# Formation Ethical Hacking

**Objectif** :

Effectuer un Test de pénétration d'un système d'information et comprendre les techniques des Pirates informatiques

**Prérequis** :

notions de réseau, de systèmes d'exploitation, de programmation.


## Jour 1

**1.Introduction**
- Historique
- Statistiques
- Qui, Quoi, Comment, Pourquoi
- Recommandations ANSSI
- méthodologie d'une attaque

**2. prise d'empreintes**
- Introduction
- Informations publiques :
  - Google Hacking
  - Whois …
- Enumération des systèmes, services, netbios…

## Jour 2

**3. Vulnérabilité 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
- Matériel hardware:
  - teensy
  - rubberducky,
  - pyborad …

**4. Vulnérabilité des réseaux**
- Attaques des règles de Firewalling
- Sniffing réseau, Spoofing réseau / Bypassing de firewall
- Idle Host Scanning
- Détournement de connexions
- Attaque des protocoles sécurisés
- Dénis de service

## Jour 3

**5. Vulnérabilité des Applications**
- Notion d'assembleur
- Stack overflow
- Heap overflow
- Format String
- Les protections : seh, canary, aslr …

**6. Vulnérabilité physiques**
- Passage de session
- Dump de la mémoire …

## Jour 4

**7. Vulnérabilité des Failles 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

**8. Vulnérabilités systèmes**
- Backdooring et prise de possession d'un système suite à une intrusion et maintien des accès :
  - Brute force d'authentification
  - Espionnage du système
  - Backdoor Kernel

## Jour 5

**9. Signature et chiffrement**
- Théorie
- Clé symétriques/asymétriques
- PGP, GPG, Truecrup, …
- Utilisation pour les clients mail.

**14. Sécurisation et surveillance réseau**
- Cryptographie
- Sécurité système
- Firewall / VPN / IDS

**15. Atelier pratique**
- Mise en place d'un challenge de sécurité
  - Web
  - Applicatif
  - Système
  - Réseau

48, Avenue Bellefontaine

59250 Halluin

(+33) 03.66.72.48.44

Pour vous inscrire, merci de nous communiquer vos besoins, identités, financements et dates par courriel :

**formations@serval-concept.com**