

Locqueneux Owen

Fen-Chong Arthur

Felicio Thomas



Projet Malware

2022-2023

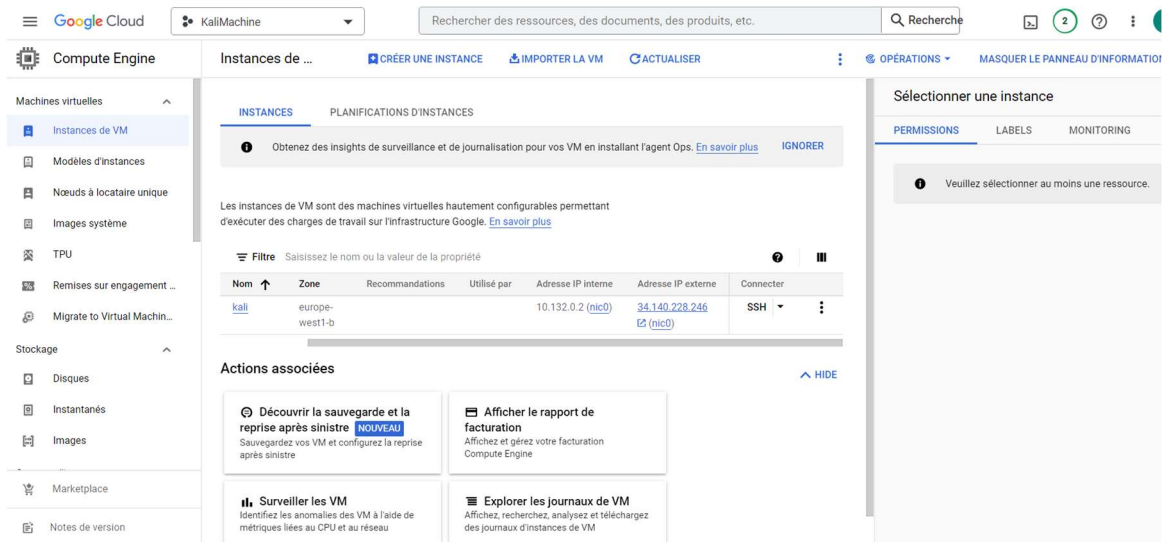
Table des matières

Mise en place.....	2
a- Installation de Kali linux en machine virtuel sur un EC2 google cloud.....	3
b- Prendre un nom de domaine 1&1 Ionos avec certificat ssl.....	4
c- Configuration des records DNS avec EC2	6
d- Création de serveurs : apache (web), smtp (postfix) gophish et evilginx2	8
e- Envoi du mail qui redirige vers une fausse page evilginx2 office365.....	14
Outils	14
1- Github et les commandes git.....	14
2- DNS et Record DNS.....	15
• SSL/TLS.....	15
• Protocoles SMTP, IMAP, POP	16
Index	17

Mise en place

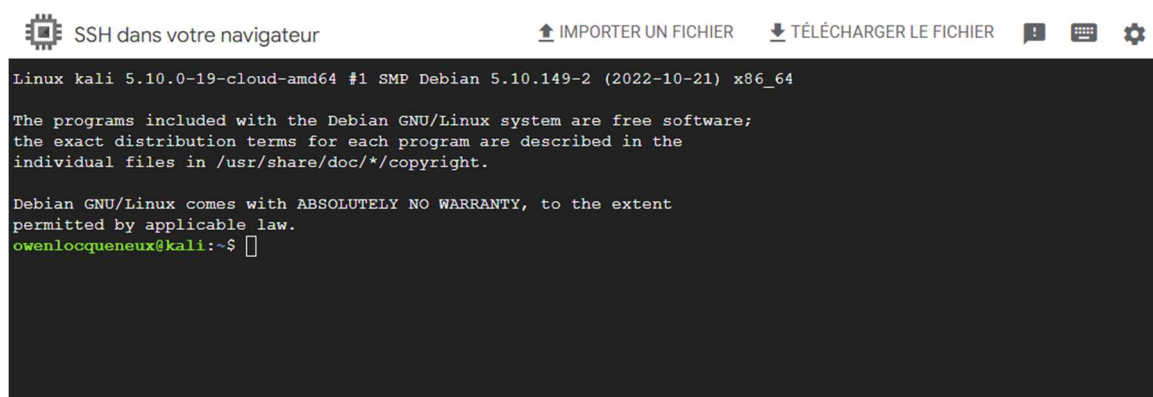
a- Installation de Kali linux en machine virtuel sur un EC2 google cloud

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 :



Plateforme Google

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



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 :

Kali linux on GCP

1. Add repo /etc/apt/source.list (<https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/>)
2. apt update
3. gpg --keyserver pgpkeys.mit.edu --recv-key ED444FF07D8D0BF6
4. gpg -a --export ED444FF07D8D0BF6 | sudo apt-key add -
5. apt upgrade
6. install metapackage (<https://www.kali.org/docs/general-use/metapackages/>)

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

```
Linux kali 5.10.0-19-cloud-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov  4 22:18:36 2022 from 35.235.243.224
└─(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/

This is a cloud installation of Kali Linux. Learn more about
the specificities of the various cloud images:
⇒ https://www.kali.org/docs/troubleshooting/common-cloud-setup/

(Run: "touch ~/.hushlogin" to hide this message)
owenlocqueneux@kali:~$ sudo -i
└─(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/


This is a cloud installation of Kali Linux. Learn more about
the specificities of the various cloud images:
⇒ https://www.kali.org/docs/troubleshooting/common-cloud-setup/

(Run: "touch ~/.hushlogin" to hide this message)
└─(root@kali) ~[~]
#
```

b- Prendre un nom de domaine 1&1 Ionos avec certificat ssl

Nous avons choisi comme nom de domaine "aot-project.com" avec un certificat ssl.

Nom de domaine disponible !

 aot-project.com

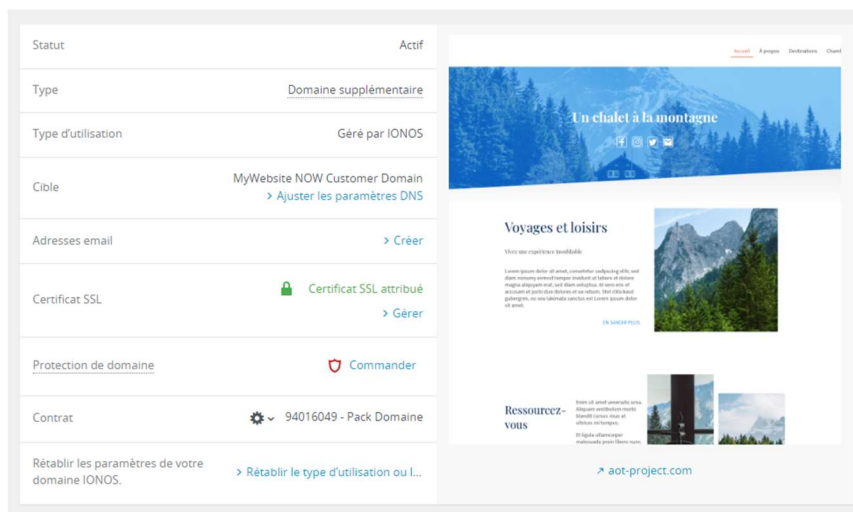
Offre de bienvenue ⓘ

~~10 € HT/an~~

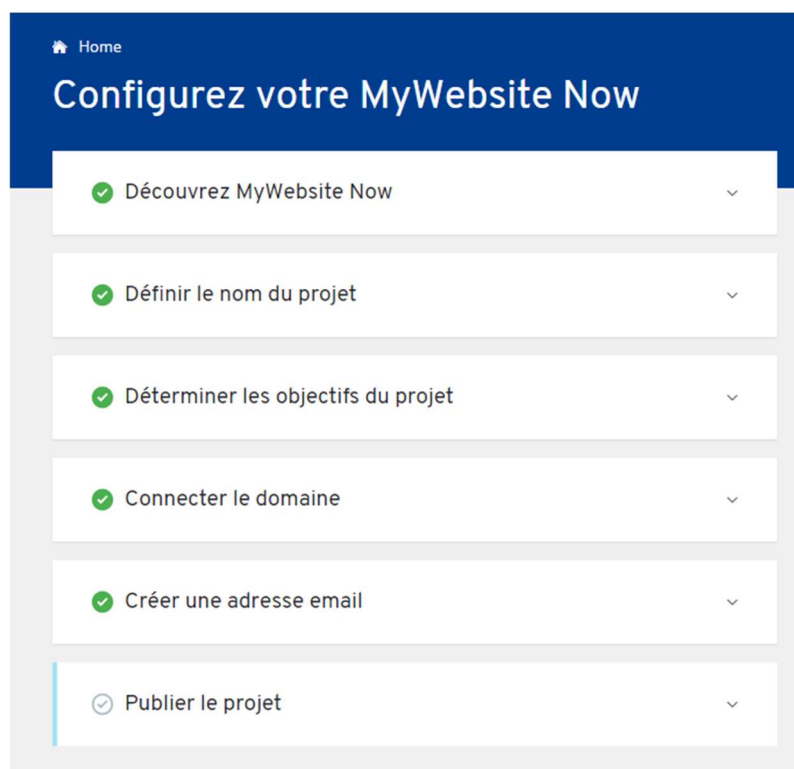
1 € HT/an

pour 1 an
























Ajouter



Pour afficher une page internet et pouvoir accéder au site via la barre de recherche, nous avons utilisé “My Website Now”, un éditeur de site.



Nous avons aussi les enregistrements dns avec une adresse IP.

Ajouter un enregistrement					
<input type="checkbox"/>	TYPE	NOM D'HÔTE	VALEUR	SERVICE ▲	ACTIONS
<input type="checkbox"/>	CNAME	_domainconnect	_domainconnect.ionos.com	Domain Connect	 
<input type="checkbox"/>	MX	@	mx00.ionos.fr	Mail	 
<input type="checkbox"/>	MX	@	mx01.ionos.fr	Mail	 
<input type="checkbox"/>	CNAME	autodiscover	adsredir.ionos.info	Mail	  
<input type="checkbox"/>	A	@	217.160.0.148	MyWebsite NOW ...	 
<input type="checkbox"/>	AAAA	@	2001:8d8:100f:f000:0:0:0:200	MyWebsite NOW ...	 
<input type="checkbox"/>	TXT	_dep_ws_mutex	"c516dc52833b95682321f2f919330e979ec03d1c...	MyWebsite NOW ...	  
<input type="checkbox"/>	A	www	217.160.0.148	MyWebsite NOW ...	 
<input type="checkbox"/>	AAAA	www	2001:8d8:100f:f000:0:0:0:200	MyWebsite NOW ...	 
<input type="checkbox"/>	TXT	_dep_ws_mutex.www	"40bd5ae2d0261c57d9b6fc451cbda2f371f13fbc...	MyWebsite NOW ...	  

c- Configuration des records DNS avec EC2

Création d'une zone publique gérée dans Cloud DNS :

Type de zone ?

☐ Privé

☒ Public

Nom de zone * ?

Exemple : exemple-nom-zone

Nom DNS * ?

Exemple : mazonex.exemple.com

DNSSEC * ▼ ?

Description

Cloud Logging ?

☐ Activé

☒ Désactivé

Une fois la zone créée, vous pouvez ajouter des ensembles d'enregistrements de ressources et modifier les réseaux sur lesquels la zone est visible.

On a bien la page détails de la zone qui s'affiche. Les enregistrements NS et SOA par défaut ont été créés automatiquement.

Services réseau

Détails de la z...

MODIFIER

CONFIGURATION DU SERVICE D'ENREGISTREMENT

my-new-zone

Nom DNS

aot-project.com.

Type

Public

DNSSEC ?

Désactivé

Cloud Logging

Désactivés

JEUX D'ENREGISTREMENTS

AJOUTER UN JEU D'ENREGISTREMENTS

SUPPRIMER LES JEUX D'ENREGISTREMENTS

ACTUALISER

Filtre

Filtrer les jeux d'enregistrements

?

III

<input type="checkbox"/>	Nom DNS ↑	Type	TTL (secondes)	Règle de routage		
<input type="checkbox"/>	aot-project.com.	SOA	21600	Par défaut	▼	✎
<input type="checkbox"/>	aot-project.com.	NS	21600	Par défaut	▼	✎

Création d'un enregistrement qui pointe le domaine vers une adresse IP externe via google cloud :

Nom DNS

aot-project.com.

?

Type d'enregistrement d...

A

?

TTL *

5

?

Unité d...

minutes

?

Règle de routage

☒ Type d'enregistrement par défaut

☐ Round robin pondéré

☐ Basée sur la géolocalisation

Adresse IPv4 ?

Adresse IPv4 1 *

217.160.0.148

Exemple : 192.0.2.91

+ AJOUTER UN ÉLÉMENT

CRÉER

ANNULER

LIGNE DE COMMANDE ÉQUIVALENTE

Création d'un enregistrement CNAME pour le sous-domaine www :

Nom DNS ?

Type d'enregistrement d...
CNAME ▼ ?

TTL * ?

Unité d...
minutes ▼ ?

Règle de routage

☒ Type d'enregistrement par défaut

☐ Round robin pondéré

☐ Basée sur la géolocalisation

Nom canonique ?

Nom canonique 1 *

Exemple : server-1.example.com.

+ AJOUTER UN ÉLÉMENT

CRÉER ANNULER

Voici tout les enregistrements DNS créés :

<input type="checkbox"/>	Nom DNS ↑	Type	TTL (secondes)	Règle de routage		
<input type="checkbox"/>	aot-project.com.	A	300	Par défaut	▼	✎
<input type="checkbox"/>	aot-project.com.	SOA	21600	Par défaut	▼	✎
<input type="checkbox"/>	aot-project.com.	NS	21600	Par défaut	▼	✎
<input type="checkbox"/>	www.aot-project.com.	CNAME	300	Par défaut	▼	✎

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

Apache2 est un serveur http qui utilise un système de module qui permet de rajouter des fonctionnalités après coup (on ne sera pas obligé de recompiler depuis les sources pour rajouter une fonction particulière).


```

(root@kali) - [~]
# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: disabled)
   Active: active (running) since Mon 2022-11-21 18:46:57 UTC; 3min 14s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 1789 (apache2)
     Tasks: 55 (limit: 4688)
    Memory: 13.2M
       CPU: 34ms
    CGroup: /system.slice/apache2.service
            └─1789 /usr/sbin/apache2 -k start
            └─1790 /usr/sbin/apache2 -k start
            └─1791 /usr/sbin/apache2 -k start

Nov 21 18:46:57 kali systemd[1]: Starting The Apache HTTP Server...
Nov 21 18:46:57 kali systemd[1]: Started The Apache HTTP Server.

```

Gophish est un framework de phishing open-source qui permet d'effectuer des campagnes de phishing plus facilement.

Installation de Gophish :

```

(root@kali) - [/home]
# ls
gophish-v0.7.1-linux-64bit.zip  leagu  owenl  owenlocqueneux  test  thomas

(root@kali) - [/home]
# unzip gophish-v0.7.1-linux-64bit.zip -d /home/owenlocqueneux/gophish/
Archive:  gophish-v0.7.1-linux-64bit.zip
  creating: /home/owenlocqueneux/gophish/static/js/dist/app/
  inflating: /home/owenlocqueneux/gophish/static/js/dist/vendor.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/users.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/dashboard.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/templates.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/campaigns.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/landing_pages.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/gophish.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/campaign_results.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/settings.min.js
  inflating: /home/owenlocqueneux/gophish/static/js/dist/app/sending_profiles.min.js
  creating: /home/owenlocqueneux/gophish/static/js/src/vendor/ckeditor/plugins/
  creating: /home/owenlocqueneux/gophish/static/js/src/vendor/ckeditor/lang/
  creating: /home/owenlocqueneux/gophish/static/js/src/vendor/ckeditor/skins/

```

```

(root@kali)-[/home/owenloqueneux]
# cd gophish/

(root@kali)-[/home/owenloqueneux/gophish]
# ls
LICENSE  README.md  VERSION  config.json  db  gophish  static  templates

(root@kali)-[/home/owenloqueneux/gophish]
# ./gophish
time="2022-11-21T21:57:27Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2022-11-21T21:57:27Z" level=warning msg="No contact address has been configured."
time="2022-11-21T21:57:27Z" level=warning msg="Please consider adding a contact_address entry in your config.js
on"
goose: migrating db environment 'production', current version: 0, target: 20180830215615
OK      20160118194630_init.sql
OK      20160131153104_0.1.2_add_event_details.sql
OK      20160211211220_0.1.2_add_ignore_cert_errors.sql
OK      20160217211342_0.1.2_create_from_col_results.sql
OK      20160225173824_0.1.2_capture_credentials.sql
OK      20160227180335_0.1.2_store-smtp-settings.sql
OK      20160317214457_0.2_redirect_url.sql
OK      20160605210903_0.2_campaign_scheduling.sql
OK      20170104220731_0.2_result_statuses.sql
OK      20170219122503_0.2.1_email_headers.sql
OK      20170827141312_0.4_utc_dates.sql
OK      20171027213457_0.4.1_maillogs.sql
OK      20171208201932_0.4.1_next_send_date.sql
OK      20180223101813_0.5.1_user_reporting.sql
OK      20180524203752_0.7.0_result_last_modified.sql
OK      20180527213648_0.7.0_store_email_request.sql
OK      20180830215615_0.7.0_send_by_date.sql
time="2022-11-21T21:57:27Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2022-11-21T21:57:27Z" level=info msg="Creating new self-signed certificates for administration interface"
time="2022-11-21T21:57:27Z" level=info msg="TLS Certificate Generation complete"
time="2022-11-21T21:57:27Z" level=info msg="Starting admin server at https://127.0.0.1:3333"

```

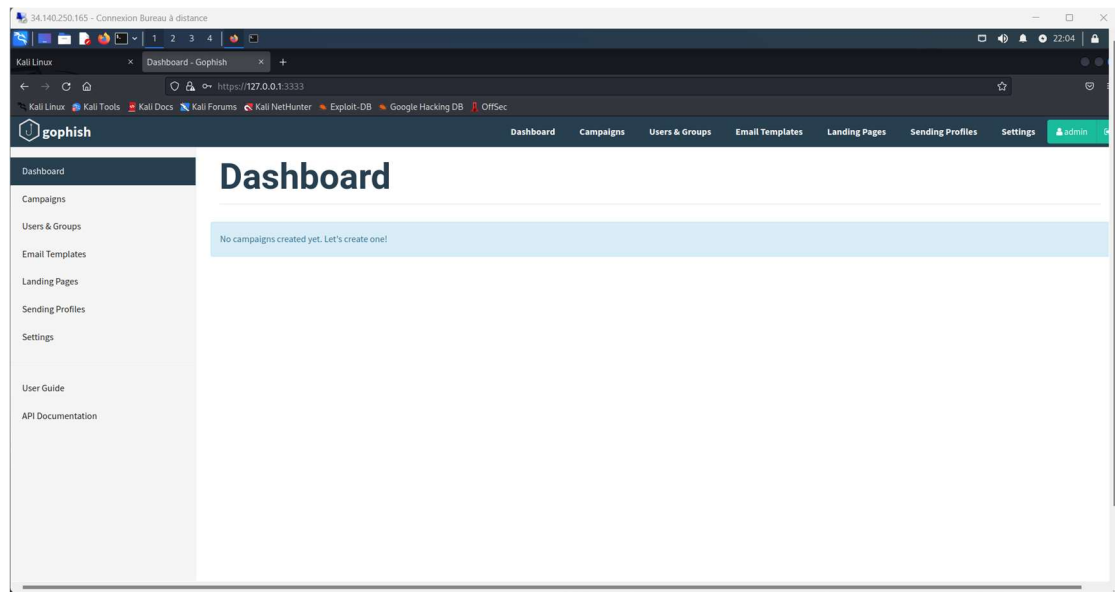
On lance gophish sur le navigateur de notre machine en tapant l'adresse IP donnée :
<https://127.0.0.1:3333>



Please sign in

Username
Password
Sign in

On se log avec le login admin et le mot de passe gophish ce qui nous permet d'accéder au Tableau de bord de gophish:

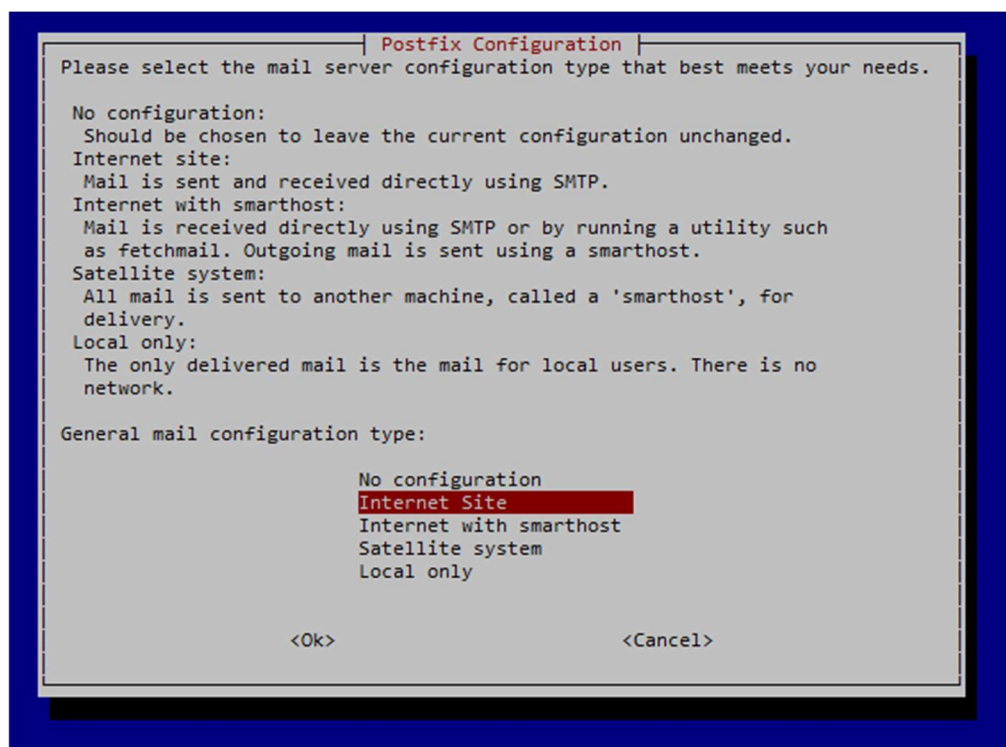


Postfix :

Postfix est un serveur de messagerie électronique. Il se charge de la livraison de courriers électroniques (courriels) et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail.

Installation de Postfix avec la commande :

“apt install postfix”



Initialisation de Postfix

Nous devons modifier le fichier de configuration main.cf pour permettre l'envoi des courriels.

```
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = www.aot-project.com
mydomain = aot-project.com
myorigin = $mydomain
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, localhost.$mydomain,, localhost, $mydomain
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Fichier de configuration main.cf

L'envoi d'un mail dans l'invité de commande se fait avec la commande suivante :

Echo "message" | -s "sujet du mail" <adresse mail>

Evilginx2 est un outil qui permet de récupérer des identifiants d'authentification. Le principe de fonctionnement est le suivant : à travers un lien malveillant, evilginx2 fait office de proxy entre le site cible et la victime afin d'intercepter ses identifiants de connexion (attaque de l'homme du milieu).

Tout d'abord, avant d'installer Evilginx2 il nous faut installer Golang qui est un langage open-source développé par google pour créer des logiciels simples, fiables et efficaces.

```
(root@kali) - [/home/owenlocqueneux]
# wget https://golang.org/dl/go1.19.3.linux-amd64.tar.gz
--2022-11-23 13:02:50-- https://golang.org/dl/go1.19.3.linux-amd64.tar.gz
Resolving golang.org (golang.org)... 66.102.1.141, 2a00:1450:400c:c06::8d
Connecting to golang.org (golang.org)|66.102.1.141|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://go.dev/dl/go1.19.3.linux-amd64.tar.gz [following]
--2022-11-23 13:02:51-- https://go.dev/dl/go1.19.3.linux-amd64.tar.gz
Resolving go.dev (go.dev)... 216.239.36.21, 216.239.34.21, 216.239.32.21, ...
Connecting to go.dev (go.dev)|216.239.36.21|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://dl.google.com/go/go1.19.3.linux-amd64.tar.gz [following]
--2022-11-23 13:02:51-- https://dl.google.com/go/go1.19.3.linux-amd64.tar.gz
Resolving dl.google.com (dl.google.com)... 64.233.184.136, 64.233.184.190, 64.233.184.93, ...
Connecting to dl.google.com (dl.google.com)|64.233.184.136|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 148907134 (142M) [application/x-gzip]
Saving to: 'go1.19.3.linux-amd64.tar.gz'

go1.19.3.linux-amd64.ta 100%[=====>] 142.01M 298MB/s in 0.5s

2022-11-23 13:02:51 (298 MB/s) - 'go1.19.3.linux-amd64.tar.gz' saved [148907134/148907134]
```

```
(root@kali) - [/home/owenlocqueneux]
# tar -C /usr/local -xzf go1.19.3.linux-amd64.tar.gz
```

```
(root@kali) - [/usr/local/go]
# echo "export PATH=$PATH:/usr/local/go/bin" >> ~/.profile

(root@kali) - [/usr/local/go]
# echo "export GOPATH=~/.go" >> ~/.profile

(root@kali) - [/usr/local/go]
# source ~/.profile

(root@kali) - [/usr/local/go]
# go version
go version go1.19.3 linux/amd64
```

Installation de evilnginx:


```
(root@kali) - [/home/owenlocqueneux]
# git clone https://github.com/kgretzky/evilnginx2.git
Cloning into 'evilnginx2'...
remote: Enumerating objects: 2722, done.
remote: Total 2722 (delta 0), reused 0 (delta 0), pack-reused 2722
Receiving objects: 100% (2722/2722), 3.61 MiB | 6.08 MiB/s, done.
Resolving deltas: 100% (1409/1409), done.

(root@kali) - [/home/owenlocqueneux]
# ls
evilnginx2  go1.19.3.linux-amd64.tar.gz  gophish  gophish-v0.7.1-linux-64bit.zip

(root@kali) - [/home/owenlocqueneux]
# cd evilnginx2/
```

```
(root@kali) - [/home/owenlocqueneux/evilnginx2]
# make install

(root@kali) - [/home/owenlocqueneux/evilnginx2]
# evilnginx
```



```
-- Gone Phishing --
by Kuba Gretzky (@mrgretzky) version 2.4.2

[13:31:01] [inf] loading phishlets from: /usr/share/evilnginx/phishlets/
[13:31:01] [inf] loading configuration from: /root/.evilnginx
[13:31:01] [inf] blacklist mode set to: off
[13:31:01] [inf] redirect parameter set to: nl
[13:31:01] [inf] verification parameter set to: wy
[13:31:01] [inf] verification token set to: be29
[13:31:01] [inf] unauthorized request redirection URL set to: https://www.youtube.com/watch?v=dQw4w9WgXcQ
[13:31:01] [inf] blacklist: loaded 0 ip addresses or ip masks
[13:31:01] [war] server domain not set! type: config domain <domain>
[13:31:01] [war] server ip not set! type: config ip <ip_address>
```

phishlet	author	active	status	hostname
outlook	@mrgretzky	disabled	available	
twitter-mobile	@white_fi	disabled	available	
twitter	@white_fi	disabled	available	
airbnb	@ANONUD4Y	disabled	available	
github	@audibleblink	disabled	available	
instagram	@charlesbel	disabled	available	
paypal	@An0nud4y	disabled	available	
protonmail	@jamescullum	disabled	available	
reddit	@customsync	disabled	available	
tiktok	@An0nud4Y	disabled	available	

```
: config domain aot-project.com
[13:39:55] [inf] server domain set to: aot-project.com
[13:39:55] [war] server ip not set! type: config ip <ip_address>
: config ip 217.160.0.148
[13:40:15] [inf] server IP set to: 217.160.0.148
: q
```


e- Envoi du mail qui redirige vers une fausse page evilginx2 office365

Outils

1- Github et les commandes git

GitHub est un service web d'hébergement et de gestion développement de logiciels utilisant le logiciel de gestion de versions Git. Git est un logiciel de gestion de versions décentralisé, open-source et gratuit, il est très utile pour les projets informatiques en équipe

Voici les commandes de base git afin de créer notre projet :

```
PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> git init
Initialized empty Git repository in C:/Users/owenl/Desktop/Cours Cyber/Proje
t Malware/.git/
PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> git add README.md
fatal: pathspec 'README.md' did not match any files
PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> git remote add origin
https://github.com/owen62/MalwareProject.git
```

```
PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> New-Item README.md

Répertoire : C:\Users\owenl\Desktop\Cours Cyber\Projet Malware

Mode                LastWriteTime         Length Name
----                -
-a-----          24/11/2022    14:14             0 README.md

PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> ls

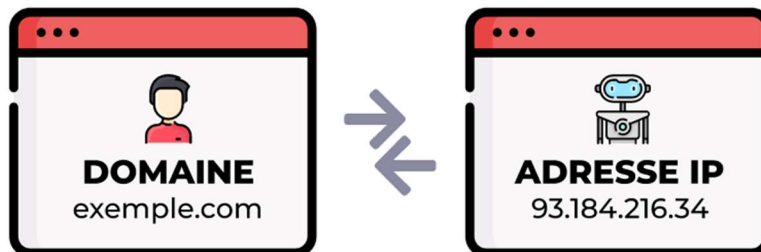
Répertoire : C:\Users\owenl\Desktop\Cours Cyber\Projet Malware

Mode                LastWriteTime         Length Name
----                -
-a-----          04/11/2022    22:36             359 notes.txt
-a-----          14/11/2022    23:28          409115 projectfirstpart.docx
-a-----          24/11/2022    14:14             0 README.md

PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> git add .\README.md
PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> git commit -m "creatin
g a README.md file"
[master (root-commit) 8c3b701] creating a README.md file
1 file changed, 0 insertions(+), 0 deletions(-)
create mode 100644 README.md
PS C:\Users\owenl\Desktop\Cours Cyber\Projet Malware> git push -u origin mas
ter
info: please complete authentication in your browser...
Enumerating objects: 3, done.
Counting objects: 100% (3/3), done.
Writing objects: 100% (3/3), 238 bytes | 238.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
To https://github.com/owen62/MalwareProject.git
```

2- 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 serveur comme 93.184.216.34



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.

Un « DNS record » est simplement une base de données qui associe les URLs à des adresses IP.

Il y a plusieurs types d'enregistrement DNS : « A record » pour la résolution d'adresse IPV4, « AAAA record » pour les adresses IPV6, « TXT record »....

- [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/TLS 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 serveur 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>

Evilginx2 + Go :

<https://kalilinuxtutorial.com/install-evilginx2-on-kali-linux/>

<https://kalilinuxtutorial.com/install-golang-on-kali-linux/>

<https://go.dev/doc/install>

IONOS:

<https://www.ionos.fr/domaine/noms-de-domaine>

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>

SSL/TLS:

<https://www.sslmarket.fr/ssl/certificats>

Gophish:

<https://kifarunix.com/install-gophish-on-ubuntu-18-04-debian-9-8/>

<https://www.golinuxcloud.com/install-gophish-phishing-framework-tutorial/>