



## Checkpoint Sécurité – « Etat de l'Art »

---

<b>Objectif</b>	Cette formation passe en revue les différents domaines de la sécurité et les outils les plus appropriés pour assurer la protection d'un système informatique. Elle donne les tendances actuelles en 2007 et les orientations futures dans le domaine sécurité réseau et applicative
<b>Pré requis</b>	Connaissance des systèmes d'exploitation Windows NT/2000 et Unix, expérience des protocoles TCP/IP et d'Internet, Connaissance de base de l'environnement réseau.
<b>Durée</b>	3 jours

### Contenu

---

#### **Module 1: statistiques sur la sécurité.**

- Objectifs du cours
- Définitions
- Dommages
- Organismes spécialisés

#### **Module 2: la sécurité humaine.**

- Qu'est-ce qu'un hacker
- Qui sont les pirates informatiques ?

#### **Module 3: sécurité physique.**

- Contrôle d'accès physique
- Systèmes d'authentification forts
- Avantages et inconvénients des systèmes d'authentification forts

#### **Module 4: sécurité système.**

- Sécurité des systèmes d'exploitation
- Deux modèles de sécurité
- Sécurité de Windows
- Sécurité sous Unix/Linux
- Virtualisation
- Menaces liées à la virtualisation
- Sécurité des postes utilisateurs

#### **Module 5: sécurité réseaux.**

- Sécurité des hubs
- Sécurité des switches
- Sécurité des routeurs

#### **Module 6: protocoles réseaux.**

- IP
- TCP et UDP
- Gestion des ports
- Translation d'adresses
- RFC 1918
- DNS
- DHCP
- IPv6

#### **Module 7: sécurisation des flux réseaux.**

- Techniques de sécurisation des flux réseaux
- Firewalls périmétriques
- Certification ICASA
- Solutions UTM
- Critères de sélection d'une solution UTM
- Solutions de proxys
- IPS/IDS
- Présentation des IDS
- Présentation des IPS
- Solutions du marché

#### **Module 8: audit.**

- Technique de scans intrusifs
- Présentation de Nmap
- Présentation de HPING
- Présentation de Nessus
- Présentation de ISS
- Présentation de SNMP

#### **Module 9: chiffrement.**

- Algorithmes symétriques et asymétriques
- Diffie Hellmann
- Fonctions de hachage
- Signatures numériques
- PKCS

#### **Module 10: technologies sans fil.**

- Présentation des technologies de Wireless Fidelity
- Risques liés aux réseaux sans fil
- Principes de sécurisation des réseaux sans fil
- WEP
- WPA / WPA2
- Outils d'audits

#### **Module 11: certificats X.509 et Autorités de Certification.**

- Présentation de X.509
- Certificats d'Autorité de Certification
- Certificats de serveurs
- Certificats clients
- Certificats de signature de code
- Limites des certificats
- Les Autorités de certification du marché



**Module 12: réseaux privés virtuels.**

- Présentation des réseaux privés virtuels
- IPSEC
- Protocole PPP
- Protocole L2TP
- MPLS

**Module 13: sécurité Web.**

- Sécurité du Web
- Sécurité SSL
- Filtrage des URLs
- Solutions de sécurité du marché
- Sécurité des serveurs Web
- Sécurité des navigateurs Internet

**Chapitre 14: sécurité de la messagerie.**

- Sécurité du protocole SMTP
- Sécurité du protocole POP3
- Sécurité du protocole IMAP
- Fonctionnalités de sécurité des serveurs de messagerie
- Statistiques concernant le spam
- Gestion du spam
- Présentation du protocole SPF
- Présentation de DomainKeys
- Techniques de lutte contre le spam

**Module 15: virus/malwares.**

- Présentation des virus
- Méthodes de protection
- Chevaux de Troie
- Présentation des produits antivirus

**Module 16: méthodologie OSSTM.**

- Présentation de la méthode OSSTM
- Collecte d'informations
- Ingénierie sociale
- Vérification de la politique de sécurité
- Vérification des mots de passe
- Vérification des réseaux de communication