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.