Manuale d’uso

Security Awareness Infrastructure

1 Accensione dei container

1.1 Utilizzo del docker compose

Da questa pagina di GitHub: https://github.com/PaascuZ/Securitiy-Awareness-Environment, è possibile visualizzare tutti i file che occorrono per l'utilizzo del sistema.

Scaricando l'intera directory SecAwarenessEnv (posta nella cartella *6_File di configurazione*) ci si assicura di avere tutto il necessario nel posto corretto.

1.2 Comandi importanti di Docker

Inoltre, sono importanti diversi comandi per l'utilizzo di Docker Engine. Comandi utili per muoversi all'interno dell'infrastruttura con facilità.

1.2.1 Accensione dei container

Per accendere i vari container dei servizi, utilizzare il seguente comando.

```
sudo docker compose up
```

1.2.2 Spegnimento dei container

Per spegnere i container, utilizzare il seguente comando.

```
^C
```

Ovvero CTRL+C, per uscire dai processi.

1.2.3 Processi dei container

Per visualizzare i vari processi dei container attivi, utilizzare il seguente comando.

```
sudo docker ps
```

Per visualizzare anche i processi non attivi, utilizzare il seguente comando.

```
sudo docker ps -a
```

1.2.4 Ispezione dei container

Per ispezionare i vari container e visualizzare le impostazioni, utilizzare il seguente comando.

```
sudo docker inspect <ID_CONTAINER>
```

Oppure

```
sudo docker inspect <NOME_CONTAINER>
```

1.2.5 Accesso alla shell dei container

Per accedere alla shell dei vari container, utilizzare il seguente comando.

```
sudo docker exec -it <ID_CONTAINER> /bin/bash
```

Oppure

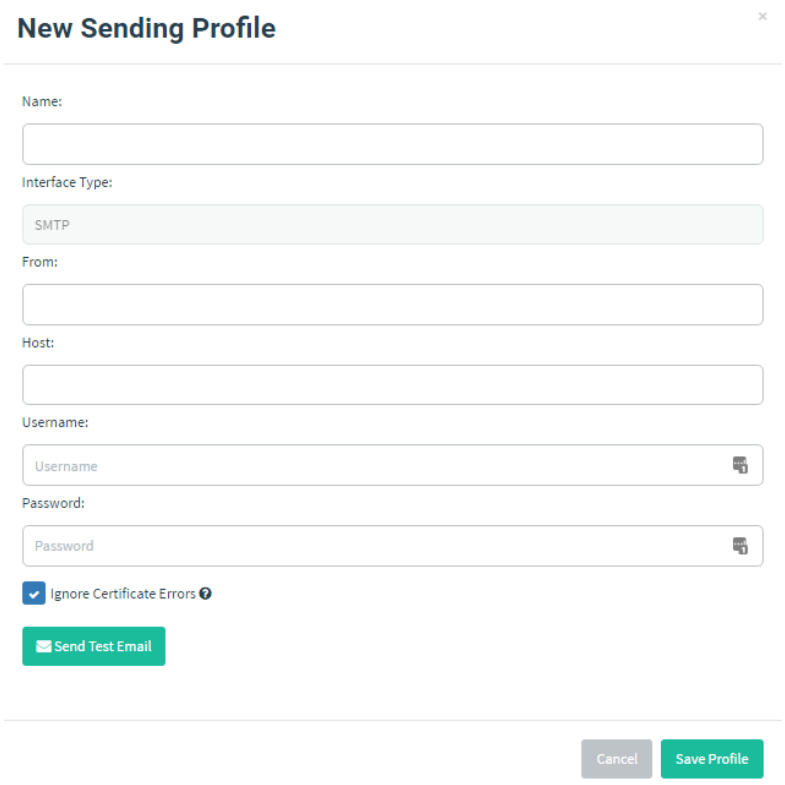
```
sudo docker exec -it <NOME_CONTAINER> /bin/bash
```

2 Creazione di una campagna

Ora è arrivato il momento di accedere all'interfaccia amministrativa di Gophish attraverso `http://localhost:3333` e accedere con le proprie credenziali.

2.1 Creazione Sending Profile

Per creare un sending profile (ovvero il profilo da dove partono le mail) cliccare su Sending profile nella barra a sinistra di Gophish.



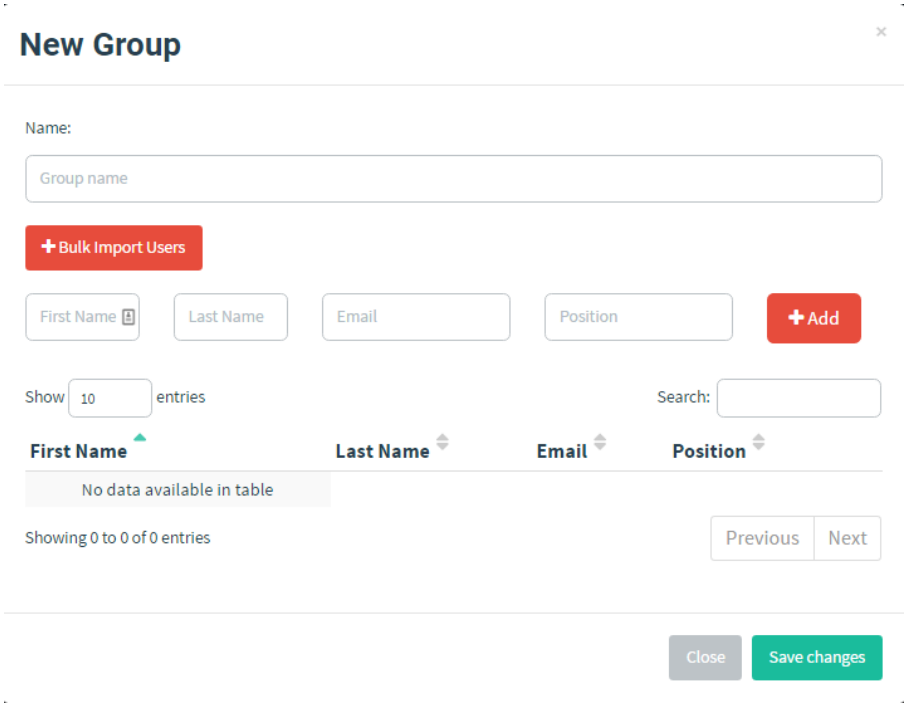
Le configurazioni da inserire sono le seguenti.

- **Name:** Il nome del sending profile
- **From:** L'indirizzo mail dell'attaccante. Per esempio: accounts@mircosoft.com
- **Host:** L'host del server mail.
  È possibile anche scrivere: <NOME_CONTAINER_POSTFIX>:25

Non sono necessari username e password.
È possibile anche inviare una e-mail di test per verificare le impostazioni siano corrette.

2.2 Creazione dei gruppi

Per creare i gruppi dirigersi nell'apposita pagina dell'interfaccia di Gophish.



I parametri da utilizzare in questo caso sono i seguenti.

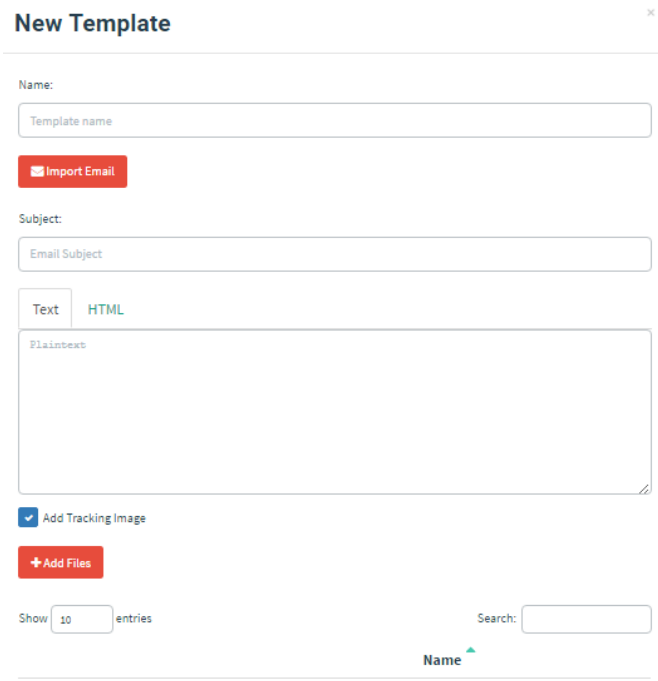
- **First Name:** Nome della vittima
- **Last Name:** Cognome della vittima
- **Email:** Email della vittima
- **Position:** La posizione in azienda della vittima. **NON OBBLIGATORIA**

È possibile inserire gli indirizzi delle varie vittime manualmente, oppure importare un file .csv impostato nel seguente modo (quello che si vede è un esempio con account non reali).

```
First Name,Last Name,Position,Email
Richard,Bourne,CEO,rbourne@morningcatch.ph
```

2.3 Creazione dei mail template

Per creare un template delle mail che vengono inviate, dirigersi nell'apposita pagina di Gophish, nel menu a sinistra dell'utente.

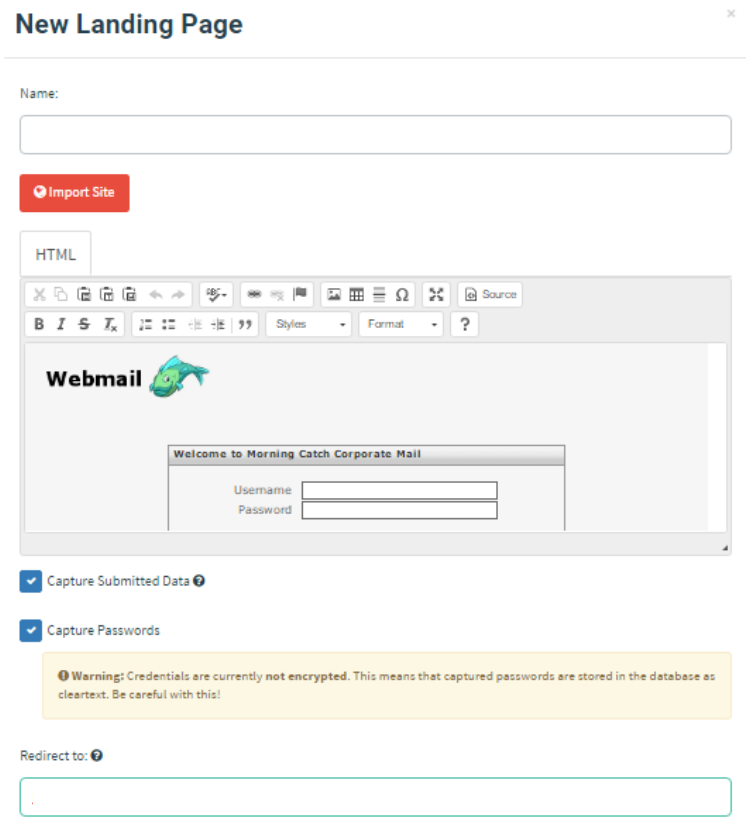


I parametri da utilizzare sono i seguenti:

- Name: Il nome del template
- Text: La mail sottoforma di testo normale
- HTML: In alternativa si può selezionare l'immissione di codice HTML

2.4 Creazione della landing page

Per creare la propria landing page



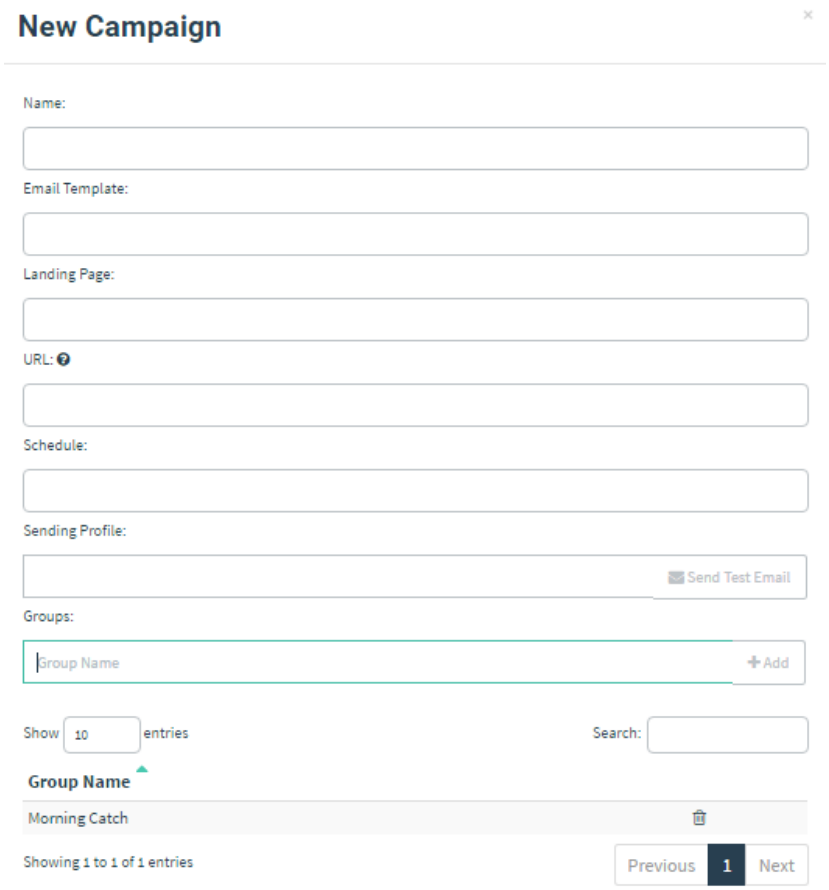
I parametri da inserire sono i seguenti.

- Name: Il nome del modello di landing page
- HTML: Il codice HTML della landing page personalizzata
- Import site: In alternativa è possibile importare un sito web inserendo l'URL dello stesso

Poi è necessario spuntare le voci *Capture Submitted Data* e *Capture Passwords* per catturare le credenziali da mostrare nella dashboard. Dopodiché è necessario inserire un parametro *redirect*, ovvero la pagina dove la vittima viene indirizzata una volta inserito le credenziali.

2.5 Lancio della campagna

Per lanciare una campagna di phishing dirigersi nell'apposita sezione dall'interfaccia amministrativa di Gophish.



I parametri da utilizzare in questo form sono i seguenti.

- **Name:** Nome della campagna
- **Email Template:** Template della mail
- **Landing page:** La pagina dove verrà indirizzata la vittima
- **URL:** L'indirizzo visualizzato sul browser (p.e. mircosoft.com)
- **Schedule:** La programmazione dell'avvio della campagna
- **Sending profile:** Il profilo d'invio delle varie email
- **Groups:** Il gruppo di vittime che si vuole attaccare

Ora è possibile lanciare la propria campagna di phishing aspettando i risultati mostrati immediatamente sulla dashboard.