Sécurité systèmes et réseaux, niveau 1

Cours Pratique de 4 jours - 28h
Réf : FRW - Prix 2024 : 2 990CHF HT

Ce stage pratique vous montrera comment mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux. Après avoir étudié quelques menaces pesant sur le Système d'Information, vous apprendrez le rôle des divers équipements de sécurité dans la protection de l'entreprise afin d'être en mesure de concevoir une architecture de sécurité et de réaliser sa mise en œuvre.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître les failles et les menaces des systèmes d'information

Maîtriser le rôle des divers équipements de sécurité

Concevoir et réaliser une architecture de sécurité adaptée

Mettre en oeuvre les principaux moyens de sécurisation des réseaux

Sécuriser un système Windows et Linux

TRAVAUX PRATIQUES

Mise en œuvre d'une solution de proxy HTTP sous Windows ou Linux, d'une solution antivirale sur les flux réseaux. Conception et mise en œuvre d'une architecture multi-firewalls, multi-DMZ. Mise en œuvre des techniques fondamentales de sécurisation du système d'exploitation.

LE PROGRAMME

dernière mise à jour : 09/2018

1) Risques et menaces

- Introduction à la sécurité.
- Etat des lieux de la sécurité informatique.
- Le vocabulaire de la sécurité informatique.
- Attaques "couches basses".
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP-SYNflood, SMURF, etc.
- Déni de service et déni de service distribué.
- Attaques applicatives.
- Intelligence gathering.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- DNS : attaque Dan Kaminsky.

Travaux pratiques : Installation et utilisation de l'analyseur réseau Wireshark. Mise en œuvre d'une attaque applicative.

2) Architectures de sécurité

- Quelles architectures pour quels besoins ?
- Plan d'adressage sécurisé : RFC 1918.
- Translation d'adresses (FTP comme exemple).
- Le rôle des zones démilitarisées (DMZ).
- Exemples d'architectures.
- Sécurisation de l'architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité.
- Actions et limites des firewalls réseaux traditionnels.

PARTICIPANTS

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en réseaux et systèmes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Evolution technologique des firewalls (Appliance, VPN, IPS, UTM...).
- Les firewalls et les environnements virtuels.
- Proxy serveur et relais applicatif.
- Proxy ou firewall : concurrence ou complémentarité ?
- Reverse proxy, filtrage de contenu, cache et authentification.
- Relais SMTP, une obligation ?

Travaux pratiques : Mise en œuvre d'un proxy Cache/Authentification.

3) Sécurité des données

- Cryptographie.
- Chiffrements symétrique et asymétrique. Fonctions de hachage.
- Services cryptographiques.
- Authentification de l'utilisateur.
- L'importance de l'authentification réciproque.
- Certificats X509. Signature électronique. Radius. LDAP.
- Vers, virus, trojans, malwares et keyloggers.
- Tendances actuelles. L'offre antivirale, complémentarité des éléments. EICAR, un "virus" à connaître.

Travaux pratiques : Déploiement d'un relais SMTP et d'un proxy HTTP/FTP Antivirus. Mise en œuvre d'un certificat serveur.

4) Sécurité des échanges

- Sécurité WiFi.
- Risques inhérents aux réseaux sans fil.
- Les limites du WEP. Le protocole WPA et WPA2.
- Les types d'attaques.
- Attaque Man in the Middle avec le rogue AP.
- Le protocole IPSec.
- Présentation du protocole.
- Modes tunnel et transport. ESP et AH.
- Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).
- Les protocoles SSL/TLS.
- Présentation du protocole. Détails de la négociation.
- Analyse des principales vulnérabilités.
- Attaques sslstrip et sslsnif.
- Le protocole SSH. Présentation et fonctionnalités.
- Différences avec SSL.

Travaux pratiques : Réalisation d'une attaque Man in the Middle sur une session SSL. Mise en œuvre d'IPSec mode transport/PSK.

5) Sécuriser un système, le "Hardening"

- Présentation.
- Insuffisance des installations par défaut.
- Critères d'évaluation (TCSEC, ITSEC et critères communs).
- Sécurisation de Windows.
- Gestion des comptes et des autorisations.
- Contrôle des services.
- Configuration réseau et audit.
- Sécurisation de Linux.
- Configuration du noyau.
- Système de fichiers.
- Gestion des services et du réseau.

Travaux pratiques : Exemple de sécurisation d'un système Windows et Linux.

6) Audit et sécurité au quotidien

- Les outils et techniques disponibles.

- Tests d'intrusion : outils et moyens.
- Détection des vulnérabilités (scanners, sondes IDS, etc.).
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure.
- Réagir efficacement en toutes circonstances.
- Supervision et administration.
- Impacts organisationnels.
- Veille technologique.

7) Etude de cas

- Etude préalable.
- Analyse du besoin.
- Elaborer une architecture.
- Définir le plan d'action.
- Déploiement.
- Démarche pour installer les éléments.
- Mise en œuvre de la politique de filtrage.

Travaux pratiques : Elaboration d'une maîtrise de flux.

LES DATES

CLASSE À DISTANCE
2024 : 28 mai, 16 juil., 10 sept.,
19 nov.