QU'EST-CE QUE L'HAMEÇONNAGE ? OU PHISHING EN ANGLAIS ?

Il vous est demandé réaliser un compte rendu sur un logiciel de traitement de texte.

ETAPE 1 :

Regarder les vidéos suivantes :

https://www.cybermalveillance.gouv.fr/nos-articles/video-phishing/

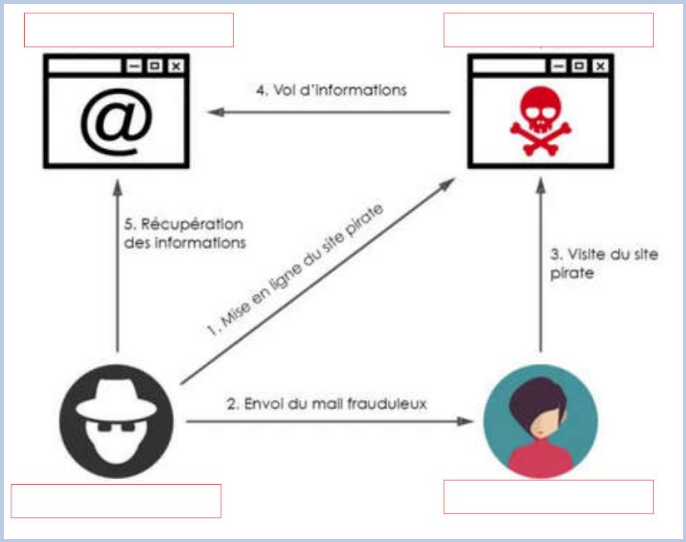
https://www.youtube.com/watch?v=N1fCXk1wQAw

https://www.youtube.com/watch?v=jYYjYaXCy7k

https://www.youtube.com/watch?v=qlFE8UGMYZ0

Quelle action de l'utilisateur peut déclencher cet hameçonnage ?

Compléter le dessin ci-dessous :



Victime

Hameçonneur

Site pirate

Serveur de mel

Regarder la vidéo exemple :

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

Que se passe-t-il dans cet exemple ? Est-ce que l'utilisateur s'en est rendu compte ?

ETAPE 2 :

Lire l'article ci-dessous :

https://lexpansion.lexpress.fr/high-tech/piratage-des-noms-de-domaine-internet-subit-une-attaque-inedite_2063749.html
https://www.futura-sciences.com/tech/actualites/securite-tout-ce-vous-devez-savoir-piratage-dns-75150/

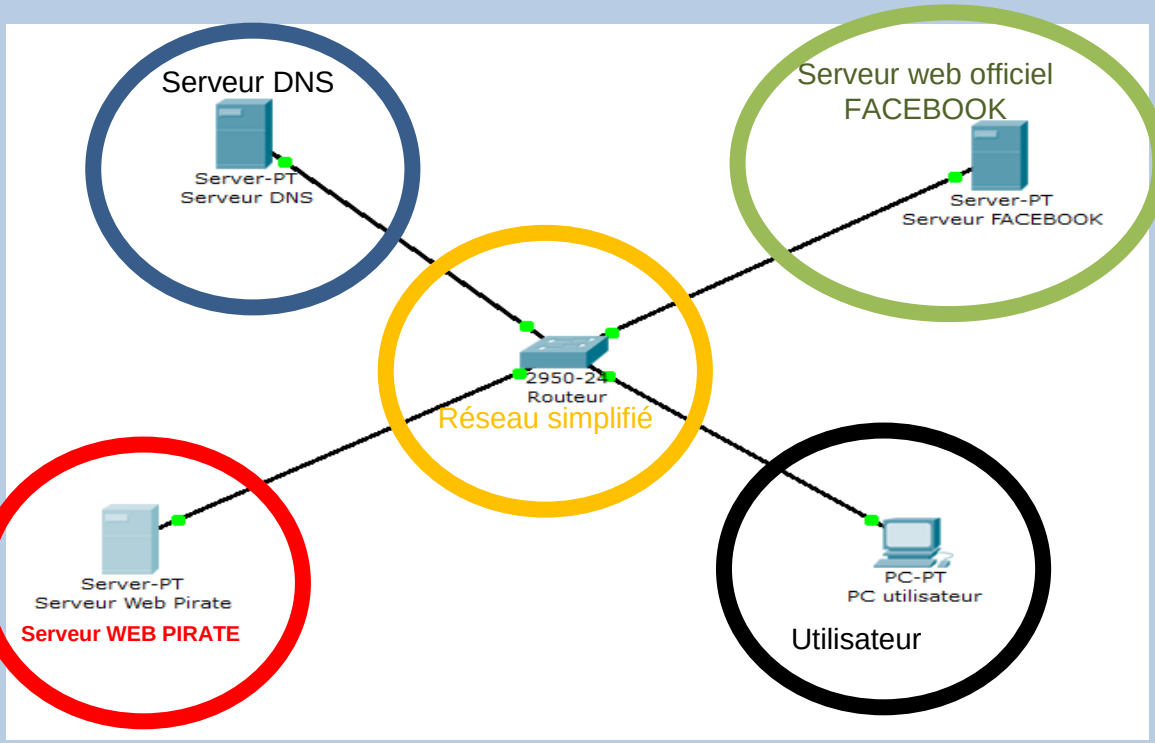
Expliquer de quel type d'attaque il s'agit :

ETAPE 3 :

Nous allons simuler une attaque du serveur DNS de Facebook

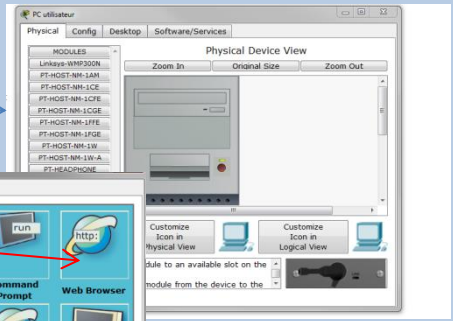
Panique sur le web ce matin : Facebook était inaccessible suite à une panne de DNS touchant principalement l'Europe. Depuis 7h20 ce matin, impossible de se connecter sur son compte Facebook, du moins sur la version Internet du site puisque sa version mobile fonctionnait correctement. Heureusement, le bug est désormais réglé.

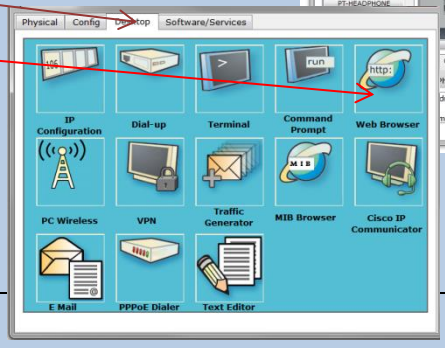
Pour cela nous allons reprendre le schéma réseau ci-dessous :



Trouver sur le net l'adresse IP du serveur de Facebook.

- Ouvrir Cisco Packet Tracer
- Cliquer sur le PC utilisateur
- Puis onglet Desktop
- Enfin sur Web Browser
- Puis entrer l'adresse IP dans L'URL.
- Commenter.

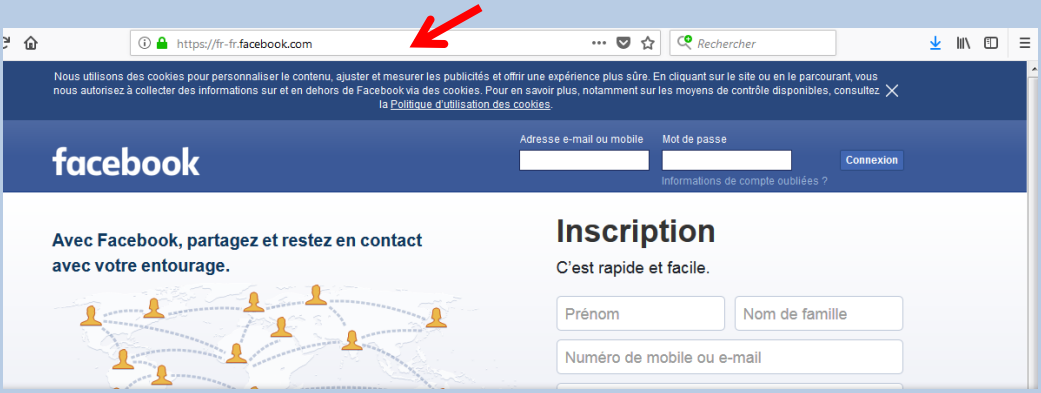




ETAPE 4 :

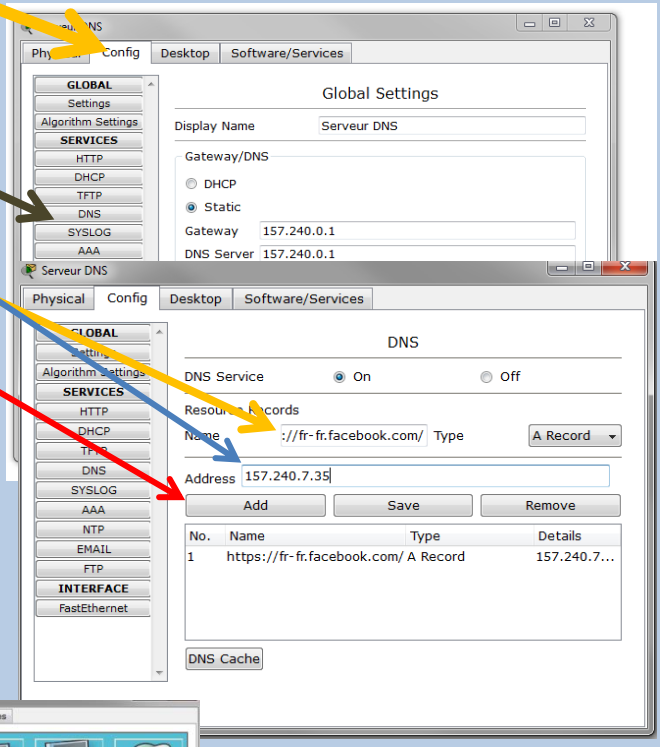
Configurer serveur DNS.

- Trouver l'adresse de Facebook sur le Net.



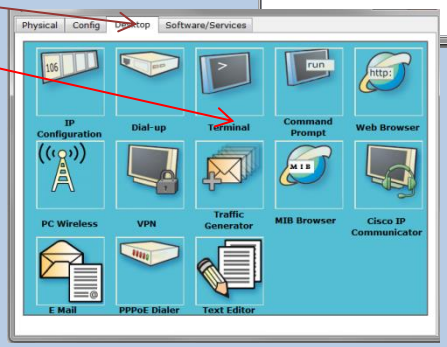
- Cliquer sur le serveur DNS, onglet Config.
- Cliquer sur DNS
- Compléter Name et adresse

  Puis cliquer sur Add.



- Cliquer ensuite sur Pc Utilisateur
- Puis onglet Desktop
- Enfin sur Web Browser
- Puis entrer l'adresse de Facebook dans L'URL.

  Commenter.



ETAPE 5 :

Mark Elliot Zuckerberg souhaite pouvoir accéder à son site, en tapant sur la barre adresse d'un navigateur web, simplement l'adresse facebook.fr . Expliquer votre démarche pour accéder à sa demande.

ETAPE 7 :

Changer les paramètres du serveur DNS :

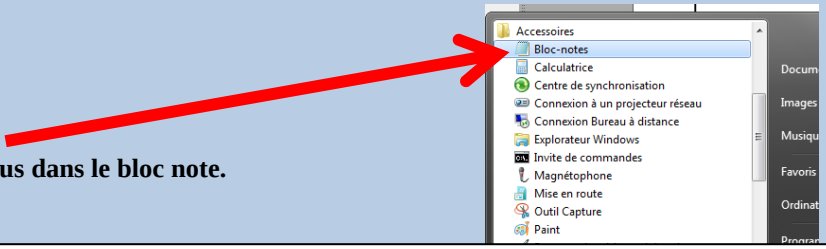
Associer l'adresse www.facebook.fr avec le serveur pirate 157.240.7.36.
Que constatez-vous ?

ETAPE 8 :

Nous allons créer une fausse page internet et pouvoir maintenant récupérer les codes de connexion Facebook de l'utilisateur.

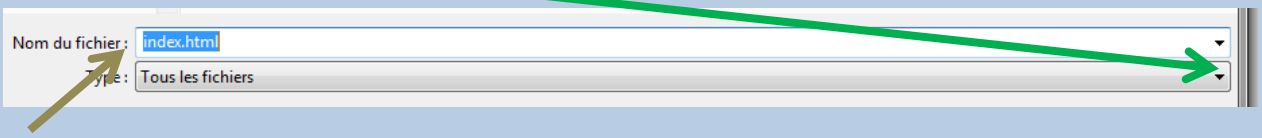
Ecriture de la page Web Pirate.

Ouvrir le Bloc-notes Windows.
Copier et coller le texte ci-dessous dans le bloc note.



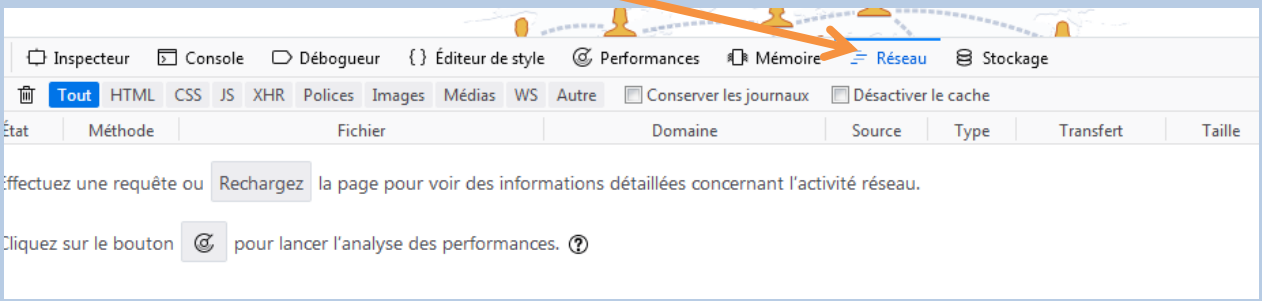

```
<form name="Changement de mot de passe Facebook" action="http://www.facebook.fr" method="get">
<center>
<img src="https://dyw7ncnq1en5l.cloudfront.net/optim/news/46/46727/f_facebook.png" align="center" height="150" width="470">

<center>
<p>
        <b>Un personne a récemment demandé à réinitialiser votre mot de pass Facebook.</b>
</p>

<p>
        <b>Vous n'avez pas demandé ce changement ?</b>
</p>
<p>
        Changer de suite votre mot de passe
</p>
<p>
  <input type="radio" name="civi" value="Mme" /> Madame
  <input type="radio" name="civi" value="Mlle" /> Mademoiselle
  <input type="radio" name="civi" value="Mr" /> Monsieur
</p>
<p>
  Votre nom :<br />
  <input type="text" name="nom" value="" />
</p>
<p>
  Votre prénom :<br />
  <input type="text" name="prenom" value="" />
</p>
<p>
  Votre email :<br />
  <input type="text" name="email" value="" />
</p>
<p>
  Votre mot de passe :<br />
  <input type="password" name="passe" value="" />
</p>
<p>
  Confirmer votre mot de passe :<br />
  <input type="repassword" name="repasse" value="" />
</p>
<p>
  <input type="submit" value="Envoyer" />
  <input type="reset" value="Annuler" />
</p>
<a href="https://fr-fr.facebook.com/">Facebook © 2019</a>
        <img src="https://static.xx.fbcdn.net/rsrc.php/v3/yi/r/OBaVg52wtTZ.png" align="center">
<a href="https://fr-fr.facebook.com/">Facebook © 2019</a>
</form>
```

Fichier / Enregistrer sous
Tous les fichiers

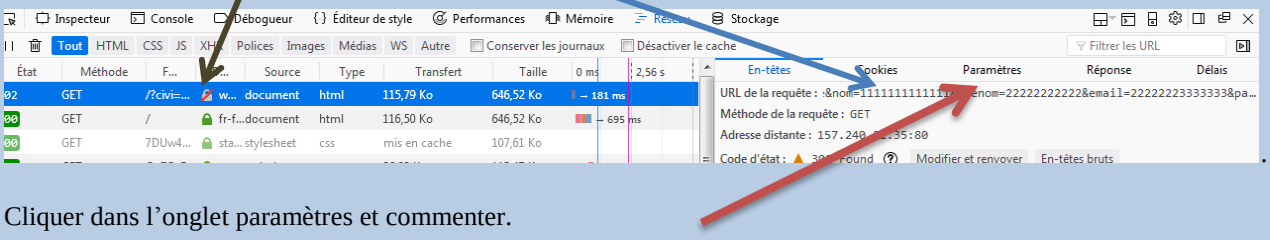


Nom du fichier index.html

- Ouvrir le fichier avec le navigateur Mozilla puis commenter votre page Web.
- Compléter la page (un bon conseil , entrer des données erronées ..).
- Appuyer sur F12 et cliquer sur réseau.



- Cliquer sur envoyer.
- Cliquer sur la 1ère requête et consulter l'URL de la requête



- Cliquer dans l'onglet paramètres et commenter.
- Imaginer si on envoie cette requête à une personne mal intentionnée, que peut-il se passer ?

Retrouver les informations de connexion :

Civilité : ○ Madame ○ Mademoiselle ✕ Monsieur

Nom : Votre nom : **muckerber**

Prénom : Votre prénom : **marc**

Email : Votre email : **muckerbermarc@facebook.com**

Mot de passe de connexion : Votre mot de passe : **fondateur**

Historique Facebook :

Mark Elliot Zuckerberg, né le 14 mai 1984 à White Plains (État de New York), est un informaticien et chef d'entreprise américain. Il est le cofondateur du site web de réseau social Facebook dont il est le président-directeur général. Facebook a été créé en 2004 par Zuckerberg

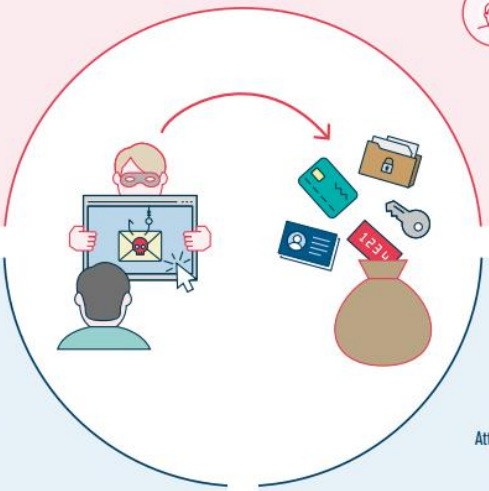
HAMEÇONNAGE

On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.

QUE SE PASSE-T-IL ?

1. Vous recevez un courriel piégé

Le courriel suspect vous invite à :
- cliquer sur une pièce-jointe ou un lien piégés
- communiquer des informations personnelles



2. L'attaquant se fait passer pour une personne ou un tiers de confiance

L'attaquant est alors en mesure de :
- prendre le contrôle de votre système
- faire usage de vos informations

Impact de l'attaque

Intégrité — Authenticité — Disponibilité — Confidentialité

Motivations principales

Atteinte à l'image — Appât du gain — Nuisance — Revendication — Espionnage — Sabotage

COMMENT RÉAGIR ?

Vous êtes victime – Ne perdez pas un instant !

1- Renouvelez immédiatement les identifiants des comptes compromis

2- Contactez votre service informatique ou un expert (ou trouvez le vôtre sur www.cybermalveillance.gouv.fr)

3- Signalez l'incident sur PHAROS (www.internet-signalement.gouv.fr)

4- Portez plainte auprès des services compétents (www.ssi.gouv.fr/en-cas-dincident)

5- Plus de conseils avec INFO ESCROQUERIES au 0 805 805 817 (numéro gratuit)

COMMENT SE PROTÉGER ?

Ne tombez pas dans le piège

- Ne cliquez jamais sur un lien ou une pièce-jointe qui vous semblent douteux
- Ne répondez jamais à un courriel suspect. Au moindre doute, contactez l'expéditeur par un autre canal.
- Evitez l'effet boule de neige ! Disposez d'un mot de passe unique pour chaque application.
  + de conseils avec la CNIL : www.cnil.fr/fr/tag/mots-de-passe
- Vérifiez les paramètres de sécurité de votre compte de messagerie.
- Activez l'authentification à double facteur (la plupart des fournisseurs de messagerie le propose)

#CyberVigilant ! En savoir plus sur les attaques par hameçonnage :
www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001
www.cybermalveillance.gouv.fr/nos-articles/hameconnage-phishing

Les bonnes pratiques de l'informatique : www.ssi.gouv.fr/precautions-elementaires
En savoir plus sur l'ANSSI : www.ssi.gouv.fr
En savoir plus sur Cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

V.1-20180530-1930