

# Activité : connaître les menaces

## Les différents profils de hackers

Les cybercriminels peuvent être des individus ou des groupes qui tentent d'exploiter des vulnérabilités des systèmes d'exploitation ou des logiciels à des fins personnelles ou financières.

Selon leurs motivations et donc le type d'intrusion, on classe les hackers en trois catégories :

- les **hackers au chapeau blanc** utilisent leurs compétences de manière éthique. Ils s'introduisent dans les systèmes informatiques pour en découvrir les vulnérabilités afin de permettre ensuite d'en améliorer la sécurité. Parfois les organisations les encouragent à le faire afin d'évaluer la sécurité de leur infrastructure pour en corriger les failles avant que celles-ci ne soient exploitées.
- les **hackers au chapeau gris** commettent des actes illégaux mais sans en retirer de profits personnels ni causer des dysfonctionnements préjudiciables aux organisations. Les organisations peuvent être informées des vulnérabilités ce qui leur permet de les corriger.
- les **hackers au chapeau noir** recherchent à tirer profit ou à nuire aux organisations en exploitant les vulnérabilités de leur système informatique.

Exercice : Indiquez à quel profil correspond les comportements suivants :

Comportement du hacker	Chapeau blanc	Chapeau gris	Chapeau noir
Après avoir piraté des guichets automatiques à distance à l'aide d'un ordinateur portable, il a travaillé avec des fabricants de guichets automatiques pour résoudre les vulnérabilités de sécurité trouvées.			
Depuis mon ordinateur portable, j'ai transféré plusieurs millions de dollars sur mon compte bancaire en utilisant les numéros de compte et les codes PIN des victimes obtenus en visionnant des enregistrements de ces personnes en train de saisir leurs numéros.			
Mon travail est d'identifier les faiblesses du système informatique de mon entreprise.			
J'ai utilisé un programme malveillant pour compromettre plusieurs systèmes d'entreprise et voler des renseignements sur les cartes de crédit, que j'ai ensuite vendus au plus offrant.			
Je travaille avec des entreprises spécialisées dans la technologie pour résoudre un problème avec le service DNS			

## Outils et exemples de menaces

Associez à chaque outil suivant les menaces possibles.

- Outils :
  - capture de trames,
  - fuite de données sur un serveur,
  - falsification de paquets IP,
  - point d'accès Wifi non protégé,
  - usurpation DNS (empoisonnement du cache DNS).
- Menaces :
  - vols de données sensibles : noms d'utilisateurs, mots de passe, numéros de carte bancaire.
  - récupération d'informations,
  - redirection vers site Web pirates,
  - modifier une communication pour la perturber ou intercepter des informations.

From:  
/ - Les cours du BTS SIO

Permanent link:  
[/doku.php/bloc3s1/hakingmenaces?rev=1642107040](http://doku.php/bloc3s1/hakingmenaces?rev=1642107040)

Last update: 2022/01/13 21:50

