Sécurité systèmes et réseaux
faire face aux menaces avec la CyberRange d'Airbus CyberSecurity

Cours Pratique de 4 jours - 28h
Réf : SCR - Prix 2024 : 2 810CHF HT

Ce cours 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.

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 œuvre les principaux moyens de sécurisation des réseaux

Sécuriser un système Windows et Linux

TRAVAUX PRATIQUES

La CyberRange d'Airbus CyberSecurity est utilisée pour réaliser et jouer des scénarios réalistes comprenant de véritables cyber-attaques.

LE PROGRAMME

dernière mise à jour : 02/2020

1) Risques et menaces

- 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.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- DNS : attaque Dan Kaminsky.

Travaux pratiques : Connexion sur la plateforme CyberRange, prise en main d'une machine Linux/Windows pour naviguer en mode commande et graphique. Utilisation de l'analyseur réseau Wireshark.

2) Les outils au quotidien

- Les outils et techniques disponibles.
- Tests d'intrusion : outils et moyens.
- Les types de scans, détection du filtrage, firewalking.
- Détection des vulnérabilités (scanners, sondes IDS, etc.).
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure.
- Monter une architecture et s'entraîner avec CyberRange (architecture, système d'exploitations, composant, etc.).

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.

- Les scénarios disponibles sur CyberRange : cyber-attaques (réseau, system, web), trafic (dns, ftp, ping, http), etc.

Travaux pratiques : Exécution d'un scénario sur CyberRange pour effectuer des scans de vulnérabilité web (ping, scan de port, scan vulnérabilité web, dump des utilisateurs en base de données, génération de trafic).

3) 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).
- Sécurisation de l'architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité. Actions et limites des firewalls réseaux traditionnels.
- Proxy serveur, firewall, relais applicatif.
- Reverse proxy, filtrage de contenu, cache et authentification.

Travaux pratiques : Mise en œuvre d'un proxy cache web (Squid) sur CyberRange.

4) Sécurité des données

- Les concepts fondamentaux de la cryptographie. Les principaux outils du marché, l'offre des éditeurs.
- Tendances actuelles. L'offre antivirale, complémentarité des éléments. EICAR, un "virus" à connaître.
- Chiffrements symétrique et asymétrique. Fonctions de hachage.
- Services et concepts cryptographiques.
- Principes et algorithmes cryptographiques (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Authentification de l'utilisateur. L'importance de l'authentification réciproque.
- Gestion et certification des clés publiques, révocation, renouvellement et archivage des clés.
- L'infrastructure de gestion des clés (IGC/PKI).
- Algorithme Diffie-Hellman. Attaque de l'homme du milieu (man in the middle).
- Certificats X509. Signature électronique. Radius. LDAP.
- Vers, virus, trojans, malwares et keyloggers.

Travaux pratiques : Déploiement d'un relais SMTP et d'un proxy HTTP/FTP Antivirus.

5) Sécurité des échanges

- 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 : Exécution d'un scénario d'analyse des vulnérabilités SSL sur CyberRange pour mettre en évidence les vulnérabilités SSL/TLS. Réalisation d'une attaque man in the middle sur une session SSL.

6) Sécuriser un système, le "hardening"

- Présentation du hardening.
- 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.

7) Audit

- Supervision et administration.
- Impacts organisationnels.
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure. Quels sont les produits disponibles ?
- Traitement des informations remontées par les différents équipements de sécurité.
- Réagir efficacement en toute circonstance.
- Veille technologique. Site de référence et panorama des outils d'audit.

Travaux pratiques : Analyse de fichiers logs système de machines sur CyberRange.

LES DATES

CLASSE À DISTANCE
2024 : 11 juin, 24 sept., 26 nov.