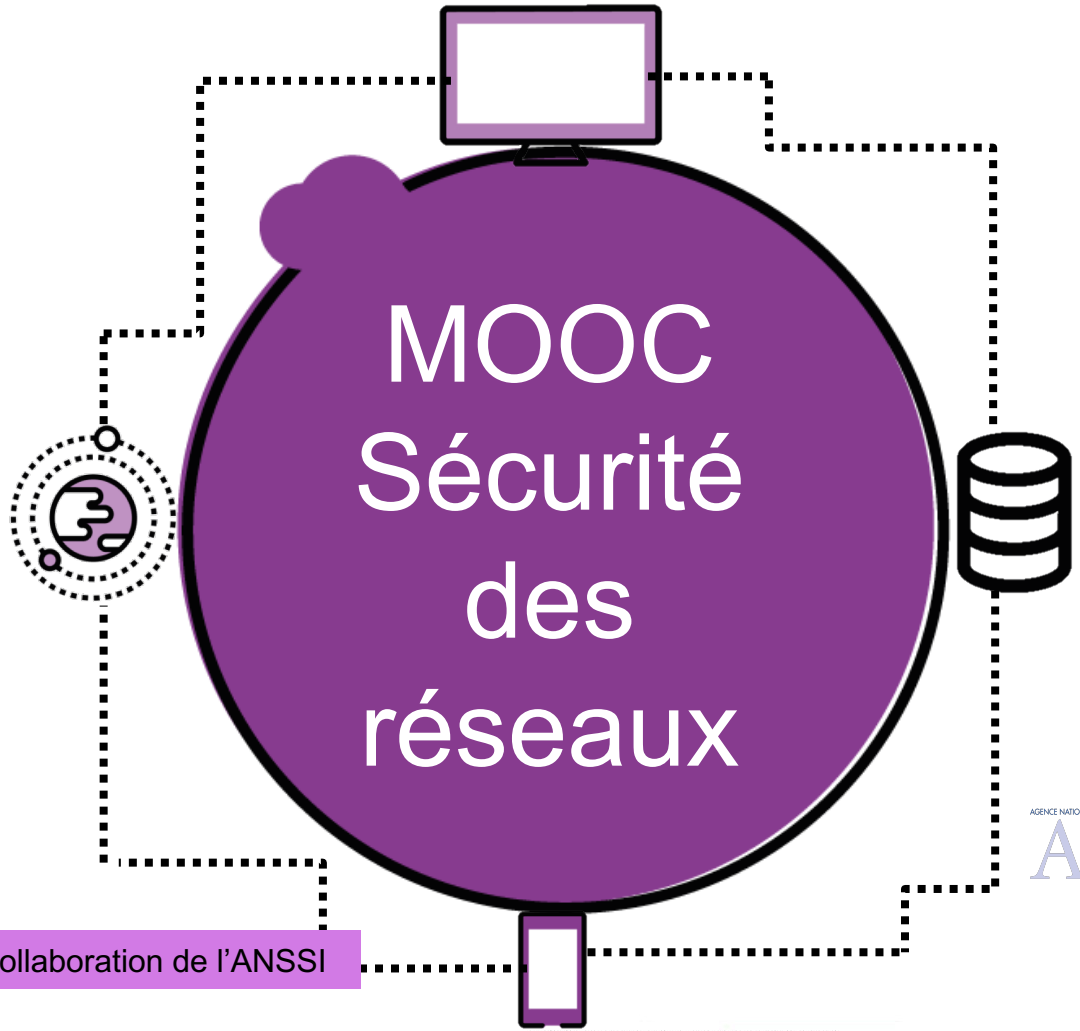



TELECOM SudParis

Une école de l'IMT

AIRBUS DEFENCE & SPACE

TELECOM Nancy

Ingénieurs du numérique • Inspiring your digital future

Inria

MINES Saint-Étienne

TELECOM ParisTech

Une école de l'IMT

Avec la collaboration de l'ANSSI

AGENCE NATIONALE DE LA RECHERCHE ANR

flirt

Formations Libres et Innovantes Réseaux & Télécom

Patrick & Lina Drahi Foundation

# Présentation

- MOOC pour Massive Open Online Course
- Thème : sécurité dans les réseaux informatiques
- Fait partie de la collection de MOOCs de l'IMT (principe de réseaux de données, supervision des réseaux et des services, A la découverte des télécommunications, Principes des réseaux de données, Routage et qualité de service dans l'Internet, Comprendre le cœur d'internet : les réseaux d'opérateurs, Les Réseaux Locaux, Supervision de Réseaux et Services, Objectif IPv6)
- Financement :
  - 50% ANR (projet FLIRT)
  - 50% Fondation Patrick et Lina Drahi
- Participation active de :
  - 4 écoles de l'IMT et INRIA Grand Est
  - Airbus Defense & Space
  - ANSSI

# Positionnement et contenu

- Positionnement exclusif sur **la sécurité dans les réseaux** – du point de vue théorique et pratique
- Prérequis en informatique (ligne de commandes) et en réseau (DNS, adressage, routage, ARP, ICMP) – assimilables en suivant d'autres MOOCs
- Positionnement plus ambitieux (de par la partie pratique importante ) que les autres MOOCs du domaine :
  - ✓ MOOC cybersécurité de l'ANSSI : un guide de bonnes pratiques, pour un bon usage de l'Internet
  - ✓ MOOCs « Arithmétique : en route vers la cryptographie » et « Code-based Cryptography » : cryptographie
  - ✓ MOOC « Access control » (Authentification, IAM, pas de TP)
  - ✓ MOOC « Introduction to cyber security » (logiciel et réseau, pas de TP)
  - ✓ MOOC « Cyber attacks countermeasures » : cryptographie appliquée (authentification, SSL), p s de TP
  - ✓ « proactive computer security » (pentesting, pas de TP)
  - ✓ MOOC « Network Security » de Rochester Institute of Technology (https://www.mooc-list.com/course/network-security-edx) : focalisé sur les attaques (Port scanning, Password cracking, exploits, DHCP, DNS, and Switch Attacks, MITM), la détection d'intrusions (snort), les preuves, et la défense face à des attaques (ACL) – pas de TP a priori

- Public attendu : les étudiants en enseignement supérieur et des professionnels en entreprise [administrateurs réseaux, intégrateurs, techniciens supérieurs Réseaux expérimentés]

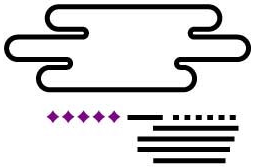
# Contenu

- 18 leçons sous format de vidéos,
- 2 interviews,
- 11 TPs,
- 1 bureau d’études

- 5 semaines  5h de travail personnel par semaine
- Evaluation par quiz qui portent sur les leçons, TPs, bureau d’études

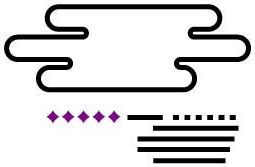
# Contenu plus détaillé

- Semaine 0 : Installation de l’environnement et test de connaissances
- Semaine 1 : Attaques liées aux réseaux (4 vidéos de cours sur les menaces de couche MAC, IP, transport et applications, 4 TPs permettant d'expérimenter ICMP redirect, ARP spoofing, session hijacking, dont 1 TP sur le vol de cookies HTTP)
- Semaine 2 : Mécanismes de filtrage (6 vidéos de cours sur le NAT et les différents types de filtrage - couche réseau, avec/sans état, applicatif, DPI - et 4 TPs permettant de tester et configurer les différents filtres, les VLANs, les proxys)
- Semaine 3 : VPNs et protocoles de sécurité (5 vidéos de cours sur les éléments protocolaires et cryptographiques utiles, certificats électroniques et PKI, ainsi que les protocoles de confidentialité TLS et IPsec, 3 TPs pour expérimenter les certificats électroniques et de configurer des VPNs)
- Semaine 4 : Synthèse des semaines précédentes et introduction des mécanismes IDS/IPS et de supervision de réseaux (2 vidéos de cours, 2 interviews sur la supervision de réseaux et le rôle des CERT, ainsi qu'un TP plus long permettant de valider les acquis)
- Semaine 5 : 2 vidéos de cours sur les architectures de sécurité, 1 bureau d’étude sur les aspects méthodologiques sur la construction d’une architecture de sécurité et des aspects méthodologiques : réglementation, normes, analyse de risques, politiques de sécurité, audit) et évaluation



# Compétences attendues

- Connaître les principales menaces contre les réseaux informatiques et les  vulnérabilités sur chaque couche/protocole
- Comprendre les principes d'exploitation des vulnérabilités
- Connaître les différents mécanismes de filtrage, les protocoles de sécurité (IPsec, TLS, wifi), et les vlans
- Etre capable de configurer des règles de filtrage, des vlans et des VPNs IPsec
- Appréhender les outils d'analyse réseau et les outils suivants sous Linux : netfilter/iptables/conntrack/ndpi/ebtables/ipsec-tool/racoon et mod_security (apache)
- Savoir positionner de façon pertinente sur une architecture de réseaux les fonctions de sécurité de base



# Environnement Labtainers

- Machine Virtuelle hébergeant Labtainers (GNU/Linux) : indépendance vis-à-vis de l'OS d'accueil
- Conteneurs sur Docker : architectures de réseau relativement complexes (10 nœuds commutateurs, routeurs, serveurs, passerelles, terminaux…) à ressources réduites
- GNU/Linux : variété des outils d'attaques/protection existants
- Choix de TPs existants dans Labtainers
- Instances locales : mode hors ligne
- Solutions libres : adaptabilité, coûts
- Evaluations automatisées

# Conclusions

- 1ère session : fin 2019, puis 1 à 2 sessions MOOC par an
- La suite :
  - Enrichir la suite de TPs réseaux/sécurité de Labtainers (licence CC BY NC SA)
  - Formation certifiante (parcours de MOOC)
  - Traduction en anglais
  - Certification CyberEdu