

## Sommaire :

### I. Fondamentaux TCP/IP

1. **Concepts IP** : Modèle TCP/IP, adresses, ports, protocoles, DNS, routage
2. **Introduction à TCPdump & TCP** : utilisation de TCPdump ; fonctionnement du protocole TCP ; problèmes liés à TCP
3. **Fragmentation IP** : principes et fragmentation malveillante
4. **ICMP** : théorie, cartographie réseau, trafic normal vs malveillant, filtrage
5. **Stimulus et réponses** : comportements attendus, détournements de protocole, stimuli anormaux
6. **DNS** : fonctionnement, collecte de renseignements, attaques via DNS

### II. Analyse du trafic

7. **Dissection de paquets avec TCPdump** : initiation à la lecture de paquets et outils associés
8. **Examen des en-têtes IP** : attaques par insertion/évasion, drapeaux IP
9. **Analyse des protocoles encapsulés (TCP, UDP, ICMP)**
10. **Analyse « terrain »** : cas pratiques (Netbus, vers RingZero...)
11. **Trafic mystérieux** : distinguer scans, DDoS, empreintes réseau

### III. Filtres et règles pour la surveillance

12. **Écrire des filtres TCPdump** : masquage binaire, filtres IP/UDP/TCP
13. **Introduction à Snort & ses règles** : mise en route de Snort, structure de base des règles **Snort – partie II** : options avancées et exemples de règles

### IV. Infrastructure d'intrusion

15. **Attaque Mitnick** : exploitation TCP, détection, prévention, IDS réseau vs hôte
16. **Questions d'architecture** : capteurs, emplacements, facteurs humains, console d'analyse, IDS réseau vs hôte
17. **Questions organisationnelles** : modèle de sécurité, gestion des risques, menaces, ROI
18. **Réponse auto et manuelle** : automatisations, honeypots, procédures manuelles
19. **Business case IDS** : enjeux managériaux, menaces, compromis, justification exécutive
20. **Orientations futures** : menaces émergentes, défense en profondeur, techniques nouvelles

### V. Annexes

- **A. Exploits et scans** : faux positifs, exploits IMAP, scans PorteMap...
- **B. Déni de service** : traces, nmap, attaques DDoS
- **C. Collecte de renseignements** : cartographie, attaques furtives, worms

