

Locqueneux Owen

Fen-Chong Arthur

Felicio Thomas

Projet Malware

2022-2023

Table des matières

[Mise en place 3](#_Toc118555737)

[1- Installation de Kali linux en machine virtuel sur un EC2 google cloud 3](#_Toc118555738)

[Prendre un nom de domaine 1&1Onos avec certificat ssl 5](#_Toc118555739)

[Configuration des records DNS avec EC2 5](#_Toc118555740)

[Création de serveurs : apache (web), smtp (postfix) gophish et evilginx2 5](#_Toc118555741)

[Installation du certificat SSL/TLS sur le serveur web 5](#_Toc118555742)

[Envoi du mail qui redirige vers une fausse page evilginx2 office365 5](#_Toc118555743)

[Outils 5](#_Toc118555744)

[1- Github et les commandes git 5](#_Toc118555745)

[2- DNS et Record DNS 5](#_Toc118555746)

[a- SSL/TLS 6](#_Toc118555747)

[b- Protocoles SMTP, IMAP, POP 6](#_Toc118555748)

[Index 6](#_Toc118555749)

# Mise en place

## Installation de Kali linux en machine virtuel sur un EC2 google cloud

On se créer un compte google cloud pour pouvoir ensuite créer une Instance de VM dans laquelle on va configurer et installer une machine Debian :

Une image contenant texte

Description générée automatiquement

Plateforme Google

Pour accéder à la machine dans le cloud on utilise une utilise une connexion sécurisée via le protocole SSH

Une image contenant texte, capture d’écran, moniteur, écran

Description générée automatiquement

Connexion SSH

Une fois l’accès au Shell on suit les étapes suivantes afin d’installer les paquets nécessaires, clés pour avoir une machine Kali dans le cloud :

Une image contenant texte

Description générée automatiquement

On peut ainsi accéder à notre machine kali en tant qu’administrateur :

Une image contenant texte

Description générée automatiquement

## Prendre un nom de domaine 1&1Onos avec certificat ssl

## Configuration des records DNS avec EC2

## Création de serveurs : apache (web), smtp (postfix) gophish et evilginx2

## Installation du certificat SSL/TLS sur le serveur web

## Envoi du mail qui redirige vers une fausse page evilginx2 office365

# Outils

## Github et les commandes git

## DNS et Record DNS

DNS ou Domain Name System est le système qui traduit un nom de domaine facile à retenir comme exemple.com en une adresse IP de server comme 93.184.216.34

Une image contenant texte, clipart, capture d’écran

Description générée automatiquement

L'association d'un nom de domaine à une adresse IP spécifique à l'aide du DNS et des serveurs de noms permet aux visiteurs d'accéder à votre contenu en ligne, y compris votre site web et votre courriel.

Les noms de domaine comme google.com sont des adresses en ligne, utilisées pour accéder à toutes sortes de sites web.

Au niveau technique, un nom de domaine est une chaîne de caractères qui, grâce au DNS, peut être traduite en une adresse électronique (aussi appelée adresse IP) par les systèmes informatiques connectés à l'Internet.

Le DNS fonctionne avec des enregistrements, il en existe plusieurs mais les plus connus sont :

* Type A : il fait correspondre une adresse IPV4 avec un nom de machine
* Type CNAME : utilisé pour crée un alias depuis un enregistrement de type A.
* Enregistrement MX : utilisé pour définir vers quel server de la zone un email à destination du domaine doit être envoyé et avec quelle priorité.
* Type AAAA : il fait correspondre une adresse IPV6 avec un nom de machine

## SSL/TLS

SSL (secure sockets layer) et TLS (transport layer security) sont deux protocoles cryptographiques qui permettent l’authentification, et le chiffrement des données qui transitent entre des serveurs, des machines et des applications en réseau (notamment lorsqu’un client se connecte à un serveur Web). Le SSL est le prédécesseur du TLS. Au fil du temps, de nouvelles versions de ces protocoles ont vu le jour pour faire face aux vulnérabilités et prendre en charge des suites et des algorithmes de chiffrement toujours plus forts, toujours plus sécurisés.

Les certificats numériques utilisent le protocole SSL/TTL destiné à garantir la sécurité de la connexion internet et la protection des données sensibles qui sont transmises entre deux systèmes.

Une deuxième caractéristique du protocole SSL/TLS, non moins importante, est une confirmation de l’authenticité du serveur avec lequel vous communiquez. Son authenticité est vérifiable dans la plupart des navigateurs. Grâce à un certificat SSL, deux serveurs sont en mesure de s’authentifier mutuellement (serveur – Client)

## Protocoles SMTP, IMAP, POP

Les trois principaux protocoles utilisés par un server de messagerie sont le SMTP (Simple Mail Transfer Protocol), le POP (Post Office Protocol) et l’IMAP (Internet Message Access Protocol).

Le protocole de messagerie **POP**

Le protocole POP fonctionne en contactant le service de messagerie et en téléchargeant tous les nouveaux messages à partir de ce service. Une fois téléchargés sur le PC, ils sont supprimés du service de messagerie. Cela signifie qu’une fois les messages électroniques téléchargés, vous ne pouvez y accéder qu’à l’aide du même ordinateur. Si vous essayez d’accéder à votre courrier à partir d’un autre appareil, vous ne pourrez pas accéder aux messages précédemment téléchargés.

Les messages envoyés sont stockés localement sur le PC, et non sur le serveur de courrier.

Le protocole de messagerie **IMAP**

Le protocole IMAP (Internet Message Access Protocol) c’est un peu l’inverse du protocole POP, c’est à dire qu’il a une connexion constante au serveur de messagerie pour pouvoir consulter ses mails. Ce protocole synchronise en permanence les messages contenus sur le serveur et sur le poste de travail. Son avantage réside donc dans la possibilité de consulter ses mails depuis n’importe quel endroit et de pouvoir synchroniser et sauvegarder ses messages sur le serveur.

Le protocole de messagerie **SMTP**

Ce protocole de communication est utilisé pour le transfert des messages électroniques sur le réseau. Il est de type client / serveur. Chaque demande d’envoi par le client est suivie par une réponse de la part du serveur. Il s’agit d’un protocole simple qui utilise le protocole de contrôle de transmissions TCP pour le transfert des données.  
Les échanges de mails sur un serveur de messagerie se font via des ports (une porte pour le serveur) et le protocole SMTP écoute, par défaut, le port 25 avec pour objectif de router les messages.

# Index

Installations de Kali dans le Cloud :

https://www.youtube.com/watch?v=XRJMA67Beh4

https://www.learningjournal.guru/article/google-cloud/free-learning-virtual-machine/

https://www.youtube.com/watch?v=S0YZnY\_4dlw

https://github.com/m0ns7er/GCP

DNS, DNS Records:

<https://whc.ca/blog/le-guide-ultime-du-dns-et-des-serveurs-de-noms-edition-2020/>

https://support.microsoft.com/fr-fr/office/que-sont-les-protocoles-pop-et-imap-ca2c5799-49f9-4079-aefe-ddca85d5b1c9