Activité 4 – Attaque par ingénierie sociale (hameçonnage associé à du typosquattage)

Propriétés	Description
Présentation	Ce TP a pour objectif de montrer un exemple d'ingénierie sociale en combinant des techniques d'hameçonnage (phishing) et de typosquattage. Concrètement nous allons mettre en ligne la page d'authentification de Facebook et inciter la victime pour qu'elle se connecte sur cette page dans le but de récupérer ses identifiants lorsqu'elle tente de se connecter à son compte.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Compétences	• Protéger les données à caractère personnel. • Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques. • Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service. • Assurer la cybersécurité d'une solution applicative.
Savoirs	• Typologie des risques et leurs impacts. • Cybersécurité : bonnes pratiques, normes et standards.
Prérequis	Connaissances de base concernant l'administration d'un système GNU/Linux.
Outils	Kali, conteneurs sur Docker (Laboratoire n°2) https://forge.aeif.fr/btssio-labos-kali/lab2
Mots-clés	Kali, hameçonnage, typosquattage, typosquating, ingénierie sociale, dns, remédiations, hygiène numérique, respect des bonnes pratiques.
Durée	1 heure
Auteurs	Apollonie Raffalli et Patrizio Valente, avec la relecture de Patrice Dignan et Valérie Martinez. Laboratoire sur Docker : Apollonie Raffalli avec les tests de Christelle Thiry

L'attaque par ingénierie sociale

Selon Wikipedia, « l'ingénierie sociale (social engineering en anglais) est, dans le contexte de la sécurité de l'information, une pratique de manipulation psychologique à des fins d'escroquerie. Les termes plus appropriés à utiliser sont le piratage psychologique ou la fraude psychologique. Les pratiques du piratage psychologique exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles des individus ou organisations pour obtenir quelque chose frauduleusement (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.). En utilisant ses connaissances, son charisme, son sens de l'imposture ou son culot, l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité de sa cible pour obtenir ce qu'il souhaite. »

À noter que ce type d'attaque peut s'effectuer avec ou sans outils informatiques. Par exemple, des hackers ont réussi à obtenir le casier judiciaire de personnalités en utilisant un simple téléphone, car elles connaissaient les habitudes et le vocabulaire généralement utilisé par des policiers. Dans d'autres circonstances, des attaquants ont réussi à obtenir des informations confidentielles en usurpant l'identité d'une personne habilitée toujours par téléphone. L'attaquant peut par exemple faire état d'une adresse de messagerie ou un nom obtenu en amont par de simples recherches sur la toile afin d'accroître sa crédibilité. On peut également citer des attaques visant à se faire passer pour un conseiller bancaire chargé d'intervenir sur un problème de sécurité d'un compte en banque. La personne « paniquée » se laisse manipuler et donne les informations nécessaires à son escroquerie.

Il existe de nombreuses autres types d'attaques (dont celle que nous allons découvrir dans ce TP) liées à l'ingénierie sociale.

Préambule

Le TP proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Plateforme utilisée

Le TP qui vous est proposé utilise le laboratoire 2 contenant 5 conteneurs pré-configurées. **Pour rappel :**

Machine	Nom de domaine pleinement qualifié	Configuration réseau	Applications et services
Serveur sous Debian 12	srvssh.local.sio.fr	Adresse IPv4 : 172.16.10.10/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Client sous Debian 12	clissh.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Client OpenSSH
Attaquant sous Kali Linux	kali.local.sio.fr	Adresse IPv4 : 192.168.56.12/24 Passerelle : 192.168.56.254 Serveur DNS :172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Metasploit Netfilter/Iptables
Routeur sous Debian 12	routeur.local.sio.fr	Adresses IPv4 : eth0 – DHCP eth1 – 192.168.56.254/24 eth2 – 172.16.10.254 Serveur DNS : 172.16.10.10	Netfilter/Iptables
Serveur Metasploitable	srvm.local.sio.fr	Adresse IPv4 : 172.16.10.5/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service Web port 80:TCP (site « mutillidae »)

Toutes les machines sont accessibles en SSH (sur le port 22 à partir de l'hôte qui les héberge) et à partir de l'extérieur.

La machine Kali Linux et le client Debian bénéficient d'une interface graphique accessible via un bureau à distance (protocole RDP sur le port 3389 à partir de l'hôte qui les héberge) et à partir de l'extérieur.

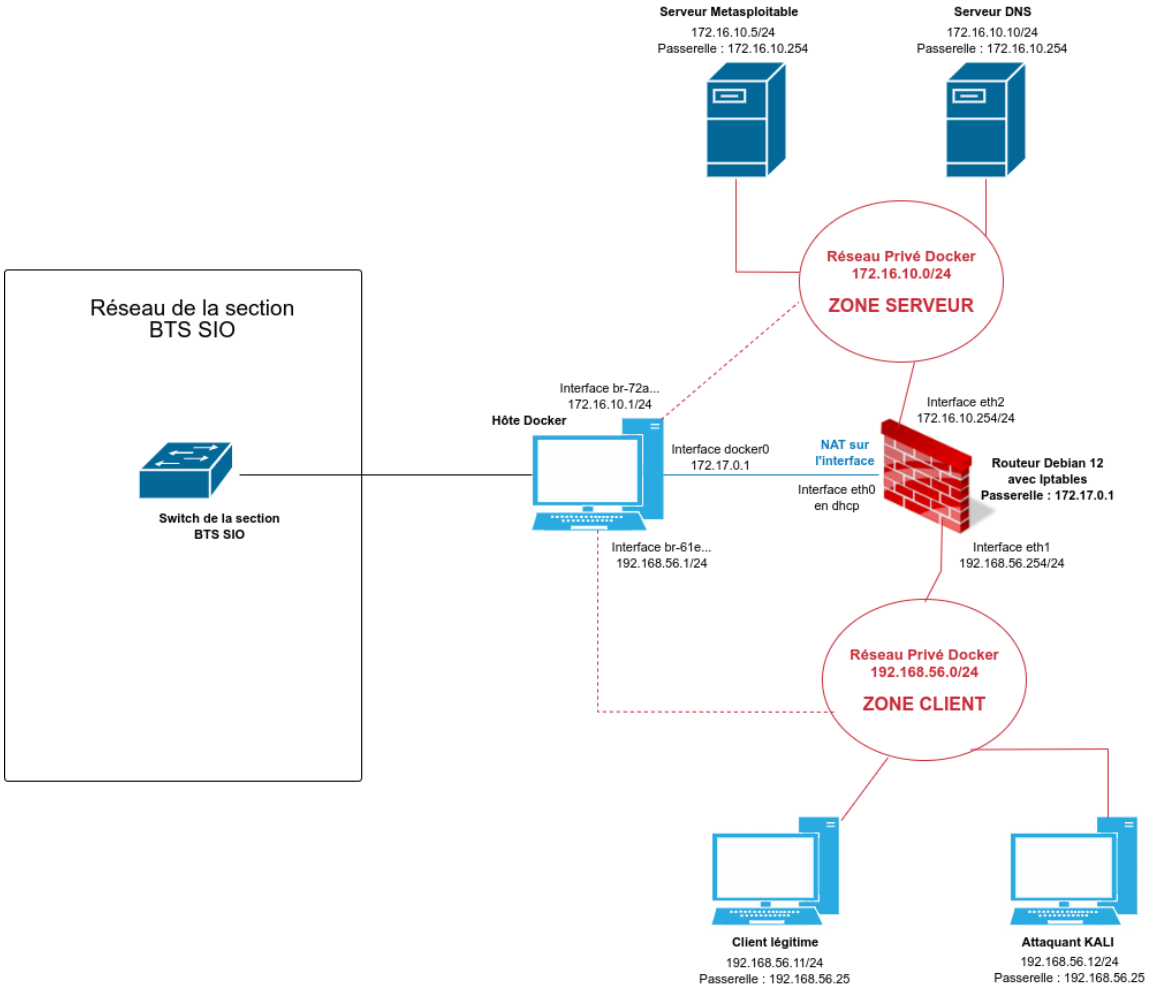
Voici les comptes, les mots de passe et les numéros de ports **accessibles de l'extérieur**, vous permettant d'accéder aux différents conteneurs :

Intitulé de la machine	Nom d'utilisateur	Mot de passe	Ports SSH	Port RDP
Serveur sous Debian 12	etusio	Fghijkl1234*	12222	
Client sous Debian 12	etusio	Fghijkl1234*	22222	23389
Attaquant sous Kali Linux 2023.3	etusio	Fghijkl1234*	32222	33389
Routeur sous Debian 12	etusio	Fghijkl1234*	42222	
Serveur Metasploitable	msfadmin	msfadmin	52222	

Lorsque des commandes nécessitant des privilèges administrateurs seront utilisées, il sera nécessaire d'utiliser la commande **sudo**.

```
etusio@srvssh:~$ sudo service ssh restart
```

Voici une représentation logique de la maquette proposée dans le cadre de ce laboratoire :



- Lancer le laboratoire : **bash gestion_lab2.sh -c**
- Vérifier que les 5 conteneurs sont actifs : **docker ps**

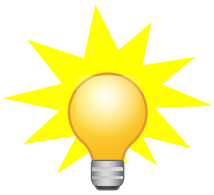
```
CONTAINER ID   IMAGE                          COMMAND                  CREATED       STATUS              PORTS
                                NAMES
dd0866a4c36d   tleemcjr/metasploitable2       "sh -c '/bin/service…"   6 days ago    Up About a minute
                                metasploitable-lab2
4136eb106769   aporaf/kalirolling:lab2        "/lib/systemd/system…"   6 days ago    Up About a minute   22/tcp, 3389/tcp
                                kali-lab2
e879e10e57a3   aporaf/clientdebian12:lab2     "/lib/systemd/system…"   6 days ago    Up About a minute   22/tcp, 3389/tcp
                                client-lab2
7c1ef0ce2e65   aporaf/serveurdebian12:lab2    "/lib/systemd/system…"   6 days ago    Up About a minute   22/tcp, 53/tcp, 53/udp
                                serveur-lab2
13a1ffaae620   aporaf/routeurdebian12:lab2    "/lib/systemd/system…"   6 days ago    Up About a minute   0.0.0.0:12222->12222/tcp, :::12222->12222/tcp, 0.0.0.0:22222->22222/tcp, :::22222->22222/tcp
, 0.0.0.0:23389->23389/tcp, :::23389->23389/tcp, 0.0.0.0:32222->32222/tcp, :::32222->32222/tcp, 0.0.0.0:33389->33389/tcp, :::33389->33389/tcp, 0.0.0.0:52222->52222/tcp, :::52222->52222/tcp, 0.0.0.0:
42222->222/tcp, :::42222->222/tcp   routeur-lab2
```

Mise en œuvre de l'attaque

La première étape consiste à mettre en service le site de « facebook » cloné. Dans notre scénario :

- nous allons récupérer le nom d'utilisateur et le mot de passe de la victime ;
- le serveur ne sera accessible que de l'intérieur du réseau local mais, sur une véritable attaque, il est bien évidemment accessible sur Internet via, très souvent, un nom de domaine proche de l'original (principe du typosquattage), par exemple « faacebook.com ».

La deuxième étape consiste à inciter la victime à se connecter sur le site cloné ou à attendre qu'elle s'y connecte seule par inadvertance.



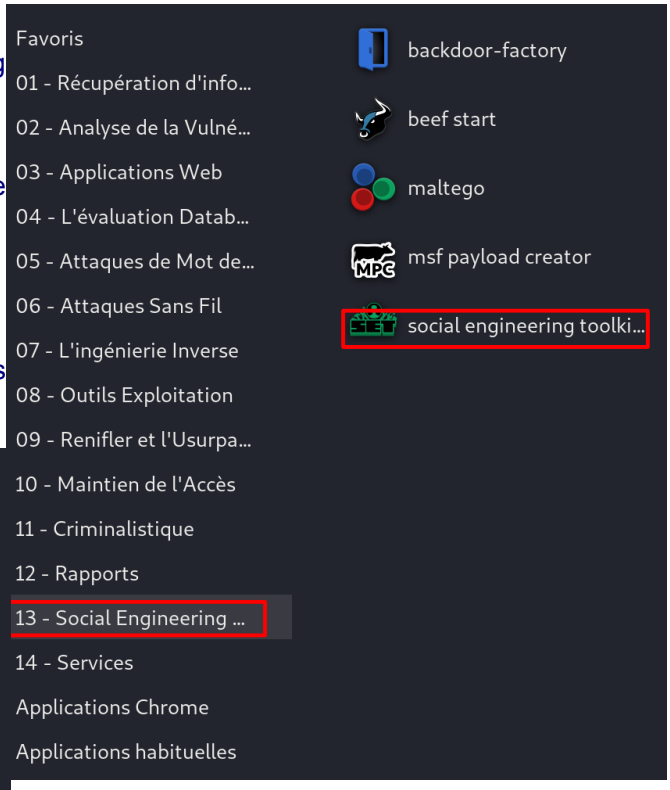
Le typosquattage est une forme de cybercriminalité qui consiste pour les pirates informatiques à enregistrer des domaines avec des noms délibérément mal orthographiés de sites Web connus. Les visiteurs peuvent arriver sur ces sites alternatifs de deux façons différentes :

- en saisissant par inadvertance le nom de sites Web populaires dans leur navigateur Web, par exemple, gooogle.com au lieu de google.com.
- en étant incité à y accéder dans le cadre d'une attaque d'hameçonnage plus large.

Clonage du site de facebook et mise en service

La machine Kali sera utilisée pour réaliser le clone du site de Facebook. L'outil SET (Social Engineering Toolkil) permet d'effectuer une multitude d'attaques de type ingénierie social.

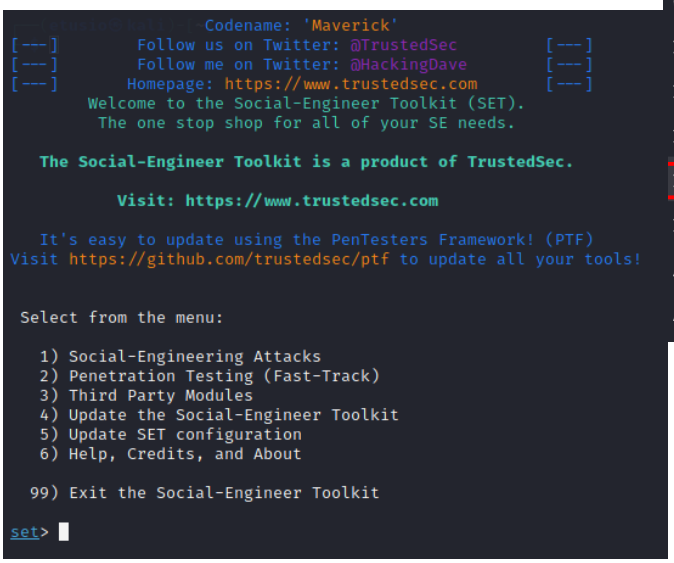
Il est installé par défaut sur Kali ==> Applications
[13] Social Engineering Tools / Social Engineering Toolkil.



Un clic sur Social Engineering Toolkil ouvre une console où il faut :

- saisir le mot de passe d'etusio ;
- accepter la licence.

Le menu du gestionnaire SET présente les outils disponibles.



Dans notre cas, nous allons suivre ce mode opératoire :

- « Social-Engineering Attacks » en tapant 1 dans la console.
- « Website Attack Vectors » en tapant 2 dans la console.
- « Credential Harvester Attack Method » en tapant 3 dans la console.
- « Site Cloner » en tapant 2 dans la console.
- L'adresse du serveur clone est pré-renseignée, il s'agit par défaut de l'adresse IP de votre serveur : dans une réelle attaque, ce serveur sera accessible sur Internet et comme cela est précisé dans le texte, il faut dans ce cas saisir l'adresse IP externe.
- Saisir l'url du site web à cloner, dans notre exemple https://fr-fr.facebook.com/

```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.
56.12]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://fr-fr.facebook.com/

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are a
vailable. 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:
```

Accès au site à partir de la machine cliente

↗ Ouvrez un navigateur, renseignez l'adresse IP du poste Kali (http://192.168.56.12)

Après avoir accepté les cookies ou gérer les paramètres, vous avez accès à l'authentification :

↗ Renseigner une adresse mail et un mot de passe puis valider.

Le site renvoie alors vers la vraie fenêtre de facebook, la victime pense qu'il y a eu juste un petit problème et recommence la procédure.

Sur Kali, l'outil SET récupère de nombreuses informations sur la connexion, dont le login et le mot de passe renseignés.

```
POSSIBLE USERNAME FIELD FOUND: email=victime@credule.fr
POSSIBLE PASSWORD FIELD FOUND: pass=azerty
```

↗ Terminez l'attaque et générez le rapport dans « /root/.set/reports/) » avec la combinaison CTRL + C.
↗ Ouvrez le rapport généré et recherchez le login et le mot de passe de la connexion cliente.

Proposition de contre-mesures

↗️ Lisez les documents suivants :
https://www.windtopik.fr/typosquattage-comment-sen-proteger/
https://www.kaspersky.fr/resource-center/definitions/what-is-typosquatting

Q1. Rappelez le mode opératoire des attaquants.

Q2. Listez les contre-mesures principales du côté des organisations pour limiter les attaques de typosquattage.

Q3. Donnez les moyens dont disposent les propriétaires des sites légitimes contre les typosquatteurs.

Q4. Listez les bonnes pratiques côté internautes afin d'éviter le typosquattage.