Hacking Ethique

5 jours
35 heures

SYSR570.pdf

loging-formation.com

Objectifs

Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques ; Réaliser un audit de sécurité de votre entreprise.

Participants

Les informaticiens qui souhaitent acquérir des notions avancées sur la sécurité informatique pour protéger le système d'information de leur entreprise.

Prérequis

Notion de réseau ; Notion d'un langage de programmation ; Connaissance de Linux.

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en oeuvre les nouveaux outils présentés au cours de la session.

Profil de l'intervenant

Consultant-formateur expert sur cette thématique. Suivi des compétences techniques et pédagogiques assurée par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Exercices individuels et collectifs durant la formation. Evaluation des acquis et attestation de fin de stage adressés avec la facture.

Programme

Introduction

Rappels TCP/IP

Prise d'informations

Présentation des techniques de prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants :

Informations publiques

Enumération des systèmes

Enumération des services

Enumération Netbios

Fingerprinting applicatif

Enumération des règles réseau

Vulnérabilités des postes utilisateurs

Intrusion à distance des postes utilisateurs par exploitation des vulnérabilités sur les navigateurs Web, clients de messagerie... :

Les troyens

Auto exécution de troyens

Vulnérabilités réseau

Attaques des règles de Firewalling, interception/analyse des transmissions réseaux cryptées :

Sniffing réseau

Spoofing réseau / Bypassing de firewall

Idle Host Scanning

Détournement de connexions

Attaque des protocoles sécurisés

Dénis de service

Vulnérabilités Web

Attaque des scripts Web dynamiques (PHP, Perl...), et des bases de données associées (MySql, Oracle...) :

Cartographie du site

Failles PHP (include, fopen...)

Attaques CGI (Escape shell...)

Injections SQL

XSS

Vulnérabilités applicatives

Intrusion à distance d'un système Windows et Linux par l'exploitation des services de type applicatif, avec la plateforme Metasploit :

Escape shell

Buffer overflow

Etude de méthodologies d'attaques avancées en local et prise de contrôle du statut administrateur :

Utilisation et intégration d'exploit à Metasploit

Failles de type système

Backdooring et prise de possession d'un système suite à une intrusion et maintien des accès :

Brute force d'authentification

Espionnage du système

Hacking Ethique

5 jours
35 heures

SYSR570.pdf

loging-formation.com

Backdoor Kernel

Sécurité générique

Outils génériques de surveillance et de sécurisation du système/réseau :

Cryptographie

Sécurité système

Firewall / VPN / IDS