

## Architectures réseaux sécurisées



ECTS



Volume horaire

24.5h

## Présentation

### Description

- Firewalls : classes (sans états, avec états, applicatif, personnel) ; architectures (routeur filtrant, bastion, zones démilitarisées) ; limites (fragmentation, tunnels, authentification par IP)
- IPsec : principes sur les tunnels (niveaux 2 et 3), protocoles AH, ESP) et modes (transport et tunnel) de IPsec, négociations (IKE, TLS), routage et utilisations classiques (lien AP-AS dans 802.1X, antennes/site central, roaming)
- Solutions VPN : OpenVPN, Cisco VPN, les solutions VPN SSL
- NIDS : outils classiques (Snort, Suricata, IDS spécialisés), la prévention (bans firewall, etc.), les sondes et SIEM
- Mise en pratique Attaques ARP + IDS/IPS
- Mise en pratique Firewalls (mise en place, contournement sans états, contournements SSH/SOCKS/DNSTOTCP)
- Mise en pratique sur ASA Cisco (Firewall, VPN, IDS)
- Sécurité des Applications Web
  - Présentation des attaques et vulnérabilités sur le web
  - Mécanismes de défense côté navigateur et serveur
  - Présentation de projets de recherche sur la détection
  - Mise en pratique des attaques et des protections
- Techniques d'intrusion réseau et système
  - Stratégies d'intrusion (recueil d'informations, exploitation de vulnérabilités, pivot, cryptanalyse, reverse engineering)

- Les outils d'intrusion (Nmap, Metasploit, Craqueurs de mots de passe, pivots ssh, proxychains, debugger, compilateur)

- Analyse forensics
  - Traitement des incidents, continuité, investigation numérique

### Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les principaux concepts associés à la conception et l'implémentation d'architectures réseaux sécurisées
- Les outils et techniques principaux permettant cette sécurisation et leur utilisation en fonction des différents contextes ainsi que des objectifs correspondants.
- Les vulnérabilités inhérentes aux architectures système et réseau et les grandes techniques d'intrusion ;
- Le fonctionnement des principales vulnérabilités du web.

L'étudiant devra être capable de :

- Distinguer les différents types de pare-feux ainsi que leurs capacités et limitations
- Définir et auditer une architecture de filtrage adaptée à un réseau informatique donné
- Choisir pour un tunnel IPsec les protocoles à utiliser, les modes de fonctionnement et un plan de routage adapté pour les passerelles associées
- Mettre en place et auditer un tel tunnel IPsec
- Mettre en place ou auditer un VPN créé sur du IPsec

manuellement ou en utilisant les outils tout-en-un du marché

- Mettre en place et auditer un système de détection d'intrusion éventuellement distribué avec des options de prévention
- Faire le design complet d'une architecture de sécurité pour un réseau complexe
  
- Identifier les limites et avantages de différentes solutions de détection d'intrusion ;
- Positionner les sondes de détection d'intrusion de manière efficace ;
- Analyser les événements collectés par les sondes et corréler ces événements pour identifier une menace réelle.
- Identifier les vulnérabilités dans les architectures web et proposer des solutions pour réaliser une protection efficace

---

## Pré-requis nécessaires

Une bonne connaissance des architectures Web, de la cryptographie et des réseaux.

---

## Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

---

## Infos pratiques

### Lieu(x)

 Toulouse