CYB-02 · INITIATION · PROGRAMME DE FORMATION

Cryptographie et sécurité — Les fondamentaux

Trois jours pour comprendre comment on protège une donnée, puis éprouver concrètement la solidité de cette protection.

DURÉE	NIVEAU	EFFECTIF	FORMAT
3 jours **21 heures**	**Initiation**	**4 à 10 stagiaires**	**Présentiel intra-entreprise ou école**

Public	Administrateurs systèmes et réseaux, développeurs, techniciens support, responsables informatiques de PME, étudiants bac+2 à bac+5
Prérequis	Bases en systèmes et en ligne de commande Linux. Aucune connaissance préalable en cryptographie ; des notions de réseau (adressage, HTTP) sont un plus
Lieu	Dans vos locaux (ou salle louée à proximité)
Tarif	**420 € net** par stagiaire et par jour, soit 1 260 € par stagiaire pour les 3 jours · minimum 4 stagiaires facturés, tarif plafonné à 6 stagiaires · TVA non applicable · frais de déplacement en sus · devis sur demande
Délai d'accès	2 à 4 semaines après accord sur le programme et signature de la convention

Objectifs

À l'issue de la formation, vous serez capable de :

- distinguer les grandes familles cryptographiques (symétrique, asymétrique, hachage) et l'usage de chacune ;
- expliquer les quatre propriétés de sécurité : confidentialité, intégrité, authenticité, non-répudiation ;
- chiffrer et déchiffrer avec un algorithme symétrique, et expliquer le rôle du sel et de la dérivation de clé ;
- mettre en œuvre le chiffrement asymétrique, l'échange de clés et la signature numérique (RSA, Diffie-Hellman) ;
- déployer une chaîne de confiance (certificats, autorité de certification) et comparer les modèles HTTPS, SSH et GPG ;
- éprouver la robustesse des secrets en cassant des hachages et des fichiers protégés (John the Ripper, Hashcat) ;
- traduire chaque attaque étudiée en bonne pratique de défense.

Programme

Bloc	Contenu	Mise en pratique	Durée
0 Vocabulaire de la sécurité	Accueil, quiz de positionnement, laboratoire Kali ; du chiffre de César à l'espace de clés, principe de Kerckhoffs, les quatre propriétés, ce que garantit le cadenas HTTPS	Casser un chiffre de César par force brute	2 h
1 Chiffrement symétrique	XOR, AES et ses tours, chiffrement par flux et par blocs, de DES à ChaCha20, problème du partage de la clé, HMAC	Chiffrer à la main avec XOR, observer l'apport d'un HMAC	2 h
2 Chiffrement asymétrique	Clés publique et privée, RSA et indicatrice d'Euler, échange Diffie-Hellman, chiffrement hybride, signature numérique	Calculer à la main un RSA et un échange Diffie-Hellman sur de petits nombres	3 h
3 Hachage et intégrité	Fonctions à sens unique, effet d'avalanche, collisions (MD5, SHA-1), stockage des mots de passe (sel, dérivation), empreinte et chiffrement	Vérifier l'intégrité d'un fichier, observer l'effet d'avalanche	2 h

Bloc	Contenu	Mise en pratique	Durée
4 Confiance et certificats	Authenticité et identité, certificats, autorité de certification, chaîne de confiance ; modèles HTTPS, SSH (TOFU) et GPG ; prise en main d'OpenSSL	Démonstration d'usurpation de clé publique	2 h
5 Atelier OpenSSL	AES en ligne de commande, dérivation PBKDF2, rôle du sel, format de sortie, octets bruts, base64 et hexadécimal	Chiffrer deux fois le même fichier et expliquer la différence	1,5 h
6 Atelier signature	Paire RSA, signature du condensat, vérification, intégrité, authenticité et non-répudiation	Signer un document, le vérifier, modifier un caractère et voir la signature tomber	1,5 h
7 Atelier certificats	Autorité de certification, demande (CSR), signature, chaîne à trois niveaux, inspection d'un vrai certificat HTTPS	Devenir sa propre autorité de certification et rejeter un imposteur	2 h
8 Atelier GPG	Paire de clés, signature, chiffrement pour un destinataire, chiffrement hybride sous le capot, révocation, vérification d'empreinte	Échanger des fichiers chiffrés et signés entre stagiaires	2 h
9 Atelier John the Ripper et Hashcat	Formats de hachage, convertisseurs (ZIP, RAR, clé SSH, PDF), dictionnaire et masque, coût d'une attaque (sel, tours), CPU et GPU	Cinq séries de cassage, du hachage brut au fichier protégé	2 h
10 Défi final et synthèse	Bonnes pratiques : choix d'un algorithme, longueur d'un secret, gestionnaire de mots de passe, sel et key stretching	Défi : casser un artefact protégé et rédiger les recommandations ; quiz de fin	1 h

Répartition indicative : jour 1, blocs 0 à 2 ; jour 2, blocs 3 à 6 ; jour 3, blocs 7 à 10. Horaires types : 9 h – 12 h 30 et 13 h 30 – 17 h.

> **Le plus de cette formation**
>
> La cryptographie n'est pas réduite à une liste d'algorithmes : chaque brique est comprise, parfois calculée à la main, puis mise à l'épreuve en ligne de commande. La formation se termine en passant de l'autre côté, pour démontrer qu'un secret faible fait tomber le chiffrement le plus solide.

Méthodes et moyens pédagogiques

- Apports courts illustrés, démonstrations et environ 60 % de pratique.
- Laboratoire isolé et reproductible : poste Kali Linux, OpenSSL, GPG, John the Ripper et Hashcat.
- Approche inductive : manipulation, question, démarche, réponse, puis encadré de synthèse.
- Ateliers guidés et mises en situation ; chaque bloc se conclut par un livrable.
- Supports remis au format PDF : diaporama, schémas et ateliers.
- À prévoir par le client : une salle avec vidéoprojecteur, un PC portable par stagiaire (le formateur peut en fournir sur demande).

Suivi et évaluation

- Feuille d'émargement signée par demi-journée.
- Quiz de positionnement identique en début et en fin de formation : il mesure la progression de chacun.
- Évaluation continue par les livrables de fin de bloc et défi final : casser un artefact protégé, puis en tirer les recommandations.
- Attestation de fin de formation remise à chaque stagiaire, avec les résultats de l'évaluation des acquis.
- Questionnaire de satisfaction rempli le dernier jour.

Accessibilité

Vous accueillez une personne en situation de handicap ? Contactez le formateur avant la formation : nous étudions ensemble les adaptations du déroulé, des supports et du matériel.

Formateur

Nicolas Lebosq : 19 ans d'expérience en réseaux et systèmes (administration réseau, encadrement d'équipe, ingénieur d'études en laboratoire de recherche), enseignant vacataire en réseaux à SeaTech, école d'ingénieurs de l'Université de Toulon, depuis 2018.

Contact et inscription

Nicolas Lebosq · nicolas.lebosq@lebosq-networks.fr · lebosq-networks.fr

Nicolas Lebosq, entrepreneur individuel (EI), nom commercial Lebosq Networks · SIRET **[SIRET]** · Déclaration d'activité enregistrée sous le numéro **[NDA]** auprès du préfet de région **[région]**. Cet enregistrement ne vaut pas agrément de l'État.

CYB-02 · version 1 · mise à jour le **[date]**