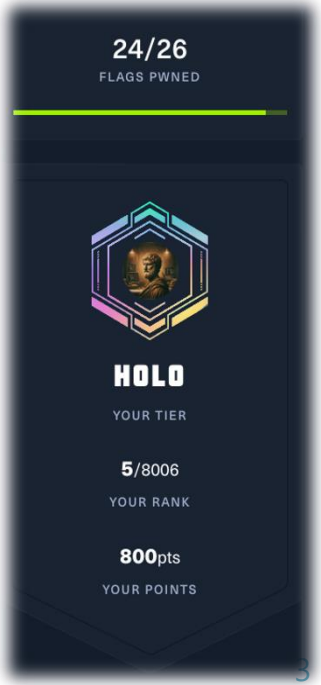
# Les différentes certifications en cybersécurité (and how to get a job in cybersecurity 101)

# Ordre du jour

- Présentation
- Revue des différentes certifications selon les 2 champs principaux en cybersécurité
- Conseils sur comment réussir ses entrevues et trouver un poste

# whoami

- Étudiant au baccalauréat par cumul en cybersécurité à polytechnique
- Pentester + IR depuis 3 ans pour le COCD de la santé
- Grand fan de HackTheBox



# Les 2 principales sphère en cybersécurité

- L'opérationnel

- La gouvernance/sécurité de l'information

# Les certifications en cybersécurité opérationelle

- Blue Team
- Red Team
- Purple Team

# Les certifications en red team : Offsec

- OSCP/OSEP (PEN-200-210/PEN-300)
- OSWA/OSWE (WEB-200/WEB-300)
- EXP-301/312/412

# Les certifications en red team : HackTheBox

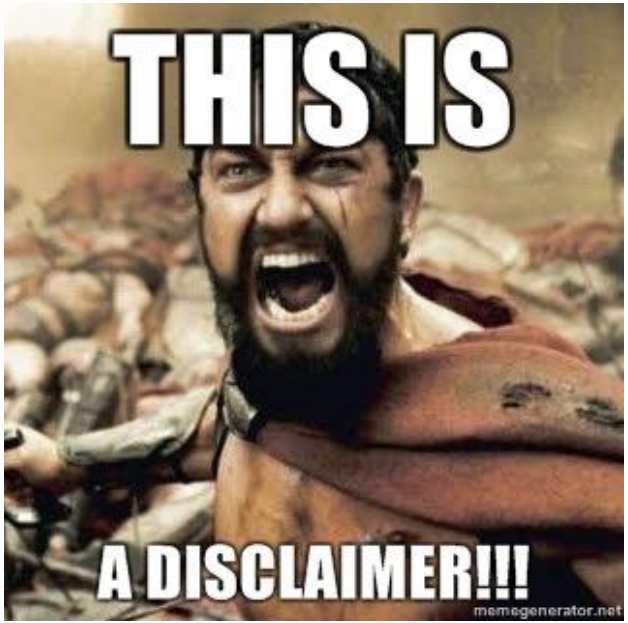
- CPTS
- CBBH
- CWEE
- CAPE

# Les certifications en red team : INE Security

- eJPT
- eCPPT
- eWPT

# Les certifications à éviter

# Les certifications en blue team



# Les certifications en blue team : Offsec

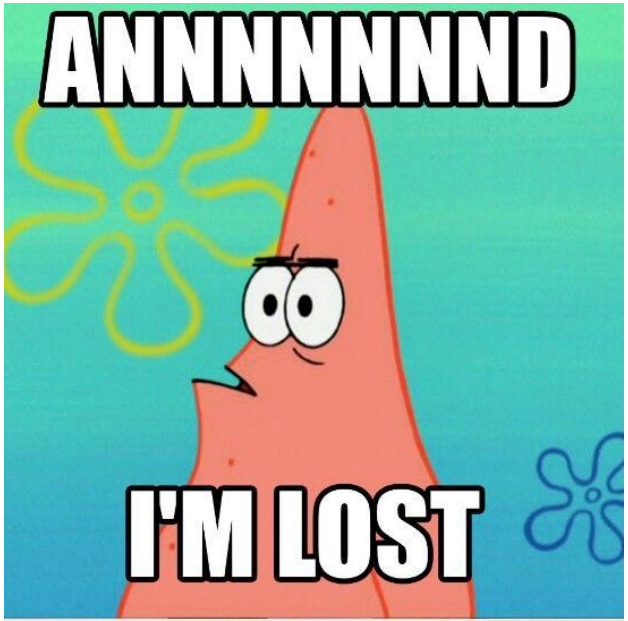
- SOC-200
- TH-200
- IR-200

# Les certifications en blue team : HackTheBox

- CDSA
- CWEE

# Les certifications en blue team : Microsoft

# Quelle certification choisir???



# Brother I'm broke

# Pleins d'autres options qui ont du poids sur un cv!

- Gros finish à des CTFs connus
- Des bon scores sur les sites comme HTB,RootMe, TryhackMe
- Un bon profil sur les différents sites de Bug Bounty

# Les certifications en gouvernance

# Les principales

- CISSP
- CISM
- CISA
- CEH
- CompTIA Security+
- ISO 27001 Lead Implementer/Lead Auditor

# Erreurs à ne pas faire lorsque l'on veut s'enroller dans une certification

- Ne pas se tromper de champ d'expertise
- Ne pas se préparer convenablement
- Ne pas s'informer sur les conditions de chaque certification

# Mes conseils pour débuter sa carrière en cybersécurité

- Mon conseil le plus important : Arrêter de vouloir faire de la cybersécurité à tout prix.

# Suite des conseils

- Il manque plus de ressources blue team que red team
- Ne pas avoir peur de commencer plus bas, la confiance viendra après
- Préparez-vous pour vos entrevues
- Les compagnies ont besoin de vous, pas l'inverse.

# Exemple de questions d'entrevues

- Connaissances générales en cybersécurité :
  - Quels sont les principaux types de cyberattaques auxquelles un SOC doit faire face ?
  - Expliquez la différence entre un risque, une menace et une vulnérabilité.
  - Quels sont les principes de base de la sécurité de l'information ?
- Détection et analyse des incidents :
  - Comment procédez-vous pour investiguer un incident de sécurité ?
  - Quels sont les principaux indicateurs de compromission (IOC) à surveiller ?
  - Comment distinguez-vous un vrai incident d'un faux positif ?
  - Quels outils utilisez-vous pour la détection des menaces et l'analyse forensique ?

# Suite

- Connaissance des protocoles réseau et sécurité :
  - Expliquez le modèle OSI et les protocoles clés à chaque couche.
  - Quels sont les principaux protocoles sécurisés (ex : HTTPS, SSH, IPsec) et comment fonctionnent-ils ?
  - Comment sécuriseriez-vous la communication entre deux réseaux distants ?
  - Quelles sont les différences entre TCP et UDP en termes de sécurité?
  - Quelles techniques utilisez-vous pour détecter une exfiltration de données sur le réseau ?
  - Expliquez le principe du moindre privilège et comment l'appliquer au contrôle d'accès réseau.
- Gestion des événements et information de sécurité (SIEM) :
  - Quelles sont les fonctions principales d'un SIEM ?
- Réponse aux incidents :
  - Quelles sont les étapes dés d'un processus de réponse aux incidents ?
  - Comment priorisez-vous les incidents de sécurité ?
  - Quelles mesures prenez-vous pour contenir une attaque en cours ?
  - Comment pouvons-nous automatiser la réponse aux incidents?

# Suite

- Scenario et cas pratiques :
  - Que faites-vous si vous détectez un trafic suspect provenant d'un poste interne ?
  - Comment réagissez-vous face à une attaque par déni de service distribuée (DDoS) ?
  - Décrivez une situation de crise cyber que vous avez gérée et les leçons apprises.
- Sécurité des applications :
  - Quels sont les principaux risques de sécurité liés au développement d'applications ?
  - Comment protégez-vous une application web contre les attaques par injection (ex : SQL injection, XSS) ?
  - Quels langages de programmation maîtrisez-vous et quelles sont leurs spécificités en termes de sécurité ?
  - Expliquez les principes de base de la cryptographie asymétrique et symétrique.
  - Expliquez la différence entre un algorithme d'encryption vs hashing.

# Exemple de questions d'examen technique

- Écrivez un programme qui convertit un nombre décimal en binaire. Vous pouvez le faire dans le langage de votre choix.
- Nommez 2 moyens d'améliorer la disponibilité d'une application.
- Complétez la commande linux pour chercher tous les fichiers .db dans le répertoire /var/logs
- Décrivez à quoi correspond une attaque SSRF et donnez un exemple d'exploitation ?
- À la suite d'une investigation, vous tombez sur la chaîne de caractères suivante: "aGVsbG8gd29ybGQNCg==", que faites-vous afin de poursuivre l'investigation?
- Selon l'entrée du fichier */etc/passwd* suivante, répondez aux 3 questions :

- john:x:1000:1000:John Doe,,,:/home/john:/bin/bash

  - Quel est le shell par défaut de l'utilisateur john et qu'est-ce que cela implique pour son accès au système ?
  - Que signifie l'UID 1000 et pourquoi est-ce significatif ?
  - Pourquoi le 2eme champ est-il un « x »?

# Exemple de questions d'examen

- Quelle est la différence entre les permissions 644 et 755 sous linux? À quoi correspondent ces chiffres ?
- À quoi sert une Stratégie de Groupe (GPO) dans un environnement Windows ?
- Lors d'une détection d'Indicateur de Compromission (IoC), vous devez bloquer les communications avec une infrastructure malveillante. Expliquez votre stratégie concernant le choix entre le blocage par nom de domaine ou par adresse IP. Argumentez votre réponse.
- Quel est le rôle d'un serveur DHCP dans un réseau ? Expliquez le processus d'attribution d'une adresse IP à un nouvel appareil.
- Quelle est la différence entre une adresse IP publique et une adresse IP privée ? Donnez des exemples de chaque type.
- Nommez 6 exemples de failles de sécurité dans une application selon OWASP ?
- Expliquez la différence entre TCP et UDP. Donnez un exemple d'application utilisant chaque protocole.

# Merci!

- .Seneque sur discord
- J'ai pas de linkedin car ce réseau social me fait peur

# Liste de box HTB OSCP like

- HTB: BoardLight
- HTB: Broker
- HTB: Keeper
- HTB: Monitored
- HTB: Manager
- HTB: Usage