Module 1 – Fondamentaux techniques et règlementaires

# Fondamentaux de la sécurité des SI et réseaux

## Séquence 2 : Principales menaces et failles

OIDANEOS

# **Présentation de la séquence**
## Les invariants d’une cyberattaque

- Leurrer les personnes et les systèmes
  - Ingénierie sociale (phishing, scareware…)
  - Usurpation d’identité ou d’adresses IP (IP spoofing)
  - Vol de connexion (session hijacking)
  - Compromission de comptes

# **Présentation de la séquence**
## Les invariants d’une cyberattaque

- Détourner le mode opératoire normal des ressources
  - Détournement des moyens de routage, de serveurs de noms, des points de connexion mobile
  - Détournement des flux applicatifs
  - Dépassement des capacités
  - Injection de code
  - Élevation de privilèges

- Exploiter des failles de sécurité et des vulnérabilités

# Présentation de la séquence
## Objectifs et notions abordées

**Comprendre les typologies d'attaques et les vulnérabilités les plus courantes**

- Les types de logiciels malveillants
- Les attaques réseaux
- Les attaques Web
- L'ingénierie sociale

# Les logiciels malveillants

# Les logiciels malveillants
## Définitions et exemples

**Programme ou logiciel conçu dans le but de nuire à un ordinateur, un réseau ou un utilisateur**

Virus et bombe logique

Vers

Cheval de Troie

Spyware / Key logger

Ransomware

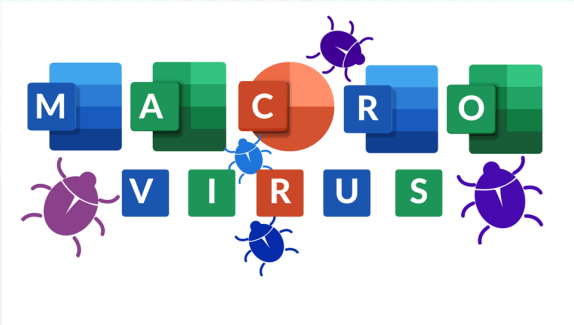
Wiper

Infostealer

# Les logiciels malveillants
## Virus

**Logiciels malveillants qui ont besoin d'un hôte pour pouvoir se diffuser**

Macro-virus





Boot sector virus

Virus furtif



Virus polymorphe

# Les logiciels malveillants

## Vers

- Malware qui se propage indépendamment de tout hôte

- Ils causent des dommages :
  - Soit par le code malicieux qu'ils transportent
  - Soit par la perte de disponibilité du réseau à cause de leur mode de propagation agressif

- Ils se propagent en plusieurs étapes :

Exploitation d'une vulnérabilité → Réplication automatique → Livraison de la charge utile

# **Les logiciels malveillants**
## Cheval de Troie

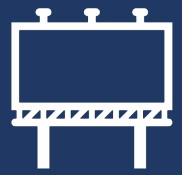
- Malware qui a une fonction bénigne (jeu) ou maligne (vol de données)

- Code malveillant caché dans un programme utile à l'utilisateur
    - L'installation permet la prise de contrôle à distance du système infecté et l'installation d'autres programmes malveillants

# Les logiciels malveillants
## Spyware / Adware / Key logger

**Spyware**

- Surveille l'activité de l'utilisateur
- Collecte des informations à vendre sur les utilisateurs
- Intercepte les données personnelles



**Adware**

- Constitué d'une partie utile et d'une partie qui gère l'affichage
- Cible la publicité selon les habitudes de l'utilisateur

**Keylogger**

- Un enregistreur de frappe peut être logiciel ou matériel
- Utilisé pour collecter des mots de passe ou des données personnelles

# Les logiciels malveillants
## Ransomware

**Logiciel malveillant qui détruit les données de systèmes critiques ou bloquent l'accès à ceux-ci jusqu'au paiement d'une rançon**

Ransomware par chiffrement

Ransomware par verrouillage

Doxware

# Les attaques réseaux

# Les attaques réseaux
## Principes généraux et types d'attaques

Actions non autorisées sur les actifs

Modification, destruction ou vol des données privées

Ciblage des périmètres du réseau pour accéder au réseau interne

**Attaques passives**

Obtention d'un accès non autorisé pour surveiller et voler des données sans effectuer de modification

**Attaques actives**

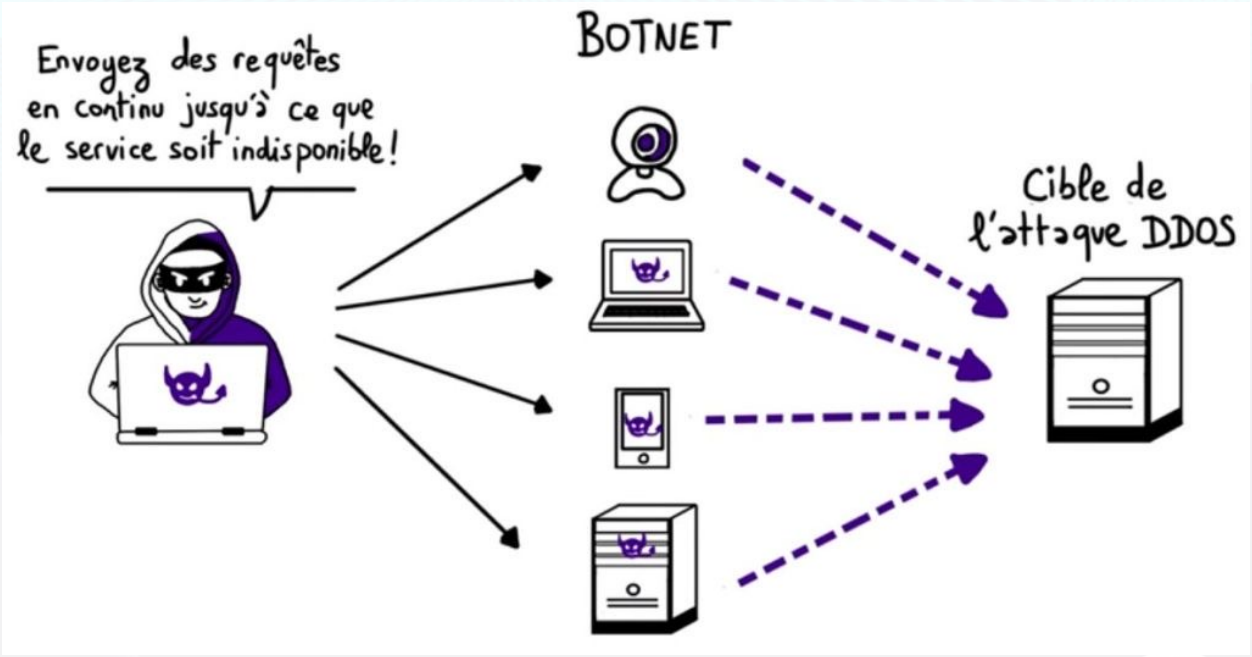
Modification, chiffrement ou endommagement des informations

# Les attaques réseaux
## Déni de Service (DoS) et Déni de Service Distribué (DDoS)

**Empêcher l'utilisation d'une machine ou d'un service**

- Le DoS peut être
  - *Local par épuisement des ressources*
  - *Réseau par consommation de la bande passante*

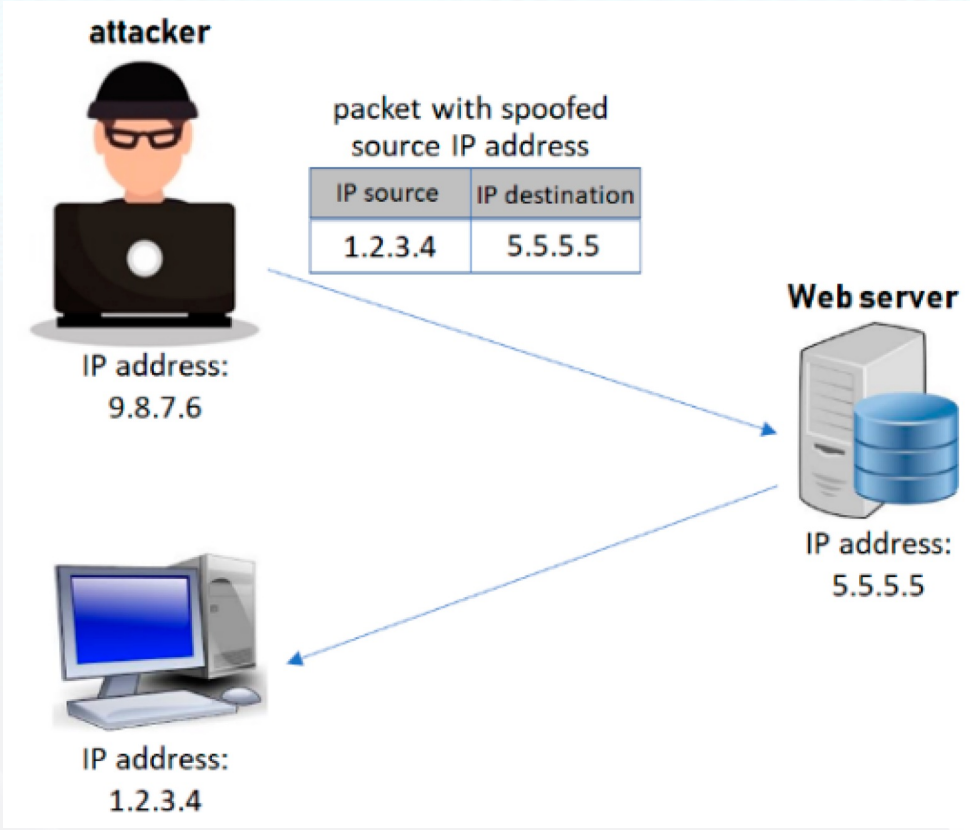
- Le DDoS est similaire avec l'utilisation de plusieurs machines contre une seule organisation



# Les attaques réseaux
## IP spoofing

**L'attaquant usurpe une autre adresse IP**

- Modification de l'adresse IP source dans l'entête des paquets IP avec l'adresse d'une autre machine
- L'objectif est de faire croire que les données viennent d'un hôte de confiance alors qu'il ne l'est pas

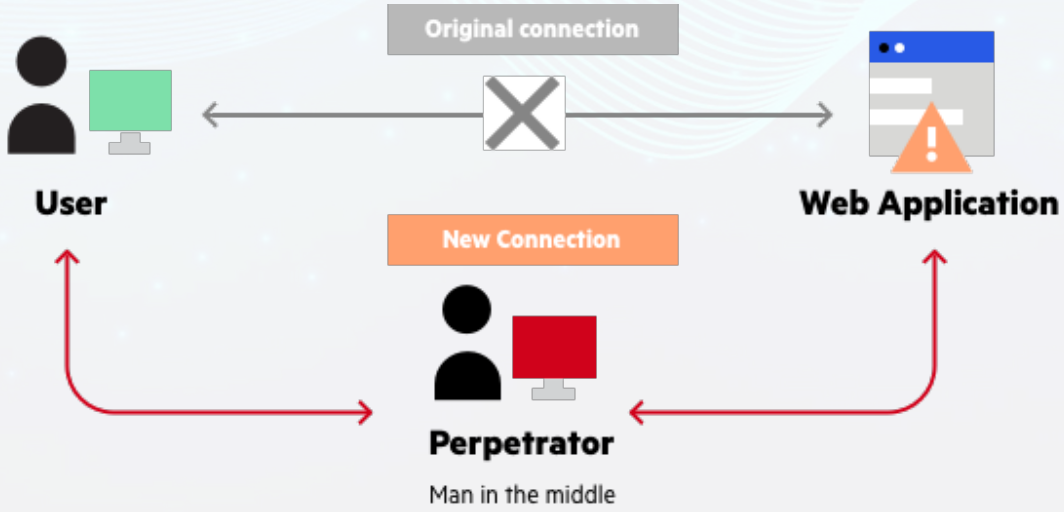


# Les attaques réseaux

## Man-in-the-Middle (MitM) ou attaque de l'homme du milieu

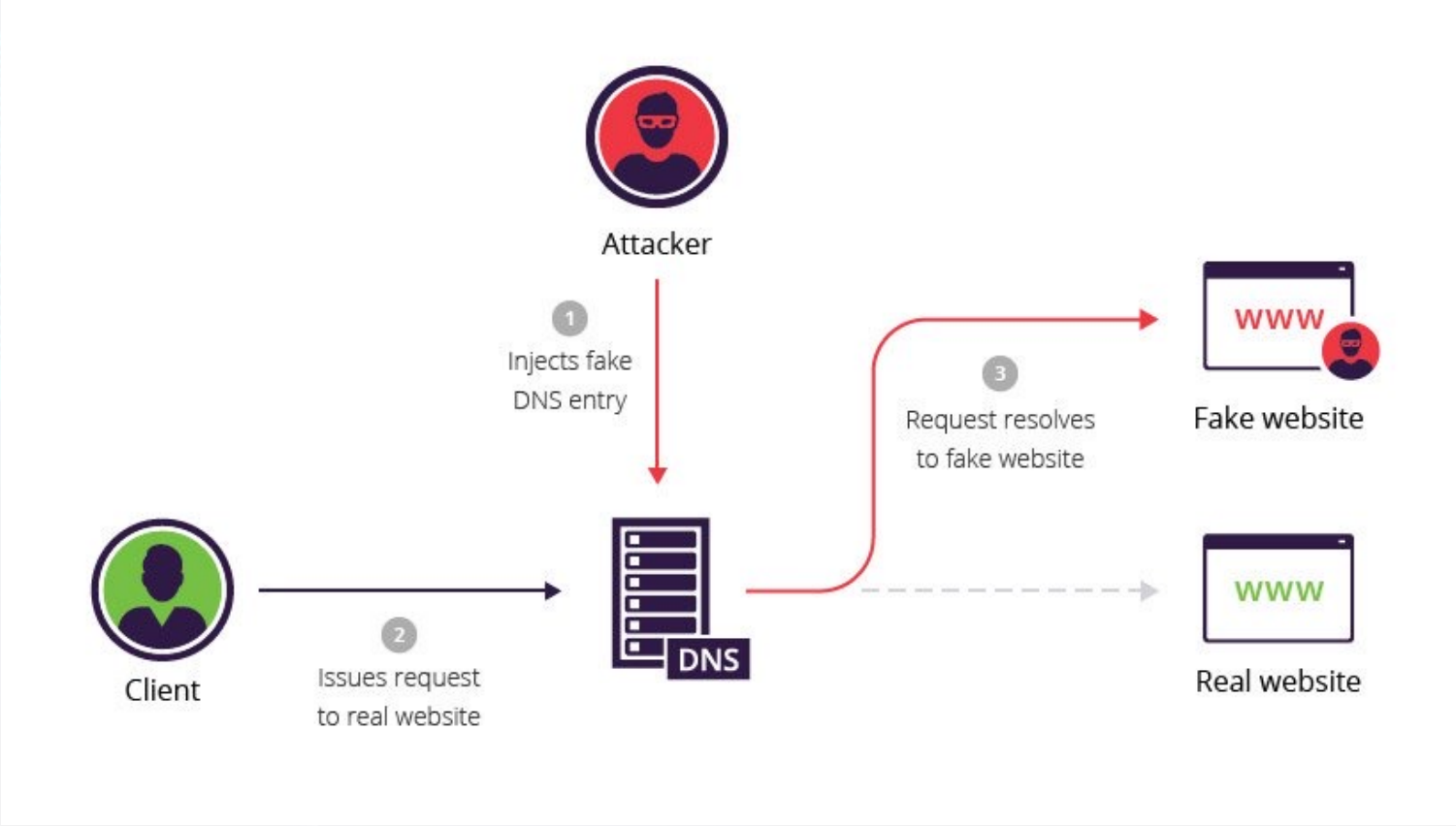
**Positionnement au milieu d'une communication par prise de contrôle d'un équipement du réseau**

- Positionnement au milieu d'une communication par prise de contrôle d'un équipement du réseau
- Il permet :
  - D'écouter les communications
  - De modifier les communications



# Les attaques réseaux
## DNS spoofing/poisoning

**Leurre des serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent alors qu'elle est frauduleuse**



# Les attaques Web

# Les attaques Web

## Qu'est-ce que l'OWASP (Open World Application Security Project) ?

- **Fondation/communauté internationale à but non lucratif qui publie des ressources ouvertes pour réduire les risques cyber liés aux applications (web, mobile, API, cloud).**

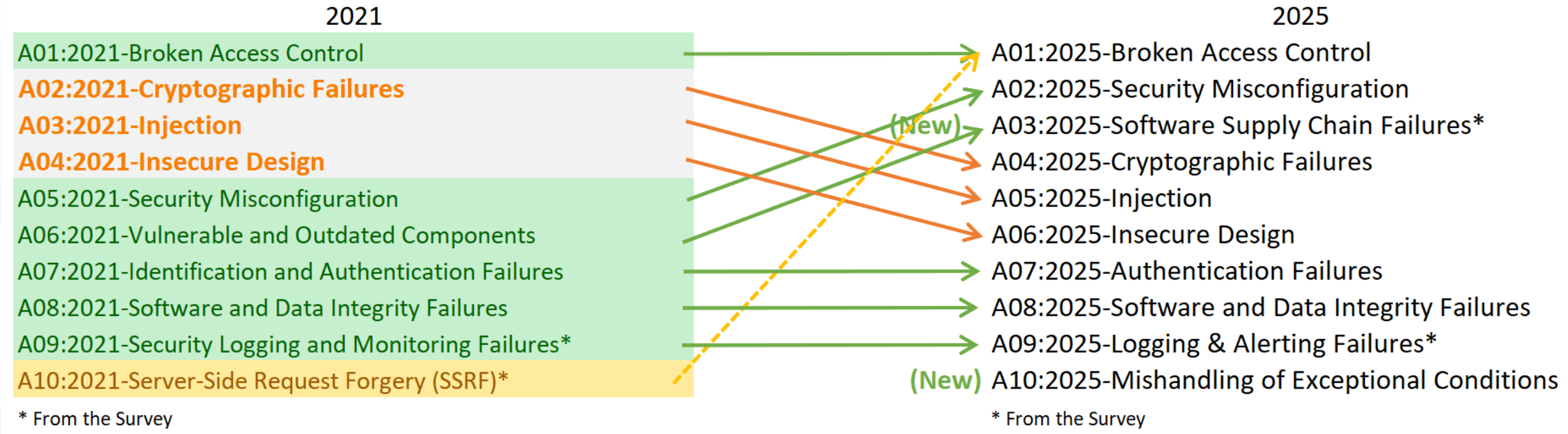
- Elle permet de fournir un langage commun et des référentiels pour cadrer les exigences sécurité, prioriser, et piloter la conformité sécurité tout au long du projet (de la conception à l'exploitation).

- Elle développe également des outils pour prévenir les risques sur les applications

- Quelques projets clés :
  - *OWASP Top 10*
  - *OWASP Application Security Verification Standard*
  - *OWASP Dependency Check*

# Les attaques Web
## OWASP Top 10 – Présentation globale

**Le Top 10 OWASP présente les 10 risques les plus critiques pour les applications Web. La dernière mise à jour de ce classement date de 2025 et identifie les catégories suivantes**



# Les attaques Web
## OWASP Top 10 – A01 : Contrôle d’accès défaillant

**Des utilisateurs non authentifiés ou non autorisés accèdent à des fonctions ou des données sensibles**

### Exemples d’attaques

- Contournement de la politique de contrôle d’accès
- Escalade de privilèges
- Accès à des API ou des interfaces d’administration

### Mesures de prévention

- Durcir les politiques de contrôles
- Appliquer le principe de moindre privilège
- Tester régulièrement les accès

### Analyse des faiblesses

- Burp Suite pour tester les failles d’authentification et d’autorisation
- OWASP ZAP pour identifier les défauts de configuration et les contrôles d’accès mal implémentés

# Les attaques Web
## OWASP Top 10 – A02 : Mauvaise configuration de sécurité

**Des paramètres par défaut non sécurisés ou des configurations incomplètes peuvent laisser l'application vulnérable**

### Exemples d'attaques

- Accès à des fichiers de configuration sensibles
- Exposition de services inutiles
- Accès non restreint à des fonctions critiques

### Mesures de prévention

- Désactiver les fonctionnalités inutiles
- Appliquer les correctifs
- Auditer régulièrement les configurations de sécurité

### Analyse des faiblesses

- Nmap pour détecter les ports ouverts, services mal configurés et erreurs de configuration réseau
- Lynis pour analyser la configuration système et repérer les failles de sécurité et les mauvaises configurations

# Les attaques Web
## OWASP Top 10 – A03 : Défaillances dans la chaîne d'approvisionnement logiciel

**L'utilisation de bibliothèques ou composants obsolètes expose les applications à des vulnérabilités connues**

### Exemples d'attaques

- Compromission d'un système suite à une mise à jour infectée d'un logiciel considéré comme fiable
- Compromission d'un framework exposé à des failles

### Mesures de prévention

- Mettre en place une politique de gestion des dépendances
- Surveiller les mises à jour de sécurité
- Remplacer les composants obsolètes

### Analyse des faiblesses

- OWASP Dependency Check qui permet d'identifier les dépendances logicielles vulnérables ou obsolètes et propose des mises à jour
- Retire.js pour scanner les dépendances Javascript pour détecter les bibliothèques obsolètes ou vulnérables

# Les attaques Web
## OWASP Top 10 – A04 : Défaillances cryptographiques

**Des informations sensibles (mots de passe, données stratégiques) ne sont pas correctement chiffrées ou protégées**

### Exemples d'attaques

- Utilisation d'algorithmes de chiffrement obsolètes
- Absence de chiffrement de bout en bout ou fuite de clés cryptographiques
- Fuite de clés cryptographiques

### Mesures de prévention

- Adopter des algorithmes de chiffrement modernes
- Protéger les clés de chiffrement
- Appliquer des protocoles de sécurité (TLS)

### Analyse des faiblesses

- John the Ripper pour cracker les mots de passe afin de tester la solidité des algorithmes cryptographiques utilisés pour le stockage des identifiants
- Hashcat pour tester la robustesse des fonctions de hachage cryptographique comme MD5 ou SHA-256

# Les attaques Web
## OWASP Top 10 – A05 : Injection

**Des attaquants injectent des commandes malveillantes via des champs utilisateur pour manipuler des bases de données ou exécuter des commandes**

### Exemples d'attaques

- Injections SQL, LDAP ou OS qui permettent de voler des données
- Injections pour modifier le système ou compromettre l'application

### Mesures de prévention

- Utiliser des requêtes paramétrées
- Valider les entrées utilisateurs
- Appliquer des contrôles stricts de sécurité

### Analyse des faiblesses

- SQLMap pour détecter et exploiter les vulnérabilités d'injection SQL dans les applications web.
- NoSQLMap pour tester les failles d'injection sur des bases de données NoSQL comme MongoDB.

# Les attaques Web
## OWASP Top 10 – A06 : Conception non sécurisée

**Les fonctionnalités de sécurité sont souvent négligées ou mal implémentées lors de la phase de conception des applications**

### Exemples d'attaques

- Mauvaise gestion des sessions
- Absence de vérifications de sécurité
- Conception vulnérable aux attaques

### Mesures de prévention

- Modéliser les menaces
- Faire des revues de codes
- Effectuer des tests de sécurité réguliers

### Analyse des faiblesses

- Threat Dragon pour modéliser les menaces et analyser les conceptions non sécurisées dans les applications web
- Tinfoil Security pour automatiser les tests d'évaluation de sécurité pour les vulnérabilités liées à une conception inadéquate

# Les attaques Web
## OWASP Top 10 – A07 : Défaillance dans l'authentification

**Les systèmes d'authentification non sécurisés permettent aux attaquants de compromettre des comptes et d'accéder à des informations sensibles**

### Exemples d'attaques

- Attaques par force brute
- Réutilisation de mots de passe
- Sessions non sécurisées
- Absence de mécanismes MFA

### Mesures de prévention

- Implémenter l'authentification multifactorielle
- Implémenter des politiques de mots de passe robustes
- Protéger les sessions

### Analyse des faiblesses

- Hydra qui permet de tester les systèmes d'authentification et d'identifier les mots de passe faibles (outil de bruteforce)
- Medusa qui permet de tester la robustesse des systèmes d'authentification multi-protocoles (outil de cracking)

# Les attaques Web

## OWASP Top 10 – A08 : Défaillance dans l'intégrité des logiciels ou des données

**L'intégrité du code peut être compromise dans des logiciels tiers, des mises à jour ou des dépendances, permettant l'insertion de logiciels malveillants**

### Exemples d'attaques

- Insertion de malwares dans des mises à jour logicielles
- Compromission des bibliothèques utilisées par une application

### Mesures de prévention

- Mettre en place des vérifications cryptographiques pour les mises à jour
- Auditer régulièrement les dépendances et les outils utilisés

### Analyse des faiblesses

- AIDE (Advanced Intrusion Detection Environment) : outil de détection d'intrusion qui vérifie l'intégrité des fichiers systèmes en détectant les modifications non autorisées
- Tripwire : outil de contrôle d'intégrité des fichiers qui permet de surveiller les changements dans les fichiers critiques pour garantir la sécurité

# Les attaques Web

## OWASP Top 10 – A09 : Défaillance dans la journalisation et la surveillance

**L'absence de journaux d'événements critiques empêche de détecter, analyser et répondre aux attaques en temps réel**

### Exemples d'attaques

- Exploitation de failles non détectées
- Persistance des attaquants

### Mesures de prévention

- Implémenter des solutions SIEM
- Surveiller activement les journaux d'événements pour une réponse rapide aux incidents

### Analyse des faiblesses

- OSSEC : système de détection d'intrusion open source qui offre des capacités avancées de journalisation et de surveillance des événements de sécurité
- Splunk : outil de gestion des journaux qui permet de collecter, analyser et corréler les données des événements pour identifier les anomalies de sécurité

# Les attaques Web

## OWASP Top 10 – A10 : Mauvaise gestion des conditions exceptionnelles

**La mauvaise gestion des conditions exceptionnelles survient quand un logiciel ne prévient pas, ne détecte pas ou ne réagit pas correctement à des situations inhabituelles et imprévisibles.**

### Exemples d'attaques

- Attaque par déni de service par épuisement de ressources
- Exposition de données sensibles
- Corruption d'état dans une transaction financière

### Mesures de prévention

- Gérer les exceptions au plus près de la source
- Handler global de secours et gestion centralisée des erreurs
- Fail-closed systématique

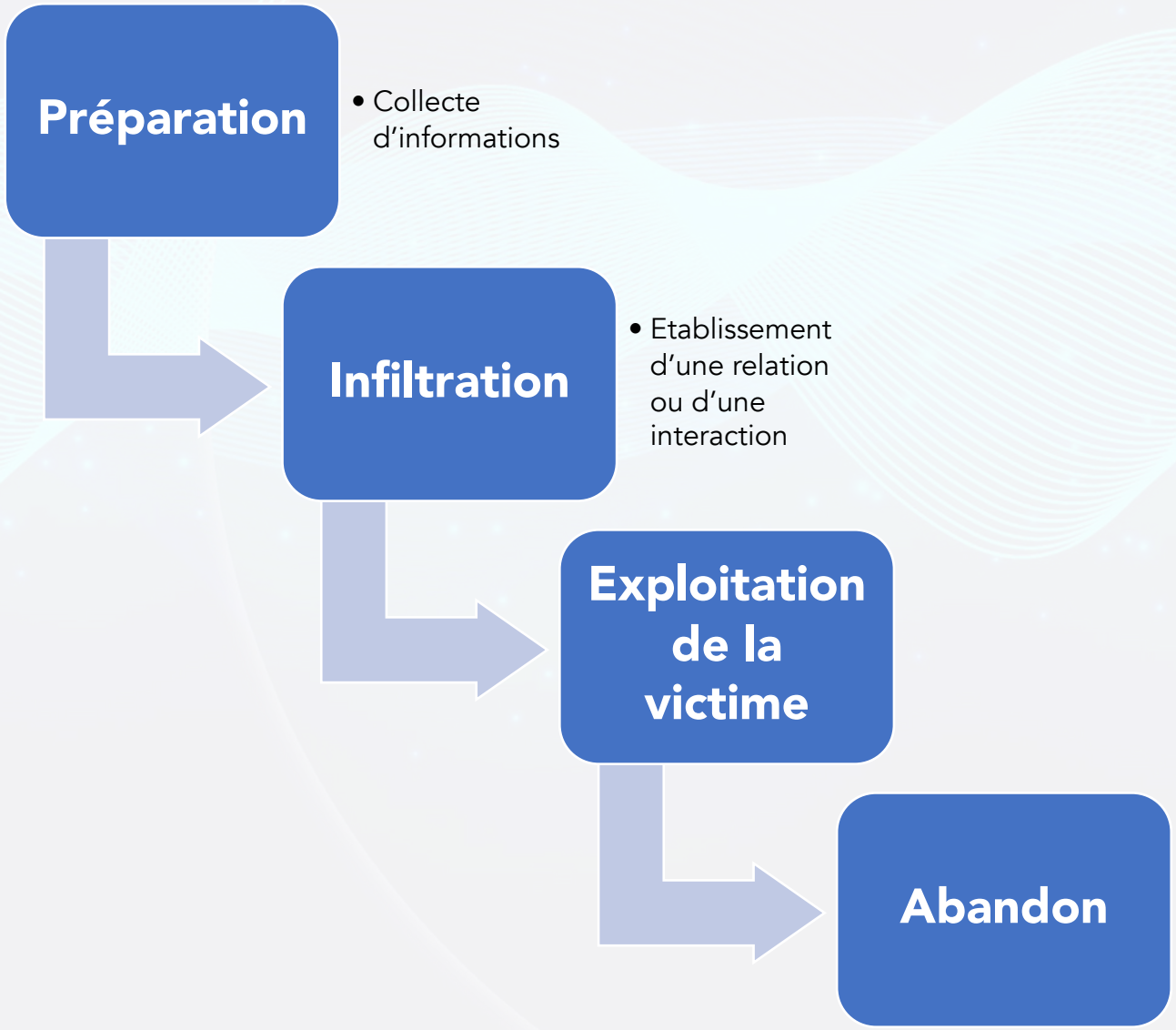
### Analyse des faiblesses

- Cartographier les surfaces d'erreur
- Tests edge cases

# L'ingénierie sociale

# Ingénierie sociale
## Définition et principes

**Technique de manipulation qui exploite l'erreur humaine dans le but d'obtenir des informations confidentielles, un accès ou des biens de valeur**



# Ingénierie sociale
## Techniques de manipulation psychologique

**L'auteur d'une attaque par ingénierie sociale exploite la confiance de ses victimes et ses capacités de persuasion**

- Réciprocité
- Preuve sociale
- Pénurie
- Engagement
- Autorité
- Amabilité
- Manipulation par distraction

# Ingénierie sociale

## Types d'attaques d'ingénierie sociale

- Prétexte
- Phishing et assimilés (smishing, vishing, spear-phishing, whaling, deepfake)
- Techniques d'usurpation d'identité (fraude au président)
- Appâtage (baiting)
- Point d'eau (waterhole)
- Quid pro quo
- Talonnage
- Dumpster diving
- Shoulder surfing