Sécurité systèmes et réseaux, niveau 2

Cours Pratique de 4 jours - 28h
Réf : SEA - Prix 2024 : 2 860€ HT

Ce stage avancé vous permettra de mesurer le niveau de sécurité de votre Système d'Information au moyen d'outils de détection d'intrusions, de détection de vulnérabilités, d'audit... Il vous apportera la connaissance de solutions avancées pour maintenir et faire évoluer dans le temps le niveau de sécurité souhaité au regard de vos besoins.

OBJECTIFS PÉDAGOGIQUES

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

Mesurer le niveau de sécurité du système d'information

Utiliser des outils de détection d'intrusions, de détection de vulnérabilités et d'audit

Renforcer la sécurité du système d'information

Connaitre le fonctionnement d'une architecture AAA (Authentication, Autorization, Accounting)

Mettre en œuvre SSL/TLS

TRAVAUX PRATIQUES

De très nombreux outils seront déployés par les participants. Sonde IDS SNORT, scan de vulnérabilité avec NESSUS, analyse et scan des réseaux avec ETHEREAL et NMAP. Sécurisation d'un réseau Wi-Fi.

PARTICIPANTS

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

PRÉREQUIS

Bonnes connaissances de TCP/IP et de la sécurité des réseaux d'entreprise. Ou connaissances équivalentes à celles apportées par le stage "Sécurité systèmes et réseaux, niveau 1" (réf. FRW).

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.

LE PROGRAMME

dernière mise à jour : 07/2019

1) Rappels

- Le protocole TCP/IP.
- La translation d'adresses.
- L'architecture des réseaux.
- Le firewall : avantages et limites.
- Les proxys, reverse-proxy : la protection applicative.
- Les zones démilitarisées (DMZ).

2) Les outils d'attaque

- Paradigmes de la sécurité et classification des attaques.
- Principes des attaques : spoofing, flooding, injection, capture, etc.
- Librairies : Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
- Outils : Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.

Travaux pratiques : Analyse de protocoles avec Wireshark. Utilisation de Scapy et Arpspoof.

3) La cryptographie, application

- Les services de sécurité.
- Principes et algorithmes cryptographique (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Certificats et profils spécifiques pour les divers serveurs et clients (X509).
- Protocole IPSEC et réseaux privés virtuels (VPN).
- Protocoles SSL/TLS et VPN-SSL. Problématiques de compression des données.

Travaux pratiques : Prise en main d'openssl et mise en œuvre d'OpenPGP. Génération de certificats X509 v3.

4) Architecture AAA (Authentication, Autorization, Accounting)

- Le réseau AAA : authentification, autorisation et traçabilité.

- One Time Password : OTP, HOTP, Google Authentificator, SSO (Protocole Kerberos).
- La place de l'annuaire LDAP dans les solutions d'authentification.
- Les module PAM et SASL.
- Architecture et protocole Radius (Authentication, Autorization, Accounting).
- Les attaques possibles.
- Comment se protéger ?

Travaux pratiques : Attaque d'un serveur AAA.

5) Détecter les intrusions

- Les principes de fonctionnement et méthodes de détection.
- Les acteurs du marché, panorama des systèmes et applications concernés.
- Les scanners réseaux (Nmap) et applicatifs (Web applications).
- Les IDS (Intrusion Detection System).
- Les avantages de ces technologies, leurs limites.
- Comment les placer dans l'architecture d'entreprise ?
- Panorama du marché, étude détaillé de SNORT.

Travaux pratiques : Installation, configuration et mise œuvre de SNORT, écriture de signature d'attaques.

6) Vérifier l'intégrité d'un système

- Les principes de fonctionnement.
- Quels sont les produits disponibles ?
- Présentation de Tripwire ou AIDE (Advanced Intrusion Detection Environment).
- L'audit de vulnérabilités.
- Principes et méthodes et organismes de gestion des vulnérabilités.
- Site de référence et panorama des outils d'audit.
- Définition d'une politique de sécurité.
- Etude et mise en œuvre de Nessus (état, fonctionnement, évolution).

Travaux pratiques : Audit de vulnérabilités du réseau et serveurs à l'aide de Nessus et Nmap. Audit de vulnérabilités d'un site Web.

7) Gérer les événements de sécurité

- Traitement des informations remontées par les différents équipements de sécurité.
- La consolidation et la corrélation.
- Présentation de SIM (Security Information Management).
- Gestion et protocole SNMP : forces et faiblesses de sécurité.
- Solution de sécurité de SNMP.

Travaux pratiques : Montage d'attaque SNMP.

8) La sécurité des réseaux WiFi

- Comment sécuriser un réseau WiFi ?
- Les faiblesses intrinsèques des réseaux WiFi.
- Le SSID Broadcast, le MAC Filtering, quel apport ?
- Le WEP a-t-il encore un intérêt ?
- Le protocole WPA, première solution acceptable.
- Implémentation WPA en mode clé partagée, est-ce suffisant ?
- WPA, Radius et serveur AAA, l'implémentation d'entreprise.
- Les normes 802.11i et WPA2, quelle solution est la plus aboutie aujourd'hui ?
- Injection de trafic, craquage de clés WiFi.

Travaux pratiques : Configuration des outils pour la capture de trafic, scan de réseaux et analyse de trafic WIFI. Configuration d'un AP (Point d'acces) et mise œuvre de solutions de sécurité.

9) La sécurité de la téléphonie sur IP

- Les concepts de la voix sur IP. Présentation des applications.
- L'architecture d'un système VoIP.

- Le protocole SIP, standard ouvert de voix sur IP.
- Les faiblesses du protocole SIP.
- Les problématiques du NAT.
- Les attaques sur la téléphonie sur IP.
- Quelles sont les solutions de sécurité ?

10) La sécurité de la messagerie

- Architecture et fonctionnement de la messagerie.
- Les protocoles et accès à la messagerie (POP, IMAP, Webmail, SMTP, etc.).
- Problèmes et classifications des attaques sur la messagerie (spam, fishing, usurpation de l'identité, etc.).
- Les acteurs de lutte contre le SPAM.
- Les méthodes, architectures et outils de lutte contre le SPAM.
- Outils de collecte des adresses de messagerie.
- Les solutions mises en œuvre contre le SPAM.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 09 juil., 22 oct.	2024 : 02 juil., 15 oct.