Hacking et Pentest : SCADA

Cours Pratique de 3 jours
Réf : HSC - Prix 2021 : 2 220€ HT

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de vos architectures SCADA. À la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à en élever le niveau de sécurité.

OBJECTIFS PÉDAGOGIQUES

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

Définir l'impact et la portée d'une vulnérabilité

Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques

Mesurer le niveau de sécurité d'une architecture SCADA

Réaliser un test de pénétration

Identifier les mesures de protection

LE PROGRAMME

dernière mise à jour : 10/2018

1) Rappel sur les systèmes de supervision et de contrôle industriel (SCADA)

- La problématique de sécurité dans les systèmes SCADA.
- La cybersécurité des systèmes industriels, les méthodes de classification.

2) Le hacking et la sécurité

- Formes d'attaques, modes opératoires, acteurs, enjeux.
- Audits et tests d'intrusion.

3) L'environnement SCADA

- Les composants des Systèmes de Contrôle Industriel (ICS)/SCADA.
- IHM (Interfaces Homme/Machine/Automate).
- Réseau : les automates via les navigateurs Web, Telnet, SSH, accès filaire TCP...)/sans-fil (WiFi, liaisons radio).
- Automate : contrôleur logique programmable (programmable Logic Controller, PLC).
- Les principaux protocoles utilisés par les architectures ICS/SCADA : DNP3, ModBus, IEC 60870, BACnet, LonWorks et EPICS.
- Appareils finaux (capteur, vanne ou pompe).

4) Vulnérabilités des architectures SCADA

- La recherche de vulnérabilités.
- Les mécanismes d'authentification, la gestion des accès distants.
- Les liaisons d'un système SCADA avec son environnement (connectivité) : réseau, capteur, automate et périphérique.
- Identifier et utiliser les applications et programmes hébergés sur un système SCADA.
- La méthodologie des tests d'intrusion.
- Les outils : framework de test d'intrusion, injecteur de code dans les automates, analyseurs de réseau, débogueurs.

Travaux pratiques : Mesurer le niveau de sécurité d'une architecture.

PARTICIPANTS

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

PRÉREQUIS

Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation. Ou connaissances équivalentes à celles du 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

L'évaluation est réalisée tout au long de la formation à travers différents moyens (QCM, mise en situation, quiz…). Le stagiaire évalue sa progression et ses acquis à l'issue de la formation. L'intervenant valide la progression pédagogique du stagiaire et précise les outils utilisés pour la validation des acquis.

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.

5) Les attaques

- Les attaques physiques.
- Les intrusions connues, les attaques APT (menaces persistantes avancées).
- Les scénarios d'attaques réelles sur les systèmes SCADA : STUXNET, FLAME.
- Les vulnérabilités liées aux IHM.
- Les automates et IHM exposés sur Internet.
- Les failles des systèmes d'exploitation gérant les systèmes SCADA (serveurs et postes de travail).

Travaux pratiques : Accéder à un système SCADA via différentes attaques. Réaliser un test de pénétration.

6) Le rapport d'audit

- Son contenu.
- Ses rubriques à ne pas négliger.

Travaux pratiques : Compléter un rapport pré-rempli.

LES DATES

Nous consulter