Chapitre 1 : La nécessité de la cybersécurité

Ce chapitre met en lumière l'importance cruciale de la cybersécurité et l'augmentation de la demande de professionnels qualifiés dans ce domaine. Il explore les notions d'identité et de données en ligne, soulignant l'attrait de ces informations pour les cybercriminels. La protection des données d'entreprise est abordée, ainsi que les motivations des pirates informatiques. Les professionnels de la cybersécurité doivent posséder des compétences similaires à celles des agresseurs, mais ils doivent agir en conformité avec les lois locales, nationales et internationales, tout en maintenant un comportement éthique. Le chapitre offre également un aperçu succinct de la guerre cybernétique et explique pourquoi les gouvernements ont besoin de spécialistes en cybersécurité pour défendre leurs citoyens et infrastructures.

I/Données personnelles :

I.1/introduction aux données personnelles :

1/Qu'est-ce que la cybersécurité ?

La cybersécurité est essentielle dans notre vie quotidienne, avec l'usage généralisé du réseau électronique par diverses entités. Elle englobe la protection des informations numériques pour garantir la sécurité nationale et la stabilité économique, impliquant la sécurisation des systèmes et des données à tous les niveaux, de l'individu à l'échelle nationale.

2/Votre identité en ligne et offline :

L'identité, en ligne et hors ligne, joue un rôle crucial dans votre vie, avec votre identité offline impliquant les interactions quotidiennes familiales et professionnelles. En ligne, il est essentiel de choisir un pseudonyme approprié et respectueux, évitant toute divulgation d'informations personnelles qui pourrait attirer des risques tels que la cybercriminalité ou une attention indésirable.

3/Vos données :

Vos données englobent toute information personnelle vous identifiant, notamment les échanges en ligne, photos, et des détails tels que votre nom, numéro de sécurité sociale, et données médicales, scolaires, financières et professionnelles. Les dossiers médicaux électroniques comprennent des informations physiques et mentales, tandis que les dossiers scolaires intègrent des détails sur vos études et performances académiques. Votre dossier financier rassemble des données sur vos revenus, dépenses et antécédents de crédit, tandis que le dossier d'emploi inclut vos emplois passés et performances.

4/Où sont vos données ?

Vos données, qu'il s'agisse de dossiers médicaux, de profils d'achat ou de photos partagées en ligne, peuvent être dispersées sur des serveurs mondiaux, sur les appareils de vos amis et même chez des partenaires commerciaux, soulevant des préoccupations sur la confidentialité et la maîtrise de l'accès à vos informations.

5/Vos périphériques informatiques :

Vos périphériques informatiques, en plus de stocker vos données, servent de portail essentiel pour accéder et générer des informations personnelles, faisant de celles-ci une cible lucrative pour les pirates en ligne.

I.2/Les données personnelles pour cible :

1/Ils veulent votre argent :

Les criminels cherchent à exploiter toutes les informations de valeur, y compris vos données d'identification en ligne, afin de voler votre argent, comme illustré par des incidents de piratage de compagnies aériennes, démontrant la nécessité de protéger ces informations pour éviter des conséquences financières et d'identité graves.

2/Ils veulent votre identité :

Les criminels visent à obtenir votre identité pour des gains à long terme, exploitant des informations telles que vos données médicales et déclarations fiscales afin de commettre des fraudes, usurper des avantages et créer des complications financières et légales.

II/Données de l’entreprise:

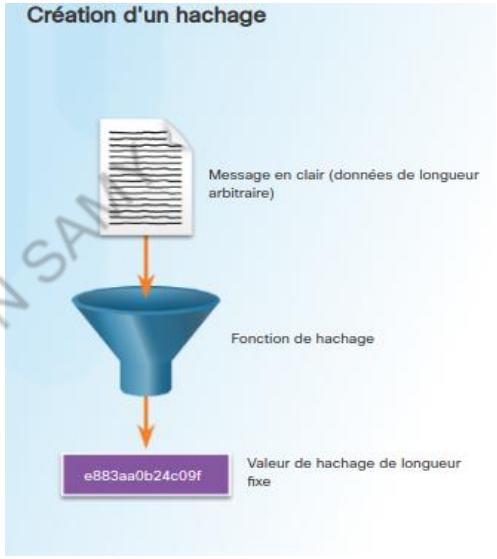
II.1/introduction aux données de l’entreprise:

1/Les différents types de données d’entreprise :

Les données d'entreprise se divisent en deux catégories : les données traditionnelles, comprenant des informations personnelles, propriétés intellectuelles et données financières, et les données générées par l'Internet des objets (IoT) et le Big Data. La gestion et la sécurité de ces données sont cruciales, car elles reflètent la santé et l'avantage concurrentiel de l'entreprise, notamment à travers des éléments tels que les brevets et les comptes financiers, nécessitant une protection rigoureuse face à la croissance exponentielle des données résultant de l'IoT et des opérations commerciales quotidiennes.

2/Confidentialité, intégrité et disponibilité :

La triade CIA, composée de la confidentialité, de l'intégrité et de la disponibilité, guide la sécurité de l'information en entreprise. La confidentialité assure l'anonymat des données par le chiffrement et l'authentification, l'intégrité garantit la précision des données tout au long de leur cycle de vie, et la disponibilité assure l'accès aux informations par des personnes autorisées. Des mesures telles que le cryptage, l'authentification à deux facteurs, les contrôles d'accès et les sauvegardes sont mises en place pour assurer ces principes de sécurité.



3/Atelier – Comparer les données hachées

Dans cet atelier, vous allez générer un hachage pour un fichier et utiliser la valeur de hachage pour comparer l'intégrité d'un fichier.

Étape 3 : Quelle est la valeur à côté de MD5 ?

0629fb721880c77d05b25f73468b5a4

Étape 5 : Quelle est la valeur à côté de MD5 ?

B144cf08a9e24209a97afc7a1b5c7dab

Étape 5 :La valeur est-elle différente de celle enregistrée à l'étape 3 ?

oui, la valeur de l'étape 5 est différente de celle de l'étape 3.

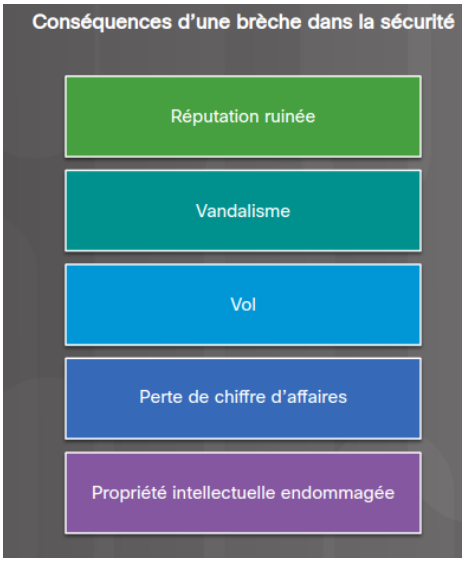
Étape 5 :Remarquez que certains types d'algorithme créent un algorithme de différente longueur. Pourquoi ?

La longueur de l'algorithme généré par un logiciel de hachage dépend du type d'algorithme utilisé. Certains algorithmes de hachage produisent des empreintes de longueurs fixes, tandis que d'autres peuvent avoir des longueurs variables. Cela est principalement dû à la façon dont ces algorithmes sont conçus et à la taille des valeurs de hachage qu'ils génèrent en fonction des données en entrée.

II.2/L'impact d'une brèche dans la sécurité:

1/Les conséquences d'une brèche dans la sécurité :

Les conséquences d'une brèche de sécurité vont au-delà des pertes matérielles et financières, englobant la compromission de données confidentielles, le risque de diffamation en ligne, la perte de crédibilité, et éventuellement des procédures judiciaires. Les répercussions incluent également la possibilité de départ d'employés et la nécessité pour l'entreprise de concentrer ses efforts sur la restauration de sa réputation plutôt que sur sa croissance.



2/Premier exemple de faille :

En juillet 2015, LastPass, un gestionnaire de mots de passe en ligne, a détecté une activité suspecte sur son réseau, révélant un vol d'adresses e-mail, de rappels de mots de passe et de hachages d'authentification par des pirates. Malgré cette faille, LastPass a réussi à protéger les informations des comptes en demandant une vérification par e-mail ou une authentification à plusieurs facteurs lors de nouvelles connexions. Les utilisateurs ont également une responsabilité dans la protection de leurs comptes en utilisant des mots de passe forts, en se méfiant des attaques d'hameçonnage, et en activant l'authentification à plusieurs facteurs lorsque cela est possible.

Remarque :SSL, ou Secure Sockets Layer, est un protocole de sécurité Internet basé sur le chiffrement. Il a été développé pour la première fois par Netscape en 1995 dans le but de garantir la confidentialité, l'authentification et l'intégrité des données dans les communications Internet.

3/Deuxième exemple de faille :

En novembre 2015, Vtech, fabricant de jouets électroniques pour enfants, a subi une grave brèche de sécurité exposant les informations sensibles de millions de clients, y compris des enfants, conduisant à la suspension de l'entreprise en bourse. La mauvaise protection des données, notamment le stockage

insuffisamment sécurisé des mots de passe et des informations de sécurité, a permis aux pirates de compromettre la confidentialité des clients, impactant la réputation de l'entreprise et soulevant des préoccupations quant à la sécurité des produits pour enfants connectés au réseau.

4/Troisième exemple de faille :

En septembre 2017, Equifax a révélé une importante faille de données causée par l'exploitation d'une vulnérabilité du logiciel Apache Struts, exposant les informations sensibles de millions de clients américains. Cette violation a soulevé des préoccupations sur la protection des données, conduisant Equifax à offrir des services de surveillance de crédit, mais a également ouvert la porte à des risques de phishing et d'usurpation d'identité, soulignant l'importance de la vigilance en matière de partage d'informations personnelles en ligne.

5/Atelier – Quelles données ont été volées ?

b. Recherchez quelques cas supplémentaires d'intrusion à la sécurité intéressants et saisissez les résultats dans le tableau ci-dessous.

Date de l'incident	Entreprise touchée	Nombre de victimes Données volées	Méthodes utilisées Mesure(s) de protection prise(s)	Source de référence
26/12	Neiman Marcus	5,200 accounts		Securityweek
				BBC

Dans cet atelier, vous étudierez quelques cas de failles pour déterminer les données volées, les exploits utilisés et les mesures à prendre pour vous protéger.

Pour renforcer la sécurité et éviter les intrusions, adoptez ces mesures générales :

1/Mots de passes sécurisées : Utilisez des mots de passe forts, uniques et changez-les régulièrement.

2/Authentification à deux facteurs(A2F) :Activez l'authentification à deux facteurs pour une sécurité supplémentaire.

3/Mises à jour régulières :Assurez-vous que tous les logiciels, systèmes d'exploitation et applications sont à jour.

4/Sensibilisation à la sécurité :Formez les utilisateurs pour reconnaître les menaces telles que l'hameçonnage.

5/Cryptage des données :Utilisez le cryptage pour sécuriser les données stockées et en transit.

6/Protection contre les logiciels malveillants :Utilisez des programmes antivirus et anti-malwares.

7/Gestion des accès :Limitez l'accès aux données aux utilisateurs autorisés.
8/Tests de sécurité :Effectuez des tests de sécurité réguliers pour identifier les vulnérabilités.
9/Plan de réponse aux incidents :Élaborez un plan pour réagir rapidement en cas de violation de sécurité.
10/Évaluation des fournisseurs :Assurez-vous que les services tiers respectent des normes de sécurité élevées.

III/Les agresseurs et les professionnels de la cybersécurité:

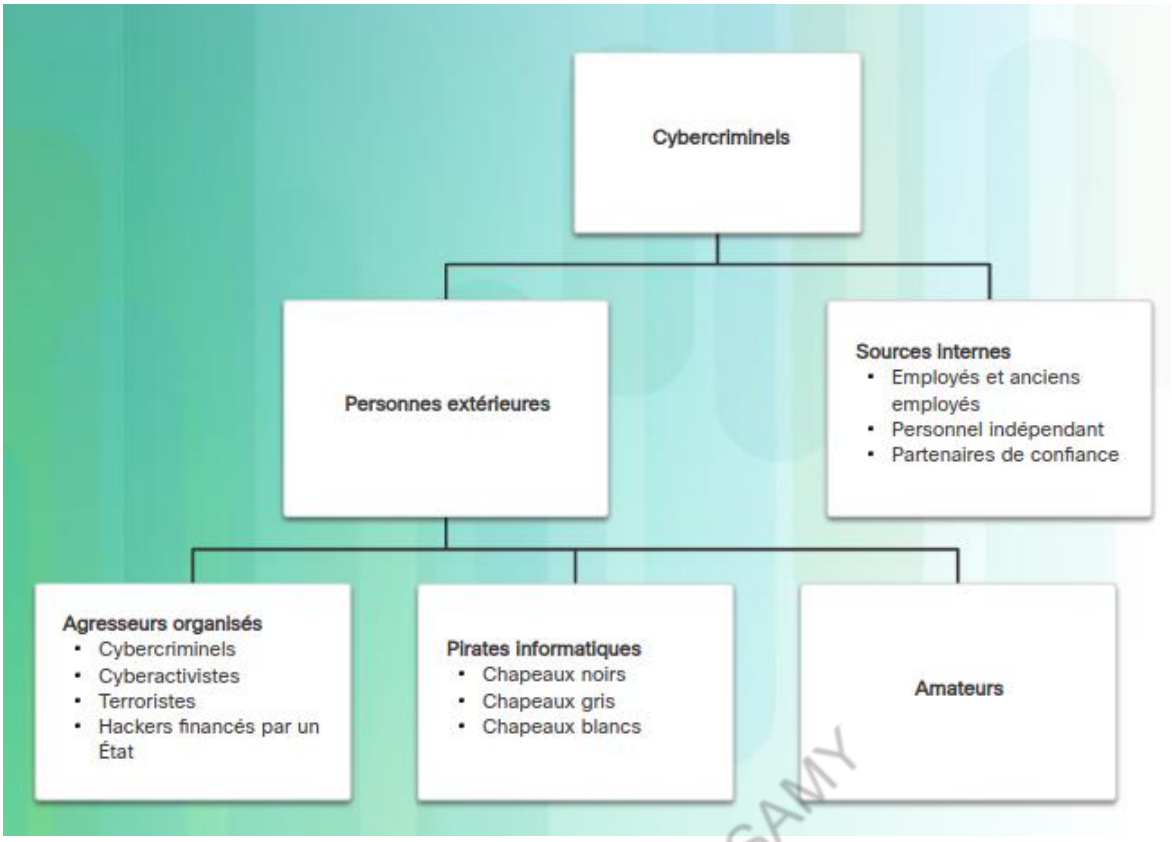
III.1/Le profil d'un agresseur:

1/Les différents types d'agresseurs :

Les agresseurs informatiques se divisent en amateurs (Script Kiddies), utilisant des outils basiques, et pirates (hackers), regroupés en chapeaux blancs (éthiques), chapeaux gris (entre éthiques et malveillants) et chapeaux noirs (malveillants). Les pirates organisés incluent des cybercriminels professionnels, des hacktivistes et des agresseurs financés par des gouvernements, tous motivés par des objectifs variés tels que le contrôle, la richesse, le pouvoir ou des motifs politiques.

2/Menaces internes et externes :

Les menaces internes à la sécurité informatique peuvent émaner d'employés ou de partenaires contractuels, intentionnellement ou accidentellement, compromettant la confidentialité des données, perturbant les serveurs internes, introduisant des malwares via des supports infectés ou facilitant des attaques externes. Les menaces externes, qu'elles proviennent d'amateurs ou d'agresseurs expérimentés, exploitent les vulnérabilités du réseau, des périphériques ou recourent à des tactiques de piratage psychologique pour accéder aux systèmes.



I***V***/Guerre cybernétique :

***IV*.1/Aperçu de la guerre cybernétique:**

1/Qu'est-ce que la guerre cybernétique ?

La guerre cybernétique est un conflit basé sur Internet, où les pays s'affrontent dans le cyberespace sans nécessiter une confrontation physique. Elle implique la pénétration des réseaux informatiques d'autres nations, permettant à des acteurs disposant de ressources et d'expertise de lancer des attaques massives en vue de causer des dommages ou de perturber les services, comme illustré par l'exemple de Stuxnet, un programme malveillant financé par des gouvernements, conçu pour endommager l'usine d'enrichissement nucléaire de l'Iran en ciblant des équipements physiques contrôlés par des ordinateurs.

Transcription video :

L'article souligne cinq éléments essentiels liés à la menace informatique Stuxnet. Premièrement, sa diffusion non triviale via des clés USB, affectant principalement les systèmes déconnectés d'Internet. Deuxièmement, sa sophistication en tant que ver intelligent ciblant spécifiquement les ordinateurs Windows et utilisant des certificats volés. Troisièmement, son codage modulaire et sa capacité à se réparer rapidement. Quatrièmement, son ciblage unique des automates programmables industriels (PLC) dans des installations industrielles. Enfin, son objectif de sabotage plutôt que d'exploitation criminelle, visant les infrastructures critiques plutôt que de voler des informations.

2/L'objectif de la guerre cybernétique :

L'objectif principal de la guerre cybernétique est d'acquérir un avantage sur les hackers, qu'ils soient des nations ou des concurrents. Cela peut inclure

l'espionnage industriel et militaire, le vol de secrets de défense, et la collecte d'informations technologiques pour renforcer ses propres industries et forces armées. La cyberguerre peut également entraîner la sabotage des infrastructures d'autres pays, provoquant des perturbations majeures, mettant des vies en danger, et compromettant la confiance des citoyens dans leur gouvernement.

V/Synthèse :

V.1/Conclusion:

Chapitre 1 : La nécessité de la cybersécurité

Le chapitre 1 met en lumière l'importance de la cybersécurité en exposant les caractéristiques et les enjeux liés à la protection des identités et des données personnelles en ligne contre les cybercriminels. Il souligne la demande croissante de professionnels de la cybersécurité et explique les compétences nécessaires pour faire face aux agresseurs informatiques. Le chapitre aborde également la protection des données d'entreprise, les motivations des agresseurs, l'éthique professionnelle, et offre une brève introduction à la guerre cybernétique, démontrant la nécessité des experts en cybersécurité pour protéger les citoyens et les infrastructures nationales.

Chapitre 2 : Attaques, concepts et techniques

Le chapitre 2 explore les méthodes d'analyse des cyberattaques par les professionnels de la cybersécurité, couvrant les vulnérabilités logicielles et matérielles, les catégories de failles de sécurité, les types de logiciels malveillants, les symptômes associés, les techniques d'infiltration et les attaques par déni de service, soulignant l'importance de comprendre ces aspects pour minimiser l'impact des attaques.

I/Analyser une cyberattaque:

I.1/Vulnérabilité de sécurité et exploits:

1/Détecter les vulnérabilités de sécurité :

Les vulnérabilités de sécurité, qu'elles soient liées au logiciel ou au matériel, représentent des failles exploitées par des attaquants. Les erreurs dans le code d'application ou le système d'exploitation introduisent souvent des vulnérabilités logicielles, nécessitant des mises à jour fréquentes pour les corriger. Les vulnérabilités matérielles, telles que celles résultant de défauts de conception, peuvent être exploitées par des exploits spécifiques, comme Rowhammer, compromettant la sécurité. Les mises à jour régulières, les tests de pénétration et la sécurité physique sont essentiels pour atténuer ces risques.

I.2/Types de failles de sécurité:

1/Catégoriser les vulnérabilités de sécurité :

La plupart des vulnérabilités de sécurité de logiciels font partie des catégories suivantes :

Débordement de tampon : modification au-delà des limites d'un tampon, pouvant causer des pannes, des compromissions de données ou une élévation des privilèges.
Entrée non validée : utilisation de données malveillantes pour dérégler les activités d'un programme.

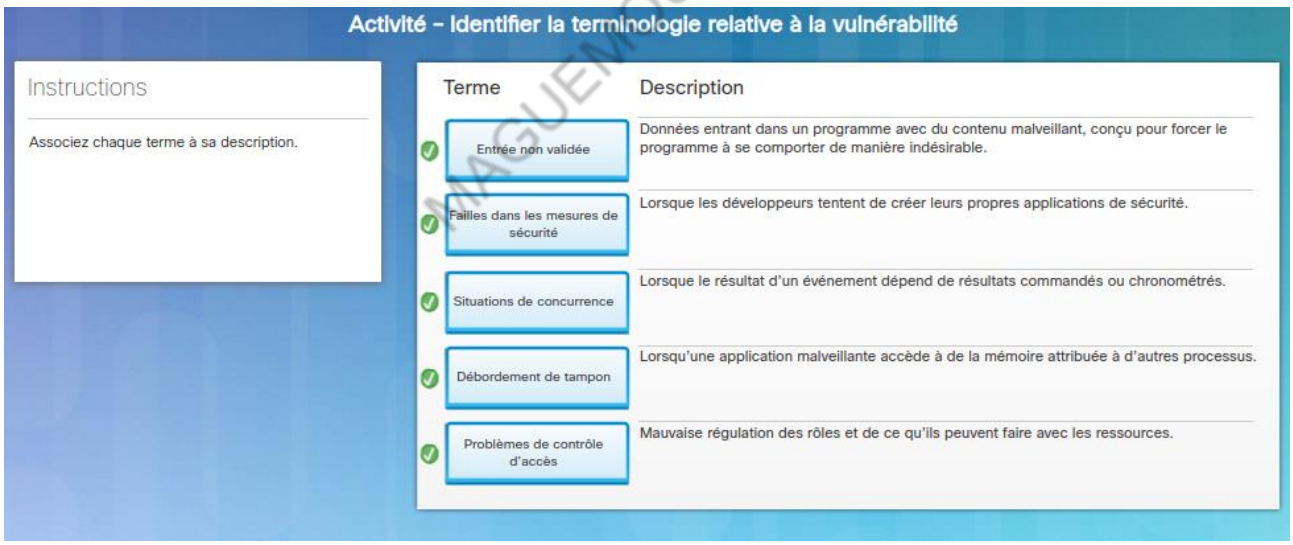
Situation de concurrence : vulnérabilité lorsque la sortie d'un événement dépend de sorties commandées ou planifiées, mais ne se produit pas dans l'ordre ou en temps voulu.

Failles dans les mesures de sécurité : protection des données par authentification, autorisation et chiffrement; les développeurs doivent éviter de créer leurs propres algorithmes de sécurité.

Problèmes de contrôle d'accès : vulnérabilités liées à une mauvaise utilisation des contrôles d'accès, avec la possibilité de contourner les autorisations via un accès physique à l'équipement cible.

L'accès physique doit être limité, et le chiffrement utilisé pour protéger les données contre le vol ou la corruption.

2/Activité-identifier la terminologie relative à la vulnérabilité :



I.3/Types de malware et symptômes:

1/Types de malwares :

Les malware, ou programmes malveillants, représentent tout code pouvant être utilisé pour voler des données, contourner les contrôles d'accès ou pour nuire à un système ou le compromettre. Voici quelques types communs de malware :

Logiciel espion : surveille et collecte des données utilisateur.
Publiciel : diffuse des publicités, souvent lié à des logiciels espions.

Bot : programme automatisé effectuant des actions en ligne.

Rançongiciel : bloque l'accès aux données et demande une rançon.

Scareware : utilise des faux avertissements pour tromper les utilisateurs.

Rootkit : modifie le système pour créer une porte dérobée.

Virus : code malveillant attaché à d'autres fichiers exécutables.

Cheval de Troie : opère sous couvert d'une opération légitime.

Vers : se réplique indépendamment au sein des réseaux.

Attaque MitM : prend le contrôle d'un appareil à l'insu de l'utilisateur.

Attaque MitMo : variante pour prendre le contrôle de terminaux mobiles.

2/Les symptômes du malware :

Symptômes communs des malware incluent : augmentation de l'utilisation du CPU, ralentissement de l'ordinateur, plantages fréquents, navigation Internet plus lente, problèmes réseau inexplicables, modifications ou suppressions de fichiers, présence d'éléments inconnus sur le bureau, exécution de processus inconnus, fermeture ou reconfiguration de programmes, envoi d'e-mails sans consentement de l'utilisateur.

3/Activité-identifier les types de programmes malveillants :

I.4/Méthodes d'infiltration:

1/Piratage psychologique :

Le piratage psychologique exploite la manipulation et les faiblesses individuelles pour obtenir des actions ou des informations confidentielles. Les attaques d'ingénierie sociale incluent l'usurpation, où l'agresseur ment pour obtenir des données privilégiées, et le talonnage, où l'agresseur suit rapidement une personne autorisée dans un lieu sécurisé. Une autre tactique est la contrepartie, où l'agresseur demande

des informations personnelles en échange de quelque chose, exploitant la cupidité ou la vanité de la cible.

2/Décryptage de mot de passe Wi-Fi :

Le décryptage de mot de passe Wi-Fi peut impliquer plusieurs techniques, notamment le piratage psychologique, où l'agresseur manipule une personne pour obtenir le mot de passe, les attaques brutales qui tentent plusieurs combinaisons possibles, et le reniflement de réseau, où l'agresseur capture et analyse les paquets envoyés sur le réseau pour découvrir le mot de passe, même s'il est chiffré. Des outils tels qu'Ophcrack, L0phtCrack, THC Hydra, RainbowCrack et Medusa peuvent être utilisés pour des attaques brutales.

3/Hameçonnage :

L'hameçonnage survient lorsque des cybercriminels envoient des e-mails frauduleux se faisant passer pour des sources fiables, dans le but de piéger les destinataires et de les inciter à installer un malware ou à divulguer des informations sensibles. L'hameçonnage ciblé va plus loin en personnalisant les e-mails pour des individus spécifiques, exploitant des informations sur leurs intérêts afin de les tromper de manière plus précise. Par exemple, en simulant la vente d'une voiture spécifique pour cibler un passionné d'automobile.

4/Exploitation des vulnérabilités :

L'exploitation des vulnérabilités est une autre méthode commune d'infiltration. Les agresseurs vont analyser les ordinateurs pour obtenir des informations à leur sujet. Voici une méthode commune pour exploiter les vulnérabilités :

Étape 1: Collecte d'infos sur la cible. Les agresseurs utilisent des outils comme WHOIS et des tactiques psychologiques pour en apprendre plus sur le système cible.

Étape 2: Identification des détails du système. Ils recherchent des informations telles que le système d'exploitation, sa version, et les services actifs.

Étape 3: Recherche de vulnérabilités. Les agresseurs ciblent les vulnérabilités spécifiques liées au système d'exploitation ou à ses services.

Étape 4: Utilisation d'exploits. Lorsqu'une vulnérabilité est trouvée, les agresseurs tentent d'utiliser des exploits existants. S'ils n'en trouvent pas, ils peuvent envisager d'écrire leur propre exploit.

Outils utilisés: WHOIS et NMAP. WHOIS fournit des détails sur les noms de domaine, et NMAP est un scanner de port permettant d'analyser les services actifs sur l'ordinateur cible.

Menaces Persistantes Avancées (MPA) : Les MPA sont des attaques sophistiquées, bien financées et complexes, visant des cibles spécifiques pour des motifs commerciaux

ou politiques. Opérant de manière furtive et à long terme, elles se caractérisent par leur complexité élevée, leur fonctionnement à plusieurs stades, et leur utilisation de malwares personnalisés adaptés à différents appareils. Souvent liées à l'espionnage réseau, ces attaques exigent des compétences approfondies, des ressources importantes, et une persévérance qui dépasse souvent les capacités d'un seul agresseur.

I.5/Déni de service (Dos) :

1/Dos :

Attaques par Déni de Service (DoS) :

Les attaques par déni de service perturbent les services réseau en saturant de trafic ou en envoyant des paquets malveillants. Deux types principaux :

1. **Quantité élevée de trafic :** Inonde le réseau, hôte ou application avec une masse de données, provoquant des ralentissements ou une panne.
2. **Paquets malveillants :** Envoie intentionnellement des paquets mal formatés, induisant des erreurs chez le destinataire et entraînant des ralentissements ou une panne.

Ces attaques sont majeures, capables de causer des perturbations significatives, avec une simplicité d'exécution, même pour des agresseurs non qualifiés.

2/DdoS :

Attaque par Déni de Service Distribué (DDoS) :

Une attaque DDoS est une version évoluée d'une attaque DoS, impliquant des sources multiples et coordonnées. Voici comment elle peut se dérouler :

1. **Établissement d'un réseau de zombies :** L'agresseur crée un réseau d'ordinateurs infectés appelé "zombies", contrôlés par des gestionnaires.
2. **Propagation constante :** Les zombies analysent et infectent davantage d'hôtes, augmentant ainsi le nombre de zombies disponibles.
3. **Activation de l'attaque :** Une fois prêt, l'attaquant utilise les gestionnaires pour orchestrer une attaque DDoS à travers le réseau de zombies.

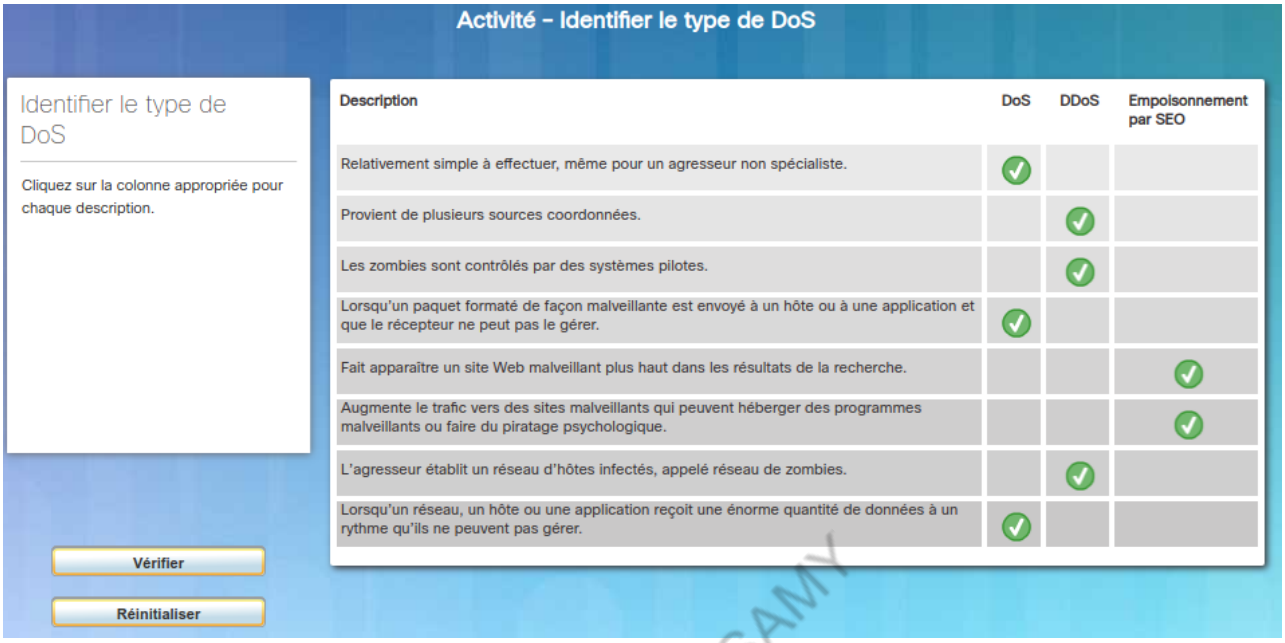
Cette attaque, avec ses multiples sources, est plus difficile à contrer et peut causer des dommages considérables.

3/Empoisonnement par SEO :

L'empoisonnement par SEO est une technique malveillante visant à manipuler le classement des moteurs de recherche. Alors que l'optimisation pour les moteurs de recherche (SEO) est normalement utilisée pour améliorer le positionnement légitime d'un site, les acteurs malveillants exploitent cette pratique. Ils créent des sites malveillants qui apparaissent en tête des

résultats de recherche en utilisant des termes populaires. L'objectif est d'attirer du trafic vers ces sites, pouvant héberger des logiciels malveillants ou être utilisés pour des attaques d'ingénierie sociale.

4/Activité-identifier le type DoS :



II/Les problématiques de la cybersécurité :

II.1/Attaque mixte :

1/Qu'est-ce qu'une attaque mixte ?

Attaques Mixtes :

Les attaques mixtes sont des attaques informatiques utilisant plusieurs techniques simultanément pour compromettre une cible. Elles englobent des malwares combinant vers, chevaux de Troie, logiciels espions, enregistreurs de frappe, pourriels et plans d'hameçonnage. Cette approche complexe met en danger les données des utilisateurs.

Un exemple fréquent d'attaque mixte implique l'utilisation de pourriels, messages instantanés ou sites légitimes pour distribuer des liens conduisant au téléchargement secret de malwares sur l'ordinateur. Une autre variante combine des attaques par déni de service distribué avec des e-mails d'hameçonnage, perturbant un site Web populaire avant d'envoyer des e-mails frauduleux aux clients affectés.

Certains vers notoires, tels que Nimbda, CodeRed, BugBear, Klez et Slammer, sont classés comme attaques mixtes en raison de leurs multiples méthodes de propagation et de leurs fonctionnalités variées. Les récents vers Conficker et ZeuS/LICAT ont également adopté cette approche mixte en utilisant diverses méthodes de distribution.

II.2/Réduction d'impact :

1/Qu'est-ce que la réduction d'impact ?

Malgré les efforts déployés par les entreprises pour prévenir les failles de sécurité, leur inévitabilité implique une nécessité de réaction rapide, tenant compte non seulement des aspects techniques et des pertes de données, mais aussi des répercussions sur la réputation de l'entreprise.

Voici quelques mesures importantes qu'une entreprise doit prendre lorsqu'une faille de sécurité est identifiée, selon l'avis de nombreux experts de la sécurité :

1/Communication Transparente :

- Informer immédiatement les employés et clients de manière transparente.
- Annoncer officiellement pour établir la confiance.

2. **Responsabilité et Transparence :**
   - Assumer la responsabilité et fournir des détails sur la faille.
   - Prendre en charge les coûts des services de protection pour les clients touchés.
3. **Assistance aux Clients :**
   - Être transparent sur les actions entreprises pour résoudre le problème.
4. **Analyse de la Cause :**
   - Engager des enquêteurs en informatique pour comprendre les causes.
5. **Mesures Correctives :**
   - Appliquer les enseignements tirés pour éviter des failles similaires.
   - Renforcer les protocoles de sécurité.
6. **Audit des Systèmes :**
   - Vérifier l'intégrité de tous les systèmes.
   - Éliminer toute porte dérobée potentielle.
7. **Formation Continue :**
   - Former régulièrement sur les meilleures pratiques de sécurité.

La gestion proactive de ces étapes minimise les impacts négatifs et renforce la posture de sécurité globale de l'entreprise.

III/Synthèse :

III.1/Conclusion:

Chapitre 2 : Attaques, concepts et techniques

Ce chapitre a exploré les méthodes employées par les professionnels de la cybersécurité pour analyser les conséquences des cyberattaques, mettant en lumière les vulnérabilités des logiciels et du matériel de sécurité, ainsi que les différentes catégories de vulnérabilités. Les types de logiciels malveillants tels que virus, vers, chevaux de Troie, logiciels espions et

publiciels ont été détaillés, tout comme les méthodes d'infiltration telles que le piratage psychologique, le décryptage de mots de passe Wi-Fi, l'hameçonnage et l'exploitation de vulnérabilités. Les attaques par déni de service, y compris les attaques distribuées (DDoS), ont également été abordées, de même que les attaques mixtes qui combinent différentes techniques. En cas d'attaque inévitable, il revient aux professionnels de la cybersécurité de minimiser son impact.

Chapitre 3 : Protection des données et confidentialité

Ce chapitre se concentre sur la sécurité de vos périphériques personnels et de vos données, offrant des conseils pour protéger vos appareils, créer des mots de passe robustes et utiliser de manière sécurisée les réseaux sans fil. Il aborde également la sécurisation des données en ligne, soulignant l'importance de l'authentification et fournissant des conseils sur les bonnes pratiques en ligne pour renforcer la sécurité de vos informations.

I/Protéger vos données:

I.1/Protéger vos données et le réseau :

1/Protéger vos périphériques informatiques:

Vos périphériques informatiques stockent vos données et représentent le portail de votre vie en ligne. Voici une liste finale des étapes à suivre pour protéger vos périphériques informatiques d'une intrusion :

1. Activez toujours le pare-feu : Que ce soit un pare-feu logiciel ou matériel, assurez-vous qu'il est activé et mis à jour pour empêcher l'accès non autorisé.
2. Utilisez un antivirus et un anti-logiciel espion : Protégez votre ordinateur contre les virus, chevaux de Troie, vers, rançongiciels et logiciels espions en téléchargeant des logiciels uniquement à partir de sites sécurisés. Mettez à jour régulièrement votre logiciel antivirus.
3. Gérez votre système d'exploitation et votre navigateur : Configurez les paramètres de sécurité à un niveau moyen ou supérieur, mettez à jour régulièrement votre système d'exploitation et téléchargez les derniers correctifs de sécurité pour vos navigateurs.

4. Protégez tous vos périphériques : Utilisez des mots de passe sur tous les périphériques informatiques, chiffrez les données sensibles et confidentielles, et limitez les informations stockées sur les terminaux mobiles. Assurez-vous que tous les appareils IoT sont connectés à un réseau isolé.

2/Utiliser les réseaux sans fil en toute sécurité :

Pour sécuriser votre réseau sans fil et protéger vos périphériques :

1. Changez l'identificateur SSID et le mot de passe : Modifiez l'identificateur SSID et le mot de passe par défaut de votre réseau sans fil pour empêcher l'accès non autorisé.
2. Désactivez la diffusion du SSID : Configurez votre routeur sans fil pour ne pas diffuser le SSID, rendant ainsi votre réseau moins visible.
3. Activez la sécurité sans fil et le chiffrement WPA2 : Cryptez votre communication sans fil en activant la sécurité sans fil et la fonctionnalité de chiffrement WPA2 sur votre routeur sans fil.
4. Mise à jour après la faille de WPA2 : Suite à la faille de sécurité de WPA2 en 2017, mettez à jour tous vos produits, y compris routeurs et appareils sans fil, pour bloquer les attaques KRACK.
5. Utilisez un service VPN fiable : Lorsque vous utilisez un réseau sans fil public, utilisez un service VPN pour sécuriser votre connexion et prévenir toute interception de données.
6. Désactivez le Bluetooth quand non utilisé : Pour éviter les risques liés au Bluetooth, désactivez cette fonctionnalité lorsque vous ne l'utilisez pas, notamment sur les smartphones et tablettes.

3/Utiliser des mots de passe uniques pour chaque compte en ligne :

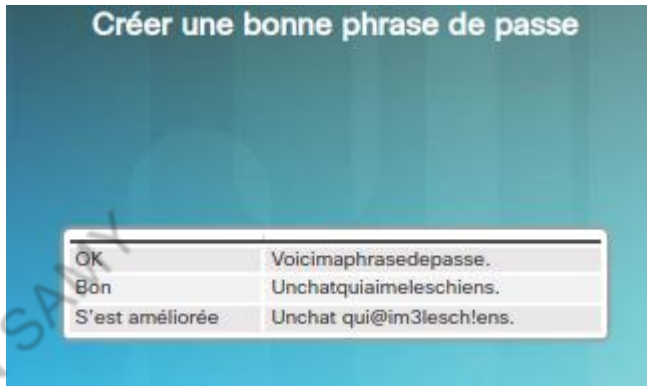
Pour sécuriser vos comptes en ligne, il est essentiel d'utiliser des mots de passe uniques et forts pour chaque compte. Réutiliser le même mot de passe expose vos données à des risques majeurs en cas de compromission d'un seul mot de passe, permettant aux cybercriminels d'accéder à plusieurs comptes. Utiliser un gestionnaire de mots de passe peut simplifier cette tâche en stockant de manière sécurisée et chiffrée tous vos mots de passe uniques et complexes. Avec un gestionnaire de mots de passe, il vous suffit de vous rappeler d'un mot de passe principal pour accéder à tous vos comptes en ligne, renforçant ainsi la sécurité de vos données.

Conseils pour choisir un bon mot de passe :

- N’utilisez pas des mots et des noms du dictionnaire, peu importe la langue.
- N’utilisez pas les fautes d’orthographe des mots du dictionnaire.
- N’utilisez pas des noms d’ordinateur ou des noms de compte.
- Si possible, utilisez des caractères spéciaux, comme ! @ # $ % ^ & * ( )
- Votre mot de passe doit comporter au moins 10 caractères

4/Utiliser une phrase secrète et non un mot de passe :

Pour renforcer la sécurité de vos périphériques informatiques, utilisez des phrases secrètes plutôt que des mots de passe, privilégiant la longueur et l'ajout de caractères spéciaux. Les nouvelles directives du NIST encouragent une approche plus flexible, sans imposer de règles strictes, tout en mettant l'accent sur la responsabilité des fournisseurs d'accès pour vérifier l'identité des utilisateurs.



En outre, même avec un accès sécurisé, la protection des données est cruciale. Assurez-vous de mettre en place des mesures de sécurité pour protéger vos informations, même en cas d'accès physique sécurisé à vos ordinateurs et périphériques réseau.

5/Atelier – Créer et stocker des mots de passe fiables :

Partie 1 :

1/Prenez un moment pour analyser les caractéristiques d’un mot de passe fiable et la politique courante relative au mot de passe indiqués ci-dessus. Pourquoi l’ensemble de politiques néglige-t-il les deux premiers critères ? Expliquez votre réponse.

La politique de mot de passe néglige les critères de facilité de mémorisation pour l'utilisateur et de résistance face à la déchiffrabilité par une tierce partie. En se concentrant sur des critères techniques de complexité, elle peut entraîner des mots de passe difficiles à retenir, poussant potentiellement les utilisateurs à des pratiques risquées, comme la note des mots de passe. Une politique plus équilibrée devrait viser à assurer à la fois la sécurité technique et la facilité de mémorisation pour promouvoir des pratiques de mot de passe sûres.

2/Le mot de passe généré est-il facile à se rappeler ?
Non, voila des exemples :
CZQt0>_@d39Jz/:(rvo+Py
Z9~09u0bp%DmeIAc$O`XV1

v_;]H%m1(p!/"wlfSiK3:U
V05^l3(LF.1W.a_R^CY-iv
a&&3|%Ie/e#ucQQw^R0Q+~

3/Le mot de passe généré est-il facile à se rappeler ?
oui, voila l'exemple : expression condition adventure coach

Partie 2 :
1/Explorez l'administrateur de mots de passe LastPass. Lorsque vous ajoutez des mots de passe dans LastPass, où ces derniers sont-ils stockés ?
Les mots de passe ajoutés à LastPass sont stockés sous forme chiffrée sur les serveurs de LastPass, mais la clé de chiffrement est générée et détenue localement sur l'appareil de l'utilisateur, assurant ainsi la confidentialité des données même en cas de compromission des serveurs.

2/À part vous, au moins une entité tierce a accès à vos mots de passe. Qui est cette entité ?

Dans le contexte de LastPass, la seule entité tierce qui a techniquement accès à vos mots de passe est LastPass en tant que service. Cependant, les mots de passe sont stockés de manière chiffrée, et LastPass n'a pas connaissance de la clé de chiffrement qui est générée localement sur l'appareil de l'utilisateur. Cela signifie que, même si LastPass est une entité tierce impliquée, elle ne peut pas déchiffrer ou accéder à vos mots de passe sans la clé locale.

3/Même si stocker tous vos mots de passe au même emplacement peut être pratique, cela présente des risques. Pouvez-vous donner un exemple ?

Stocker tous les mots de passe au même endroit, comme un gestionnaire de mots de passe, présente le risque que la compromission d'un seul point puisse compromettre l'ensemble de vos informations d'identification.

I.2/Maintenance des données :

1/Chiffrer vos données :

Le chiffrement convertit les données en un format non accessible en lecture pour les parties non autorisées, offrant ainsi une protection contre l'interception par des tiers. Le système EFS de Windows, par exemple, permet de chiffrer des fichiers et dossiers, assurant que seul l'utilisateur autorisé peut y accéder en utilisant son compte d'utilisateur associé.

2/Sauvegarder vos données :

La sauvegarde des données est cruciale pour éviter la perte irréversible d'informations en raison de défaillances matérielles, pertes d'appareils ou suppressions accidentelles. Vous pouvez choisir des solutions de stockage local, comme des disques durs externes, des réseaux domestiques, ou des services de stockage en ligne tels que le cloud. Le stockage local offre un contrôle total, tandis

que le cloud offre la flexibilité et l'accès à distance. Il est essentiel de considérer les coûts, la maintenance et la sécurité lors du choix d'une méthode de sauvegarde.

3/Atelier – Sauvegarder les données dans un stockage externe :

Partie 1 :Étape 2 :

Établissez un calendrier de sauvegarde. Pour cet atelier, configurez sur 3 h pour tous les jours. Pourquoi choisir d'effectuer des sauvegardes à 3 h ?

Choisir d'effectuer des sauvegardes à 3 heures présente l'avantage de sélectionner un moment où l'utilisation de l'ordinateur est généralement faible souvent pendant la nuit, minimisant ainsi l'impact sur les performances du système et assurant que les sauvegardes ne perturbent pas l'activité normale de l'utilisateur.

Parti 2 : étape 1:

a. Citez quelques services de sauvegarde basés sur le cloud.

b. Recherchez les services que vous avez mentionnés plus haut. Ces services sont-ils gratuits ?

c. Les services que vous avez mentionnés dépendent-ils de la plate-forme ?

d. Pouvez-vous accéder à vos données à partir de tous les appareils que vous possédez (PC de bureau, ordinateur portable, tablette et téléphone) ?

a. Quelques services de sauvegarde basés sur le cloud sont :
Google Drive,Dropbox,Microsoft OneDrive,Amazon Drive

b. La gratuité de ces services dépend du niveau d'espace de stockage que vous utilisez. Ils proposent souvent une certaine quantité d'espace gratuit, mais des frais peuvent s'appliquer si vous avez besoin de plus d'espace.

c. Ces services sont généralement disponibles sur plusieurs plateformes, y compris Windows, macOS, Android et iOS.

d. Oui, en règle générale, vous pouvez accéder à vos données à partir de tous les appareils que vous possédez, car ces services sont conçus pour être accessibles depuis différents appareils via des applications dédiées ou des interfaces Web.

Étape 2 :

1. Quels sont les avantages de la sauvegarde des données sur un disque externe local ?
2. Quels sont les inconvénients de la sauvegarde des données sur un disque externe local ?
3. Quels sont les avantages de la sauvegarde des données sur un disque basé sur le cloud ?
4. Quels sont les inconvénients de la sauvegarde des données sur un disque basé sur le cloud ?

1./Avantages de la sauvegarde sur un disque externe local :

- Contrôle direct : Vous avez un contrôle total sur vos données, car elles sont stockées localement.

- Coût initial unique : L'achat d'un disque externe peut représenter un coût unique sans frais récurrents.

2/Inconvénients de la sauvegarde sur un disque externe local :
- Risque physique : En cas de dommages, vol ou perte du disque externe, vos données peuvent être irrécupérables.
- Manque de redondance : En cas de défaillance du disque, il peut ne pas y avoir de copies de sauvegarde.

3/Avantages de la sauvegarde sur un disque basé sur le cloud :
- Accessibilité : Vous pouvez accéder à vos données de n'importe où avec une connexion Internet.
- Redondance : Les services cloud ont souvent des mécanismes de sauvegarde et de redondance intégrés.

4/Inconvénients de la sauvegarde sur un disque basé sur le cloud :
- Dépendance à Internet : L'accès à vos données dépend de la disponibilité d'une connexion Internet.
- Coûts récurrents : Certains services cloud facturent des frais mensuels ou annuels, ce qui peut entraîner des coûts continus.

4/Supprimer définitivement vos données :

Lorsque des fichiers sont supprimés, ils restent potentiellement récupérables en raison de l'empreinte magnétique sur le disque dur. Pour assurer une suppression définitive, des outils spécialisés tels que SDelete, Shred (pour Linux), et Secure Empty Trash (pour Mac OSX) sont recommandés. Cependant, la certitude totale de l'irrécupérabilité nécessite la destruction physique du dispositif de stockage. Il est crucial de considérer la protection des données en ligne et de s'interroger sur leur emplacement, leur chiffrement et la sécurisation lors de la suppression de disques durs ou d'ordinateurs.

5/Atelier – Qui détient vos données ?

Partie 1 :

a. Possédez-vous un compte auprès d'un prestataire de services en ligne ? Si oui, avez-vous consulté les conditions de service ?
b. Quelle est la politique d'utilisation des données ?
c. Quels sont les paramètres d'accès ?
d. Quelle est la politique de sécurité ?
e. Quels sont vos droits concernant vos données ? Pouvez-vous demander une copie de vos données ?
f. Que peut faire le fournisseur des données que vous téléchargez ?
g. Qu'arrive-t-il à vos données lorsque vous fermez votre compte ?

a/Oui,j'ai jamais consulté les conditions de service.

b/ La politique d'utilisation des données varie selon le service ou le site web. Elle définit comment les données des utilisateurs sont collectées, stockées et utilisées.

c/ Les paramètres d'accès déterminent qui peut accéder aux données. Certains services permettent de définir des paramètres de confidentialité pour contrôler l'accès aux informations.

d/ La politique de sécurité concerne les mesures mises en place pour protéger les données contre les accès non autorisés ou les violations.

e/ Les droits concernant les données varient selon les réglementations locales. Dans certains cas, les utilisateurs peuvent demander une copie de leurs données.

f Le fournisseur des données peut avoir des droits spécifiés dans les conditions d'utilisation, tels que l'utilisation à des fins publicitaires, mais cela dépend du service.

g/ Lors de la fermeture d'un compte, la manière dont les données sont traitées dépend des politiques du service. Certains services peuvent supprimer les données, tandis que d'autres peuvent les conserver pendant un certain temps ou anonymiser les informations personnelles.

Partie 2 :

a. Que pouvez-vous faire pour vous protéger ?
b. Que pouvez-vous faire pour protéger votre compte ainsi que vos données ?

a /Pour protéger votre vie privée en ligne, lisez attentivement les conditions de service, comprenez la politique de confidentialité, soyez sélectif dans les informations partagées, utilisez les paramètres de confidentialité, soyez prudent avec l'accès aux services tiers et envisagez le chiffrement pour des données sensibles.

B/Pour protéger votre compte et vos données, utilisez des mots de passe forts et uniques, activez l'authentification à deux facteurs lorsque possible, soyez vigilant face aux tentatives de phishing, maintenez vos logiciels à jour, utilisez des paramètres de confidentialité appropriés et évitez de partager des informations sensibles en ligne.

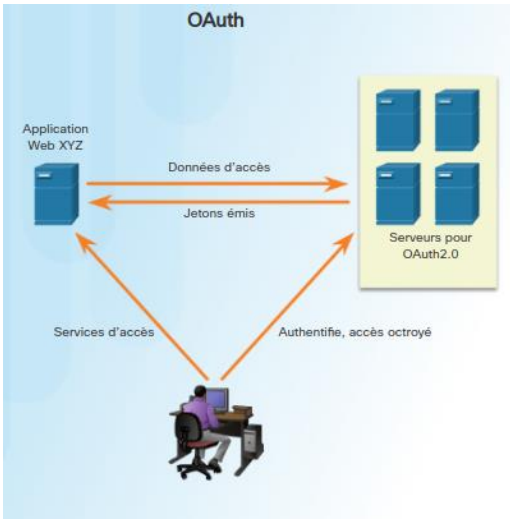
II/Protéger votre confidentialité en ligne:

II.1/Authentification performante:

1/Authentification à deux facteurs :

L'authentification à deux facteurs, utilisée par des services en ligne tels que Google, Facebook, etc., renforce la sécurité en exigeant un second élément, comme un objet physique ou un balayage biométrique, en plus du nom d'utilisateur et du mot de passe. Cependant, les pirates peuvent encore compromettre les comptes par des moyens tels que l'hameçonnage, les programmes malveillants et le piratage psychologique.

2/OAuth 2.0 :



OAuth (Open Authorization) est un protocole ouvert normalisé qui facilite l'accès à des applications tierces sans exposer le mot de passe de l'utilisateur. Il agit comme un intermédiaire dans l'autorisation d'accès, permettant par exemple à une application XYZ de se connecter via les informations d'identification d'un site de réseaux sociaux ABC, sans que XYZ ait accès aux informations d'identification de l'utilisateur. L'utilisation de jetons secrets renforce la sécurité en empêchant les applications malveillantes d'accéder aux informations de l'utilisateur.

II.2/Partagez-vous trop d'informations:

1/Ne partagez pas trop d'informations sur les réseaux sociaux :

Pour préserver votre vie privée sur les réseaux sociaux, limitez la quantité d'informations partagées en évitant de divulguer des détails personnels tels que votre date de naissance, adresse e-mail ou numéro de téléphone. Ne remplissez que les champs essentiels de votre profil et configurez vos paramètres pour restreindre l'accès à vos activités et discussions aux seules personnes que vous connaissez. Évitez également d'utiliser des questions de sécurité facilement accessibles en ligne pour la récupération de compte, et utilisez plutôt un gestionnaire de mots de passe pour gérer ces informations de manière sécurisée.

2/Confidentialité des e-mails et sur navigateur Web :

Les e-mails et les activités de navigation en ligne peuvent compromettre votre vie privée, car ils sont transmis en texte brut et peuvent être archivés sur des serveurs. L'historique de navigation Web peut être exploité, mais l'utilisation du mode de navigation privée et d'autres précautions, comme la désactivation des cookies, peut aider à minimiser ces risques. Il est crucial de prendre des mesures pour protéger vos données, votre identité et vos périphériques informatiques.

3/Atelier - Découvrez votre propre comportement à risque en ligne :

Partie 1 :

a. 3) Ça dépend ; je filtre ce que je partage et avec qui je le partage. (1 point)
b. 5) créez un tout nouveau mot de passe fiable. (0 point)
c. 4) vous pointez votre souris sur les liens pour vérifier l'URL de destination avant de cliquer dessus. (1 point)
d. 3) vous ignorez le message, en veillant à ne pas cliquer dessus ou à télécharger le programme et vous fermez le site Web. (0 point)
e. 2) vous vérifiez l'URL pour vous assurer que c'est bien votre institution avant d'entrer les renseignements ; (0 point)
f. 2) recherchez des informations complémentaires sur le développeur du programme avant de le télécharger ; (1 point)

g. 4) ne le prenez pas. (0 point)
h. 2) ne vous connectez pas au réseau et patientez jusqu'à ce que vous ayez accès à une connexion sécurisée ; (0 point)
Score total : 3 points

Partie 2 :

Il semble qu'il manque la possibilité pour moi de réaliser une analyse de votre comportement en ligne. Cependant, je peux fournir des conseils généraux basés sur les informations que vous avez partagées.

1/Réduisez les informations partagées sur les réseaux sociaux :** Limitez la quantité d'informations personnelles que vous partagez en ligne, car cela peut être exploité par des cybercriminels.

2/Utilisez des mots de passe forts et uniques :** Évitez de réutiliser les mots de passe et créez des combinaisons complexes pour renforcer la sécurité de vos comptes en ligne.

3/Soyez prudent avec les e-mails :** Ne cliquez pas sur des liens dans des e-mails suspects et soyez conscient des tentatives de phishing.

4/Évitez les téléchargements non sollicités :** Ne téléchargez pas de logiciels non demandés, car cela peut introduire des logiciels malveillants sur votre système.

5/Vérifiez l'authenticité des sites Web financiers :** Avant de fournir des informations financières en ligne, assurez-vous que le site Web est authentique en vérifiant l'URL.

6./Examinez attentivement les programmes téléchargés :** Assurez-vous que les programmes téléchargés proviennent de sources légitimes et fiables.

7/Soyez prudent avec les clés USB trouvées :** Évitez de connecter des clés USB inconnues à votre ordinateur, car elles pourraient contenir des logiciels malveillants.

8/Utilisez des réseaux Wi-Fi sécurisés :** Évitez de vous connecter à des réseaux Wi-Fi non sécurisés, et utilisez un réseau privé virtuel (RPV) pour chiffrer votre trafic.

Après avoir pris en considération ces conseils, assurez-vous d'ajuster vos comportements en ligne en conséquence pour renforcer votre sécurité sur Internet.

III/Synthèse :

III.1/Conclusion:

Chapitre 3 : Protection des données et confidentialité

Ce chapitre met l'accent sur la protection des périphériques, la création de mots de passe robustes, l'utilisation sécurisée des réseaux sans fil, les sauvegardes de données, le stockage sécurisé, la suppression définitive des données, et les techniques d'authentification pour renforcer la sécurité des données personnelles.

Chapitre 4 : Protection de l'entreprise

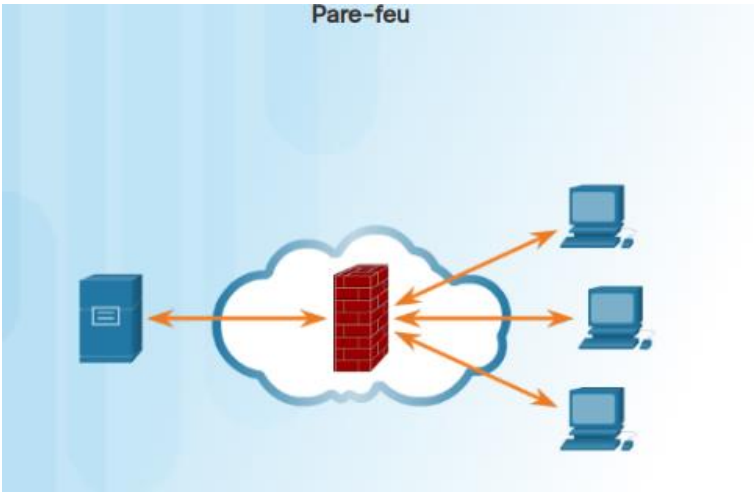
Ce chapitre explore les technologies et les processus employés par les experts en cybersécurité pour protéger les réseaux, les équipements et les données des entreprises. Il couvre divers types de pare-feu, d'appliances de sécurité et de logiciels, ainsi que des pratiques recommandées. Le contenu aborde également des sujets tels que les réseaux de zombies, la chaîne de frappe, la sécurité basée sur le comportement, l'utilisation de NetFlow pour la surveillance réseau, et présente l'approche de Cisco en matière de cybersécurité, y compris l'équipe CSIRT et le guide sur la sécurité, tout en explorant les outils de détection et de prévention des attaques réseau.

I/Pare-feu:

I.1/Types de pare-feu :

1/Types de pare-feu:

Les pare-feu, qu'ils soient déployés au niveau d'un seul ordinateur (pare-feu propre à un hôte unique) ou comme un dispositif réseau autonome (pare-feu basé sur le réseau), jouent un rôle crucial dans la prévention des attaques informatiques en filtrant et contrôlant les flux de données autorisés.

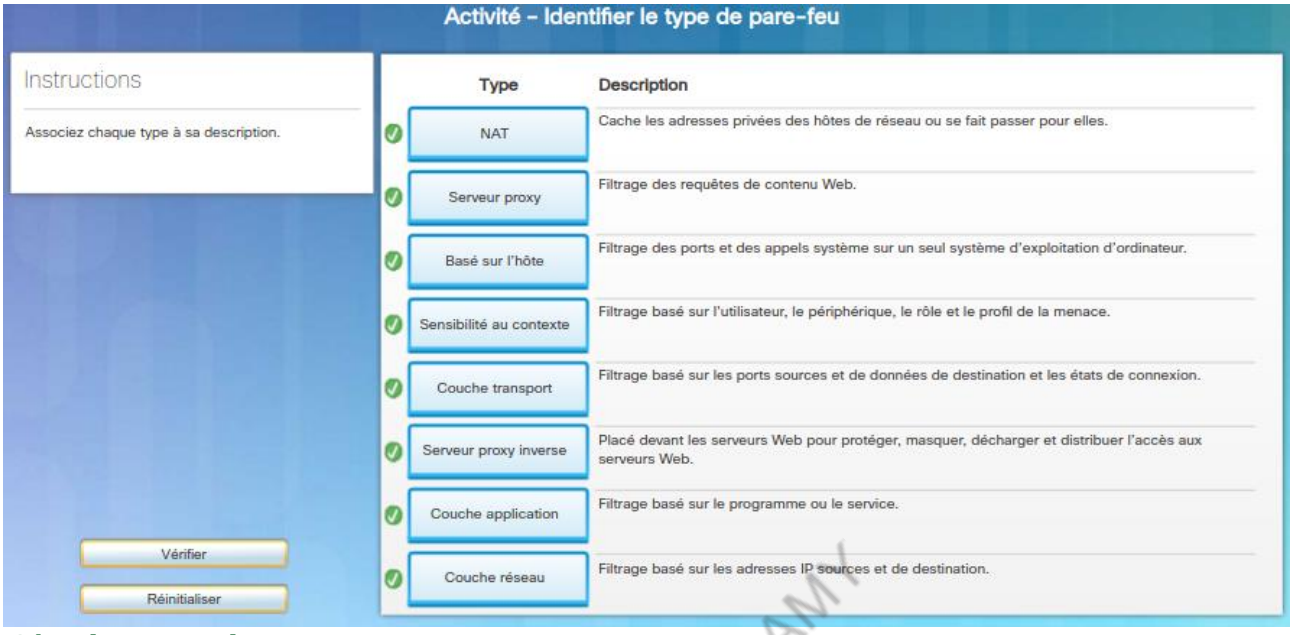


Voici une liste des types de pare-feu courants :

Les différents types de pare-feu incluent le pare-feu de la couche réseau qui filtre selon les adresses IP, le pare-feu de la couche transport qui se base sur les ports et les états de connexion, le pare-feu de la couche application qui filtre par applications ou services, le pare-feu pour applications sensibles au contexte qui se base sur divers critères, le serveur proxy qui filtre les demandes de contenu Web, le serveur proxy inverse qui protège et distribue l'accès aux serveurs Web, le pare-feu NAT qui cache les

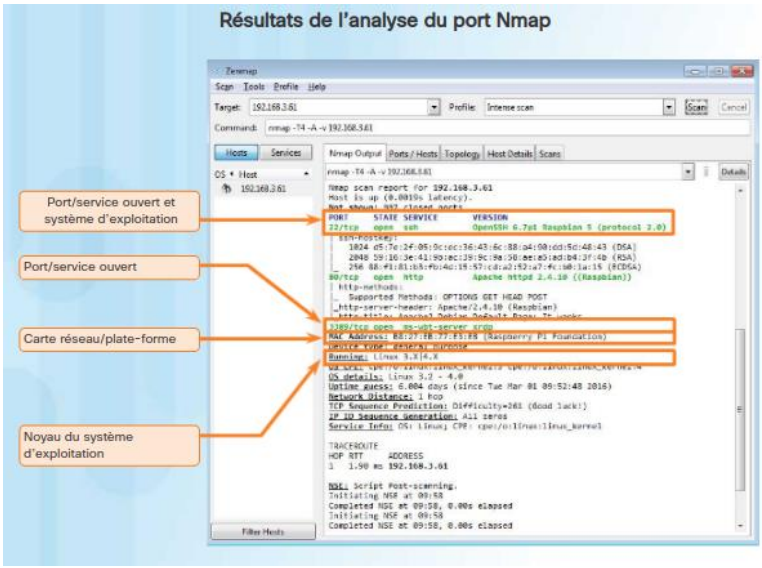
adresses privées, et le pare-feu propre à un hôte unique qui filtre les ports et les appels de service sur un système d'exploitation individuel.

2/Activité-identifier le type de pare-feu :



3/Balayage des ports :

Le balayage des ports est un processus qui consiste à sonder un ordinateur, un serveur ou un autre hôte de réseau pour détecter les ports ouverts. Chaque application sur un périphérique est associée à un numéro de port, facilitant la transmission des données vers l'application appropriée. Le balayage des ports peut être utilisé de manière malveillante pour identifier le système d'exploitation et les services, mais aussi de manière légitime par un administrateur réseau pour évaluer la sécurité du réseau. Il est essentiel de l'utiliser avec précaution, en évitant les serveurs publics sur Internet sans permission. Des outils comme Nmap peuvent être utilisés pour effectuer le balayage des ports, fournissant un rapport des services en cours d'exécution et des numéros de ports associés.



Le balayage d'un port entraîne habituellement l'une des trois réponses suivantes :

1/Ouvert ou Accepté :L'hôte indique qu'un service est en attente de requête sur le port.
2/Fermé, Refusé ou Pas en attente de requête :L'hôte indique que les connexions au port seront refusées.
3/Filtré, Ignoré ou Bloqué : Aucune réponse n'est reçue de la part de l'hôte.

Pour effectuer un balayage des ports depuis l'extérieur du réseau, il faut le faire contre le pare-feu ou l'adresse IP publique du routeur. En connaissant l'adresse IP publique (accessible via un moteur de recherche), on peut utiliser des outils comme le Scanner de ports en ligne Nmap pour analyser les ports communs (21, 22, 25, 80, 443, 3389). Si l'un de ces ports est ouvert, cela suggère un transfert de port activé sur le routeur ou le pare-feu, permettant l'accès aux serveurs du réseau privé.

4/Activité-identifier la réponse d'analyse du port:

L'hôte n'a pas répondu

L'hôte a répondu en indiquant que les connexions seront refusées sur le port

L'hôte a répondu en indiquant que les connexions seront refusées sur le port

L'hôte a répondu en indiquant qu'un service est écoute sur le port

L'hôte n'a pas répondu

L'hôte a répondu en indiquant que les connexions seront refusées sur le port

L'hôte a répondu en indiquant qu'un service est écoute sur le port

I.2/Appliances de sécurité:

1/Appliances de sécurité :

Pour assurer une sécurité réseau complète, il est essentiel d'utiliser une combinaison d'outils et d'appliances de sécurité. Ces éléments doivent travailler de concert pour garantir une protection efficace. Les appliances de sécurité, qu'elles soient des périphériques autonomes tels que des routeurs ou des pare-feu, des cartes installées dans des périphériques réseau, ou des modules logiciels, fonctionnent mieux lorsqu'elles font partie d'un système intégré.
Cisco propose diverses appliances de sécurité pour répondre aux besoins en matière de sécurité réseau, dont certaines sont les suivantes :

1/Routeurs (ISR) :Les routeurs de services intégrés Cisco (ISR) offrent des fonctionnalités de pare-feu, de filtrage du trafic, de prévention des intrusions (IPS), de chiffrement et de VPN pour une connectivité sécurisée.

2/Pare-feux nouvelle génération :Les pare-feu de nouvelle génération de Cisco, tels que l'Adaptive Security Appliance (ASA), intègrent des fonctionnalités avancées d'analyse et de gestion de réseau en plus des fonctions de routage.

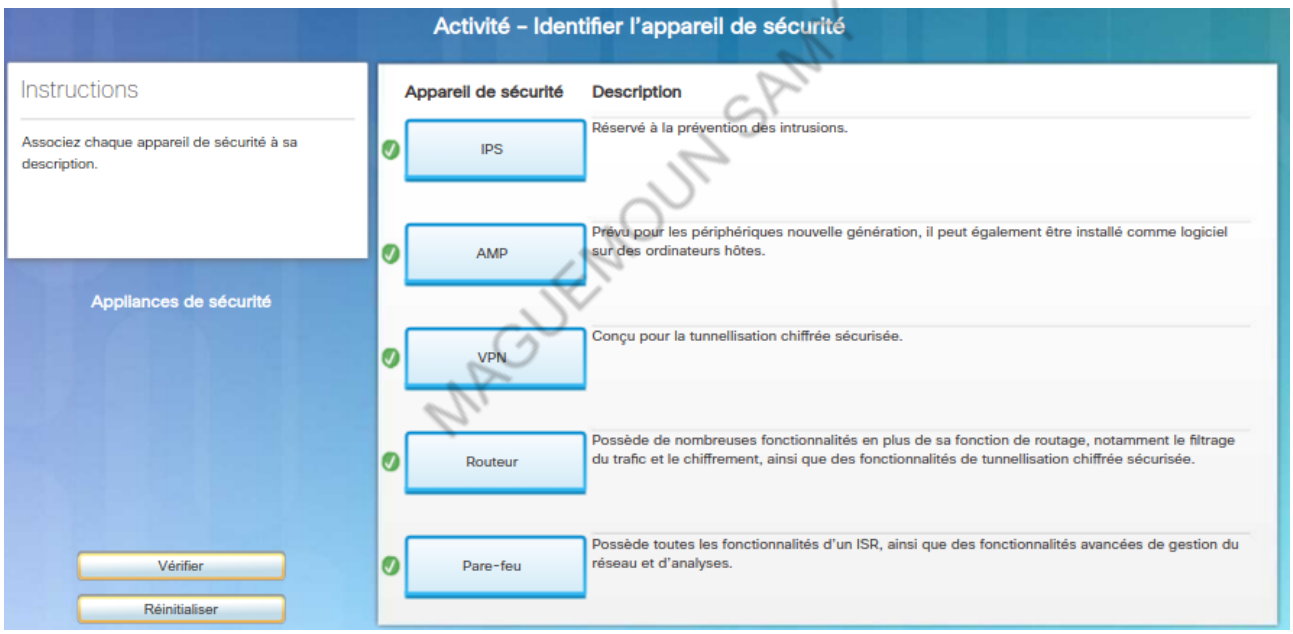
3/Systèmes de prévention des intrusions (IPS) :Les périphériques IPS de nouvelle génération de Cisco sont dédiés à la prévention des intrusions, renforçant la sécurité contre les menaces.

4/VPN :Les appliances de sécurité Cisco incluent des serveurs et des technologies client pour les réseaux privés virtuels (VPN), permettant des connexions chiffrées et sécurisées.

5/Malware/Antivirus :Cisco Advanced Malware Protection (AMP) est intégré aux routeurs, pare-feu, IPS, ainsi qu'aux appliances de sécurité de la messagerie et du Web pour la protection contre les logiciels malveillants.

6/Autres périphériques de sécurité : Cette catégorie englobe les appliances de sécurité de la messagerie et du Web, les périphériques de déchiffrement, les serveurs de contrôle d'accès client et les systèmes de gestion de la sécurité, offrant une approche complète de la protection.

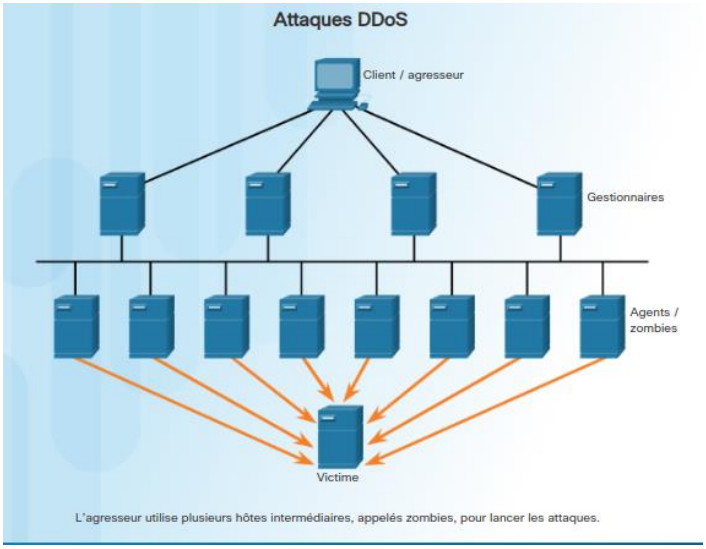
2/Activité-identifier l'appareil de sécurité :



I.3/Détecter les attaques en temps réel :

1/Détecter les attaques en temps réel :

Les attaques 0-day exploitent les vulnérabilités d'un logiciel avant que des correctifs ne soient disponibles, et en raison de leur fréquence croissante, la performance d'une défense est désormais évaluée par la rapidité de la réponse du réseau. L'idéal est de détecter et d'arrêter en temps réel les attaques, mais de nombreuses entreprises ne peuvent les repérer que plusieurs jours voire mois après leur survenue.



*/L'analyse en temps réel des attaques implique une détection active utilisant des pare-feu, des dispositifs IDS/IPS, ainsi que des solutions de détection de malware de nouvelle génération en collaboration avec des centres de menaces en ligne.

La détection des anomalies réseau repose sur une analyse contextuelle et une détection comportementale.

*/Les attaques DDoS, parmi les menaces les plus significatives, nécessitent une réponse immédiate en raison de leur difficulté à être prévenues, provenant de nombreux hôtes zombies et ressemblant à un trafic légitime. La détection et la réaction rapides aux attaques DDoS sont cruciales pour maintenir la disponibilité du réseau.

I.4/Détecter les malware :

1/Se protéger des malware :

Pour contrer les attaques 0-day et les menaces persistantes avancées (APT) qui opèrent sur de longues périodes, l'utilisation d'une solution avancée de détection de malware au niveau de l'entreprise, telle que Cisco Advanced Malware Protection (AMP) Threat Grid, est recommandée. Cette solution offre une détection de malware en temps réel en analysant des millions de fichiers et les comparant à des centaines de millions d'autres artefacts de malware. AMP Threat Grid fournit une vue globale des attaques, des campagnes de malware et de leur distribution. Il peut être déployé sur des terminaux d'hôtes, en tant que serveur autonome ou sur d'autres périphériques de sécurité du réseau, offrant ainsi une protection étendue contre les menaces.

I.5/Meilleures pratiques de sécurité :

1/Meilleures pratiques de sécurité :

Voici une liste de bonnes pratiques de sécurité recommandées par plusieurs organisations nationales et professionnelles :

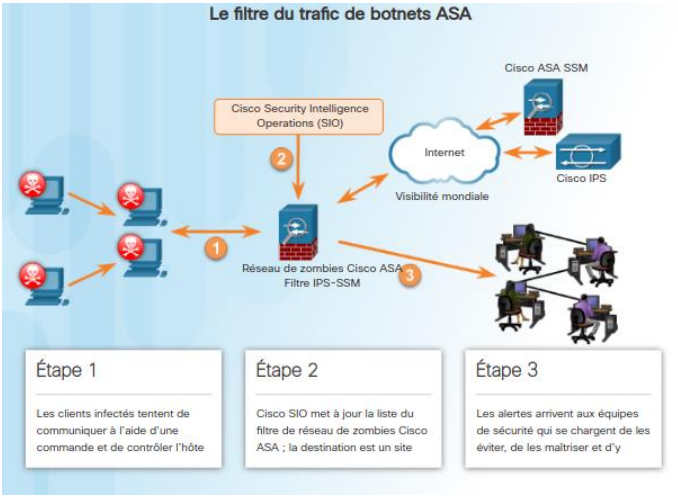
1. Effectuer une évaluation des risques : Évaluer la valeur des actifs à protéger pour justifier les dépenses de sécurité.
2. Créer une politique de sécurité : Élaborer des règles claires, des postes, des responsabilités et des attentes en matière de sécurité au sein de l'entreprise.
3. Mesures de sécurité physique : Limiter l'accès aux salles réseau et aux serveurs, et prendre des mesures de prévention des incendies.
4. Mesures de sécurité des ressources humaines : Effectuer des enquêtes approfondies sur les antécédents des employés.
5. Effectuer et tester les sauvegardes : Réaliser des sauvegardes régulières et tester la récupération des données à partir de celles-ci.
6. Maintenir les correctifs de sécurité et les mises à jour : Mettre à jour régulièrement les serveurs, clients, systèmes d'exploitation et programmes des périphériques réseau.
7. Utiliser des contrôles d'accès : Configurer les rôles des utilisateurs, les niveaux de privilège et une authentification rigoureuse des utilisateurs.
8. Tester régulièrement la réponse en cas d'incident : Employer une équipe chargée de la gestion des incidents et tester les scénarios de réponse d'urgence.
9. Implémenter un outil de surveillance, d'analyse et de gestion du réseau : Choisir une solution de sécurité qui s'intègre avec d'autres technologies.
10. Implémenter des appliances de sécurité du réseau : Utiliser des routeurs, pare-feu et autres appliances de sécurité de nouvelle génération.
11. Implémenter une solution de sécurité complète pour les terminaux : Utiliser des logiciels antimalware et antivirus professionnels.
12. Former les utilisateurs : Former les utilisateurs et employés aux procédures sécurisées.
13. Crypter les données : Chiffrer toutes les données sensibles de l'entreprise, y compris les e-mails.

Ces directives sont souvent basées sur des ressources telles que le centre de ressources de sécurité de l'Institut national des normes et de la technologie (NIST) et le SANS Institute, qui est une organisation de formation renommée en cybersécurité.

II/Approche comportementale de la cybersécurité:

II.1/Botnet :

1/Botnet :



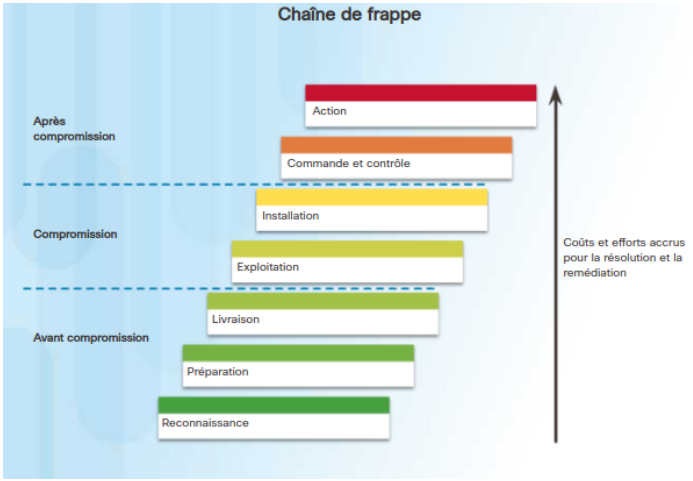
Un botnet est un réseau d'ordinateurs zombies connecté à Internet, contrôlé par un individu ou un groupe malveillant. L'infection des ordinateurs zombies se produit généralement par le biais de sites Web malveillants, d'e-mails avec des pièces jointes infectées ou de fichiers média corrompus. Ces réseaux peuvent comprendre des dizaines de milliers voire des centaines de milliers de robots, utilisés pour distribuer des malwares, lancer des attaques DDoS, envoyer du pourriel ou effectuer des attaques par force brute sur les mots de passe. Les cybercriminels louent souvent ces réseaux à des tiers à des fins malveillantes. Des filtres de trafic de botnets sont utilisés pour informer la communauté mondiale de sécurité sur les emplacements des réseaux de zombies.

II.2/Chaîne de frappe :

1/La chaîne de frappe dans la cyberdéfense :

La chaîne de frappe, développée par Lockheed Martin pour la détection et la réponse aux incidents en cybersécurité, comprend les étapes suivantes :

1/Reconnaissance : L'agresseur rassemble des informations sur la cible.
2/Préparation : L'agresseur crée un exploit et une charge utile malveillante.

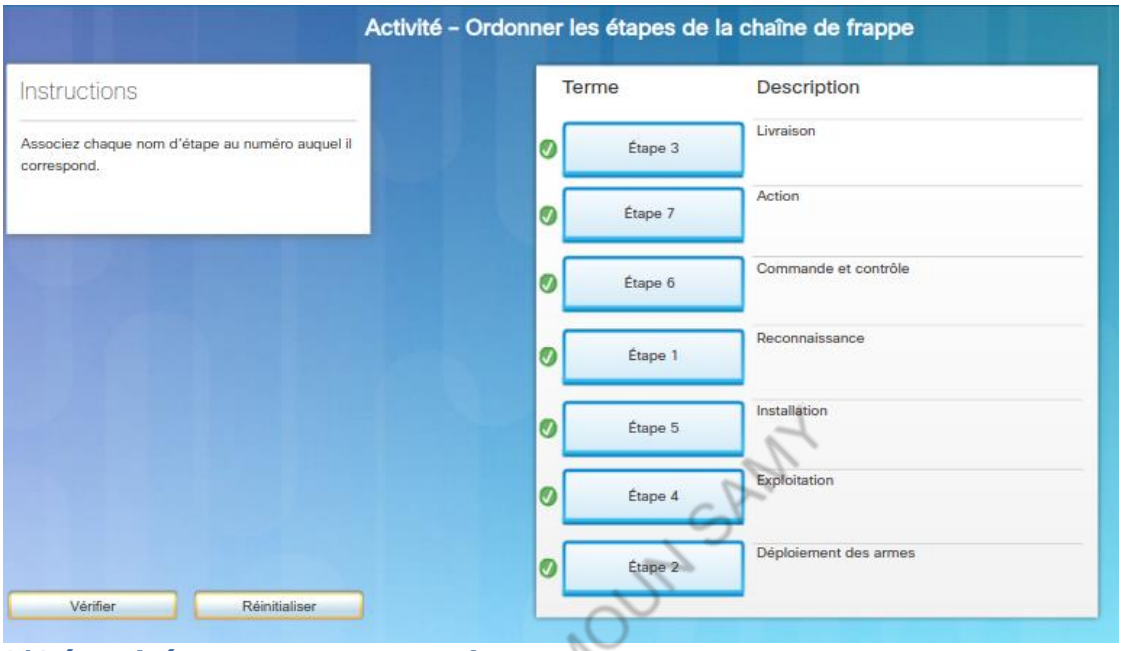


3/Livraison :L'exploit et la charge utile malveillante sont envoyés à la cible.
4/Exploitation :L'exploit est exécuté.
5/Installation :Le malware et les portes dérobées sont installés.
6/Commande et contrôle : Le contrôle à distance de la cible est établi.
7/Action :L'agresseur effectue des actions malveillantes, telles que le vol d'informations.
Pour lutter contre la chaîne de frappe, les défenses de la sécurité du réseau sont basées sur ces étapes. Les questions suivantes guident la mise en place de ces défenses :

- Quels sont les indicateurs d'attaque à chaque étape ?
- Quels outils de sécurité sont nécessaires pour détecter ces indicateurs à chaque étape ?

- Y a-t-il des lacunes dans la capacité de l'entreprise à détecter une attaque à une étape spécifique ?
Comprendre ces étapes permet de mettre en place des obstacles défensifs, de ralentir l'attaque et de prévenir la perte de données. Chaque étape correspond à une augmentation dans le niveau d'effort et le coût pour bloquer et remédier aux attaques.

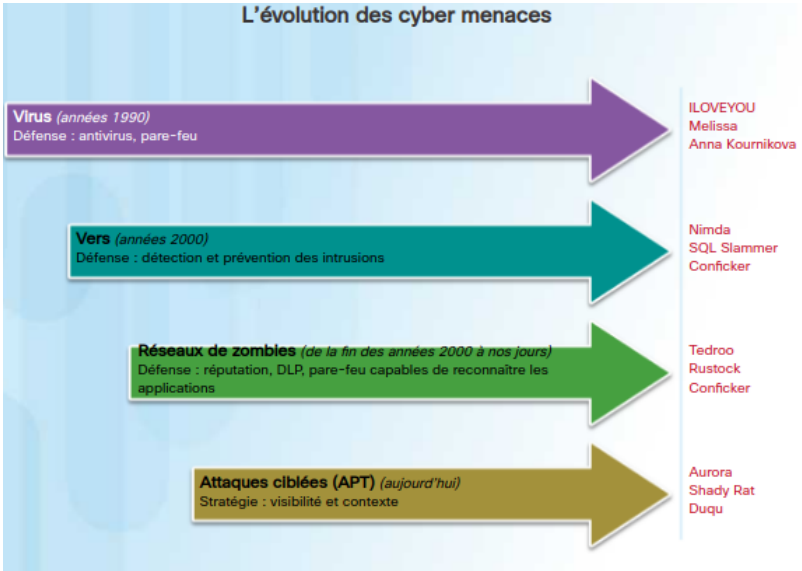
2/Activté-ordonner les étapes de la chaine de frappe :



II.3/Sécurité comportementale :

1/Sécurité comportementale :

La sécurité basée sur le comportement est une approche de détection des menaces qui se distingue par son indépendance vis-à-vis des signatures malveillantes connues, préférant utiliser le contexte informationnel pour repérer les anomalies dans le réseau. Cette méthode implique la capture et l'analyse du flux de communication entre un utilisateur sur le réseau local et une destination, locale ou distante. L'analyse de ces communications permet de révéler des modèles de comportement et de contexte qui peuvent être utilisés pour détecter les anomalies, notamment les modifications du comportement normal pouvant indiquer la présence d'une attaque.

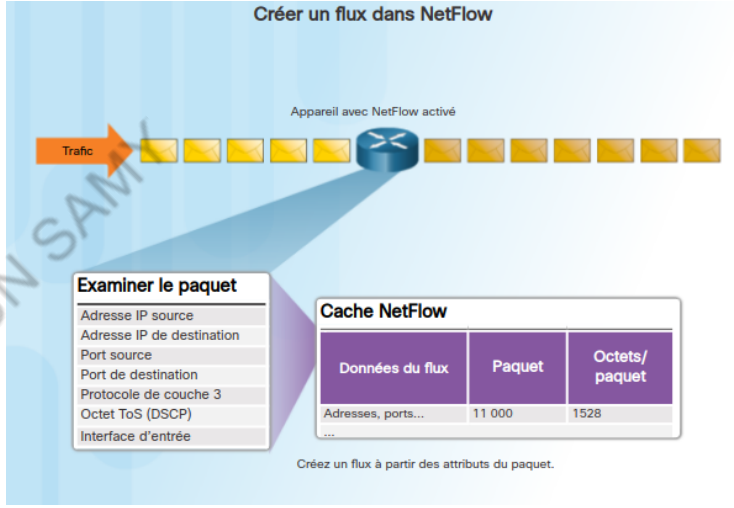


*/Honeypots :Les honeypots sont des outils de détection basée sur le comportement qui attirent délibérément les attaquants en reproduisant des comportements malveillants prévus. Une fois qu'un attaquant est captivé, l'administrateur réseau peut observer, enregistrer et analyser son comportement. Cela permet d'acquérir des connaissances approfondies pour élaborer des défenses plus efficaces.

*/Architecture de solutions de protection contre les cyberattaques de Cisco :
Cette architecture de sécurité mise sur la détection basée sur le comportement et les indicateurs pour fournir une visibilité accrue, un contexte amélioré et un meilleur contrôle. Son objectif est d'identifier l'origine de l'attaque, sa nature, son timing et sa méthode. La solution exploite diverses technologies de sécurité dans le but d'atteindre ces objectifs.

II.4/Netflow et cyberattaque :

1/Netflow :



La technologie NetFlow permet la collecte d'informations détaillées sur le flux de données à travers un réseau, fournissant une visibilité approfondie sur les activités, les utilisateurs et les périphériques. Elle facilite la détection basée sur le comportement en recueillant des données sur plus de 90 attributs pour analyser les schémas de comportement du réseau.

III/Approche de Cisco pour la cybersécurité :

III.1/CSIRT :

1/CSIRT :

Les grandes organisations mettent en place des équipes de gestion des incidents de sécurité informatique (CSIRT) chargées de recevoir, examiner et répondre aux incidents de sécurité. La mission principale de ces équipes, comme celle de Cisco CSIRT, est de garantir la protection des systèmes et des données en effectuant des enquêtes approfondies, offrant une évaluation proactive des menaces et collaborant avec d'autres organisations du domaine.

III.2/Guide sur la sécurité :

1 /Guide sur la sécurité :

Les entreprises doivent adopter une approche proactive pour anticiper, prévenir et gérer les cyberattaques en constante évolution. Cela implique l'identification des risques de cybersécurité, la mise en place de mesures de protection et de formation du personnel, ainsi que la détection rapide des événements de cybersécurité. En cas de brèche, un plan de réponse flexible doit être mis en œuvre pour minimiser les impacts, suivis de mises à jour des mesures de sécurité basées sur les leçons apprises, toutes documentées dans un guide de sécurité structuré incluant la détection des malwares, des activités suspectes, des tentatives d'authentification irrégulières, et des analyses du trafic réseau.

III.3/Outils pour la prévention et le détection des incidents :

1/Outils pour la prévention et le détection des incidents :

Pour détecter et prévenir les incidents de sécurité, plusieurs outils sont utilisés, notamment :
1/SIEM (Système de gestion des événements et des informations de sécurité): Logiciel qui collecte et analyse les alertes, les journaux de sécurité, et d'autres données provenant des périphériques sur le réseau en temps réel, offrant une vue holistique de la sécurité.
2/DLP (Prévention des pertes de données) : Logiciel ou système matériel visant à prévenir le vol ou la fuite de données sensibles du réseau. Il surveille les autorisations d'accès, les échanges de données, la copie de données et surveille les activités des utilisateurs pour protéger les données en cours d'utilisation, en cours de transfert, et au repos.
3/Cisco ISE et TrustSec : Cisco ISE (Identity Services Engine) et Cisco TrustSec renforcent la sécurité en créant des politiques de contrôle d'accès basées sur les rôles, permettant une segmentation efficace de l'accès réseau pour différents utilisateurs (invités, employés) sans complexité supplémentaire. La classification du trafic est basée sur l'identité de l'utilisateur ou du périphérique.

Transcription vidéo :

Cisco ISE (Identity Services Engine) offre une solution complète pour simplifier la gestion des politiques de sécurité. En tant que composant central de la solution TrustSec de Cisco, ISE fournit l'authentification, l'autorisation et la comptabilité (Triple A), ainsi que des fonctionnalités de gestion des invités et de profilage des périphériques. La plate-forme, compatible avec divers périphériques réseau, propose une flexibilité étendue avec des options matérielles variées. Grâce à son interface conviviale, ses capacités de gestion des événements en temps réel et son adaptabilité, Cisco ISE constitue une solution complète pour restaurer la visibilité et le contrôle des réseaux.

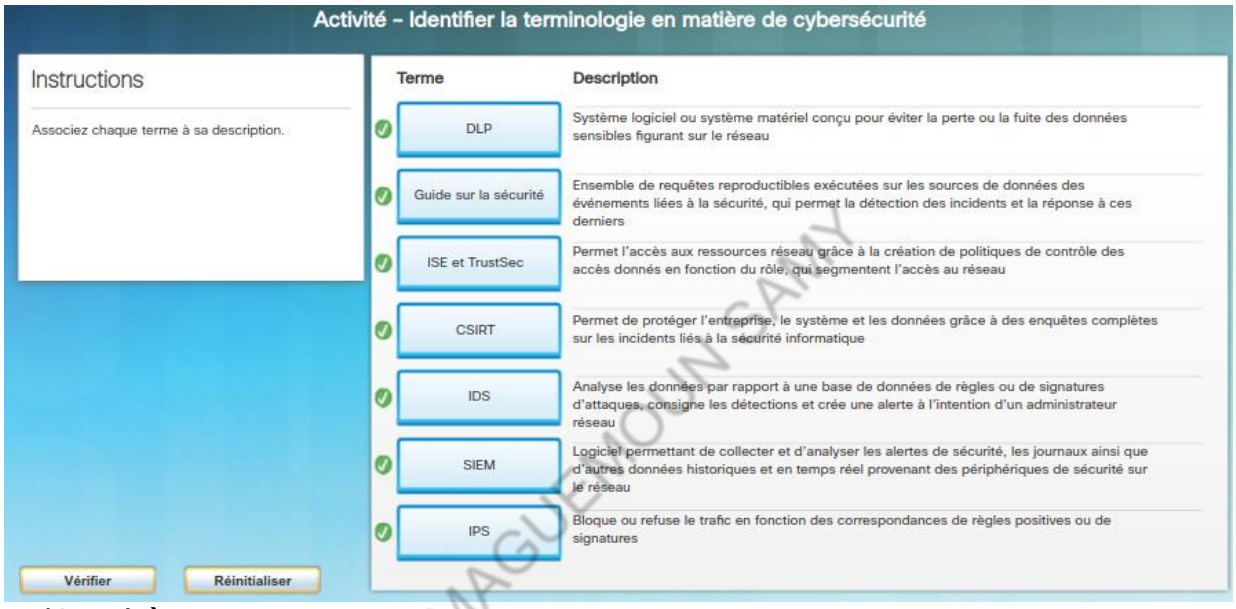
III.4/IDS et IPS:

1/IDS et IPS :

Un système de détection d'intrusion (IDS) est un dispositif réseau ou un outil intégré dans le serveur ou le pare-feu, chargé d'analyser les données à l'aide d'une base de règles ou de signatures d'attaque pour repérer un trafic malveillant. Lorsqu'une correspondance est détectée, l'IDS enregistre l'incident et envoie une

alerte à l'administrateur réseau, sans toutefois intervenir pour prévenir l'attaque. Pour éviter la latence du réseau, les IDS sont généralement déployés offline, hors du chemin du trafic normal.
En revanche, un système de prévention des intrusions (IPS) a la capacité de bloquer ou de refuser du trafic en fonction de règles prédéfinies et de correspondances de signatures. Snort, appartenant à la filiale Sourcefire de Cisco, est un exemple connu d'IPS/IDS capable d'effectuer une analyse en temps réel du trafic, des ports, des sessions et de faire correspondre les contenus. Il peut également détecter les sondes, les attaques et les balayages de ports, intégrant des fonctionnalités de création de rapports et s'interfaçant avec d'autres outils tiers pour l'analyse des performances et des enregistrements.

2/Activité-identifier en matiere de cybersecurité :



IV/Synthèse :

IV.1/Conclusion:

Chapitre 4 : Protection de l'entreprise

Le chapitre a débuté en présentant diverses technologies et processus employés par les professionnels de la cybersécurité pour assurer la protection des réseaux, des équipements et des données d'une entreprise. Cela inclut les pare-feu, les appliances de sécurité, le logiciel, ainsi que des concepts tels que les réseaux de zombies, la chaîne de frappe, la sécurité basée sur le comportement et l'utilisation de NetFlow pour la surveillance réseau.

En outre, l'approche spécifique de Cisco en matière de cybersécurité a été expliquée, mettant en avant des éléments tels que l'équipe CSIRT (Computer Security Incident Response Team) et le guide sur la sécurité. Le chapitre a également abordé brièvement divers outils utilisés par les professionnels de la cybersécurité pour détecter et prévenir les attaques réseau, notamment SIEM (Security Information and Event Management), DLP (Data Loss Prevention), Cisco ISE et TrustSec, ainsi que les systèmes IDS (Intrusion Detection System) et IPS (Intrusion Prevention System).

Chapitre 5 : La cybersécurité dans votre futur

Ce chapitre aborde les aspects éthiques et juridiques liés à la cybersécurité tout en explorant les parcours de formation et les opportunités professionnelles dans ce domaine. Il met en lumière les programmes de formation offerts par la Cisco Networking Academy, dont certains débouchent sur des certifications. Ces certifications, préalables à des certificats de spécialisation dans divers domaines, incluent la cybersécurité.

La page "Networking Academy Talent Bridge" sur le site netacad.com propose des ressources de qualité pour aider à la rédaction de CV et à la préparation d'entretiens d'embauche. Elle présente également une liste d'emplois chez Cisco et ses partenaires, ainsi que trois moteurs de recherche d'emploi en ligne.

I/Enjeux juridiques et éthiques,formations et carrières dans le domaine de la cybersécurité :

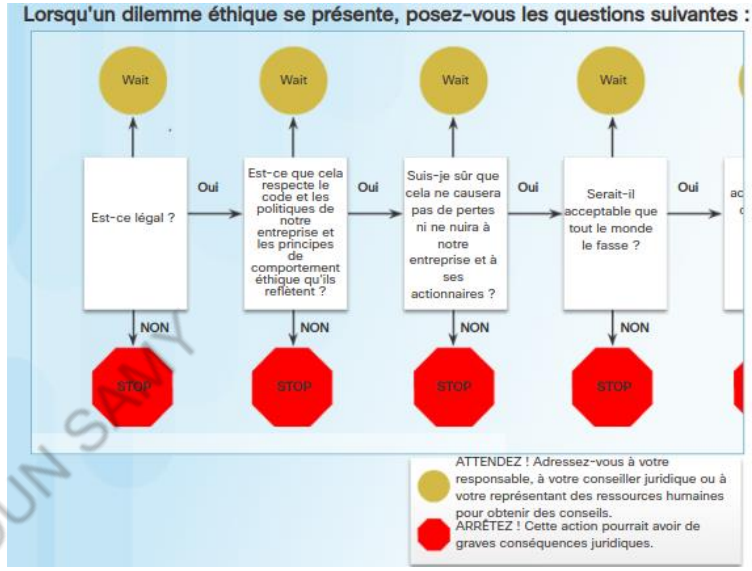
I.1/Enjeux juridiques et éthiques des postes liés à la cybersécurité :

1/Enjeux juridiques en matière de cybersécurité :

Ce passage souligne que les professionnels de la cybersécurité nécessitent des compétences similaires à celles des pirates informatiques, mais ils opèrent dans le

cadre légal. Les enjeux juridiques personnels et professionnels liés à la cybersécurité sont abordés. Les compétences développées par ces professionnels peuvent être utilisées de manière positive ou négative. L'importance du respect des lois de cybersécurité est soulignée, avec des conséquences potentielles pour les individus et les entreprises en cas de non-respect. La section mentionne également que la législation internationale dans le domaine de la cybersécurité est en constante évolution.

2/Enjeux éthiques en matière de cybersécurité :

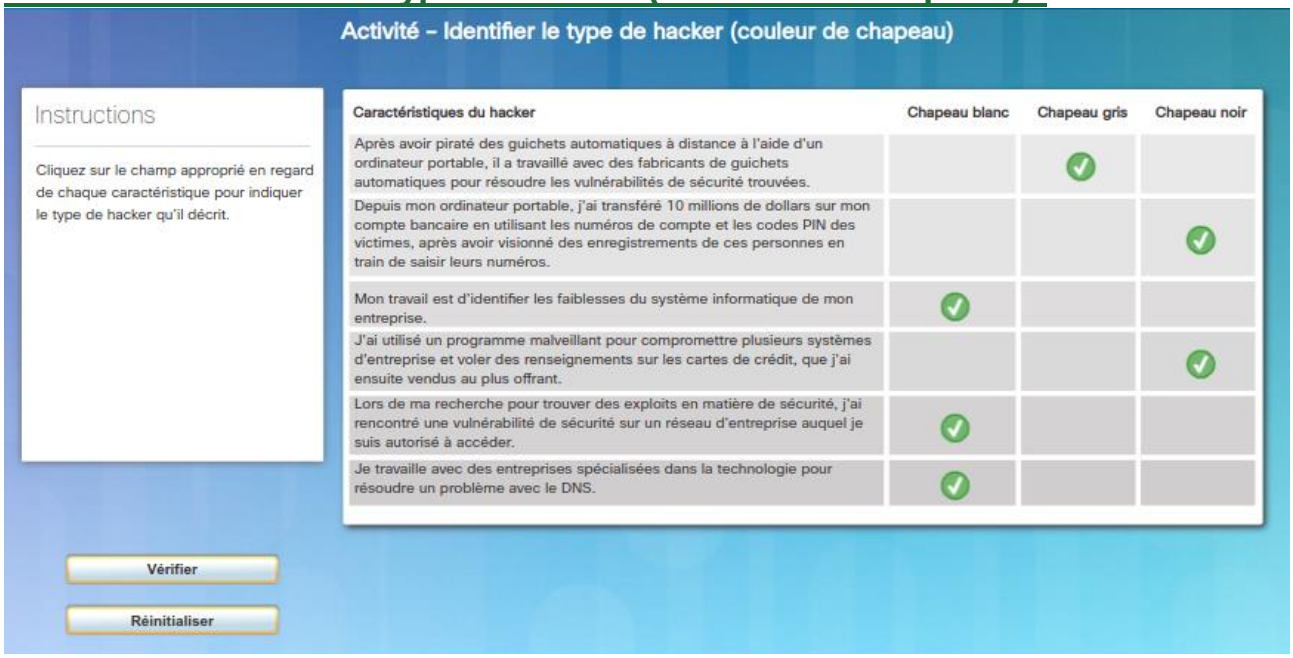


Les professionnels de la cybersécurité doivent, en plus de respecter la loi, démontrer un comportement éthique. Sur le plan personnel, agir de manière contraire à l'éthique peut ne pas entraîner de sanctions légales, mais cela ne signifie pas que le comportement est acceptable. Le texte propose deux exemples pour évaluer l'éthique de ses actions. Au niveau professionnel, de nombreux domaines de la cybersécurité ne sont pas couverts par la législation, conduisant à la création de codes d'éthique par des organisations professionnelles. Des exemples d'organisations avec des codes d'éthique incluent le CyberSecurity Institute (CSI), l'ISSA (Information Systems Security Association), et l'Association des professionnels des technologies de l'information (AITP). Cisco dispose également d'une équipe dédiée à la conduite éthique, avec un code de conduite professionnelle disponible en ligne. Le texte encourage à rechercher d'autres organisations du secteur informatique avec des codes d'éthique et à maintenir une conduite éthique basée sur des codes et des principes partagés.

3/Emplois dans le domaine de la cybersécurité :

- Les professionnels cybersécurité doivent agir légalement et éthiquement.
- Enjeux juridiques : lois régissant la cybersécurité, sanctions pour actions illégales.
- Enjeux éthiques : codes d'éthique, comportement professionnel.
- Moteurs recherche emploi : ITJobMatch, Monster, CareerBuilder.
- Types emplois cybersécurité, certifications spécifiques.
- Cours Cybersecurity Essentials Cisco Networking Academy.
- Ressources recherche emploi et codes éthique disponibles.
- Lien vers livre illustré super-héros cybersécurité.

4/activité-identifier le type de hacker(couleur de chapeau) :



II/Synthèse :

II.1/Conclusion:

Chapitre 5 : La cybersécurité dans votre futur

Ce chapitre a commencé par l'analyse des enjeux juridiques et éthiques que les professionnels de la cybersécurité rencontrent fréquemment. Il a également présenté les cursus de formation et les parcours professionnels pour ceux qui souhaitent devenir des professionnels de la cybersécurité. Trois moteurs de recherche d'emploi en ligne sont mis à votre disposition.