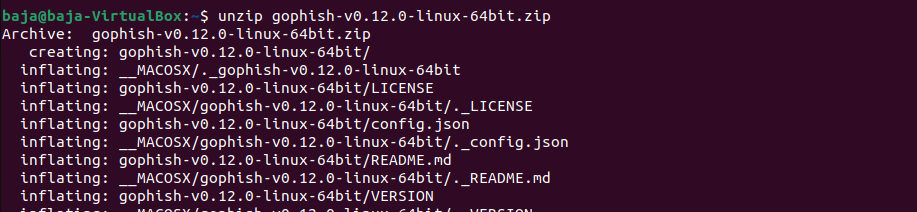
1. Open a terminal on your Ubuntu VM.
2. Use wget to download the Linux version of GoPhish.

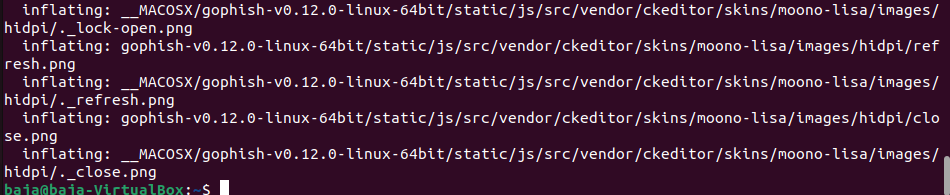
wget <https://github.com/gophish/gophish/releases/download/v0.12.0/gophish-v0.12.0-linux-64bit.zip>





1. Unzip the downloaded file.



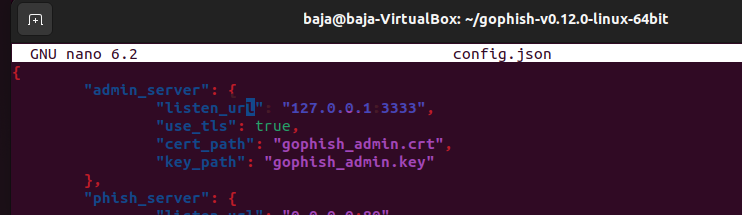


1. Navigate into the new GoPhish directory.

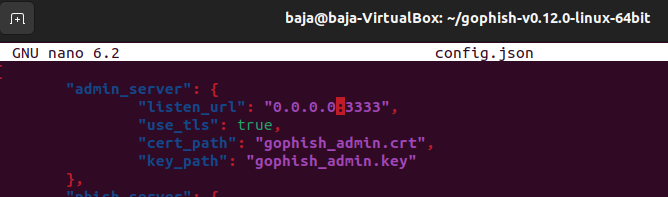


### 1.2. Configure and Launch GoPhish

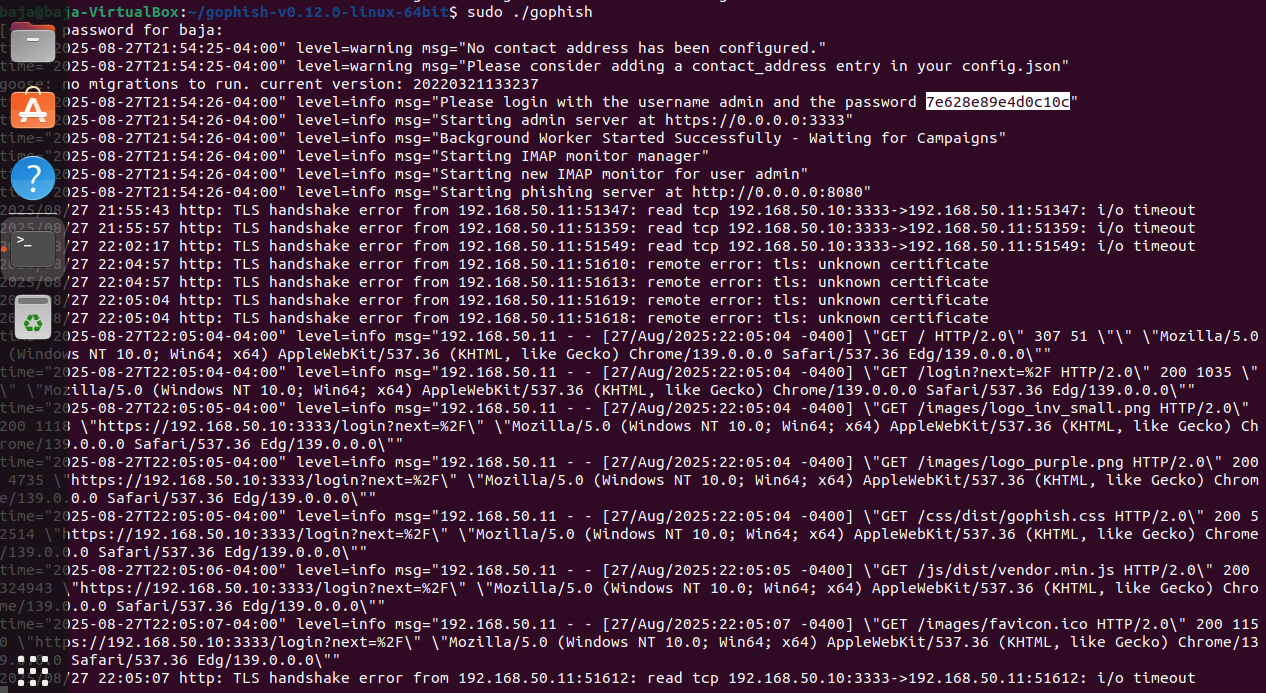
1. Open the config.json file in a text editor (like nano).



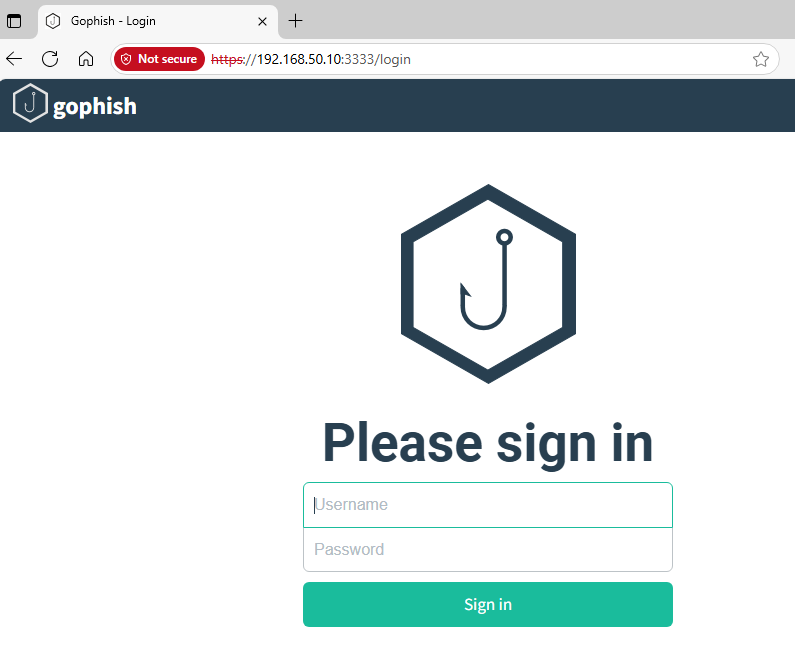
1. Find the line "listen\_url": "127.0.0.1:3333" and change it to "listen\_url": "0.0.0.0:3333". *This tells GoPhish to listen for connections from all network interfaces, allowing your Windows VM to connect.*



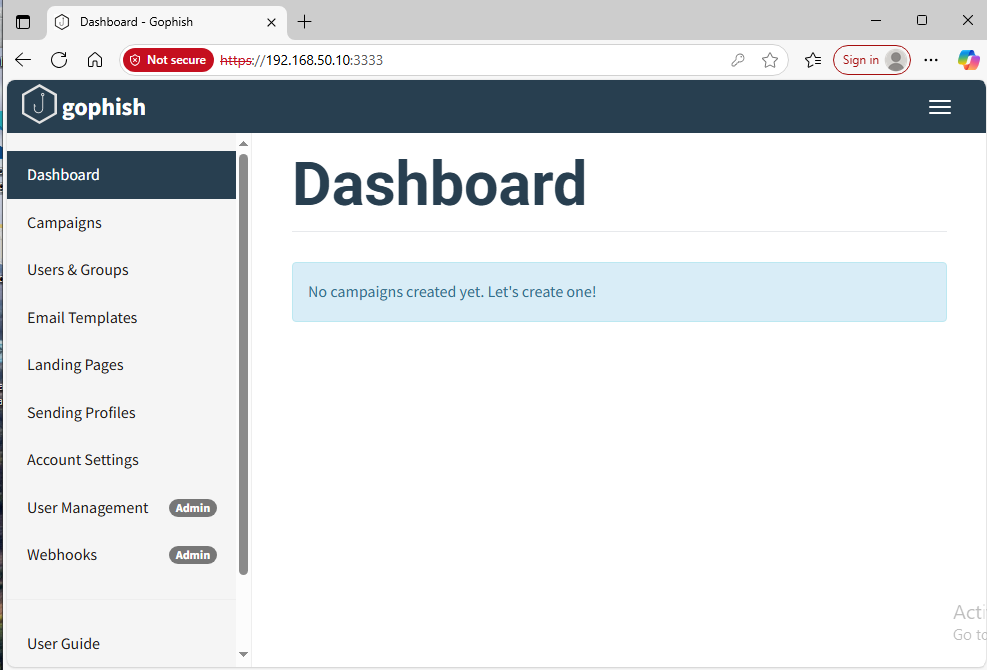
1. Save and close the file (Ctrl + O, then Enter, then Ctrl + X in nano).
2. Run the GoPhish executable to start the server.



User: admin, Password: 7e628e89e4d0c10c



User: admin, password : jan081985

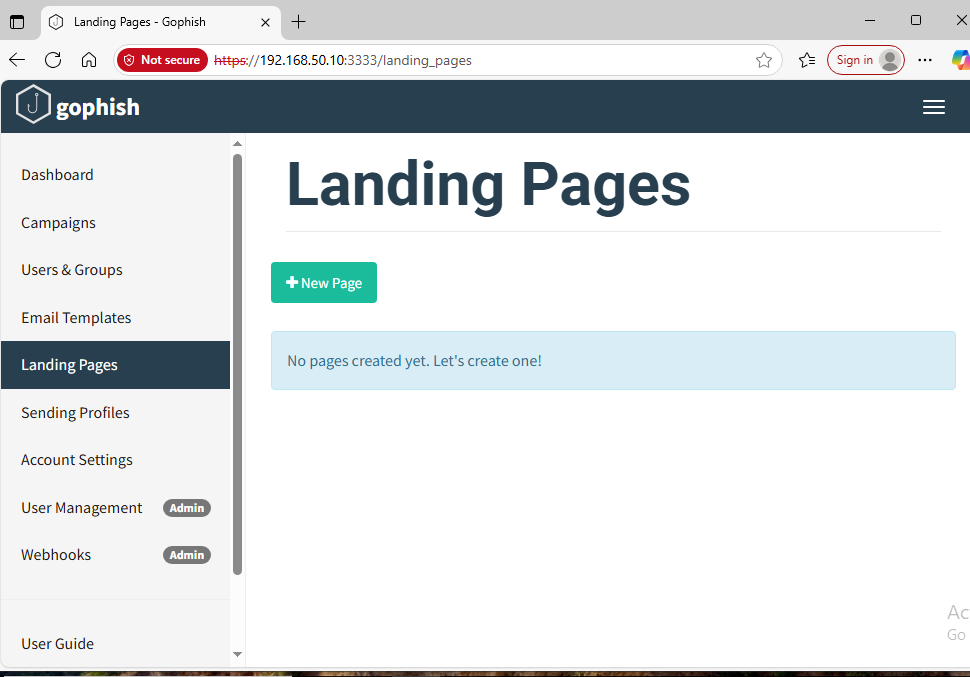


## Step 2: Creating a Phishing Campaign (GoPhish GUI)

#### Step 1: Create a Landing Page

The landing page is the fake website that will capture the user's credentials. GoPhish has a simple cloning feature that makes this easy.

1. Log in to the GoPhish admin panel.
2. Navigate to **Landing Pages** on the left menu and click **New Page**.
3. Give your page a recognizable name, like Fake Microsoft Login.
4. To clone a real website, find a simple login page and copy its URL. For example, a company's internal login portal.
5. In the "Import Site" box, paste the URL you copied. GoPhish will pull in the HTML and images for you.
6. Make sure to check the boxes for **Capture Submitted Data** and **Capture Passwords**. This tells GoPhish to save any information the user types into the form.
7. Click **Save Page** to finish.



Imported simple login html landing page as seen in the below screen shot

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>COVID-19 Response Fund</title>

</head>

<body>

<div style="text-align: center; font-family: Arial, sans-serif;">

<h2>COVID-19 Employee Response Fund</h2>

<p>Please log in to verify your eligibility and claim your funds.</p>

<form action="/" method="post">

<label for="email">Work Email:</label><br>

<input type="email" id="email" name="username" placeholder="name@company.com"><br>

<label for="password">Password:</label><br>

<input type="password" id="password" name="password"><br><br>

<input type="submit" value="Verify and Continue" style="background-color: #007BFF; color: white; padding: 10px; border: none; cursor: pointer;">

</form>

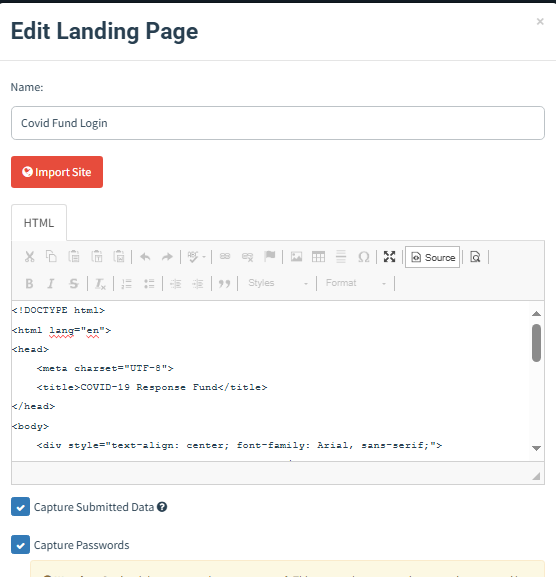
<br>

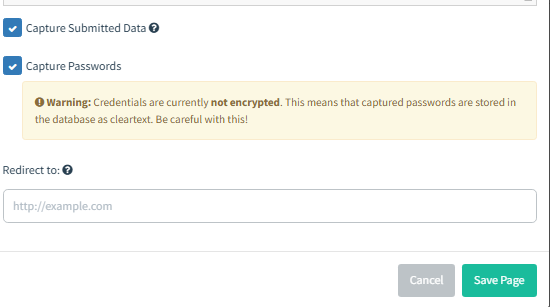
<p style="font-size: 12px; color: #666;">This portal is for internal use only. All data is securely handled.</p>

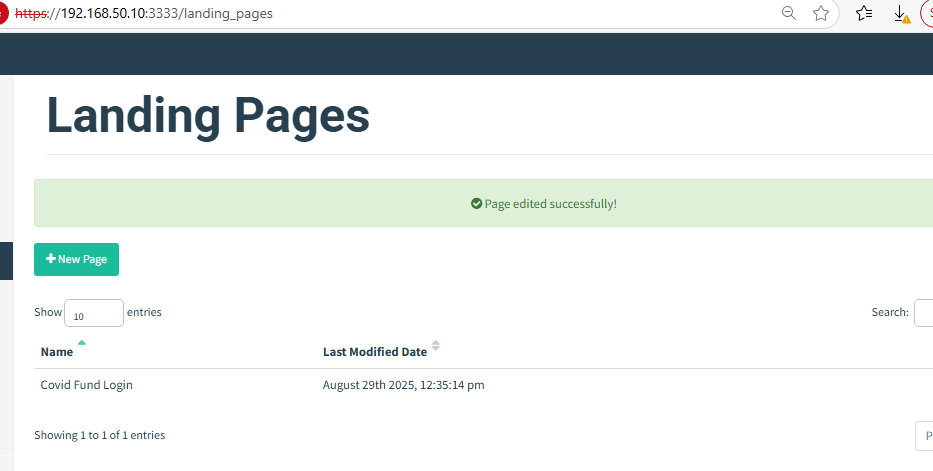
</div>

</body>

</html>



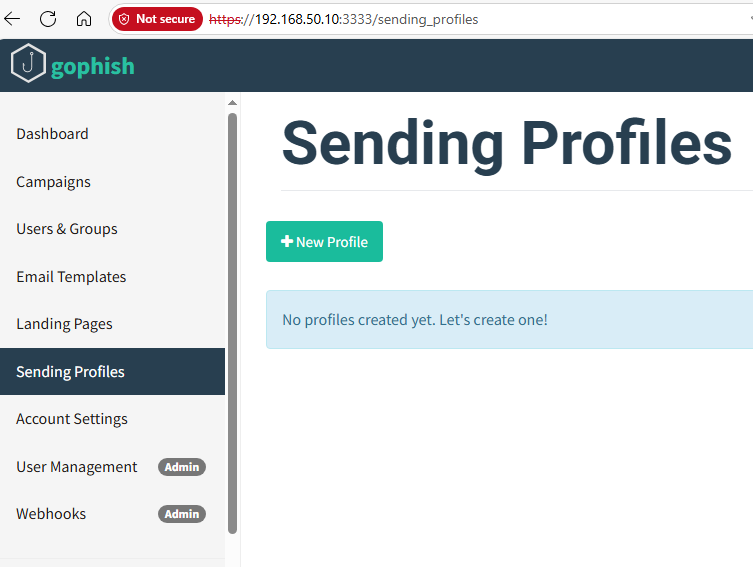


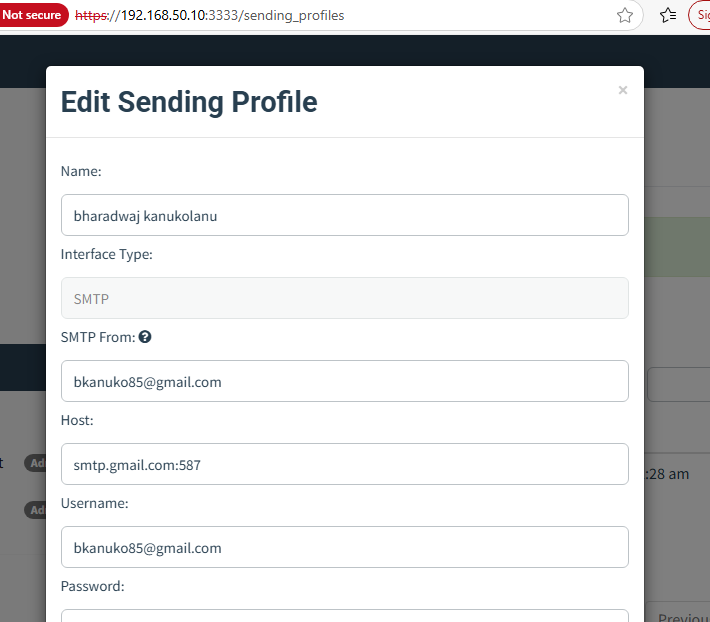


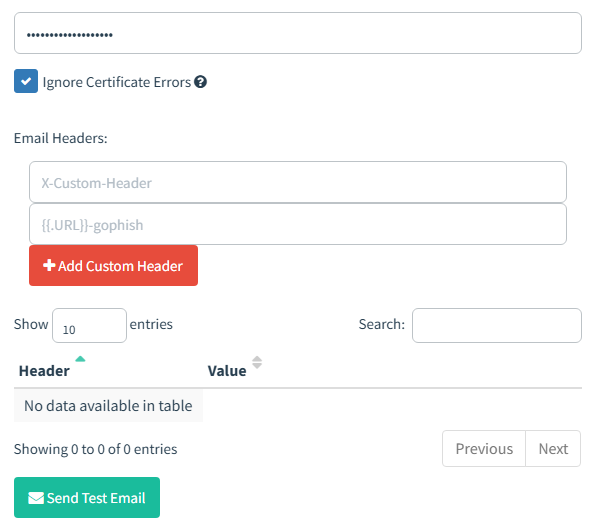
#### Step 2: Configure a Sending Profile

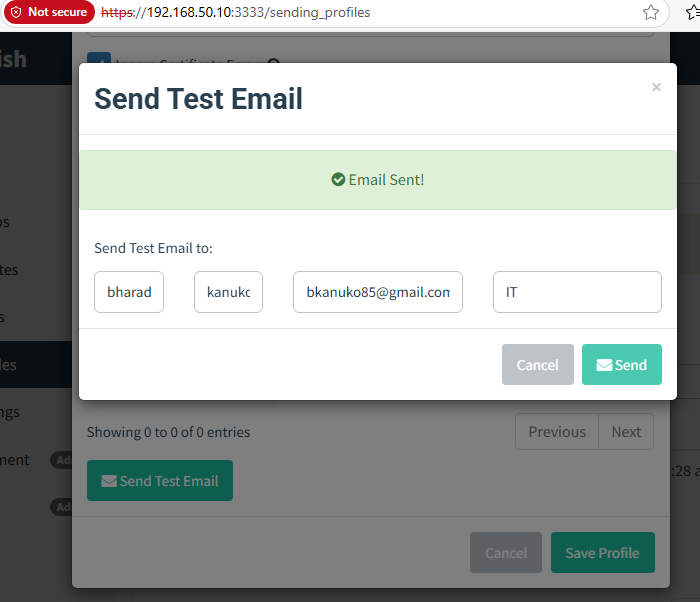
The sending profile tells GoPhish which email account to use to send the phishing emails. You'll need to use a real email account for this, such as a free Gmail or Outlook account.

1. Go to **Sending Profiles** and click **New Profile**.
2. Give the profile a name.
3. Fill in the required information:
   * **From:** The email address and name you want the email to appear from (e.g., IT Security <security@yourcompany.com>).
   * **Host:** The SMTP server address of your email provider (e.g., smtp.gmail.com:587).
   * **Username/Password:** The credentials for the email account you're using.
4. Click **Send Test Email** to make sure the connection works. When it's successful, click **Save Profile**.





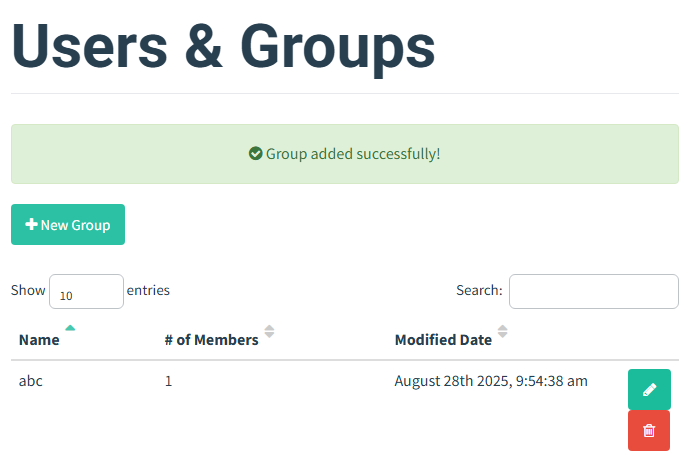




#### Step 3: Add Your Target

For this lab, the target is you! You'll add your own email address so you can act as the victim.

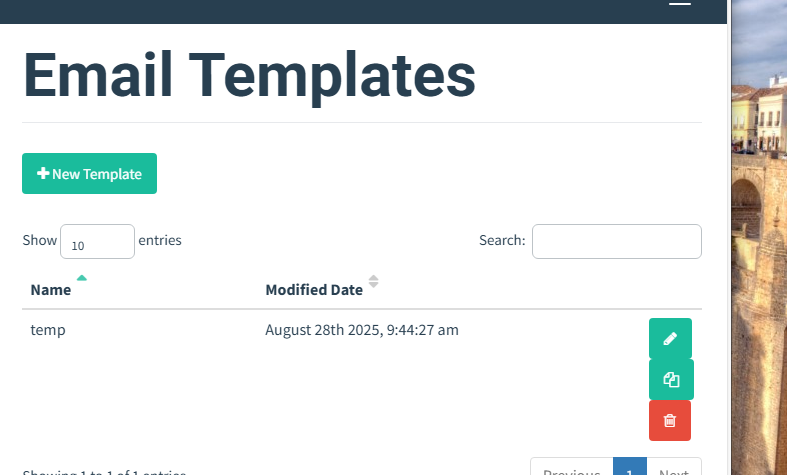
1. Go to **Users & Groups** and click **New Group**.
2. Give the group a name.
3. Add yourself as a user by typing in your name and email address. You can also import a list if you have a CSV file.
4. Click **Save Group**.



#### Step 4: Craft the Email Template

The email template is the message that will contain your phishing link.

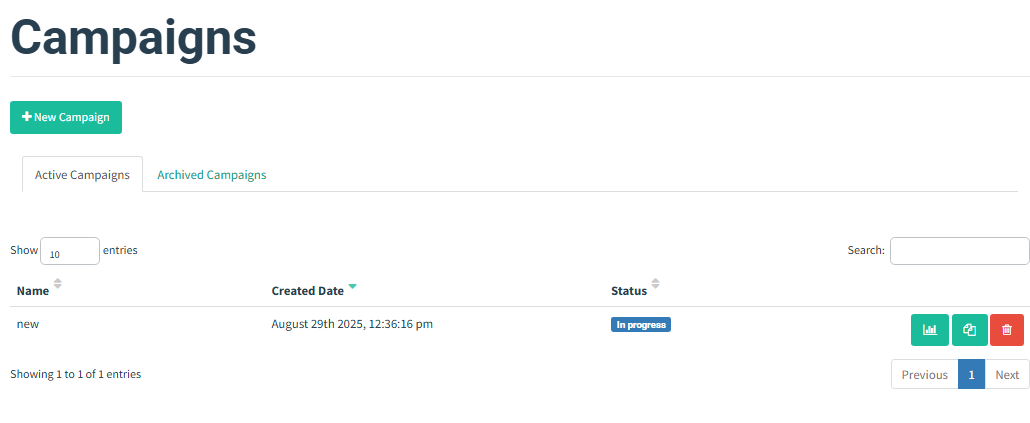
1. Go to **Email Templates** and click **New Template**.
2. Give the template a name and a compelling subject line, like Urgent Security Alert: Your Account Has Been Locked.
3. In the body of the email, write a message that encourages the victim to click the link.
4. To insert the phishing link, highlight the text you want to hyperlink and click the link icon in the editor. In the URL field, use the GoPhish placeholder {{.URL}}.
5. Click **Save Template**.

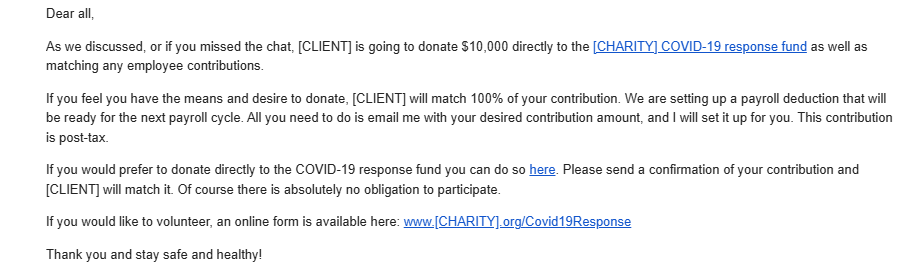


#### Step 5: Launch the Campaign

This is the final step where you bring everything together and launch the attack.

1. Go to **Campaigns** and click **New Campaign**.
2. Give it a descriptive name.
3. Select the **Email Template**, **Landing Page**, and **Sending Profile** you just created from the dropdown menus.
4. Choose the **User Group** you created.
5. Under the "URL" field, enter the full URL for your phishing page, using the IP address of your Ubuntu VM and the GoPhish server's phishing port (by default, it's port 80).
   * Example: http://192.168.1.100 (The port is not needed if you leave it on 80).
6. Click **Launch Campaign**.





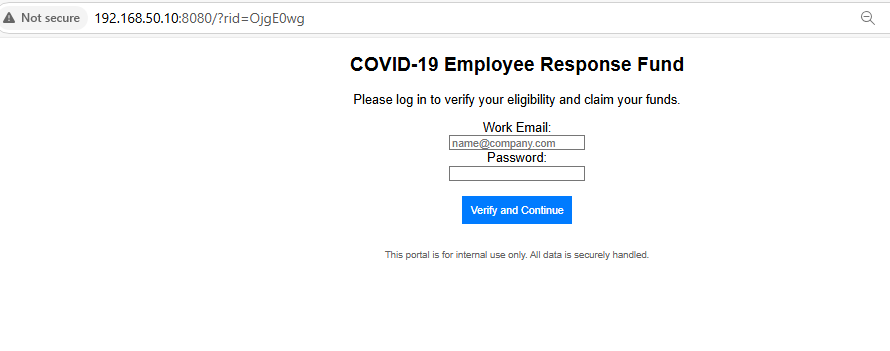
# Phase 2: The Blue Team (Defender) Detection

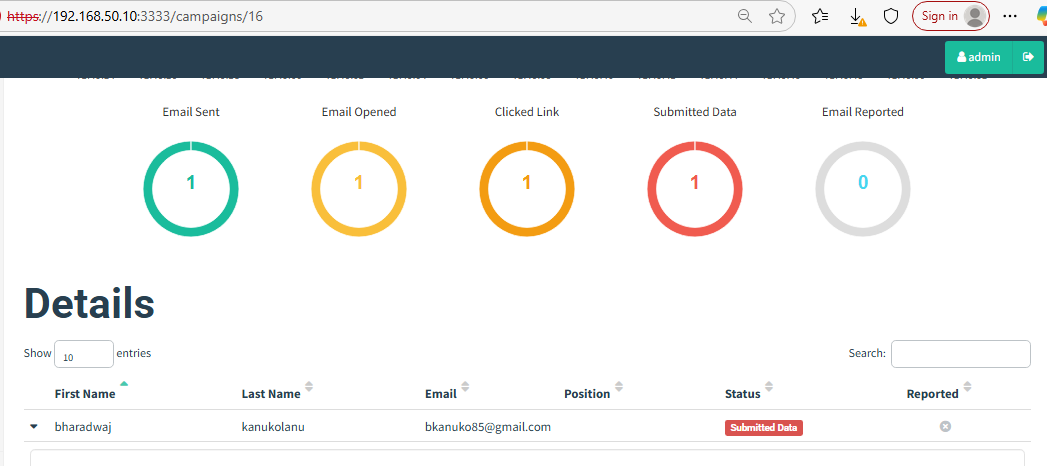
## Step 1: Host-Level Analysis (On the Windows VM)

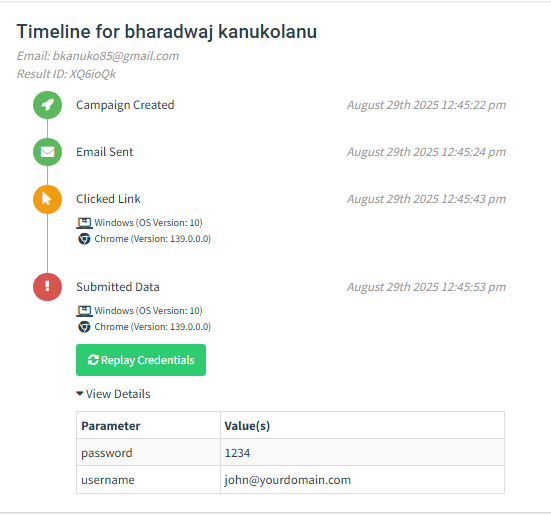
This part of the analysis focuses on the logs generated by the victim machine itself.

1. **Open Windows Event Viewer:** On your Windows VM, go to the Start Menu, type Event Viewer, and open the application.
2. **Navigate to Security Logs:** In the left-hand panel, navigate to Windows Logs > Security.
3. **Filter for Logon Events:** A real-world attack generates many logs. To make it easier, filter the logs. In the right-hand panel, click Filter Current Log....
4. **Look for Logon Attempts:** For an attack like a phishing login, look for logon-related Event IDs, such as 4625 (An account failed to log on) or 4624 (An account successfully logged on). A login attempt to your fake page should generate a log entry here.
5. **Examine the Logs:** Analyze the details of the log entry. Can you see a logon attempt at the exact time you submitted the fake credentials? This confirms the attack was logged.

Provided work email: [john@yourdomain.com](mailto:john@yourdomain.com), password: 1234.







## Step 2: Network-Level Analysis (On the Windows VM)

This part of the analysis focuses on the network traffic.

1. **Start a Wireshark Capture:** Before you click the phishing link in your email, open Wireshark on your Windows VM and start a new packet capture on your network adapter.
2. **Act as the Victim:** Now, open the phishing email and click the link. On the fake login page, enter some fake credentials and click "submit."
3. **Stop the Capture:** Go back to Wireshark and stop the capture.
4. **Analyze the Packets:**
   * Use the filter bar to narrow down the traffic. Try a filter like http or ip.addr == [Your Ubuntu VM's IP Address].
   * Find the HTTP packet where your browser sent the credentials. In the packet details, expand the Hypertext Transfer Protocol section. You should be able to see the username and password you entered, often in clear text if you didn't use HTTPS. This is your evidence of the attack.

