Détection d'intrusion et SOC

Cours Pratique de 4 jours - 28h
Réf : TRU - Prix 2024 : 2 860CHF HT

Ce cours très pratique présente les techniques d'attaque les plus évoluées à ce jour et montre comment les détecter. A partir d'attaques réalisées sur des cibles identifiées (serveurs Web, clients, réseaux, firewall, bases de données...), vous apprendrez à déclencher la riposte la plus adaptée. Vous apprendrez également le concept de SOC ainsi que l'ensemble des outils nécessaires en tant qu'analyste SOC.

OBJECTIFS PÉDAGOGIQUES

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

Identifier et comprendre les techniques d'analyse et de détection

Acquérir les connaissances pour déployer différents outils de détection d'intrusion

Mettre en œuvre les solutions de prévention et de détection d'intrusions

Comprendre les concepts et l'environnement d'un SOC

Savoir utiliser les outils d'analyse

LE PROGRAMME

dernière mise à jour : 10/2018

1) Bien comprendre les protocoles réseaux

- D'autres aspects des protocoles IP, TCP et UDP.
- Zoom sur ARP et ICMP.
- Le routage forcé de paquets IP (source routing).
- La fragmentation IP et les règles de réassemblage.
- De l'utilité d'un filtrage sérieux.
- Sécuriser ses serveurs : un impératif.
- Les parades par technologies : du routeur filtrant au firewall stateful inspection ; du proxy au reverse proxy.
- Panorama rapide des solutions et des produits.

Travaux pratiques : Visualisation et analyse d'un trafic classique. Utilisation de différents sniffers.

2) Les attaques sur TCP/IP

- Comment les pirates informatique mettent en œuvre le "Spoofing" IP.
- Réaliser des attaques par déni de service.
- La technique de la prédiction des numéros de séquence TCP.
- Vol de session TCP : Hijacking (Hunt, Juggernaut).
- Comprendre comment les pirates arrivent à réaliser des attaques sur SNMP.
- Attaque par TCP Spoofing (Mitnick) : démystification.

Travaux pratiques : Injection de paquets fabriqués sur le réseau. Utilisation au choix des participants d'outils graphiques, de Perl, de C ou de scripts dédiés.

3) Intelligence Gathering

- Chercher les traces : interrogation des bases Whois, les serveurs DNS, les moteurs de recherche.
- Apprendre les techniques pour mettre en place l'identification des serveurs.

PARTICIPANTS

Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en réseaux et sécurité. Connaître le guide d'hygiène sécurité de l'ANSSI. Avoir suivi le parcours introductif à la cybersécurité.

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.

- Comprendre le contexte : analyser les résultats, déterminer les règles de filtrage, cas spécifiques.

Travaux pratiques : Recherche par techniques non intrusives d'informations sur une cible potentielle (au choix des participants). Utilisation d'outils de scans de réseaux.

4) Détecter les trojans et les backdoors

- Etat de l'art des backdoors sous Windows et Unix. Qu'est ce un backdoor ?
- Comment mettre en place des backdoors et des trojans.
- Le téléchargement de scripts sur les clients, exploitation de bugs des navigateurs.
- Les "Covert Channels" : application client-serveur utilisant ICMP.
- Exemple de communication avec les Agents de Déni de Service distribués.

Travaux pratiques : Analyse de Loki, client-serveur utilisant ICMP. Accéder à des informations privées avec son navigateur.

5) Attaques et exploitation des failles

- Prise de contrôle d'un serveur : recherche et exploitation de vulnérabilités.
- Exemples de mise en place de "backdoors" et suppression des traces.
- Comment contourner un firewall (netcat et rebonds) ?
- Les techniques pour effectuer la recherche du déni de service.
- Qu'est ce que le déni de service distribué (DDoS)? Comment les pirates s'organisent pour effectuer une telle attaque ?
- Les attaques par débordement (buffer overflow).
- Exploitation de failles dans le code source. Techniques similaires : "Format String", "Heap Overflow".
- Quelles sont les vulnérabilités dans les applications Web ? Comment les détecter et se protéger ?
- Comment les personnes malveillantes arrivent à voler les informations dans une base de données.
- Qu'est ce que sont les RootKits.

Travaux pratiques : Exploitation du bug utilisé par le ver "Code Red". Obtention d'un shell root par différents types de buffer overflow. Test d'un déni de service (Jolt2, Ssping). Utilisation de netcat pour contourner un firewall. Utilisation des techniques de "SQL Injection" pour casser une authentification Web.

6) Le SOC (Security Operation Center)

- Qu’est-ce qu’un SOC ?
- A quoi sert-il ? Pourquoi de plus en plus d'entreprises l'utilisent ?
- Les fonctions du SOC : Logging, Monitoring, Reporting audit et sécurité, analyses post incidents.
- Les bénéfices d’un SOC.
- Les solutions pour un SOC.
- Le SIM (Security Information Management).
- Le SIEM (Security Information and Event Management).
- Le SEM (Security Event Management).
- Exemple d’une stratégie de monitoring.

7) Le métier de l’analyste SOC

- En quoi consiste le métier de l’analyste SOC ?
- Quelles sont ses compétences ?
- Monitorer et trier les alertes et les événements.
- Savoir prioriser les alertes.

8) Comment gérer un incident ?

- Les signes d'une intrusion réussie dans un SI.
- Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
- Comment réagir face à une intrusion réussie ?
- Quels serveurs sont concernés ?
- Savoir retrouver le point d'entrée et le combler.

- La boîte à outils Unix/Windows pour la recherche de preuves.
- Nettoyage et remise en production de serveurs compromis.

LES DATES

CLASSE À DISTANCE
2024 : 16 juil., 05 nov.