Détection d'intrusions
comment gérer les incidents de sécurité

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

Cette formation à la fois théorique et pratique présente les techniques d'attaque les plus évoluées à ce jour et montre comment y faire face. A partir d'attaques réalisées sur cibles identifiées (serveurs Web, clients, réseaux, firewall, bases de données...), le participant apprendra à déclencher la riposte adaptée (filtrage d'anti-trojan, filtrage d'URL mal formée, détection de spam et détection d'intrusion en temps réel avec sonde IDS).

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

Gérer un incident d'intrusion

Connaître le cadre juridique

TRAVAUX PRATIQUES

Des architectures sécurisées et "normalement " protégées (firewall multi-DMZ, applications sécurisées) seront la cible des attaques.

LE PROGRAMME

dernière mise à jour : 09/2018

1) Le monde de la sécurité informatique

- Définitions "officielles" : le hacker, le hacking.
- La communauté des hackers dans le monde, les "gurus", les "script kiddies".
- L'état d'esprit et la culture du hacker.
- Les conférences et les sites majeurs de la sécurité.

Travaux pratiques : Navigation Underground. Savoir localiser les informations utiles.

2) TCP/IP pour firewalls et détection d'intrusions

- IP, TCP et UDP sous un autre angle.
- 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.

3) Comprendre les attaques sur TCP/IP

- Le "Spoofing" IP.
- Attaques par déni de service.
- Prédiction des numéros de séquence TCP.

PARTICIPANTS

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

PRÉREQUIS

Bonnes connaissances des réseaux TCP/IP. Connaissances de base en sécurité informatique.

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.

- Vol de session TCP : Hijacking (Hunt, Juggernaut).
- 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. Hijacking d'une connexion telnet.

4) Intelligence Gathering : l'art du camouflage

- Chercher les traces : interrogation des bases Whois, les serveurs DNS, les moteurs de recherche.
- Identification des serveurs.
- 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.

5) Protéger ses données

- Systèmes à mot de passe "en clair", par challenge, crypté.
- Le point sur l'authentification sous Windows.
- Rappels sur SSH et SSL (HTTPS).
- Sniffing d'un réseau switché : ARP poisonning.
- Attaques sur les données cryptées : "Man in the Middle" sur SSH et SSL, "Keystoke Analysis" sur SSH.
- Détection de sniffer : outils et méthodes avancées.
- Attaques sur mots de passe.

Travaux pratiques : Décryptage et vol de session SSH : attaque "Man in the Middle". Cassage de mots de passe avec LophtCrack (Windows) et John The Ripper (Unix).

6) Détecter les trojans et les backdoors

- Etat de l'art des backdoors sous Windows et Unix.
- Mise en place de backdoors et de 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.

7) Défendre les services en ligne

- 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) ?
- La recherche du déni de service.
- Les dénis de service distribués (DDoS).
- Les attaques par débordement (buffer overflow).
- Exploitation de failles dans le code source. Techniques similaires : "Format String", "Heap Overflow".
- Vulnérabilités dans les applications Web.
- Vol d'informations dans une base de données.
- 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.

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.

9) Conclusion : quel cadre juridique ?

- La réponse adéquate aux hackers.
- La loi française en matière de hacking.
- Le rôle de l'Etat, les organismes officiels.
- Qu'attendre de l'Office Central de Lutte contre la Criminalité (OCLCTIC) ?
- La recherche des preuves et des auteurs.
- Et dans un contexte international ?
- Le test intrusif ou le hacking domestiqué ?
- Rester dans un cadre légal, choisir le prestataire, être sûr du résultat.

LES DATES

CLASSE À DISTANCE
2024 : 16 juil., 15 oct.