Découverte de la cybersécurité via les Capture The Flag (CTF)

Ugo Proietti et François Vion

Universtité de Mons

February 4, 2022

Principe

Les Capture The Flag sont des compétitions durant lesquelles vous allez devoir trouver des flags. Ils suivent un format standard en fonction de l'évènement {CPU69420}.
Chaque flag rapporte un certain nombre de points.

Il existe un grand nombre de catégories ayant chacune leurs caractéristiques, nous allons vous présenter les plus connues.

Catégories

- Stéganographie
- Cryptographie
- Web
- Réseau
- Forensic
- Reverse Engineering

Stéganographie

La Stéganographie est l'art de la dissimulation. Il s'agit en général de cacher une information là où on ne s'y attend pas.

Exemples

Cacher un message dans un fichier audio
Message écrit en très petit sur une image
Cacher une image dans une autre image

Comptétences utiles

Observation
Utilisation de scripts
Réflexion

Difficulté

1/5

Cryptographie

Contrairement à la stéganographie, la cryptographie n'essaie pas de cacher un message. Elle se contente de le rendre illisible par toute personne n'ayant pas la clé pour le déchiffrer.

Exemples

Cryptage d'un message

Compétences

Connaissance de divers formats d'encodage
Mathématiques pour craquer un code

Difficulté

2/5

Web

Un site web peut cacher un mot de passe, un fichier ou une faille permettant de s'y connecter sans autorisation.

Exemples

Un flag peut être caché dans le code HTML
Un lien vers une ressource cachée
Un faille de sécurité dans un système de connexion

Compétences

HTML, JavaScript, PHP
Structure d'un site web

Difficulté

2/5

Réseau

Surveiller un réseau peut révéler des informations concernant les clients connectés et les données qui y sont échangées.
On peut imaginer récupérer des indentifiants de connexion en interceptant ce qui transite sur le réseau.

Exemples

Lire le contenu des paquets envoyés depuis un PC

Compétences

Difficulté

4/5

Forensic

Une machine peut contenir des informations critiques qui sont récupérables en exploitant la mémoire, le stockage ou des logs générés par le système d'exploitation.
La mémoire peut contenir des mots de passe utilisés par l'OS ou des tokens de connexion utilisés par le navigateur web.

Exemples

Compétences

Difficulté

Reverse Engineering

Un fichier exécutable peut être analysé pour comprendre son fonctionnement et en tirer des informations.

Exemples

Compétences

Difficulté

Blocks of Highlighted Text

Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.

Block 3

Suspendisse tincidunt sagittis gravida. Curabitur condimentum, enim sed venenatis rutrum, ipsum neque consectetur orci, sed blandit justo nisi ac lacus.

Multiple Columns

Heading

1. Statement
2. Explanation
3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Table

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table: Table caption

Theorem

Theorem (Mass–energy equivalence)

$E = mc^2$

Verbatim

Example (Theorem Slide Code)

```
\begin{frame}
\frametitle{Theorem}
\begin{theorem}[Mass--energy equivalence]
$E = mc^2$
\end{theorem}
\end{frame}
```

Figure

Uncomment the code on this slide to include your own image from the same directory as the template .TeX file.

Citation

An example of the `\cite` command to cite within the presentation:

This statement requires citation [**?**].

Plateformes

- root-me.org
- CyberSecurityChallengeBElgium(CSCBE)

Mise en pratique

C'est votre tour ! Créez un comte sur root-me.org et essayez les exercices faciles