Compte rendu : Mission 10

Noah Ripert 1SIOB

Module 1 : Panorama de la SSI :

UNITÉ 1: Un monde numérique hyper-connecté Cette unité donne un aperçu d'un monde numérique fortement interconnecté, soulignant les aspects clés de cette hyper-connectivité.

UNITÉ 2: Un monde à hauts risques L'unité explore les risques élevés liés au monde numérique, examinant les diverses menaces et vulnérabilités auxquelles les systèmes informatiques sont confrontés.

UNITÉ 3: Les acteurs de la cybersécurité Cette unité se concentre sur les différents acteurs impliqués dans le domaine de la cybersécurité, offrant un aperçu des entités travaillant pour garantir la sécurité des systèmes d'information.

UNITÉ 4: Protéger le cyberespace Explorant les différentes stratégies et mesures pour protéger le cyberespace, cette unité met en lumière les efforts déployés pour contrer les menaces potentielles.

UNITÉ 5: Les règles d’or de la sécurité La dernière unité présente les règles fondamentales de la sécurité dans le contexte numérique, offrant des lignes directrices essentielles pour assurer une posture de sécurité robuste.

En résumé, le MODULE 1 offre une vision complète de la Sécurité des Systèmes d'Information (SSI), couvrant des sujets tels que l'hyper-connectivité, les risques, les acteurs de la cybersécurité, les stratégies de protection du cyberespace, et les règles fondamentales de la sécurité.

Le Module 1 sur le "Panorama de la Sécurité des Systèmes d'Information" m'a offert une compréhension approfondie des enjeux de la sécurité dans le monde numérique. En explorant les risques élevés associés à notre interconnexion constante, j'ai acquis une conscience aiguë des menaces qui pèsent sur les systèmes informatiques.

Module 2 : Sécurité de l’authentification :

UNITÉ 1: Principes de l’authentification La première unité explore les principes fondamentaux de l'authentification, fournissant une compréhension de base des mécanismes utilisés pour vérifier l'identité des utilisateurs.

UNITÉ 2: Attaques sur les mots de passe Cette unité examine les différentes attaques ciblant les mots de passe, mettant en évidence les vulnérabilités et les stratégies des cybercriminels pour compromettre ces informations sensibles.

UNITÉ 3: Sécuriser ses mots de passe L'unité 3 offre des conseils pratiques sur la sécurisation des mots de passe, abordant les bonnes pratiques et les mesures pour renforcer la robustesse des informations d'identification.

UNITÉ 4: Gérer ses mots de passe Cette unité se concentre sur la gestion efficace des mots de passe, explorant les méthodes et les outils pour assurer une gestion sécurisée des informations d'identification.

UNITÉ 5: Notions de cryptographie La dernière unité introduit les notions de cryptographie, élargissant la compréhension des mécanismes de sécurité liés à l'authentification.

En résumé, le MODULE 2 aborde en profondeur la Sécurité de l’authentification, couvrant les principes, les attaques potentielles sur les mots de passe, la sécurisation et la gestion des mots de passe, ainsi que des notions de cryptographie pour renforcer la compréhension globale de la sécurité de l'authentification.

L'unité consacrée aux attaques sur les mots de passe a éclairé les risques potentiels auxquels sont confrontés ces éléments clés de la sécurité. Cette prise de conscience me permettra d'appréhender les vulnérabilités et d'adopter des stratégies défensives appropriées.

Définitions

Cyberspace : Le terme "cyberspace" se réfère à un concept abstrait qui désigne l'environnement virtuel où les activités liées à l'informatique, à l'Internet et aux communications électroniques ont lieu. Il s'agit d'un espace numérique non physique où les données, les informations, les communications et les interactions électroniques se produisent.

Attaque ciblée : Une attaque ciblée, dans le contexte de la cybersécurité, fait référence à une méthode d'attaque informatique soigneusement planifiée et exécutée visant spécifiquement une personne, une organisation, un système ou un réseau particulier. Contrairement aux attaques génériques ou automatisées qui visent un large éventail de cibles potentielles, une attaque ciblée est conçue pour être précise et adaptée à sa cible.

Livre blanc de la défense : Le terme "livre blanc de la défense" se réfère généralement à un document officiel publié par un gouvernement, dans lequel sont détaillées les politiques, les orientations et les stratégies liées à la défense nationale. Ces documents fournissent souvent des informations sur les menaces perçues, les priorités en matière de sécurité, les capacités militaires, les alliances internationales, et d'autres aspects clés de la politique de défense.

Identité numérique : L'identité numérique fait référence à l'ensemble des informations qui permettent de décrire et d'identifier une entité (personne, organisation, appareil, etc.) dans le contexte numérique. Cela inclut les données personnelles, les attributs spécifiques, les interactions en ligne, les activités numériques, et d'autres éléments qui contribuent à la représentation numérique d'une identité.

Donnée : Le terme "donnée" fait référence à des faits, des informations ou des éléments bruts qui peuvent être collectés et stockés. Les données peuvent prendre différentes formes, notamment des nombres, des textes, des images, des vidéos, des enregistrements audio, etc. Elles sont souvent utilisées comme matière première pour générer des informations significatives et prendre des décisions.

Authentification : L'authentification est le processus de vérification de l'identité d'une entité, telle qu'une personne, un appareil ou un système informatique, afin de garantir l'accès à des ressources, des données ou des services. L'objectif principal de l'authentification est de s'assurer que l'entité prétendant être ce qu'elle prétend être est effectivement légitime.
Le processus d'authentification implique généralement l'utilisation de facteurs d'authentification, qui peuvent être classés en trois catégories principales :

Facteurs de connaissance : L'entité doit fournir des informations que seule la personne légitime devrait connaître. Cela peut inclure des mots de passe, des codes PIN, des réponses à des questions secrètes, etc.

Facteurs de possession : L'entité doit démontrer qu'elle possède un objet physique spécifique. Cela peut inclure l'utilisation de cartes à puce, de jetons d'authentification, de clés physiques, etc.

Facteurs biométriques : L'entité doit démontrer une caractéristique physique ou comportementale unique. Cela peut inclure la reconnaissance d'empreintes digitales, la reconnaissance faciale, la reconnaissance de l'iris, etc.

Les termes "attaques directes" et "attaques indirectes" sont souvent utilisés pour décrire différentes approches ou méthodes d'attaque, que ce soit dans le contexte militaire, informatique, ou d'autres domaines. Voici une explication générale de ces concepts :
Attaques Directes : Les attaques directes se produisent lorsque l'attaquant cible spécifiquement une entité ou un objectif sans utiliser d'intermédiaire.
Attaques Indirectes : Les attaques indirectes impliquent souvent l'utilisation d'intermédiaires ou de moyens détournés pour atteindre l'objectif final.

Le chiffrement symétrique et le chiffrement asymétrique sont deux méthodes de cryptographie utilisées pour sécuriser les données en les rendant inintelligibles sans la clé appropriée. Voici une explication de chacun de ces concepts :

Chiffrement Symétrique :

Principe : Aussi appelé chiffrement à clé secrète, le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer les données. Clé : Une seule clé partagée entre l'expéditeur et le destinataire.
Processus : L'expéditeur utilise la clé pour chiffrer le message, puis le destinataire utilise la même clé pour déchiffrer le message.
Avantages : Plus rapide et moins gourmand en ressources que le chiffrement asymétrique.

Chiffrement Asymétrique :

Principe : Aussi appelé chiffrement à clé publique, le chiffrement asymétrique utilise une paire de clés : une clé publique et une clé privée.
Clé : La clé publique est partagée librement, tandis que la clé privée est gardée secrète. Processus : L'expéditeur utilise la clé publique du destinataire pour chiffrer le message, et seul le destinataire, possédant la clé privée correspondante, peut déchiffrer le message.
Avantages : Permet l'échange sécurisé de clés sur des canaux non sécurisés. Convient à la signature numérique et à la gestion des identités.

Cryptographie : La cryptographie est l'art et la science de sécuriser les communications et les informations en les transformant de manière à ce qu'elles soient incompréhensibles pour des personnes non autorisées. Elle repose sur l'utilisation de techniques mathématiques et informatiques pour encrypter (chiffrer) et décrypter (déchiffrer) des données.