Cours 6 :

Phase 1 : La Reconnaissance

JACQUEMIN Mathieu

Disclaimer

- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

La Reconnaissance

En apprendre un maximum sur la cible

Qui, quoi, où, quand, comment

Active ou passive

Les différentes ressources

Internet :
- **Whois (enregistrement d'un domaine)**
- **Mentions légales**
- **Communiqués de presse**
- **Réseaux sociaux**

Internet, plus technique :
- **Adresses IP**
- **Technologies utilisées (serveur mail, web, etc..)**

Les différentes ressources

Hors ligne :
- **Catalogues**
- **Documents internes**

Hors ligne, plus direct :
- **Dumpster diving (faire les poubelles)**
- **Shoulder surfing (observer au dessus de l'épaule**
- **Eavesdropping (écouter des conversations)**

Le Google Hacking

Utiliser l'indexation et la puissance de recherche de Google

Opérateurs de recherche spécifiques (filetype, inurl, etc..)

Permet de trouver du contenu qui ne devrait pas être public

Permet de faire de la recherche d'images

Autres outils de recherche

EPIOS : Retrouve des informations depuis un mail

TinEye : Moteur de recherche inversé d'images

PimEyes : Recherche par reconnaissance faciale

Les réseaux sociaux

Exemples de reconnaissances

En savoir plus

Who is
https://who.is/

Localisation d'IP
https://www.iplocation.net/

Cours 6 :

Phase 1 : La Reconnaissance

SUITE

JACQUEMIN Mathieu

Disclaimer

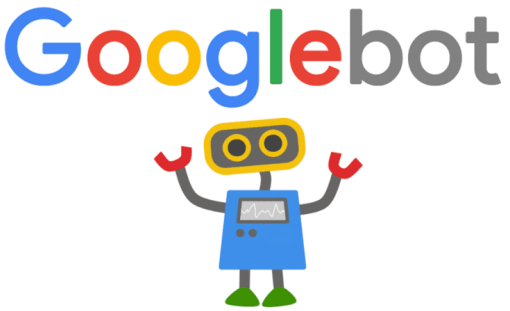
- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

L'indexation

Indexation via un bot (robot ou crawler)

Scan de la page

Fichier robot.txt



L'indexation

Contenu du fichier robots.txt :

```
User-agent: *
Disallow: /wp-admin/
```

Contenu du fichier robots.txt :

```
User-agent: *
Disallow: /*.pdf$
```

Le Google Hacking

Utiliser l'indexation et la puissance de recherche de Google

Opérateurs de recherche spécifiques

Permet de trouver du contenu qui ne devrait pas être public

Google Hacking

Equipements non protégés (Caméra, routeur, imprimante)

Documents sensibles

Page d'authentification d'application web

Opérateurs de recherche

Opérateurs : « »	- Recherche une expression exacte dans l'ordre indiqué
Opérateurs : *	- Remplace des caractères ou des mots
Opérateurs : site:	- Recherche uniquement sur le site web
Opérateurs : inurl:	- Restreint la recherche à l'URL des pages
Opérateurs : intitle:	- Restreint la recherche au titre des pages (balise title)
Opérateurs : filetype:	- Recherche un type d'extension de fichier (pdf,, doc, etc..)
Opérateurs : domaine:	- Restreint la recherche à un domaine
Opérateurs : ip:	- Restreint la recherche à l'ip de la machine
Opérateurs : before/after:	- Permet de rechercher avant ou après une date précise

Exemples

Bonnes pratiques

Tester site:votre_ip_publique (ou nom de domaine)

Tester inurl:/wp-admin/ site:votre_site

Prendre ces précautions grâce à l'utilisation de :

- Navigateur anonyme ou VPN
- Utilisation de la navigation privée
- Utilisation de sandbox (ou VM)

Sandbox Windows

1. Dans la recherche Windows, tapez « Fonctionnalités » ou alors via le « Panneau de configuration », « Programmes et fonctionnalités », puis « Activer ou désactiver des fonctionnalités Windows »

2. Chercher « Bac à sable Windows »

3. Cochez la case puis cliquez sur « Ok », un redémarrage du poste sera nécessaire

4. Vous n'avez plus qu'a rechercher le programme et à l'ouvrir

Permet de créer un environnement sécurisé et isolé du reste du système afin de pouvoir y exécuter des programmes et des fichiers en toute sécurité.

OSINT

Open Source Intelligence

Enquêter sur quelque chose ou quelqu'un

L'exploitation de sources d'informations publiques à des fins de renseignements

Utilisé par le gouvernement, les entreprises, les particuliers, les hackeurs, etc..

DNS
Domain Name System

Protocole permettant de traduire un nom d'hôte en IP

Il utilise le port 53 (UDP)

Un client fait une demande à un serveur DNS, puis ce serveur lui fournit l'adresse IP

NSLOOKUP, PING et TRACEROUTE

NSLOOKUP (ou DIG) permet d'interroger les serveurs DNS pour obtenir les infos pour un nom de domaine

PING sert à tester la communication entre deux équipements

TRACERT (ou TRACEROUTE) permet de suivre les chemins qu'un paquet de données va prendre pour aller de la machine locale à la machine voulue

En savoir plus

Recherche avancée Google
https://www.google.com/advanced_search?hl=fr

Google Hacking Database
https://www.exploit-db.com/google-hacking-database

Shodan
https://www.shodan.io/explore

Internet Archive
https://archive.org/web/