

Titre	Fonctionnement, configuration et tests d'un serveur SSL (Ubuntu)
Motivation	Les échanges <i>web</i> sécurisés avec le protocole SSL (https) jouissent d'une grande popularité alors qu'ils présentent des risques qui doivent être pris en compte
Objectif	<p>Cette formation est destinée aux personnes qui veulent comprendre les mécanismes de sécurité liés au protocole SSL (<i>Secure Socket Layer</i>).</p> <p>Elle se veut utile avec plusieurs travaux pratiques dirigés sur l'infrastructure du laboratoire (autorité de certification, divers serveurs SSL, ...) après une mise à niveau théorique des participants.</p> <p>A l'issue de cette journée, le participant est capable de configurer un serveur SSL (Ubuntu) et d'évaluer son niveau de sécurité (tests à distance & audit sur le serveur).</p>
Pré requis	Aucun; bien que la connaissance des services de sécurité (confidentialité, intégrité, ...) et la pratique des échanges sécurisés sur <i>internet</i> facilitent la compréhension du cours
Public cible	Administrateur système, architecte des SI, spécialiste sécurité, ingénieur réseau, utilisateur curieux, ...
Dates	19 janvier 2010
Horaire	8h30 – 12h 13h30 – 17h
Lieu	Laboratoire de transmission de données www.tdeig.ch Haute école du paysage, d'ingénierie et d'architecture (hepia) – Prairie 4 – 1202 Genève
Programme	<p>Mise à niveau</p> <p>Cours 1 : Chiffrements symétrique & asymétrique (RSA), fonction de hachage, signature numérique</p> <p>Labo 1 Etude pratique basée sur l'excellent outil http://www.cryptool.org/</p> <p>Infrastructure à clé publique</p> <p>Cours 2 Autorité de certification, certificat numérique, chaîne de certification, authentications du serveur et du client</p> <p>Labo 2 Connexions sur les serveurs SSL du labo (divers cas d'erreur)</p> <p>Protocole SSL</p> <p>Cours 3 : Principaux paquets (en clair ou chiffrés) et paramètres importants</p> <p>Labo 3 Analyse avec l'excellent outil http://www.wireshark.org/</p> <p>Tests et Best Practices</p> <p>Labo 4 Obtention d'un certificat numérique serveur conforme aux bonnes pratiques avec l'excellent outil http://www.openssl.org/ Tests à distance du serveur SSL avec ce même outil</p> <p>Cours 4 : Que faut-il contrôler lors d'un audit d'un serveur SSL ?</p>
Cadre pédagogique	L'enseignement se répartit entre 50% de théorie et 50% de pratique L'infrastructure du labo, mise à disposition, comprend une autorité de certification basée sur Windows Server 2008, divers serveurs SSL reposant sur Apache/2.2.8 (Ubuntu) - mod_ssl/2.2.8 et des postes client Windows (XP & Vista)
Langue	Enseignement (théorique & pratique) dispensé en français Supports (cours + laboratoire) en français
Nombre de participants	Limité à 10 pour garantir un suivi optimal lors des travaux pratiques individuels .
Producteur & Intervenants	Cette formation, dispensée dans l'enseignement Bachelor&Master HESSO, a été intégralement développée par Gérald Litzistorf (professeur) et José Tavares (ingénieur HES en télécommunications) et sera dispensée par les mêmes personnes.
Prix	650.-