



## Procédures Informatique

### Le serveur Gophish

L'objectif de cette procédure est d'expliquer la mise en place , l'installation et le paramétrage d'un serveur go phish

#### 1 – Location d'une VM AWS

Dans un premier temps, il faut prendre une VM Windows server 2022 via Aws. Le paramétrage est aussi possible avec une VM Linux, ici nous verrons sous OS Microsoft.

Config minimum de la VM : 4Go de Ram.

#### 1 – Installation de Go Phish

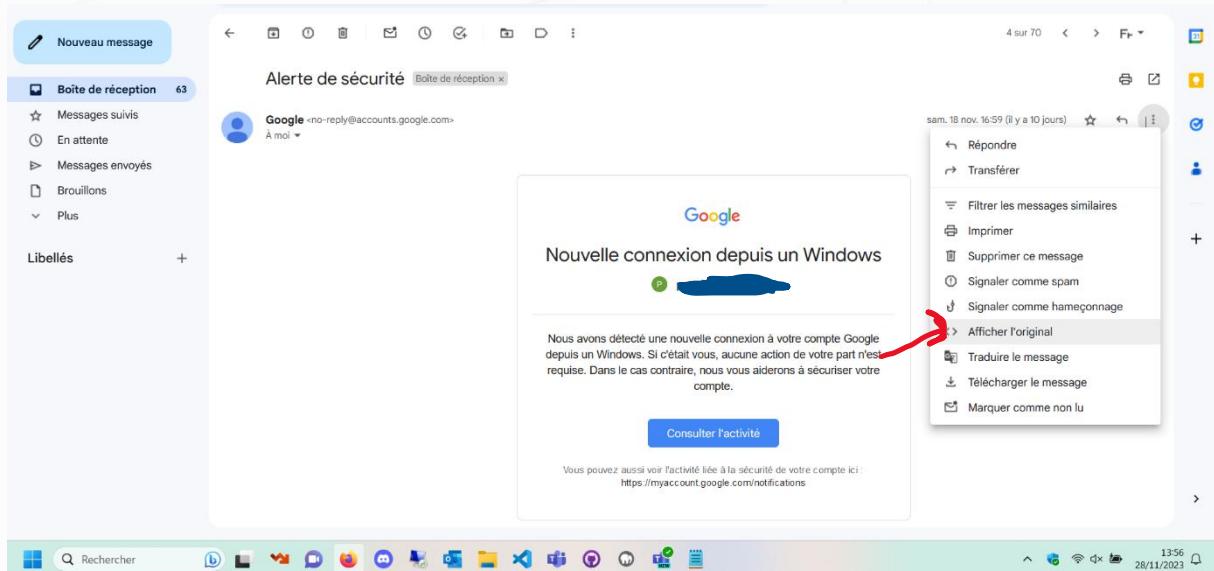
Tout d'abord, télécharger l'exécutable sur internet et le lancer sur le bureau de la VM. Bien penser à ouvrir les ports **443 et 80** du pare-feu . Par défaut , l'adresse du server d'admin est sur localhost (127.0.0.1) . Pour le modifier, chercher le fichier config.json dans le dossier où Go phish a été installé puis modifier les adresses IP en 0.0.0.0 :443 et 0.0.0.0 :80 (cf photo ci jointe)

```
{
    "admin_server": {
        "listen_url": "0.0.0.0:443",
        "use_tls": true,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key",
        "trusted_origins": []
    },
    "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": ""
    }
}
```

## 1 – Paramétrage de Go Phish

### Email Template :

Dans cette section il est possible de créer le template du mail via du code html. Plusieurs solutions sont possibles comme notamment récupérer le code source d'un mail via google mail (envoyer le template du mail sur une boîte google et explorer le contenu pour récupérer le code, ne marche qu'avec les boîtes mail Google). L'url du credential est ainsi renseigné automatiquement



### Landing pages :

Il s'agit de la fausse page d'authentification vers laquelle l'utilisateur va être redirigé. Contrairement au template du mail, la page peut être fait en full html.

### New campaign :

Pour lancer une nouvelle campagne, il faut choisir un template , une landing page et le groupe d'utilisateurs destinataires du phishing.

Pour l'url de retour des informations, il faut renseigner l'ip du serveur précédé de http (sans s).



Dans le portail 365, il faut autoriser l'adresse d'expéditeur à ne pas être bloquée par Defender. Pour cela il faut créer une règle dans Exchange Admin Center :

<https://admin.exchange.microsoft.com/>

The screenshot shows the Exchange Admin Center interface. On the left, a sidebar lists various management categories. The main pane displays a table of rules with columns for State, Rule, Priority, and Action. One rule, 'Autoriser phishing', is highlighted with a checkmark in the 'Enabled' column and has a priority of 3. The right-hand panel provides detailed settings for this specific rule, including its description ('Appliquer cette règle si'), audit severity ('Set audit severity level to "Do not audit"'), and spam confidence level ('Set the spam confidence level (SCI) to "-1"').

Il faut également autoriser l'envoi des liens de phishing dans le mail en passant par le portail de sécurité Microsoft : <https://security.microsoft.com/>

The screenshot shows the Microsoft 365 Defender interface under the 'Stratégies et règles' (Strategies and Rules) section. The 'Liens fiables' (Trusted Links) sub-section is displayed, listing various security policies. The policy 'Enable\_GoPhish' is selected and highlighted with a green dot, indicating it is active with a priority of 0. A tooltip for this policy explains its function: preventing users from clicking on URLs in emails and Microsoft Teams that have been flagged as malicious.

Reste à voir l'autorisation de l'adresse mail pour que Go Phish modifier l'expéditeur dans le header du mail