email : info@sysdream.com
www.sysdream.com

Hacking et Sécurité : Avancé v6

Accroche

Pratiquez les attaques avancées pour mieux vous défendre.

Descriptif

Ce cours est une approche avancée et pratique des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises. Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes.
L'objectif est de vous fournir les compétences techniques nécessaires à la réalisation d'audits de sécurité (tests de pénétration), en jugeant par vous-même de la criticité et de l'impact réel des vulnérabilités découvertes sur le SI.
La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux).

Objectifs

- Comprendre et détecter les attaques sur un SI
- Définir l'impact et la portée d'une vulnérabilité
- Réaliser un test de pénétration
- Corriger les vulnérabilités
- Sécuriser un réseau, et intégrer des outils de sécurité adéquats

Public visé

- RSSI, DSI
- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Développeurs

Pré-requis

- Administration Windows/Linux
- TCP/IP
- Maitrise de Linux en ligne de commande est un plus

Ressources

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne / Internet
- Metasploit

Formations associées

- Hacking & Sécurité : Expert v4
- Certified Ethical Hacker v9
- Test d'intrusion : Mise en situation d'audit

email : info@sysdream.com
www.sysdream.com

Programme

Jour 1

Introduction

- Rappel TCP/IP / Réseau Matériel
- Protos / OSI - Adressage IP

Introduction à la veille

- Vocabulaire
- BDD de Vulnérabilités et Exploits
- Informations générales

Prise d'informations

- Informations publiques
- Moteur de recherche
- Prise d'information active

Scan et prise d'empreinte

- Enumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation
- Prise d'empreinte des services

Jour 2

Vulnérabilités réseaux

- Idle Host Scanning
- Sniffing réseau
- Spoofing réseau
- Hijacking
- Attaque des protocoles sécurisés
- Dénis de service

- Firewalking
- Anti port scan

Vulnérabilités clients

- Modes et signes d'infection
- Vulnérabilités courantes
- Introduction à Metasploit
- Conception de malwares
- Types de malwares
- Méthodes de détection

Jour 3

Vulnérabilités Web

- Cartographie du site et identification des fuites d'informations
- Failles PHP (include, fopen, upload, etc.)
- Injections SQL
- Cross-Site Scripting (XSS)
- Cross-Site Resquest Forgery (CSRF)

Jour 4

Vulnérabilités applicatives

- Escape shell
- Buffer overflow
- Etude de méthodologies d'attaques avancées en local et prise de contrôle du statut administrateur
- Race Condition

Vulnérabilités système

- Backdooring et prise de possession d'un système suite à une intrusion et maintien des accès
- Élévation de privilèges
- Le fichier passwd d'Unix

- Le fichier SAM de Windows
- Service d'authentification
- Espionnage du système
- Systèmes de détection d'intrusion
- Cryptographie
- Intégrité système

Jour 5

Challenge final

- Mise en pratique des connaissances acquises durant la semaine sur un TP final.