**PEREIRA Romain**

**BTS SIO 1B**

**Liste de définitions :**

****Cybersécurité** : Protection des systèmes informatiques contre le vol ou les dommages à leur matériel, logiciel ou données, ainsi que contre la perturbation ou la désorientation des services qu'ils fournissent.**

****Cyberespace** : Environnement virtuel où s'effectuent les échanges d'informations via des réseaux informatiques.**

****Cryptographie** : Science de la sécurisation de la communication et des informations, en utilisant des codes pour que seules les personnes auxquelles elles sont destinées puissent lire et les traiter.**

****Authentification** : Processus de vérification de l'identité d'un utilisateur ou d'un dispositif dans un système informatique.**

****Phishing** : Technique utilisée par les cybercriminels pour obtenir des informations sensibles (comme les mots de passe et les détails de carte de crédit) en se faisant passer pour une entité de confiance.**

****Brute Force** : Méthode d'attaque qui consiste à essayer toutes les combinaisons possibles de mots de passe ou de clés cryptographiques.**

****Gestionnaire de mots de passe** : Logiciel qui aide à créer, stocker et gérer des mots de passe sécurisés pour les utilisateurs.**

****Hachage** : Transformation d'une chaîne de caractères en une valeur fixe ou un mot de passe, généralement pour des raisons de sécurité.**

****Ingénierie sociale** : Manipulation psychologique des personnes dans le but de les amener à divulguer des informations confidentielles.**

****Authentification à deux facteurs (2FA)** : Méthode de sécurité qui requiert deux types de preuves d'identité distinctes pour accéder à un compte ou un système.**

****Chiffrement asymétrique** : Système de cryptage utilisant une paire de clés, une publique et une privée, pour sécuriser les communications.**

****Chiffrement symétrique** : Cryptage où la même clé est utilisée pour chiffrer et déchiffrer des données.**

****Token d'authentification** : Dispositif utilisé pour accéder à un réseau ou à un système informatique, généralement en complément d'un nom d'utilisateur et d'un mot de passe.**

****Protocole d'authentification** : Ensemble de règles qui déterminent comment les utilisateurs sont vérifiés avant d'accéder à un système ou à un réseau.**

****Attaque par déni de service (DoS)** : Tentative de rendre une machine ou un réseau indisponible en le surchargeant de requêtes.**

****Attaque de l'homme du milieu (MitM) :** Attaque où la communication entre deux parties est interceptée et éventuellement altérée par un intrus.**

****Politique de sécurité** : Ensemble de règles et de pratiques qui régissent la manière dont une organisation gère et protège ses ressources informatiques.**

****Signature numérique** : Méthode cryptographique utilisée pour vérifier l'authenticité et l'intégrité d'un message, d'un logiciel ou d'un document numérique.**

****Principe de moindre privilège** : Pratique de sécurité qui consiste à accorder aux utilisateurs uniquement les accès strictement nécessaires à l'exécution de leurs tâches.**

****Audit de sécurité** : Examen complet des systèmes d'information d'une organisation pour évaluer leur conformité aux normes de sécurité.**

****Faille Zero-Day** : Faille de sécurité d'un logiciel qui est inconnue du fournisseur et pour laquelle il n'existe pas encore de correctif.**

****Contrôle d'accès** : Mécanisme par lequel un système détermine quels utilisateurs ont le droit d'accéder à une ressource informatique.**

****Identification biométrique** : Utilisation de caractéristiques physiques ou comportementales uniques (empreintes digitales, reconnaissance faciale, etc.) pour identifier une personne.**

****Intrusion Detection System (IDS)** : Système conçu pour détecter les activités suspectes ou malveillantes sur un réseau ou un système informatique.**

****OCLCTIC**: Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.**

****TCP/IP** : Protocole de communication définissant comment les données sont échangées sur Internet, comprenant le protocole de contrôle de transmission (TCP) et le protocole Internet (IP).**

****DNS** : Système de noms de domaine qui traduit les noms de domaine faciles à retenir en adresses IP numériques.**

****Adresses IP** : Identifiants uniques attribués à chaque appareil connecté à un réseau informatique utilisant le protocole Internet.**

****HTTPS** : Protocole de transfert hypertexte sécurisé, version sécurisée de HTTP, utilisant le cryptage pour protéger l'échange de données.**

****SSL/TLS** : Protocoles de cryptage assurant la sécurité des communications sur Internet, utilisés notamment pour le HTTPS.**

****SMTP** : Protocole simple de transfert de courrier, utilisé pour l'envoi d'emails sur des réseaux informatiques.**

****IMAP** : Protocole d'accès aux messages Internet, permettant de récupérer des emails depuis un serveur.**

****PGP** : Cryptage de données de bout en bout (Pretty Good Privacy), utilisé pour sécuriser la communication par email.**

****Firewall** : Système de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant selon des règles de sécurité définies.**

****Antivirus** : Logiciel conçu pour détecter, prévenir et éliminer les logiciels malveillants.**

****Malware** : Logiciel malveillant conçu pour endommager ou exploiter des systèmes informatiques.**

****Ransomware** : Type de malware qui chiffre les données de l'utilisateur et demande une rançon pour les déchiffrer.**

****Phishing** : Technique de fraude en ligne visant à obtenir des informations sensibles (comme les identifiants de connexion) en se faisant passer pour une entité de confiance.**

****Cryptage** : Processus de conversion de données en un format codé pour empêcher l'accès non autorisé.**

****Wi-Fi** : Technologie permettant des connexions sans fil à un réseau informatique.**

****Patch de sécurité** : Mise à jour logicielle destinée à couvrir des vulnérabilités de sécurité identifiées.**

****Cookies** : Petits fichiers enregistrés sur votre appareil par les sites web, souvent utilisés pour stocker des préférences ou suivre l'activité en ligne.**

****WPA2** : Protocole de sécurité Wi-Fi Protected Access 2, utilisé pour sécuriser les réseaux sans fil.**

****Internet** : Réseau informatique mondial qui relie des millions de réseaux privés, publics, académiques et gouvernementaux.**

****Client** : Programme ou appareil qui accède aux services fournis par un serveur dans un réseau informatique.**

****Serveur** : Système informatique ou logiciel qui fournit des fonctionnalités ou des données à d'autres programmes ou appareils, appelés clients.**

****Spam** : Messages indésirables, souvent de nature publicitaire, envoyés en masse par e-mail ou d'autres moyens de communication électronique.**

****Botnet** : Réseau d'ordinateurs infectés par des logiciels malveillants, contrôlés à distance par un attaquant.**

****Typosquatting** : Pratique consistant à enregistrer des noms de domaine ressemblant à des marques connues, en espérant profiter des erreurs de frappe des utilisateurs.**

****Serveur mandataire (Proxy)** : Serveur intermédiaire qui agit comme un intermédiaire entre un utilisateur et Internet, souvent utilisé pour l'anonymat ou la sécurité.**

****Cryptographie** : Science de la sécurisation de la communication en utilisant le codage pour protéger les informations.**

****Whitehat** : Expert en sécurité informatique qui utilise ses compétences pour améliorer la sécurité et aider à prévenir les attaques.**

****Greyhat** : Spécialiste de la sécurité qui peut enfreindre des lois ou des normes éthiques typiques, mais sans intention malveillante.**

****Blackhat** : Pirate informatique qui viole la sécurité informatique pour des motifs personnels ou financiers malveillants.**

****Plugins** : Composants logiciels additionnels qui ajoutent des fonctionnalités spécifiques à un programme existant, comme un navigateur web.**

****Navigateur web** : Logiciel utilisé pour accéder et afficher des pages sur Internet.**

****Système d'exploitation** : Logiciel de base qui gère les ressources informatiques et offre des services communs aux programmes d'application.**

****BYOD (Bring Your Own Device)** : Politique permettant aux employés d'utiliser leurs appareils personnels pour le travail.**

****Clé USB** : Dispositif de stockage amovible et portable utilisant une connexion USB pour le transfert de données.**

****Charte informatique** : Document définissant les règles d'utilisation des ressources informatiques et des services Internet au sein d'une organisation.**