PLAN

CH1-Introduction à la Sécurité des Données

1. Définitions clés : • Données sensibles, confidentialité, intégrité, disponibilité (CIA).
2. Types de données : • Données personnelles, professionnelles, financières, médicales.
3. Enjeux légaux et éthiques :

- Règlement Général sur la Protection des Données (RGPD).
- Loi HIPAA (USA) pour les données médicales.

CH2-Menaces et vulnérabilités

1. Catégories de menaces :• Menaces internes (employés malveillants).• Menaces externes (pirates, ransomwares).
2. Vulnérabilités courantes :• Mots de passe faibles, logiciels non mis à jour, ingénierie sociale.
3. Études de cas réels :• Exemples d'attaques célèbres (Target, Equifax).

CH3. Cryptographie et sécurité des communications

1. Principes de la cryptographie :

- Symétrique (AES, DES) et asymétrique (RSA, ECC).
- Hashing (MD5, SHA-256).

2. Applications pratiques :• Chiffrement des emails.• Sécurisation des connexions (HTTPS, VPN).
3. Défis et limites de la cryptographie :• Attaques par force brute, certificats compromis.

4. Sécurité réseau

- Architecture réseau et points d'entrée : Routeurs, firewalls, VLAN.
- Outils de surveillance : IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems).
- Sécurisation des réseaux Wi-Fi :Protocole WPA3, attaques de type "Man-in-the-Middle".

CH5. Sécurité des systèmes d'exploitation et applications

Gestion des accès : Modèles DAC (Discretionary Access Control), MAC (Mandatory Access Control).
Mise à jour et gestion des correctifs : Importance des mises à jour automatiques.
Sécurité applicative : OWASP Top 10 pour les applications web.

CH6. Protection contre les malwares et ransomwares

1. Types de malwares : • Virus, vers, chevaux de Troie, ransomwares.
2. Détection des malwares : • Outils antivirus et anti-malware.
3. Stratégies de mitigation : • Segmentation réseau, sauvegardes régulières.

CH7. Sauvegarde et récupération des données

1. Types de sauvegardes :• Complète, différentielle, incrémentale.
2. Stockage sécurisé :• Sur site (NAS) et dans le cloud (AWS S3, Google Cloud).
3. Tests de récupération : • S'assurer de la validité des sauvegardes.

8. Sécurité des bases de données

1. Risques spécifiques : • Injection SQL, mauvaise configuration.
2. Meilleures pratiques : • Cryptage des données sensibles. • Authentification robuste.
3. Audit et surveillance : • Journaux d'accès, gestion des privilèges.

9. Éthique et législation en cybersécurité

1. Lois internationales : • RGPD (Europe), CCPA (Californie).
2. Dilemmes éthiques : • Surveillance, confidentialité, protection des données.

10. Projet final intégratif

1. Analyser les menaces.
2. Proposer des solutions techniques (firewall, sauvegardes, chiffrement).
3. Démontrer les résultats (via TP pratiques ou simulations).

CH1. INTRODUCTION À LA SÉCURITÉ DES DONNÉES

1 Définition et Importance de la Sécurité des Données

La sécurité des données est un ensemble de pratiques et de technologies visant à protéger les informations contre tout accès non autorisé, modification ou destruction. Elle est essentielle pour garantir la confidentialité, l'intégrité et la disponibilité des données.

2 Enjeux et Risques Associés

Les enjeux de la sécurité des données incluent la protection des données personnelles, la prévention des pertes financières et la réputation de l'organisation. Les risques peuvent provenir de cyberattaques, de fuites de données internes ou de défaillances techniques.

CH1. INTRODUCTION À LA SÉCURITÉ DES DONNÉES

3. Définitions Clés

Données Sensibles

Les données sensibles sont des informations qui nécessitent une protection supplémentaire en raison de leur nature sensible. Elles peuvent inclure des données personnelles, financières, médicales, et autres informations confidentielles.

Concepts fondamentaux de la sécurité (Modèle CIA)

Confidentialité : Garantir que seules les personnes autorisées accèdent aux données.

- Exemples : Mots de passe, chiffrement.

Intégrité : Assurer que les données ne sont pas altérées de manière non autorisée.

- Exemples : Contrôle des versions, signatures numériques.

Disponibilité : S'assurer que les données sont accessibles en temps voulu.

- Exemples : Sauvegardes régulières, serveurs redondants.

4. Types de Données

Données Personnelles - Données Professionnelles - Données Financières - Données Médicales

CH1. INTRODUCTION À LA SÉCURITÉ DES DONNÉES

5. Impact en cas de compromission :

. **Fuite de données personnelles :** Usurpation d'identité.

. **Perte de données professionnelles :** Perte financière, atteinte à la réputation.

. **Accès non autorisé à des données médicales :** Violation de la vie privée.

6- Les risques peuvent provenir de :

- **Cyberattaques :** Attaques de type phishing, ransomware, DDoS, etc.
- **Fuites de données internes :** Erreurs humaines, vols de données par des employés.
- **Défaillances techniques :** Pannes matérielles, erreurs de configuration, etc.

CH1. INTRODUCTION À LA SÉCURITÉ DES DONNÉES

8-REGLEMENTATION LÉGAUX ET ÉTHIQUES

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Le **RGPD** est une réglementation européenne entrée en vigueur en mai 2018. Il vise à harmoniser les réglementations sur la protection des données personnelles dans l'ensemble de l'Union européenne. Les principales obligations du RGPD incluent :

Droit à l'information : Les organisations doivent informer les individus sur la collecte et le traitement de leurs données personnelles.
Droit d'accès : Les individus ont le droit d'accéder à leurs données personnelles et de demander une copie de ces données.
Droit de rectification : Les individus ont le droit de demander la correction de leurs données personnelles si elles sont inexactes ou incomplètes.
Droit à l'oubli : Les individus ont le droit de demander la suppression de leurs données personnelles dans certaines conditions.
Droit à la limitation du traitement : Les individus ont le droit de demander la limitation du traitement de leurs données personnelles.
Droit à la portabilité des données : Les individus ont le droit de recevoir leurs données personnelles dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement.

CH1. INTRODUCTION À LA SÉCURITÉ DES DONNÉES

Certification ISO/IEC 27001 :

Norme internationale qui définit les bonnes pratiques pour la gestion de la sécurité de l'information.

Loi HIPAA (USA) pour les Données Médicales

La loi HIPAA (Health Insurance Portability and Accountability Act) est une loi américaine entrée en vigueur en 1996. Elle vise à protéger les données médicales des individus. Les principales obligations de la HIPAA incluent :

- **Confidentialité :** Les organisations doivent protéger la confidentialité des données médicales des individus.
- **Sécurité :** Les organisations doivent mettre en place des mesures de sécurité pour protéger les données médicales contre les accès non autorisés, les modifications et les pertes.
- **Transparence :** Les organisations doivent informer les individus sur les pratiques de protection des données médicales.

%TP1 Identifier et classer les risques dans un environnement de données info

CHAPITRE 2 : MENACES ET VULNÉRABILITÉS

2.1 Catégories de menaces

1. Menaces internes

Les menaces internes proviennent d'individus ayant accès à l'organisation, comme les employés ou partenaires, et représentent une source significative de risques.

- **Exemples de menaces internes :**
  - **Accès non autorisé :** Employés utilisant des données sensibles en dehors de leur rôle.
  - **Vol d'informations :** Extraction de données par des employés mécontents ou malveillants.
  - **Erreur humaine :** Suppression ou modification accidentelle de données.
- **Statistique clé :** Selon IBM, 60 % des violations de données impliquent des acteurs internes, qu'elles soient accidentelles ou intentionnelles.

2. Menaces externes

Les menaces externes proviennent d'acteurs extérieurs tels que :

- **Pirates informatiques (Hackers) :** Exploitent les vulnérabilités des systèmes pour voler des données ou perturber les services.
  Exemple : Attaques par injection SQL pour accéder à des bases de données.
- **Ransomwares :** Logiciels malveillants qui chiffrent les données et demandent une rançon pour les restaurer.
  Exemple : L'attaque WannaCry en 2017.
- **Botnets :** Réseaux de machines infectées utilisés pour des attaques distribuées, comme les DDoS (Distributed Denial of Service).

CHAPITRE 2 : MENACES ET VULNÉRABILITÉS

2.2 Vulnérabilités courantes

1. Mots de passe faibles

- Utiliser des mots de passe simples comme "123456" ou "password" rend les systèmes vulnérables aux attaques par force brute.
- **Exemple :** Une entreprise peut être compromise si un compte administrateur a un mot de passe faible.

2. Logiciels non mis à jour

- Les logiciels obsolètes contiennent des failles de sécurité non corrigées.
- **Exemple :** La faille EternalBlue exploitée par WannaCry affectait des systèmes Windows non mis à jour.

3. Ingénierie sociale

- Technique où les attaquants manipulent les individus pour obtenir des informations sensibles.
- **Exemple :** Un attaquant appelle un employé en prétendant être du service IT et lui demande ses identifiants

%TP COMMENT DETECTER LES INTRUSIONS DANS MON SYSTEME WINDOWS

RECAPITULATIF

1. Donnez la définition de la sécurité des données
2. Donnez le concept fondamental de la sécurité des données
3. Que veut dire l'intégrité des données et donnez un exemple
4. Citez les types de données
5. Donnez des exemples d'impacts en cas de compromission de données
6. De quoi peuvent provenir les risques sur les données
7. Que veux dire le RGPD
8. Donnez les droits du RGPD
9. Que représente le ISO/IEC 27001
10. Que représente le HIPAA
11. Donnez qq exemples de menaces internes
12. Donnez qq exemples de menaces Externes
13. Donnez qq types de vulnérabilités

CHAPITRE 2 : MENACES ET VULNÉRABILITÉS

2.3 Études de cas réels

1. Target (2013)

- **Contexte :** Une attaque sur la chaîne de magasins Target a compromis 40 millions de numéros de cartes de crédit.
- **Cause :** Les pirates ont accédé au réseau via une société tierce (chauffagiste) ayant des identifiants faibles.
- **Impact :** Coût de l'incident : 18,5 millions de dollars en règlement.

2. Equifax (2017)

- **Contexte :** Une violation massive a exposé les données personnelles de 147 millions de clients.
- **Cause :** Logiciel non mis à jour (Apache Struts).
- **Impact :** Perte de confiance des clients, amendes réglementaires importantes.

3. WannaCry (2017)

- **Contexte :** Ransomware ciblant des organisations dans le monde entier, notamment des hôpitaux.
- **Cause :** Failles de sécurité dans les systèmes Windows.
- **Impact :** Perturbations massives des services de santé et pertes financières.

TP - Étude de Cas d'un Incident de Sécurité: L'attaque NotPetya contre Maersk

TP : Comment suivre et installer les mises à jour de sécurité Microsoft **21/03/2025**

Chapitre 2 : Menaces et Vulnérabilités

Scanner un réseau avec Nmap

- **Présentation de l'outil :**
  - **Nmap (Network Mapper)** est un outil open-source pour l'analyse de réseaux et la détection de vulnérabilités.
  - Permet d'identifier les hôtes actifs, les ports ouverts, et les services exposés.
- **Étapes du TP :**
  - **Pré-requis :**
    - Installer Nmap : https://nmap.org/download.html.
    - Travailler sur un réseau local ou un environnement virtuel (pour éviter des problèmes légaux).
  - **Commandes de base :**
    - Scanner une machine spécifique :
      ØⓂ◿Ⓟ −ⓈV 192.168.1.10
    - Scanner tout un réseau local :
      ØⓂ◿Ⓟ −ⓈØ 192.168.1.0/24
    - Rechercher des vulnérabilités connues :
      ØⓂ◿Ⓟ −−Ⓢ▱◯=Ⓟ◿◿ ⌴—ⓁØ 192.168.1.10
  - **Analyse des résultats :**
    - Identifier les ports ouverts (par exemple : 22 pour SSH, 80 pour HTTP).
    - Rechercher des services obsolètes ou non sécurisés.
- **Objectif final**
  - Évaluer si des services inutiles ou vulnérables sont exposés.
  - Proposer des recommandations pour sécuriser le réseau (fermeture des ports inutiles, mise à jour des services).

CHAPITRE 3. CRYPTOGRAPHIE ET SÉCURITÉ DES COMMUNICATIONS

3.1 Principes de la cryptographie

La cryptographie est l'art de sécuriser les données en les rendant illisibles sans une clé appropriée.

1. Cryptographie symétrique

- **Principe :**
  - Une seule clé est utilisée pour chiffrer et déchiffrer les données.
  - Rapide, mais moins sécurisée pour des communications longues ou entre plusieurs parties.
- **Exemples :**
  - **AES** (Advanced Encryption Standard 1997) **:** Algorithme de référence utilisé dans les applications modernes.
  - **DES** (Data Encryption Standard 1977) **:** Ancien standard, remplacé par AES à cause de sa vulnérabilité.
- **Formule :** $C=E_k(M)$ et $M=D_k(C)$

où M est le message, C le texte chiffré, k la clé.

Avantages :

- Vitesse de chiffrement et de déchiffrement élevée.
- Utilisation de clés de petite taille (128, 192, 256 bits pour AES).

Inconvénients :

- Problème de distribution des clés : la clé doit être partagée de manière sécurisée entre les parties.

CHAPITRE 3. CRYPTOGRAPHIE ET SÉCURITÉ DES COMMUNICATIONS

2. Cryptographie asymétrique

Principe :

- Utilise deux clés :
- Clé publique (pour chiffrer).
- Clé privée (pour déchiffrer).
- Plus lente mais idéale pour les échanges sécurisés.

Exemples :

- **RSA** (Ron, Shamir, Adleman 1978): Premier algorithme asymétrique largement utilisé.
- **ECC (**Elliptic Curve Cryptography 1985) **:** Offre la même sécurité avec des clés plus courtes, optimisée pour les appareils mobiles.

Formule : $C = E_{K_{pub}}(M)$ et $M = D_{K_{priv}}(C)$

Avantages :

- Sécurité accrue : la clé privée n'a pas besoin d'être partagée.
- Utilisation pour l'authentification et la signature numérique.

Inconvénients :

- Vitesse de chiffrement et de déchiffrement plus lente par rapport au chiffrement symétrique.
- Utilisation de clés de plus grande taille (2048 bits pour RSA).

TP : Chiffrement et déchiffrement avec AES 11/04/2025

CHAPITRE 3. CRYPTOGRAPHIE ET SÉCURITÉ DES COMMUNICATIONS

3. Hashing

Principe :

- Transforme les données en une empreinte unique, irréversible.
- Utilisé pour vérifier l'intégrité des données ou stocker des mots de passe.

Exemples :

- MD5 : Obsolète à cause de vulnérabilités.
- SHA-256 : Standard moderne pour le hachage sécurisé.

Formule : H = Hash(M) où H est le hash et M le message d'origine.

3.2 Applications pratiques de la cryptographie

1. Chiffrement des emails

- PGP (Pretty Good Privacy) : Utilise la cryptographie asymétrique pour sécuriser les emails.
- Fonctionnement :
  1. L'expéditeur chiffre l'email avec la clé publique du destinataire.
  2. Le destinataire déchiffre avec sa clé privée.

2. Sécurisation des connexions

1. HTTPS :

- Utilise TLS/SSL pour sécuriser les communications entre navigateurs et serveurs.
- Garantit : - Confidentialité grâce au chiffrement. - Intégrité grâce aux certificats.

2. VPN (Virtual Private Network) : Chiffre tout le trafic Internet d'un utilisateur pour éviter l'espionnage.

Protocoles utilisés : OpenVPN, IPsec, WireGuard.

CHAPITRE 3. CRYPTOGRAPHIE ET SÉCURITÉ DES COMMUNICATIONS

3.3 Fonctionnement des Certificats Numériques

Les certificats numériques sont utilisés pour authentifier les identités numériques et garantir la sécurité des communications. Un certificat numérique contient :

Identité du propriétaire : Nom, adresse e-mail, etc.

Clé publique du propriétaire : Clé publique associée à l'identité.

Signature numérique de l'autorité de certification (CA) : Signature numérique de l'autorité de certification qui garantit l'authenticité du certificat.

Les certificats numériques sont utilisés dans des protocoles comme SSL/TLS pour sécuriser les communications sur Internet.

3.4 Défis et limites de la cryptographie

1. Attaques par force brute

Consistent à tester toutes les combinaisons possibles d'une clé jusqu'à trouver la bonne.

Contre-mesures :

- Utiliser des clés longues (ex. : 2048 bits pour RSA).
- Limiter les tentatives de connexion.

2. Certificats compromis

Si un certificat SSL/TLS est compromis, l'intégrité des communications est rompue.

Exemples : Mauvaise gestion des certificats ou vols de clés privées.

3. Vulnérabilités des algorithmes

MD5 et SHA-1 : Considérés comme faibles en raison des collisions possibles.

Importance de rester à jour sur les algorithmes sécurisés.

TP : Analyse SSL/TLS avec SSL Labs

RECAPITULATIF

1. Donnez la différence entre menace et vulnérabilité
2. Donnez une présentation de Nmap
3. Quel le principe de la cryptographie
4. Qu'est ce que la cryptographie symétrique
5. Donnez la formule de la cryptographie symétrique
6. Qu'est ce que AES et DES
7. Donnez les avantages et les inconvénients de la cryptographie symétrique
8. Qu'est ce que la cryptographie asymétrique
9. Qu'est ce RSA et ECC
10. Donnez la formule de la cryptographie asymétrique
11. Donnez les avantages et les inconvénients de la cryptographie asymétrique
12. Qu'est ce que le Hashing
13. Qu'est ce que MD5 et SHA256
14. Expliquez l'utilisation de la cryptographie pour le Chiffrement des emails
15. Expliquez l'utilisation de la cryptographie pour la Sécurisation des connexions
16. A quoi sert le VPN est donnez qq exemples
17. Expliquez le Fonctionnement des Certificats Numériques
18. Donnez les Défis et limites de la cryptographie

18/04/2025

CHAPITRE 3. CRYPTOGRAPHIE ET SÉCURITÉ DES COMMUNICATIONS

3.5 AUTHENTIFICATION ET AUTORISATION

AUTHENTIFICATION :

VÉRIFIER L'IDENTITÉ D'UN UTILISATEUR AVANT DE LUI ACCORDER L'ACCÈS AUX RESSOURCES. LES MÉTHODES COURANTES INCLUENT LES MOTS DE PASSE, LES CERTIFICATS NUMÉRIQUES, L'AUTHENTIFICATION MULTIFACTEUR (MFA) ET LES MÉTHODES BIOMÉTRIQUES.

AUTORISATION :

DÉTERMINER LES DROITS D'ACCÈS D'UN UTILISATEUR AUTHENTIFIÉ. CELA IMPLIQUE DE DÉFINIR DES RÔLES ET DES PERMISSIONS POUR CONTRÔLER L'ACCÈS AUX RESSOURCES EN FONCTION DES BESOINS DE L'UTILISATEUR.

CHAPITRE 3. CRYPTOGRAPHIE ET SÉCURITÉ DES COMMUNICATIONS

MFA = Authentification Multifacteur (Multi-Factor Authentication)

Définition :

L'authentification multifacteur est une méthode de sécurité qui exige **plusieurs preuves d'identité** avant d'autoriser l'accès à un système ou une application.
Plutôt que de se baser uniquement sur un mot de passe (**quelque chose que l'on sait**), on ajoute d'autres éléments comme :
•**Quelque chose qu'on a** (ex. : téléphone avec un code ou une app comme Google Authenticator),
•**Quelque chose qu'on est** (ex. : empreinte digitale, reconnaissance faciale).
But : renforcer la sécurité contre les accès non autorisés, même si un mot de passe est compromis.

Exemples :

- **Google Authenticator** : Application mobile simple pour générer des codes à usage unique.
- **Microsoft Authenticator** : Permet l'authentification à deux facteurs pour les comptes Microsoft et autres services.
- **Authy** : Similaire à Google Authenticator mais avec sauvegarde cloud.
- **Duo Mobile** (Cisco) : Utilisé dans les environnements professionnels, avec gestion centralisée.

TP METTRE EN PLACE UNE AUTENTIFICATION MULTIFACTEUR 2FA (Google Authenticator, Microsoft Autenticateur, …)

CHAPITRE 4 : SÉCURITÉ DES RÉSEAUX

4.1 Architecture réseau et points d'entrée

Un réseau est une structure complexe composée de différents éléments interconnectés. Les **points d'entrée** représentent les endroits où des attaquants peuvent potentiellement accéder.

1. Routeurs

- Fonction principale : Acheminer le trafic entre différents réseaux.
- Rôle en sécurité :
  - Mettre en place un **pare-feu intégré**.
  - Désactiver le **téléchargement à distance du firmware** pour éviter les manipulations malveillantes.

2. Firewalls

- Les **pare-feux** filtrent le trafic entrant et sortant basé sur des règles définies.
- Types :
  - **Pare-feu matériel :** Intégré dans les routeurs ou boîtiers dédiés.
  - **Pare-feu logiciel :** Configurable dans les systèmes d'exploitation (ex. : Windows Firewall, iptables sous Linux).
- Exemple d'utilisation :
  - Bloquer les ports inutilisés pour limiter les surfaces d'attaque.

3. VLAN (Virtual LAN)

- Les VLAN permettent de segmenter un réseau physique en plusieurs réseaux logiques.
- Avantages en sécurité :
  - Limiter la propagation d'une attaque.
  - Séparer le trafic sensible (ex. : finance, ressources humaines) du reste.

CHAPITRE 4 : SÉCURITÉ DES RÉSEAUX

4.2 Outils de surveillance

Les **IDS** et **IPS** permettent de détecter et prévenir les intrusions dans un réseau.

1. IDS (Intrusion Detection System)

- Fonction : Surveiller et alerter en cas de comportement anormal dans le réseau.
- Types :
  - **Basé sur les signatures :** Compare le trafic avec une base de données de modèles connus d'attaques.
  - **Basé sur l'analyse comportementale :** Détecte les anomalies (trafic inhabituel).
- Exemples d'IDS : Snort, Suricata.

2. IPS (Intrusion Prevention System)

- Fonction : Non seulement détecter, mais aussi bloquer activement les menaces.
- Différence IDS/IPS : L'IPS agit en temps réel, tandis que l'IDS se limite à l'alerte.
- **Outils courants :** Snort, Suricata, Palo Alto Networks.

4.3 Protocoles de Sécurité Réseau (SSL/TLS, VPN)

TP sur la mise en place et l'utilisation d'un IPS sous Windows A MODIFIER 02/01/2025

SSL/TLS (Secure Sockets Layer / Transport Layer Security)

- **SSL/TLS :** Protocoles de sécurité pour les communications sur Internet. Ils assurent la confidentialité, l'intégrité et l'authentification des données transmises entre deux parties.
- **Fonctionnement :** SSL/TLS utilise le chiffrement asymétrique pour établir une connexion sécurisée, puis le chiffrement symétrique pour la transmission des données.
- **Utilisation :** SSL/TLS est largement utilisé pour sécuriser les communications web (HTTPS), les e-mails (SMTPS, IMAPS), et les services FTP (FTPS).

VPN (Virtual Private Network)

- **VPN :** Réseau privé virtuel pour sécuriser les communications sur des réseaux publics. Il permet de créer une connexion sécurisée entre un utilisateur distant et un réseau privé.
- **Protocoles courants :** IPSec, OpenVPN, WireGuard.

TP4a Configuration d'un VPN Sécurisé et Firewall
TP4b Analyse du trafic réseau avec Wireshark

CHAPITRE 4 : SÉCURITÉ DES RÉSEAUX

4.3 Sécurisation des réseaux Wi-Fi

Les réseaux sans fil sont particulièrement vulnérables car les données circulent dans l'air.

1. Protocole WPA3

- WPA3 est la dernière norme de sécurité Wi-Fi.
- **Avantages par rapport à WPA2 :**
  - Chiffrement des données individuelle pour chaque client.
  - Protection contre les attaques par dictionnaire (grâce à SAE : Simultaneous Authentication of Equals).

2. Attaques courantes sur Wi-Fi

- **Man-in-the-Middle (MITM) :**
  - L'attaquant intercepte le trafic entre deux parties.
  - Utilisé pour voler des informations sensibles ou injecter du contenu malveillant.
- **Rogue Access Point :**
  - L'attaquant crée un faux point d'accès Wi-Fi pour tromper les utilisateurs.
- **Sniffing :**
  - Capture et analyse du trafic non chiffré.

3. Meilleures pratiques

- Utiliser uniquement WPA3 ou, à défaut, WPA2 avec un mot de passe robuste.
- Désactiver le SSID broadcast pour cacher le réseau.
- Filtrer les adresses MAC pour limiter l'accès

TP Sécurisation des réseaux Wi-Fi

RECAPUTILATIF

1. Qu'est ce l'authentification multifacteur, donnez qq exemple d'outils MFA
2. Quel le Rôle en sécurité d'un Routeur
3. Quel le role d'un Firewall
4. Qu'est ce qu'un VLAN
5. Quelles sont les avantages en sécurité d'un VLAN
6. Quel est le rôle des **IDS** et **IPS**
7. Quels sont les types d'un IDS
8. Qu'est ce que **SSL/TLS**
9. Citez qq protocoles sécurisés par SSL/TLS
10. Qu'est ce qu'un VPN et donnez des protocoles VPN
11. Pourquoi les réseaux sans particulièrement vulnérables et donnez qq exemples de protocoles de sécurité
12. Donnez qq exemples d'attaques de réseaux sans files
13. Quelles les meilleurs pratiques pour les réseaux sans fils

RESUME

Catégorie	Type spécifique	Description	Vulnérabilité exploitée	Corrections/Mesures préventives
Malware	Virus	Code malveillant se répliquant en infectant des fichiers.	Exécution de code non autorisé, propagation sur le système.	Antivirus/Antimalware à jour, analyse régulière des fichiers, ne pas exécuter de fichiers provenant de sources non fiables, activer le pare-feu.
	Ver	Logiciel autonome se propageant via les réseaux.	Propagation rapide sur le réseau, saturation de la bande passante.	Patchs de sécurité pour les systèmes d'exploitation et les applications, pare-feu configuré, segmentation du réseau, systèmes de détection d'intrusion (IDS/IPS).
	Cheval de Troie (Trojan)	Se fait passer pour un logiciel légitime pour tromper l'utilisateur et exécuter des actions malveillantes.	Exécution de code malveillant, vol de données, accès à distance.	Ne télécharger des logiciels que depuis des sources officielles et de confiance, analyser les fichiers téléchargés avec un antivirus, être vigilant face aux pièces jointes et aux liens dans les courriels.
	Ransomware	Chiffre les données et exige une rançon.	Prise d'otage des données, extorsion financière.	Sauvegardes régulières et hors ligne, sensibilisation au phishing, mises à jour des systèmes et des applications, solutions anti-ransomware.
	Spyware	Collecte des informations à l'insu de l'utilisateur.	Vol de données personnelles, surveillance des activités.	Antivirus/Antimalware, outils anti-spyware, vérification des permissions des applications, être vigilant face aux téléchargements.
Ingénierie sociale	Phishing	Courriels frauduleux incitant à divulguer des informations personnelles.	Vol d'identifiants, accès non autorisé aux comptes.	Formation et sensibilisation des utilisateurs, authentification multi-facteurs (MFA), vérification de l'expéditeur et du contenu des courriels, ne pas cliquer sur des liens suspects.
	Spear Phishing	Phishing ciblé sur une personne ou un groupe.	Ciblage précis, taux de réussite potentiellement plus élevé.	Même mesures que pour le phishing, avec une attention particulière à la vérification de l'identité de l'expéditeur et à la cohérence du message avec le contexte.
Attaques réseau	Déni de service (DoS/DDoS)	Surcharge un serveur pour le rendre inaccessible.	Indisponibilité du service, interruption d'activité.	Pare-feu, systèmes de détection d'intrusion (IDS/IPS), mitigation DDoS (services spécialisés), limitation du trafic, configuration robuste des serveurs.
	Attaque par interception (MitM)	L'attaquant se place entre deux parties communicantes pour intercepter les données.	Vol de données, modification des communications.	Chiffrement des communications (HTTPS, VPN), utilisation de réseaux Wi-Fi sécurisés, vérification des certificats de sécurité.
	Spoofing (IP, ARP, DNS)	Usurpation d'identité pour tromper les systèmes et les utilisateurs.	Redirection vers des sites malveillants, interception de trafic.	Validation des adresses IP et des noms de domaine, utilisation de DNSSEC, configuration sécurisée des routeurs et des serveurs, filtres anti-spoofing.
Menaces internes	Erreurs humaines	Actions involontaires causant des problèmes de sécurité.	Perte de données, divulgation d'informations.	Formation et sensibilisation des utilisateurs, politiques de sécurité claires, contrôle d'accès basé sur les rôles, procédures de gestion des incidents.
	Actes malveillants	Actions intentionnelles visant à nuire à l'organisation.	Vol de données, sabotage, atteinte à la réputation.	Politiques de sécurité strictes, contrôle d'accès, surveillance des activités, séparation des tâches, audits réguliers, procédures de gestion des départs d'employés.
Vulnérabilités logicielles	Bugs/Failles de sécurité	Erreurs de programmation permettant l'exploitation par des attaquants.	Exécution de code non autorisé, accès non autorisé aux données.	Mises à jour régulières des logiciels, tests de pénétration, développement sécurisé, utilisation d'outils d'analyse de code.
	Vulnérabilités Zero-day	Vulnérabilités inconnues du public et pour lesquelles il n'existe pas de correctif.	Exploitation immédiate sans défense connue.	Systèmes de détection d'intrusion avancés, solutions de sécurité basées sur l'analyse comportementale, surveillance proactive, segmentation du réseau, mise en place de mesures de confinement.
Vulnérabilités matérielles	Défauts de conception/Obsolescence	Faiblesses inhérentes au matériel ou dues à son ancienneté.	Exploitation des faiblesses pour compromettre le système.	Mises à jour du firmware, remplacement du matériel obsolète, segmentation du réseau pour isoler les systèmes vulnérables, compensation par des mesures de sécurité logicielles.
Vulnérabilités humaines	Manque de sensibilisation	Ignorance des risques et des bonnes pratiques.	Augmentation du risque d'être victime d'attaques d'ingénierie sociale ou d'erreurs.	Formation et sensibilisation continue des utilisateurs, simulations de phishing, communication claire sur les politiques de sécurité.
	Mots de passe faibles	Mots de passe faciles à deviner.	Accès non autorisé aux comptes.	Politique de mots de passe forts (longueur, complexité), gestionnaire de mots de passe, authentification multi-facteurs (MFA).
	Erreurs de configuration	Mauvaise configuration des systèmes et des applications.	Ouverture de portes d'entrée pour les attaquants.	Audits de sécurité réguliers, configuration standardisée et sécurisée (hardening), documentation de la configuration, utilisation d'outils d'automatisation de la configuration.

5. SÉCURITÉ DES SYSTÈMES D'EXPLOITATION ET APPLICATIONS

Objectifs

- Apprendre les principes fondamentaux pour sécuriser les systèmes d'exploitation et les applications.
- Comprendre la gestion des accès, l'importance des mises à jour et des correctifs.
- Identifier les principales vulnérabilités applicatives et apprendre à les corriger.

5.1 Gestion des accès

1. Modèles de contrôle d'accès (Access Control Models)

La gestion des accès vise à s'assurer que seules les personnes autorisées peuvent interagir avec des ressources spécifiques.

- **DAC (Discretionary Access Control)**
  - Les propriétaires des ressources (fichiers, dossiers) définissent les permissions.
  - Exemple : Sur un système Linux, un utilisateur peut décider qui peut lire/écrire/exécuter ses fichiers.
  - **Limite** : Risque d'erreurs humaines.
- **MAC (Mandatory Access Control)**
  - Les permissions sont gérées par le système, souvent basé sur des règles prédéfinies.
  - Exemple : Utilisé dans les environnements militaires où les données sont classifiées en niveaux (Confidentiel, Secret, Top Secret).
  - **Avantage** : Plus sécurisé que DAC car il limite la discrétion des utilisateurs.
- **RBAC (Role-Based Access Control)**
  Permissions attribuées en fonction des rôles des utilisateurs (exemple : administrateur, utilisateur standard)

5. SÉCURITÉ DES SYSTÈMES D'EXPLOITATION ET APPLICATIONS

5.2 Mise à jour et gestion des correctifs

1. Importance des mises à jour

- Les failles de sécurité sont régulièrement découvertes dans les systèmes d'exploitation et les applications.
- Les mises à jour corrigent ces vulnérabilités et préviennent les attaques.
- Exemple célèbre : L'attaque WannaCry (2017) exploitait une faille corrigée par Microsoft plusieurs mois avant l'incident.

2. Types de mises à jour

- **Correctifs de sécurité :** Réparent des vulnérabilités critiques.
- **Mises à jour fonctionnelles :** Ajoutent de nouvelles fonctionnalités.
- **Mises à jour automatiques :**
  - **Avantages :** Réduisent le risque d'oublis.
  - **Inconvénients :** Risque de conflits avec des logiciels existants.

3. Outils de gestion des mises à jour

- **Sous Windows :** Windows Update (automatisé par défaut).
- **Sous Linux :** Commandes `apt` ou `yum` pour appliquer des mises à jour.

5. SÉCURITÉ DES SYSTÈMES D'EXPLOITATION ET APPLICATIONS

5.3 Sécurité applicative

1. Principales vulnérabilités (OWASP Top 10)

L'**OWASP** (Open Web Application Security Project) identifie les vulnérabilités les plus courantes dans les applications web. Parmi elles :

- **Injection :**
  - Exemple : Injection SQL pour accéder à une base de données.
  - Contre-mesure : Utiliser des requêtes préparées.
- **Authentification insuffisante :**
  - Mot de passe faible ou stockage non sécurisé.
  - Contre-mesure : Authentification multi-facteurs (MFA).
- **Exposition des données sensibles :**
  - Données stockées sans chiffrement.
  - Contre-mesure : Utiliser des protocoles comme HTTPS.
- **Failles de configuration :**
  - Oublier de désactiver des fonctionnalités inutilisées ou mal sécurisées.
- **XSS (Cross-Site Scripting) :**
  - Injection de scripts malveillants dans des pages web.
  - Contre-mesure : Valider et échapper les entrées utilisateur.

2. Meilleures pratiques de sécurité

- **Vérifications régulières :**
  - Effectuer des audits pour identifier les failles potentielles.
- **Principes de moindre privilège :**
  - Les applications ne doivent pas avoir plus de permissions que nécessaire.
- **Surveillance des journaux :**
  - Configurer des logs pour détecter des activités suspectes.

%TP5b : Identifier des vulnérabilités d'une application web avec OWASP ZAP

%TP5a Analyse des permissions utilisateurs sous Linux

RECAPUTILATIF

1. Que vise La gestion des accès ?
2. Que signifie le DAC (Discretionary Access Control)
3. . Que signifie le MAC (Mandatory Access Control)
4. Que signifie le RBAC (Role-Based Access Control)
5.Pourquoi Les mises à jour sont important
6. Quels sont les Types de mises à jour
7. Quels sont les Outils de gestion des mises à jour dans windows et Linux
8.Qu'est ce que L'OWASP
9. Donnez qq vulnirabilités à qui les applications sont exposées
10. Quelles sont les meilleurs pratiques de sécurité

EXPOSES1

1. L'IA DANS LA DÉTECTION DES MENACES

EXPLORER COMMENT L'IA EST UTILISÉE POUR DÉTECTER LES CYBERMENACES EN TEMPS RÉEL, NOTAMMENT LES LOGICIELS MALVEILLANTS, LES ATTAQUES PAR PHISHING ET LES INTRUSIONS RÉSEAU.

2. L'IA ET LA LUTTE CONTRE LES RANSOMWARES ANALYSER COMMENT L'IA PEUT AIDER À PRÉVENIR, DÉTECTER ET RÉPONDRE AUX ATTAQUES DE RANSOMWARE, AINSI QUE LES LIMITES DE CETTE APPROCHE.

3. LES ALGORITHMES DE CHIFFREMENT BASÉS SUR L'IA

ÉTUDIEZ LES NOUVELLES APPROCHES DU CHIFFREMENT BASÉES SUR L'IA, TELLES QUE L'UTILISATION DE L'APPRENTISSAGE AUTOMATIQUE POUR CONCEVOIR DES SYSTÈMES CRYPTOGRAPHIQUES PLUS ROBUSTES OU POUR OPTIMISER LES CLÉS DE CHIFFREMENT.

4. L'IA DANS LA GESTION DES VULNÉRABILITÉS

ÉTUDIER COMMENT L'IA PEUT AUTOMATISER L'IDENTIFICATION, LA CLASSIFICATION ET LA CORRECTION DES VULNÉRABILITÉS LOGICIELLES.

EXPOSES2

5. L'IA et la sécurité des données personnelles
Discuter des enjeux liés à l'utilisation de l'IA pour protéger les données personnelles, notamment dans le contexte du RGPD (Règlement Général sur la Protection des Données).

6. L'IA dans la sécurité des réseaux
Explorer comment l'IA est utilisée pour surveiller et sécuriser les réseaux informatiques, notamment grâce à l'analyse du trafic et à la détection d'anomalies.

7. Les risques liés à l'IA générative en sécurité
Analyser les risques posés par les outils d'IA générative (comme ChatGPT) en matière de création de phishing, de deepfakes et d'autres menaces.

8. L'IA et la sécurité des systèmes IoT
Étudier comment l'IA peut améliorer la sécurité des appareils IoT (Internet des Objets), souvent vulnérables aux attaques.

9. L'IA dans la réponse aux incidents de sécurité
Explorer comment l'IA peut automatiser et accélérer la réponse aux incidents de sécurité, notamment grâce à l'orchestration et à l'automatisation des processus (SOAR).

10. L'éthique de l'IA en sécurité informatique
Discuter des questions éthiques liées à l'utilisation de l'IA en sécurité, notamment les biais algorithmiques, la transparence et la responsabilité. **20 DIAPOS+TP**

EXPOSES3

11. [illegible]

12. Perspectives Futures de l'IA en Sécurité Informatique
Évolution des technologies d'IA et leur impact sur la cybersécurité.
Défis à relever : régulation, éthique, formation.
Scénarios futurs : IA défensive vs IA offensive.

13. **Détection des Menaces avec l'IA**
Comment l'IA analyse les comportements suspects.
Utilisation du machine learning pour identifier les anomalies.
Études de cas : Détection de ransomwares ou de phishing.

14. Authentification et Biométrie avec l'IA
Reconnaissance faciale, vocale et comportementale.
Sécurisation des systèmes d'authentification.
Risques liés à la biométrie et à la vie privée.

EXPOSES4

1. TECHNOLOGIE BLOCKCHAINE KAWTHAR OUALLA
2. APPLICATIONS BLOCKCHAINE MOHAMMED KHATTABI
3. CRYPTOMONNAIE BITCOIN MED AMINE ELJABBARI
4. CRYPTOMONNAIE ETHEREUM KHADIJA BOUKHRISS
5. SMART CONTRACTS : VERS DES CONTRATS AUTO-EXÉCUTABLES
6. BLOCKCHAIN VS BANQUE TRADITIONNELLE : MENACE OU COMPLÉMENT ?
7. BLOCKCHAIN ET TRAÇABILITÉ : APPLICATION DANS LA CHAÎNE LOGISTIQUE
8. CADRE JURIDIQUE DE LA BLOCKCHAIN AU MAROC ET DANS LE MONDE ZAKRI FATIMZAHRA
9. BLOCKCHAIN ET INTELLIGENCE ARTIFICIELLE : VERS DES SYNERGIES ?
   20 DIAPOS+TP