**QCM : Questionnaire des attaquants et leurs outils**

1. Laquelle de ces propositions est un exemple de cyberactivisme ?

Un groupe d’écologistes lance une attaque par déni de service contre une entreprise pétrolière responsable d’une grande marée noire.

Des criminels utilisent Internet pour essayer de voler de l’argent à une banque.

Un pays tente de voler les secrets de la défense d’un autre pays en infiltrant des réseaux gouvernementaux.

Un adolescent pénètre par effraction dans le serveur Web d’un journal local et publie une image de son personnage de dessin animé préféré.

1. Quel énoncé décrit la cybersécurité ?

C’est un cadre pour l’élaboration de politiques de sécurité.

C’est un modèle basé sur les normes pour l’élaboration de technologies de pare-feu qui serviront à lutter contre les cybercriminels.

C’est le nom d’une application de sécurité complète destinée aux utilisateurs finaux pour protéger les postes de travail contre les attaques.

Elle consiste en l’effort continu pour protéger les systèmes connectés à Internet et les données qui leur sont associées contre l’utilisation ou le méfait non autorisés.

1. Quel accent décrit une caractéristique d'un indicateur d'attaque (IOA)?

Il se concentre davantage sur les stratégies de gestion des risques après une attaque et une compromission des systèmes.

Il se concentre davantage sur l'atténuation après une attaque et sur les vulnérabilités potentiellement compromises.

Il met davantage l'accent sur la motivation derrière une attaque et sur les moyens utilisés pour compromettre les vulnérabilités afin d'accéder aux actifs.

Il met davantage l'accent sur l'évitement des menaces après une attaque et sur les implications potentielles en termes de coûts.

1. Quelle est la motivation d’un agresseur white hat ?

régler précisément des périphériques réseau pour améliorer leurs performances et leur efficacité

profiter de toute vulnérabilité à des fins personnelles illégales

étudier les systèmes d’exploitation de diverses plateformes pour élaborer un nouveau système

rechercher les points faibles de réseaux et de systèmes pour améliorer leur niveau de sécurité

1. Quel plan de gestion des risques prévoit l'interruption d'une activité qui crée un risque ?

évitement des risques

conservation des risques

partage des risques

réduction des risques

1. Quel type de menace de réseau est utilisé pour empêcher les utilisateurs autorisés d'accéder aux ressources ?

Attaques DoS.

Attaques d'accès

Exploitation de confiance

Attaques de reconnaissance

1. Quel outil de sécurité permet à un acteur de menace d'attaquer un réseau sans fil et de détecter les vulnérabilités de sécurité?

Cliquez sur Générateurs de bruit.

SuperScan

NMap

KISMac

1. Quelle affirmation décrit le terme « surface d'exposition aux attaques » ?

Il s'agit de la somme totale des vulnérabilités d'un système qu'un hacker peut exploiter.

Il s'agit du nombre total d'attaques ciblant une entreprise au cours d'une journée.

Il s'agit du groupe d'hôtes qui subit la même attaque.

Il s'agit de l'interface réseau d'où proviennent les attaques.

1. Quelle stratégie de gestion des risques nécessite une évaluation minutieuse des coûts des pertes, de la stratégie d'atténuation et des avantages tirés de l'exploitation ou de l'activité à risque ?

réduction des risques

évitement des risques

acceptation des risques

transfert des risques

1. Quelle caractéristique décrit un script kiddies?

les hackers en chapeau gris qui tentent de découvrir des exploits et de les signaler aux fournisseurs, parfois pour des prix ou des récompenses.

des acteurs de menaces inexpérimentés qui utilisent des scénarios, des outils et des exploits existants pour causer du tort, mais généralement sans but de profit

Les acteurs de menace qui volent des secrets d'État, collectent des informations stratégiques et mènent des actions de sabotage visant des réseaux ou des gouvernements étrangers, des groupes terroristes ou des entreprises.

les hackers qui se rassemblent et protestent contre différents idéaux politiques et sociaux

1. Quelle caractéristique décrit un hacker en chapeau gris?

Il s'agit de personnes qui commettent des cyber-crimes, mais qui ne le font pas pour leur gain personnel ou pour causer des dommages.

Il s'agit de personnes éthiques qui utilisent leurs compétences en matière de programmation à des fins bénéfiques, éthiques et légales.

Il s'agit de personnes qui conçoivent des stratégies d'adoption des risques

Il s'agit de criminels malhonnêtes qui enfreignent la sécurité des ordinateurs et des réseaux pour leur gain personnel ou à des fins malveillantes, telles que l'attaque de réseaux.

1. Une entreprise a conclu un contrat avec une entreprise de sécurité réseau pour aider à identifier les vulnérabilités du réseau d'entreprise. L'entreprise envoie une équipe pour effectuer des tests de pénétration sur le réseau de l'entreprise. Pourquoi l'équipe utiliserait-elle des outils médico-légaux?

Ce sont des systèmes d'exploitation spécialement conçus préchargés avec des outils optimisés pour le piratage.

pour détecter les outils installés dans les fichiers et répertoires qui fournissent aux acteurs des menaces un accès à distance et un contrôle sur un ordinateur ou un réseau

pour inverser l'ingénierie des fichiers binaires lors de l'écriture d'exploits et lors de l'analyse de logiciels malveillants

pour détecter toute preuve d'un piratage ou d'un programme malveillant dans un ordinateur ou un réseau