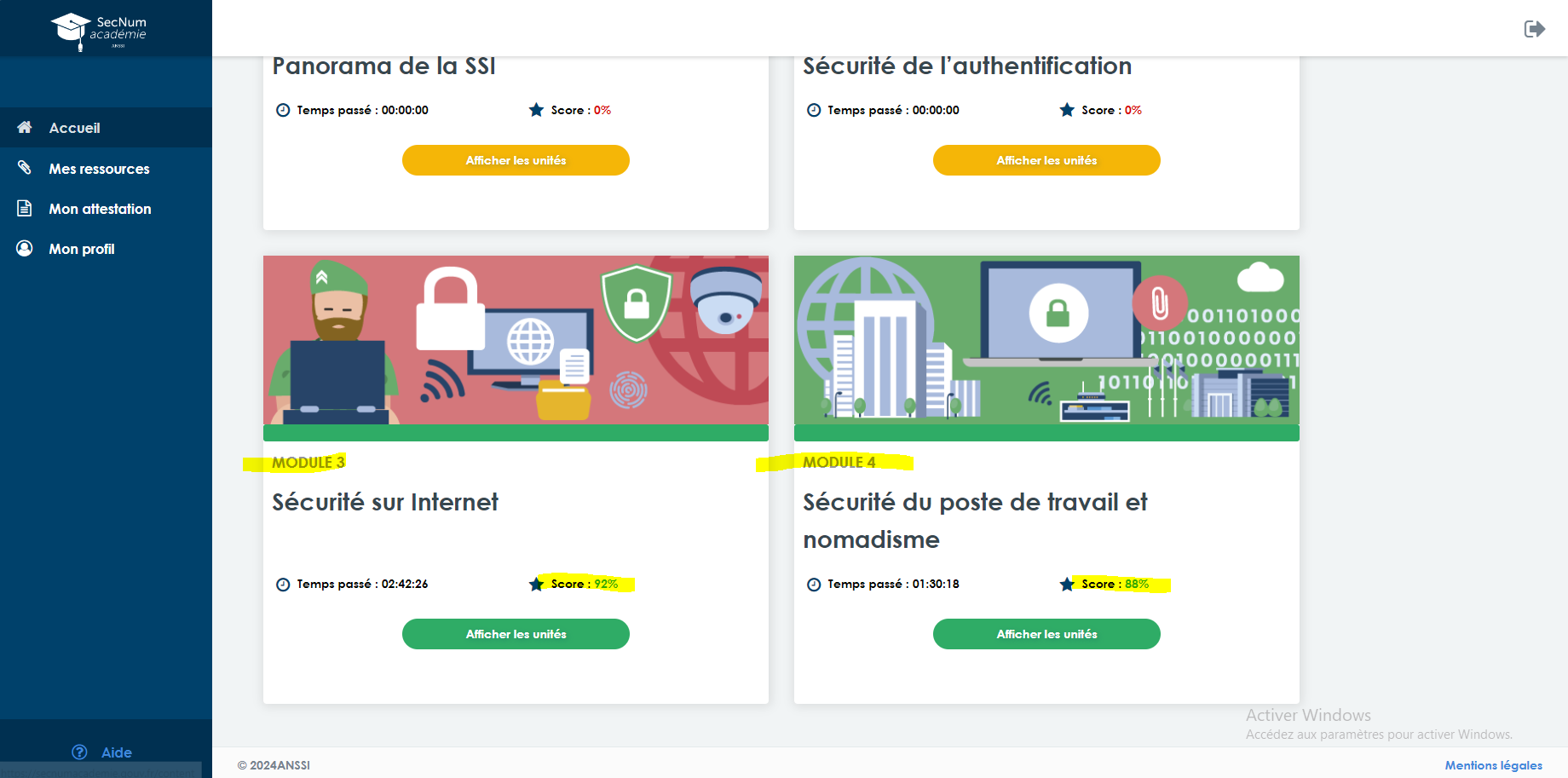
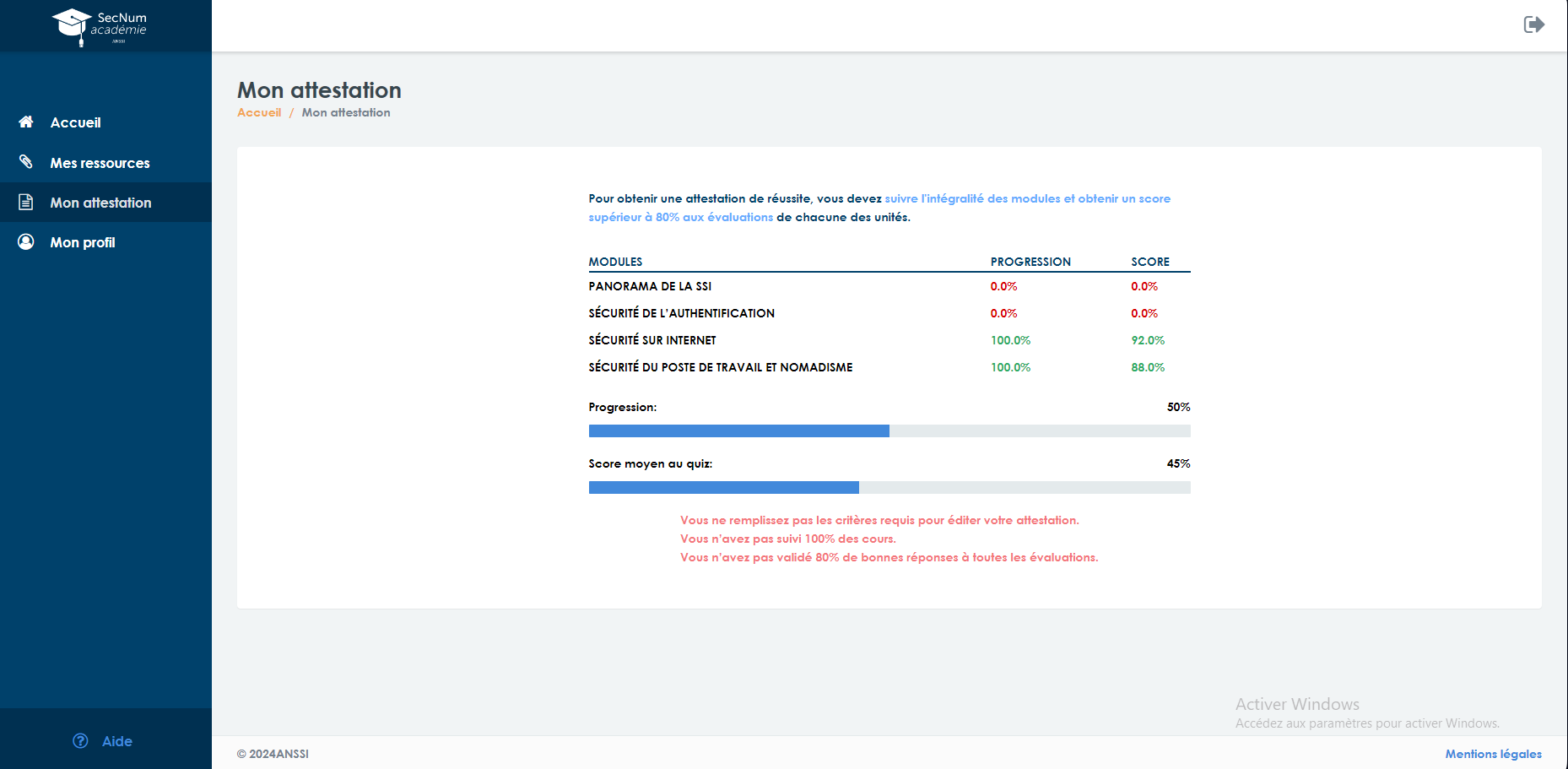
***Compte rendu MOOC***

HAURET Lucien

1SIOB

***Captures écrans des modules complétés :***





**Tout ce que j'ai appris au cours des modules**

**MODULE 1**

**Un monde numérique hyperconnecté :**

Le cyberespace, un univers numérique en constante évolution, permet une interconnexion mondiale grâce à une multitude de technologies. Cet environnement offre de nombreuses opportunités, mais soulève aussi des défis, notamment en matière de sécurité et de régulation. Il peut parfois sembler être un espace sans règles, où les lois traditionnelles peinent à s'appliquer, créant ainsi des risques pour la protection des individus et la régulation des pratiques en ligne.

**Un monde à haut risque :**

Le cyberespace expose individus, entreprises et gouvernements à de multiples menaces. Les cyberattaques peuvent être massives, affectant un grand nombre de victimes, ou ciblées, visant des institutions spécifiques. Ces attaques, menées par des cybercriminels, des hacktivistes ou des États, peuvent entraîner de lourdes conséquences : pertes financières, vol de données, atteinte à la réputation ou perturbation des services essentiels. La cybersécurité, la vigilance et la réaction rapide sont donc cruciales.

**Les acteurs de la cybersécurité :**

Les acteurs de la cybersécurité, comme l'ANSSI (Agence nationale de la sécurité des systèmes d'information), jouent un rôle clé dans la protection des systèmes numériques. La France, par exemple, a mis en place des stratégies pour renforcer la sécurité des infrastructures critiques. D'autres acteurs, comme les entreprises spécialisées et les experts en cybersécurité, apportent leur expertise pour sécuriser les systèmes et lutter contre les cybermenaces.

**Protéger le cyberespace :**

La sécurité du cyberespace repose sur des pratiques simples : utiliser des mots de passe robustes, mettre à jour les logiciels régulièrement, réaliser des sauvegardes et sécuriser l'accès Wi-Fi. De plus, il est important de protéger son identité numérique pour éviter l'usurpation d'identité et les violations de la vie privée, notamment en séparant les usages personnels et professionnels.

**Les règles d’or de la sécurité :**

La protection des données passe par des mesures comme le chiffrement, la gestion des accès et la mise en place de sauvegardes régulières. Chaque utilisateur, qu'il soit individuel ou organisationnel, a la responsabilité de respecter les bonnes pratiques pour limiter les risques d'attaques et garantir la sécurité des données.

**MODULE 2**

**Principes de l’authentification :**

L’authentification vérifie l'identité des utilisateurs via trois méthodes : quelque chose que vous savez (mot de passe), que vous avez (appareil) et que vous êtes (biométrie). Ces méthodes assurent que seuls les utilisateurs autorisés accèdent aux ressources sensibles.

**Attaques sur les mots de passe :**

Les mots de passe sont fréquemment ciblés par des attaques comme la force brute, le phishing ou l'attaque par dictionnaire. Ces techniques permettent aux pirates d’accéder à des comptes et de voler des données.

**Sécuriser ses mots de passe :**

Pour protéger ses comptes, il est essentiel de créer des mots de passe complexes, d'utiliser un gestionnaire de mots de passe et d'activer l'authentification à deux facteurs (2FA). Il est également important de changer régulièrement ses mots de passe et de ne pas les réutiliser sur plusieurs sites.

**Gérer ses mots de passe :**

Utiliser un gestionnaire de mots de passe permet de stocker et organiser des mots de passe sécurisés, réduisant ainsi les risques liés à l'oubli ou à la réutilisation de mots de passe faibles.

**Notions de cryptographie :**

La cryptographie protège les informations en les rendant illisibles pour toute personne non autorisée. Elle est essentielle pour assurer la confidentialité des communications et la sécurité des transactions en ligne.

**MODULE 3**

**Internet schématisé :**

La navigation sur Internet repose sur une architecture client/serveur. Le client envoie des demandes au serveur, qui répond avec les informations requises. Internet utilise le protocole IP pour connecter des millions d'ordinateurs à l’échelle mondiale, tandis que le Web est un système qui permet de naviguer entre des pages via des hyperliens.

**Cybermalveillance :**

La cybermalveillance touche non seulement les grandes entreprises, mais aussi les particuliers. Des exemples courants incluent les spams, le suivi d’activité en ligne (tracking) et l’utilisation de malwares pour infecter des ordinateurs. Les rançongiciels (ransomwares) bloquent l’accès aux données et demandent une rançon en cryptomonnaie pour les libérer, sans garantie de succès.

**Ingénierie sociale :**

L’ingénierie sociale exploite les vulnérabilités humaines pour tromper les victimes. Des techniques comme le phishing (hameçonnage) sont couramment utilisées. La prévention passe par la vérification des interlocuteurs et la double vérification des opérations sensibles.

**Réseaux sociaux :**

Les réseaux sociaux sont des outils puissants pour rester en contact et s’exprimer, mais leur usage est aussi un terrain idéal pour la cybermalveillance. Les utilisateurs doivent être vigilants aux risques liés à la divulgation de données personnelles.

**Les formats et les extensions de fichiers :**

Les extensions de fichiers permettent d’identifier leur type et de déterminer quel programme les ouvre. Toutefois, des pirates peuvent exploiter ces extensions pour inciter les utilisateurs à ouvrir des fichiers malveillants. Il est important de vérifier la source des fichiers téléchargés et de les analyser avec un antivirus.

**La navigation web :**

Le navigateur permet de visualiser les pages web après avoir envoyé une requête à un serveur. Les moteurs de recherche indexent des milliards de pages, et les cookies stockent des informations sur l’utilisateur, souvent utilisées pour le suivi publicitaire.

**La messagerie électronique :**

L’e-mail est un moyen de communication essentiel, mais il est vulnérable aux attaques comme le phishing, les virus et les spams. La vérification des expéditeurs et l’utilisation de mots de passe forts sont des mesures essentielles pour se protéger.

**L'envers du décor d'une connexion Web :**

Lorsqu'un utilisateur entre une adresse web, une requête DNS est envoyée pour résoudre le nom de domaine en adresse IP. HTTPS chiffre les échanges pour garantir la sécurité des données, avec un certificat SSL pour authentifier le serveur

**MODULE 4**

**Sécurité du poste de travail et nomadisme :**

La sécurité des appareils, particulièrement avec le travail à distance, est cruciale. Les applications doivent être régulièrement mises à jour, et les vulnérabilités doivent être corrigées pour protéger les systèmes contre les menaces.

**Options de configuration de base :**

Lors de l’installation d’un appareil, il est important de configurer les paramètres essentiels comme la langue, la connexion Wi-Fi et la sécurité du compte utilisateur. Les technologies d'authentification avancées comme la biométrie offrent une sécurité supplémentaire.

**Sécurité des périphériques amovibles :**

Les périphériques amovibles comme les clés USB peuvent introduire des malwares. Le chiffrement des données et l'effacement sécurisé des périphériques sont essentiels pour protéger les informations sensibles.

**Séparation des usages :**

Il est risqué de mélanger les usages professionnels et personnels sur le même appareil. Utiliser des périphériques distincts et des comptes séparés permet de mieux protéger les données sensibles.

***Ce compte rendu m'a permis de mieux comprendre l'importance de la sécurité numérique et des bonnes pratiques. J'ai appris à mieux protéger mes données, à sécuriser mes mots de passe et à comprendre le fonctionnement du Web, des risques liés à la cybermalveillance, et les stratégies de défense à adopter. Ces connaissances me permettent de naviguer en ligne de manière plus sûre et responsable.***