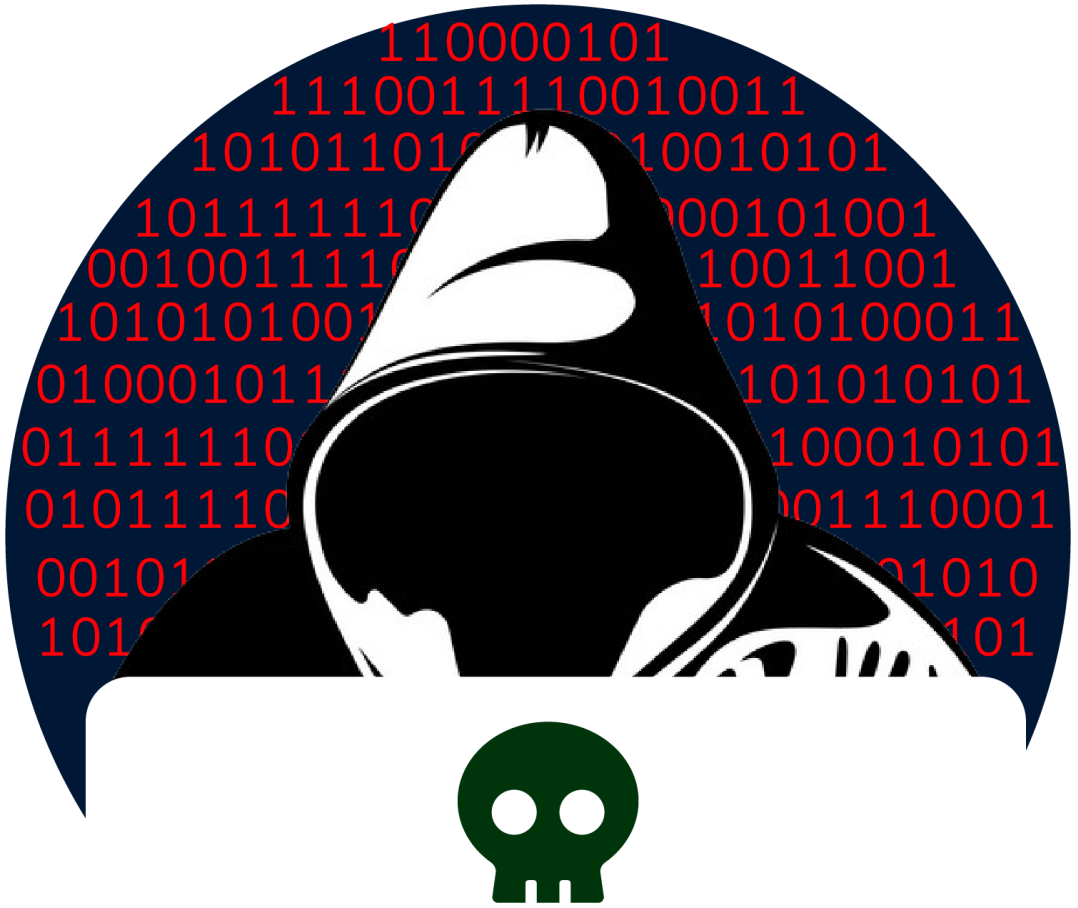
INFORMATIC CENTER HACKING DIVISON

Présentés par

Shadow_Complier

Black_Script

ETHICAL HACKING



INFORMATIC CENTER

INTRODUCTION AU ETHICAL **HACKING**

Le hacking éthique

Dans cette formation spécialement dédiée à la sécurité informatique . Nous allons aborder divers sujets sur la question de la sécurité informatique et sa place dans l'informatique en général.

Dans cette formation nous serons deux .Pour certaines raisons ,nous utiliserons nos pseudos **Shadow_Complier** & **Black_Script**. Nous avons présenterons dans cette formation ,le nécessaire pour être un expert en sécurité informatique .

➔ Origine du mot Hack

➔ Définition du mot dans le jargon informatique

➔ Qu'est ce qu'un hackeur?

➔ Les bases de la sécurité informatique

➔ Vulnérabilité

➔ Divulgation

➔ But de l'hackeur éthique

➔ Origine du mot Hack

Beaucoup d'entre vous demande certainement que signifie le mot **hack? HACK** désigne est un mot Anglais qui qui signifie *To hack (***Découper).**

➔ Définition du mot dans le jargon informatique

Dans le jargon informatique ,le mot **hack** signifie découper une information en **blocs logiques** et le **réassembler**. A ce niveau (**sécurité informatique**) ,l'idée renvoie aux éléments suivants:

1. La modification
2. Le détournement du système de son but initial
3. But du détournement Malveillant ou Bienveillant

➔ Qu’est ce qu’un hackeur?

Prenons un petit instant pour vous détendre. Alors qu’est ce qu’un hackeur ?

Un **hacker éthique** est une personne qui connaît les même outils et techniques qu’un hackeur malveillant en but de résoudre une faille ou vulnérabilité dans un système informatique .

Un **hackeur** est aussi un **bon programmeur** .Dans cette partie essayons d’enlever cette idée préconçue dans tète qu’un hackeur est surement un gars avec un *chapeau noir* car ceci est juste une façon symbolique de de représenter les hackeurs .

➔ Les bases de la sécurité informatique

Sachez que en sécurité informatique il y a des bases aussi .Et nous allons aborder les **4 grands piliers** de la sécurité informatique dont voici ::

1. *La confidentialité*

La confidentialité des informations de deux parties de telle sorte que quand l'information quitte d'un point **A** ➔ vers un point **B** doit ,elle doit rester secret

Exemple:

Quand un message est transmis sur le réseau est que seul **l'émetteur** et **le destinataire** peuvent lire le contenu du message. Il y'a une clause de confidentialité

2. *L' Authenticité*

L'authenticité , la véracité des informations que nous recevons .Le principe est que le récepteur et émetteur soient bonne. Nous aborderons un peu plus le problème d'authenticité avec la célèbre attaque (Man in This middle) dans les autres sessions de cette formation. **MITM**

➔ Les bases de la sécurité informatique

3. *Intégrité*

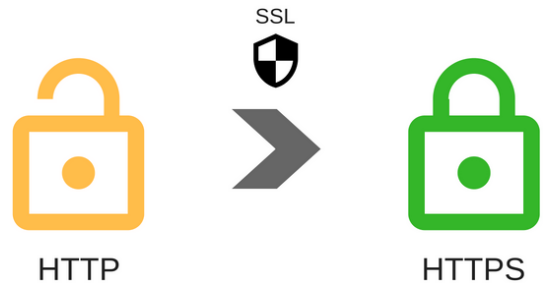
Le message doit être vérifié si elle ne contient pas de mauvais contenu .La vérification des informations ,si l'information est crédible

4. *Disponibilité*

Les informations que nous recevons doivent être disponibles car en informatique l'indisponibilité provoque des disfonctionnements d'un système d'information.

❖ Scénario

Un exemple du **protocole HTTPS** qui est l'association de **Http** + **TLS /SSL**



Validation de l'authenticité quand on sait que c'est Google alors vu que Google fonctionne avec le protocole HTTPS il y a va voir avec un cadenas vert

SI il y a eut validation de la confidentialité **Alors** on est sûr que seul l'émetteur et le destinateur sont les seuls à lire **le message**

➔ Vulnérabilité

Alors ce mot vous l'avez sans doute écouté plusieurs fois mais que signifie t'il?

Une vulnérabilité : on peut la définir comme une faille qui existe dans un système informatique et qui peut être exploiter.

Prenons un exemple simple :

Nous avons une *porte* qui à des deux serrures d'ouvertures, donc pour l'ouvrir il vous faut la clé de ces deux serrures sachant qu'il existe .
Une clé pour chaque serrure donnant accès à la porte .Vous allez me dire il n'y a rien de sorcier la bas à ouvrir la porte ,
il faut donc les deux clés. L'information que nous vous avons caché dans ce cas est la suivante :

En fait l'une des serrures ne fonctionne plus même avec une clé trouvée c'est dire le vrai(celle qui va pour la porte) vous pouviez avoir accès à la porte:

Là c’est une **vulnérabilité** que la porte comporte et qui peut être exploitée par un individu ayant analyser les différentes **options d’intrusions** de la porte.

Dans notre cas ci notre porte peut être vue comme un système C’est comme désactiver un firewall dans un système d’exploitation (Mur de feu) qui protégé une enceinte ou un local dans le terme vulgaire.

➔ Types de vulnérabilités

❖ **Un bug** en français (bestiole) est un disfonctionnement qui survient dans un système ou un programme informatique et qui l'empêche de fonctionner .

Un **bug** peut être volontaire ou involontaire.
Il est **volontaire** lorsqu'il est provoqué délibérément par un programmeur qui décide laisser un **bug** dans un programme ou **une bombe logique**. Il est **involontaire** lorsque le programmeur n'a pas eut l'intention de faire du tord au système et que c'est subvenir par erreur .

❖ Les failles

Une faille est une faiblesse que contient un SI(Système d'informatique)
Les failles sont classées en plusieurs catégories .Nous avons des

- ✓ Failles matérielles
- ✓ Failles logiciels (comment la manipulation du logiciel de n'importe quelle façon)
- ✓ Failles humaines (Elle est la plus importante car elle constitue la clé du hackeur)

Les vulnérabilités sont standardisées par le CVE (COMMON VULNERABILITIES AND EXPOSURES)
Ces Identifiants de vulnérabilités sont fournis par des organismes de sécurité .

➔ Exemple de vulnérabilités informatique

- **Faille XSS** (**Cross-Site Scripting**) dans WordPress **CVE 2016-5834** identifiant

Explication de la faille

Visitez le site regroupant les failles www.xss cve mitre.org

- **Vulnérabilité dans une fonction PHP de WordPress** qui retourne un lien vers un fichier joint

- **Faille XSS**

➔ Divulgation

Il existe des types de divulgations comme :

- ✓ **Full disclosure**(Quand l'on décide de divulguer une faille trouvée dans un système au grand public avec des mauvaises intentions .
- ✓ **Reponsible disclosure**(A ce niveau l'on cache la faille trouvée et l'on essai de le résoudre ou en parle à l'entité concernée .
- ✓ **Darkweb**(nous allons pas faire d'histoires ,c'est la partie cachée du Web)
- ✓ **bug Bounty** (Propose de trouver des bug et vulnérabilités dans un système et toucher une récompense en fonction de la nature de la vulnérabilité)

Par exemple :: ***Facebook*** va payé des hackeurs pour faire des test d'intrusions pour voir si la plateforme est à jour.

Nous allons faire simple car le but de cette formation est de vous expliquer de façon simple .Donc on parle de faille XSS quand un script JS se déclenche tout simplement.

➔ Menaces informatiques

- Intentionnelles
- Accidentelles

Selon **Microsoft Corporation** il existe plusieurs types de menaces dont

- L' Usurpation d'identité
- Le déni service
- L' altération des données

Risques = **MENACES X VULNEABILITES**

➔ Exploits

Des mesures ou techniques qui permettent d'exploiter des vulnérabilités dans un **SI**

➔ But de l'hackeur éthique

Alors vu de tout de ceci quel est le rôle de **l'hackeur éthique**.

- ✓ **Faire des tests**
- ✓ **corriger les bugs et les failles**
- ✓ **Apporter des solutions adéquates aux problèmes en sécurité informatique**