# Formation Sécurité des systèmes Industriels

**Objectif** :

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

**Prérequis** :

Notions de réseau, de systèmes d'exploitation, de programmation, systèmes industriels.


## 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, Shodan, Whois …
- Enumération des systèmes, services, netbios…

## Jour 2

**3. Automates PLC / télétransmetteurs RTU / Automates de sécurité**
- Services couramment présents
- Vulnérabilités rencontrées
- Protocoles courants ( Modbus ,CAN, interbus, i2c…:
- Déni de service / robustesse des automates

**4. IHM (Interfaces Homme-Machine)Vulnérabilités rencontrées**
- 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

**5. Accès distants**
- RTC
- VPN
- Boîtiers de télétransmission
- Sans-fil (Wi-Fi, liaisons radio)
- Problèmes des automates et IHM exposés sur Internet (exemples avec Shodan et Eripp)

## Jour 3

**6. Vulnérabilité des postes utilisateurs**
- Intrusion à distance des postes utilisateurs par exploitation des vulnérabilités sur les navigateurs Web, clients de messagerie... :
- Les troyens
- Matériel hardware:
  - teensy
  - rubberducky,
  - pyboard …

**7. 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 4

**8. Retour d'expérience Audits sécurité / Tests d'intrusion**
- Compromission des systèmes
- Rebonds du réseau bureautique vers le réseau industriel
- Compromission des IHM
- Accès aux automates
- Modification du processTunnels (DNS, ICMP, RDP)

**9. Exemples d'attaques ciblées (APT) et d'incidents**
- Stuxnet
- Etc.

**10. Recommandations générales**
- Séparation réseau industriel / réseau bureautique
- DMZ internes
- Cloisonnement réseau / Défense en profondeur
- Zones
- Niveaux

## Jour 5

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

**12. Sécurisation et surveillance réseau**
- Cryptographie
- Sécurité système
- Supervision

**13. Les matériels industriels**
- Protection USB
- Firewall industriels
- Diode réseau
- Modem/routeur sécurisé
- …

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**