Solutions Informatiques Télécoms

Séminaire de formation sur la sécurité des Systèmes d'Information sous le thème :

« Ethical Hacking & Penetration Testing »

Cutting-Edge Hacking Techniques:
Learn the IT Ninja Attacks From
The #1 Certified Tunisian H@cker

Durée

05 Jours du 8 au 12 juin 2014 au Centre de Formation et d'Echange à Distance (CFED) Palais de Congrès – Nouakchott –Mauritanie.

Objectifs de la formation de la formation

Ce cours vous permettra d'acquérir un niveau d'expertise élevé dans le domaine de la sécurité en réalisant différents scénarios complexes d'attaques. L'objectif est de se préparer à effectuer avec succès des projets de tests d'intrusion et d'Ethical Hacking.

A qui s'adresse la formation

Décideur, architecte, administrateur réseaux et systèmes concernés par les problèmes de sécurité, Chef de Projet Informatique, RSSI, consultant SSI

Prérequis

Il est recommandé d'avoir une expérience en administration de systèmes, une bonne compréhension des systèmes d'exploitation (*Linux* et *Windows*) et d'avoir des notions des concepts de base de la sécurité de l'information.

Informations Générales

- La formation est dispensée en français.
- Plus de 15 Go d'outils et des vidéos sur le piratage seront remis à chaque participant.
- Chaque session est limitée à un maximum de 15 personnes.

Contenu de la formation

Jour 1

- Introduction
- Guerre de l'information
- Les séquences d'attaques
- Etudes de cas
- Récupération d'informations publiques
- Google Hacking
- Balayages des réseaux
- Scans avancés des ports
- Scans avancés des vulnérabilités
- **Attaques Ninja**

Jour 2

- Enumération des ressources
- Enumération de comptes
- Attaques sur les mots de passes Windows
- Attaques par recherche exhaustive
- Monitoring des actions systèmes Windows
- Monitoring d'un système linux
- Attaques sur les mots de passes Linux
- Amplification de trafic
- Création des malwares
- Rootkits - Désobfuscation de code malveillant
- Débugging de shellcode

Jour 3

- Interception de trafic et analyse
- Récupération des mots de passe
- Reconstitution des sessions
- Attaques sur les protocoles de routage
- Attaques sur les adresses MAC
- Attaques sur les serveurs DHCP
- Attaques sur les serveurs DNS
- Attaques sur le protocole ARP
- Extraction des données
- Attaques non électroniques
- Attaques par Flooding
- Attaques DoS, DDoS et remèdes associés.
- Détournements de sessions

Jour 4

- Vulnérabilités Web
- Failles applicatives OWASP
- Failles XSS
- Attaque CSRF
- Exemples d'attaques Web
- TP : Prise de contrôle d'un serveur Web
- Contournement de htaccess
- Détection de fichiers sensibles
- Faille Include
- Utilisation des filtres PHP
- Utilisation de la console Metasploit
- Exploitations de vulnérabilité sous Metasploit
- Attaques scénarisées sous Metasploit
- TP : Prise de contrôle d'un Active Directory
- Injection SQL
- Injection SQL par concaténation
- Injection SQL en aveugle

Jour 5

- Attaques sur les réseaux sans fil
- Sécurité par clés WEP, WPA et WPA2
- Maîtrise de l'AirpCap, Cain & Abel et AirCrack-ng.
- Débordements de tampon et remèdes associés
- Contournement de pare-feu
- Exploitation par combinaison de vulnérabilités
- Système de détection/prévention d'intrusion
- Intégrer un IDS dans un réseau
- Gestion des alertes
- Ecriture de règles snort
- Evasion d'IDS/IPS
- Détournement des attaques par Honeypots
- Cryptage symétrique et asymétrique, hashing et signature électronique
- Cryptage des disques
- Cryptanalyse
- Challenge Final

Avenue Charles de Gaulles, 99TZ Tevragh-zeina – Nouakchott – Mauritanie Téléphones : +222 44 24 48 48 ou + 222 222 000 22 E-mail contact@syskat.com Web : www.syskat.com