Chiffrement et SSL/TLS

Programme *(Mis à jour le 12/02/2021)*

Définition des concepts relatifs à la cryptographie

- Confidentialité / Authenticité / Intégrité
- Chiffrement / Déchiffrement / Décryptage

Historique de la cryptographie

Utilisation des méthodes cryptographique

Présentation de méthodes connues et mise en oeuvre

- Code de César, présentation et exercices
- Chiffre de Vigenère, présentation et exercices

Faiblesses et attaques possibles (analyse statistique, bruteforce)

- TP Décryptage

Principes de Kerckhoff

- Connaissance > Sécurité par obscurité

Chiffrement symétrique

- Présentation et algorithmes majeurs
- Différentes approches (flow / block)
- TP AES – Chiffrement Symétrique

Chiffrement asymétrique

- Présentation et algorithmes majeurs
- Les concepts mathématiques
- Les cas d'utilisation
- SSH
- PGP / GPG
- SSL
- Différence entre clés publiques, privées et privées avec passphrase
- Diffusion de sa clé publique
- TP RSA
- TP SSH

PGP / GPG

- Sécurisation des échanges
- Signature de documents
- Extensions pour clients mails
- TP GPG + diffusion clé publiques

Un mot sur le stockage des mots de passe

- Notion de hash et d'irréversibilité
- Algorithmes

Présentation de SSL

Référence

THIS1947

Durée

3 jours / 21 heures

Prix HT / stagiaire

2550€

Objectifs pédagogiques

- Utiliser les différentes technologies de chiffrement
- Analyser le trafic TLS
- Sécuriser et configurer manière forte les clients et serveurs TLS
- Distinguer les attaques sur TLS

Niveau requis

- Garantir avoir des connaissances générales avancées en programmation et développement informatique

Public concerné

- Développeurs informatiques.

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d'émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM) et/ou mises en situation
Questionnaires de satisfaction (enquête électronique privilégiée)

- La notion de certificat et de ses propriétés
- Les différents types de certificat
- Les différents formats de certificat
- Les différentes versions de SSL
- Attaques connues
- Définition de la PKI/IGC et des entités
- Workflow de demande et de génération d'un certificat
- La notion de confiance, CA et certificats auto-signés
- Les commandes utiles
- Utilisation d'openssl (Linux)
- Utilisation de certutil (Windows)

TP SSL

- Visualisation de certificats
- Création d'une CA
- Création de demande de certificats
- Génération d'un certificat
- Débuggage d'erreurs SSL
- Best practices actuelles (algorithmes et ciphers)
- Exemples d'installation et TP
- Apache / Nginx (personnalisable)
- Visualisation de trafic réseau SSL
- Déchiffrement de trafic réseau capturé ou à la volée
- TP Wireshark / SSL
- Obtenir des certificats
- Les autorités de confiance
- Les niveaux de certification
- Le cas de Let's Encrypt
- Demo / TP Let's Encrypt

Obtention de certificats

- Les autorités de confiance
- Les différents niveaux de certification
- Le cas de Let's Encrypt
- Demo / TP Let's Encrypt

Utilisation de certificats clients pour l'authentification

- Sites web
- VPN (OpenVPN / IPSEC)

Chiffrement de fichiers

Obtention de certificats

- Les autorités de confiance
- Les différents niveaux de certification
- Le cas de Let's Encrypt
- Demo / TP Let's Encrypt

Utilisation de certificats clients pour l'authentification

- Sites web
- VPN (OpenVPN / IPSEC)

Chiffrement de fichiers

Conteneurs chiffrés

- TrueCrypt / VeraCrypt
- Zed
- TP Création de conteneurs

Chiffrement de disque

- LUKS / FileVault / BitLocker / TrueCrypt

Homologation de produits (hardware/software) utilisant des moyens cryptographiques