**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 importants 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 Internet.**

**L'unité sur les fichiers d'Internet révèle comment les malwares et les ransomwares peuvent se cacher dans des téléchargements a priori « safe ». Elle insiste sur l'usage de firewalls et d'antivirus pour contrer ces menaces. Dans la section sur la messagerie électronique, on souligne la sécurisation des communications via des protocoles comme SMTP et IMAP, et l'importance du cryptage, notamment par PGP, pour protéger les informations sensibles.**

**Le module 4, "Sécurité du Poste de Travail et Nomadisme", commence en mettant en avant l'importance des applications et de leurs mises à jour régulières. Il explique comment les patchs de sécurité contribuent à maintenir la sécurité des systèmes en les protégeant contre de nouvelles vulnérabilités. La formation aborde ensuite les configurations de base et complémentaires des systèmes d'exploitation, mettant en évidence la nécessité de séparer les usages pour renforcer la 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 WPA2, 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 sur la sécurité informatique.**

****Certification ci-dessous :****

