**PEREIRA Romain**

**BTS SIO 1B**

**Mission 10**

**Compte rendu :**

**Le module 3 de la formation SecNumacadémie, intitulé "Sécurité sur Internet", commence par explorer la structure et le fonctionnement d'Internet, mettant en lumière l'importance des protocoles TCP/IP et DNS dans la navigation quotidienne. On comprend vite que les adresses IP ne sont pas de simples chiffres, mais des identifiants cruciaux dans le monde du réseau. Le module souligne également l'importance du HTTPS, renforcé par les protocoles SSL/TLS, pour une navigation web sécurisée, protégeant les utilisateurs des dangers cachés sur le web .**

**L'unité sur les fichiers d'Internet révèle comment les malwares et les ransomwares peuvent se cacher dans des téléchargements apparemment inoffensifs. Elle insiste sur l'usage de firewalls et d'antivirus pour contrer ces menaces. Dans la section sur la messagerie électronique, l'accent est mis sur la sécurisation des communications via des protocoles comme SMTP et IMAP, et l'importance du cryptage, illustrée par PGP, pour protéger les informations sensibles.**

**Le module 4, "Sécurité du Poste de Travail et Nomadisme", s'ouvre sur l'importance cruciale des applications et de leurs mises à jour régulières. Il explique comment les patchs de sécurité aident à garder les systèmes à l'abri des nouvelles vulnérabilités. La formation aborde ensuite les configurations de base et complémentaires des systèmes d'exploitation, soulignant l'importance de séparer les usages pour une meilleure sécurité, notamment dans un contexte BYOD.**

**La sécurité des périphériques amovibles, comme les clés USB, est également discutée, mettant en évidence les risques de fuites de données et l'importance de crypter les informations sensibles. La formation termine en insistant sur l'importance de respecter la charte informatique de chaque organisation pour maintenir un environnement de travail sécurisé.**

**Tout au long des deux modules, des termes techniques tels que Wi-Fi, WPA2, spam, botnet, et typosquatting sont intégrés pour illustrer diverses menaces et stratégies de défense dans le monde numérique. Des notions comme serveur mandataire (proxy) et navigateur web sont également abordées pour comprendre leur rôle dans la sécurisation des données.**

**En conclusion, ces modules offrent une compréhension approfondie de la sécurité sur Internet et du poste de travail, tout en mettant l'accent sur l'importance des pratiques de cybersécurité dans notre monde connecté. Les rôles des différents acteurs de la cybersécurité, tels que les whitehats, greyhats, et blackhats, sont également évoqués pour donner une vision complète de l'écosystème de la sécurité informatique.**

**Liste de définitions :**

**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.**

**Certification :**

