Syllabus de la Voie d'Appronfondissement

Sécurité des Systèmes et des Réseaux

(VAP SSR)

Responsable :	**Gregory Blanc** **Email :** gregory.blanc@telecom-sudparis.eu
Co-responsables :	**Christophe Kiennert** **Email :** christophe.kiennert@telecom-sudparis.eu **Olivier Levillain** **Email :** olivier.levillain@telecom-sudparis.eu

1 Objectifs et compétences

Objectifs

La cybersécurité est aujourd'hui un enjeu essentiel pour nos sociétés modernes. Avec les évolutions des technologies (Cloud, Big Data, Internet des Objets, etc.) et des vecteurs d'attaque, les entreprises doivent disposer de spécialistes et d'experts en sécurité capables de protéger les informations sensibles et de suivre l'évolution des menaces et des vulnérabilités.

La situation a évolué récemment avec la réglementation européenne (NIS), qui impose désormais aux opérateurs de services essentiels de mettre en place des mesures de sécurité sur leurs systèmes d'information. C'est notamment aux personnels actuels et futurs de ces opérateurs que cette formation s'adresse.

Avec une pénurie de main d'œuvre en Europe estimée en 2019 à 291 000 emplois par l'*International Information System Security Certification Consortium*, un effort conséquent en formation est nécessaire, afin de, ne serait-ce que, pourvoir les nouveaux postes qui se créent. Afin de contribuer à cet effort, cette VAP se propose de former des ingénieurs aux techniques de sécurisation qui peuvent être utilisés dans les systèmes et les réseaux en vue d'assurer l'authentification des utilisateurs, protéger l'accès aux informations, préserver la confidentialité et l'intégrité des données.

Un point essentiel de ce cursus est d'être en adéquation avec les besoins du marché, c'est pourquoi l'implication des industriels est forte et une grande part du temps est consacrée aux aspects pratiques.

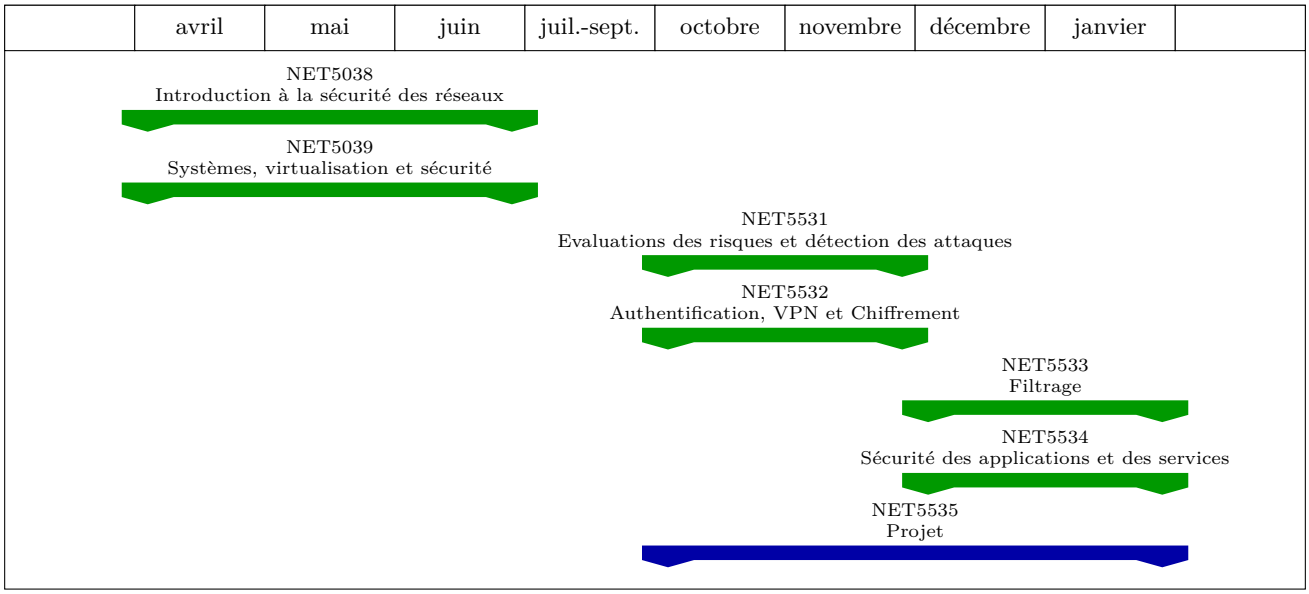
Compétences

Les compétences acquises au cours de cette formation permettront aux participants :
- évaluer les risques et les failles inhérentes aux systèmes et réseaux informatiques
- auditer un réseau et préconiser des outils de prévention et de détection
- concevoir et appliquer une politique de sécurité
- préconiser et déployer des méthodes de protection des échanges de données basés sur des méthodes d'authentification, de tunneling ou de chiffrement
- définir et mettre en œuvre une politique de filtrage basée sur les contraintes et besoins de l'entreprise
- concevoir et mettre en œuvre des architectures réseaux et systèmes sécurisées globales

Outre le diplôme d'ingénieur de Télécom SudParis, cette VAP permettra aux étudiants (sous réserve de satisfaire aux critères de validation spécifiques à la convention de collaboration signée entre Télécom SudParis et l'ANSSI) d'obtenir le titre d'*Expert en Sécurité des Systèmes d'Information* (ESSI) délivré par l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI).

2 Contenu de la formation

Partie académique



Stage ingénieur

À partir du mois de février, les étudiants partiront en stage ingénieur, pour une durée de 24 semaines.

Présentation du programme

Code	Intitulé du cours	Volume horaire [1]				Crédits
		Prés.	Proj.	TPers.	Total	ECTS
Semestre 8						
NET5038	Introduction à la sécurité des réseaux	45		45	**90**	5
NET5039	Systèmes, virtualisation et sécurité	45		45	**90**	5
Semestre 9						
NET5531	Evaluations des risques et détection des attaques	45		45	**90**	5
NET5532	Authentification, VPN et Chiffrement	45		45	**90**	5
NET5533	Filtrage	45		45	**90**	5
NET5534	Sécurité des applications et des services	45		45	**90**	5
NET5535	Projet	5	220		**225**	8
Stage ingénieur		*24 semaines*				30

1. Les volumes horaires correspondent au temps de cours en présentiel (Prés.), au temps dédié dans l'emploi du temps aux projets (Proj.), au temp de travail personnel estimé pour chaque module (TPers.), et au volume horaire total (Total).

2.1 NET5038 : Introduction à la sécurité des réseaux

Responsable : Christophe Kiennert

Volume horaire : 45h en présentiel, 45h de travail personnel, soit **90h** au total

Crédits ECTS : 5 crédits ECTS

Période : avril-juin

Objectifs du cours et compétences acquises :

À l'issue de ce module, les étudiants seront capables de :

- connaître les risques associés à la cybercriminalité et identifier les outils de protection associés (cybersécurité) ;
- configurer un réseau en mobilisant leurs connaissances sur les protocoles TCP/IP ;
- identifier et découvrir les risques associés au serveur LDAP ;
- connaître et appliquer les techniques de filtrage réseau sur les routeurs ;
- connaître les moyens techniques et non techniques (outils, protocoles et procédures) de protection des systèmes d'information dans le cyberespace ;
- connaître la typologie des menaces et les scénarios de cyber-attaques ;
- étudier les modèles formels de contrôle d'accès logique et les appliquer dans la mise en œuvre d'une politique de sécurité ;
- appréhender les enjeux de l'intelligence économique et du métier de RSSI ;
- réaliser un projet bibliographique en anglais sur un sujet de sécurité (1ère partie).

Contenu détaillé du cours :

- Rappels TCP/IP : architecture, adressage, routage, services réseaux, etc.
- Sécurité et LDAP
- Mécanismes de filtrage réseaux
- Cybercriminalité, cybersécurité et cyberdéfense
- Modèles de contrôle d'accès : DAC, MAC, RBAC
- Intelligence économique
- Métier RSSI
- Projet bibliographique (poursuivi et évalué en NET5039)

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + projet en binôme (12h) + examen (3h)

Modalités d'évaluation : Examen

2.2 NET5039 : Systèmes, virtualisation et sécurité

Responsable : Joaquin Garcia-Alfaro

Volume horaire : 45h en présentiel, 45h de travail personnel, soit **90h** au total

Crédits ECTS : 5 crédits ECTS

Période : avril-juin

Objectifs du cours et compétences acquises :

À l'issue de ce module, les étudiants seront capables de :

- identifier les problématiques liées à la sécurité des architectures des systèmes d'information actuels (architectures Web, architectures pour les technologies de virtualisation, architectures décentralisées de type blockchain) ;
- consolider la compréhension de la sécurité du poste de travail et des outils ou logiciels associés aux architectures des systèmes d'information choisis (navigateurs Web, hyperviseurs, portefeuilles Bitcoin) ;
- expérimenter avec des mécanismes d'attaque (injection de malware, cross-site scripting) en examinant les vulnérabilités des architectures des systèmes d'information choisis tout en comprenant les conditions nécessaires pour la mise en place des attaques et leur détection avec des outils de type détection d'intrusions ou des activités de type *Capture the Flag* (CTF) ;
- produire et défendre en anglais un projet bibliographique sur un sujet de sécurité des systèmes d'information, réalisé en binôme, tout en développant un sujet relatif au programme du cours, par la production d'un rapport technique, qui sera ensuite publiquement défendu devant un jury composé des intervenants de cours.

Contenu détaillé du cours :
- Architectures des systèmes d'information
- Architectures et usages de la technologie blockchain
- Architectures des services Cloud et des applications Web
- Attaques, exploitation et activités de type *Capture the Flag*
- Projet bibliographique

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + projet en binôme (12h) + examen (3h)

Modalités d'évaluation : Examen + rapport + soutenance

2.3 NET5531 : Evaluations des risques et détection des attaques

Responsable : Grégory Blanc

Volume horaire : 45h en présentiel, 45h de travail personnel, soit **90h** au total

Crédits ECTS : 5 crédits ECTS

Période : octobre – novembre

Objectifs du cours et compétences acquises :

À l'issue de ce module, sur un cas d'étude de réseau informatique ou industriel simple, mais réaliste, l'étudiant pourra :
- identifier les risques, découvrir les vulnérabilités et évaluer la sécurité du réseau ;
- appréhender la démarche d'analyse de risque EBIOS et employer les outils d'audit d'un réseau.

Sur une application Web réaliste, l'étudiant est capable de mettre en oeuvre des techniques d'audit d'application Web et réaliser un rapport d'audit.

Quel que soit le contexte, l'étudiant aura acquis les compétences suivantes :
- expliquer le fonctionnement des centres de sécurité opérationnelle (SOC) et de réponse à incident (CERT) ;
- expliquer la méthodologie de la réponse à incident et inspecter partiellement des cas d'études.

Contenu détaillé du cours :
- Sécurité des réseaux : menaces et parades
- Méthodologies d'Analyse des Risques
- Audits techniques
- Réponse à incident
- Sécurité des systèmes industriels

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + examen (3h)

Modalités d'évaluation : TP noté + examen

2.4 NET5532 : Authentification, VPN et Chiffrement

Responsable : Maryline Laurent

Volume horaire : 45h en présentiel, 45h de travail personnel, soit **90h** au total

Crédits ECTS : 5 crédits ECTS

Période : octobre – novembre

Objectifs du cours et compétences acquises :

À l'issue du module, les étudiants pourront :
- mettre en œuvre les services d'authentification et de chiffrement, notamment sur des boitiers Stormshield et sur des systèmes Linux ;
- citer et décrire les mécanismes de gestion d'identité tels que le SSO (*Single Sign On*) et les infrastructures de clefs publiques (PKI, *Public Key Infrastructure* en anglais) ;
- pratiquer la génération et l'utilisation de certificats électroniques à l'aide de la librairie OpenSSL ;
- connaître les mécanismes utilisés dans les VPNs (*Virtual Private Networks*) ;
- configurer des VPNs basés sur IPsec, notamment sur des boitiers Stormshield et sur des systèmes Linux ;
- expliquer la cryptographie, discuter les algorithmes de chiffrement les plus couramment utilisés et appréhender les mécanismes avancés ;
- exprimer les bases et les enjeux de sécurité des protocoles associés aux nouveaux services.

Contenu détaillé du cours :
- Architecture et protocoles d'authentification (EAP, AAA)
- Solutions PKI et SSO (Single Sign On), protocoles d'authentification
- Cryptographie : mécanismes mathématiques et algorithmes, protocoles et applications
- VPN (Réseaux privés virtuels) et IPsec
- Mise en œuvre d'un VPN et du NAT
- Mise en œuvre de la génération et de l'utilisation de certificats électroniques
- Protocoles de Sécurité

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + examen (3h)

Modalités d'évaluation : TP noté + examen

2.5 NET5533 : Filtrage

Responsable : Olivier Paul

Volume horaire : 45h en présentiel, 45h de travail personnel, soit **90h** au total

Crédits ECTS : 5 crédits ECTS

Période : décembre – janvier

Objectifs du cours et compétences acquises :

À l'issue de ce module, les étudiants auront acquis les compétence suivantes :
- connaitre les problèmes que les systèmes de filtrage visent à résoudre ainsi que les mécanismes qui peuvent déployer dans un réseau ;
- expliquer le fonctionnement de ces mécanisme de filtrage ;
- dans le cadre d'une politique de sécurité donnée, être capable de comparer l'utilité des mécanismes et de sélectionner le plus approprié ;
- mettre en œuvre les mécanismes de filtrage (à base de routeurs, firewalls) en tenant compte d'une politique de sécurité.

Contenu détaillé du cours :
- Introduction aux problèmes de filtrage (cours, 2 heures)
- TP filtrage sur architecture éclatée Cisco IOS FW, AWS SG et NACL et proxy WAF sous AWS (TP, 6 heures)
- Problèmes et techniques de filtrage pour les couches 2, 2.5 (cours, 3 heures)
- TP filtrage au niveau 2, 2.5 (TP, 6 heures)
- Architectures des outils de filtrage (cours, 6 heures)
- NAT, Filtrage et applications multimédia (cours, 3 heures)
- TP NAT et VoIP (TP, 4,5 heures)
- Techniques de traitement des déni de service (cours, 4 heures)
- TP filtrage avancé sur architecture intégrée Checkpoint (TP, 9 heures)

Méthodes et/ou moyens pédagogiques : Cours (18h) + TP (25,5h) + examen (1,5h)

Modalités d'évaluation : TP noté + examen

2.6 NET5534 : Sécurité des applications et des services

Responsable : Olivier Levillain

Volume horaire : 45h en présentiel, 45h de travail personnel, soit **90h** au total

Crédits ECTS : 5 crédits ECTS

Période : décembre – janvier

Objectifs du cours et compétences acquises :

À la fin de ce module les étudiants devront :
- comprendre les problématiques de sécurité des applications informatiques et appréhender les principales stratégies de prévention et de résolution de ces problèmes ;
- expérimenter les méthodes d'injection de code dans les applications et les techniques permettant d'y résister ;

— comprendre les relations entre la sécurité des applications et l'établissement de réseaux de confiance en particulier pour les applications Java, et les distributions Linux ;
— comprendre les problématiques de sécurité associées à l'échange de documents ;
— comprendre le fonctionnement des virus et des anti-virus ;
— comprendre les interfaces entre les applications et le système d'exploitation (Linux / Windows + Active Directory).

Contenu détaillé du cours :
— Sécurité des applications en Java
— Sécurité Windows et Active Directory
— Virus et anti-virus
— Sécurité des documents
— Sécurité Linux
— Sécurité des développements

Méthodes et/ou moyens pédagogiques : Cours intégré (42h) + examen (3h)

Modalités d'évaluation : TP noté + examen

2.7 NET5535 : Projet

Responsable : Olivier Paul

Volume horaire : 5h en présentiel, 220h de projets, soit **225h** au total

Crédits ECTS : 8 crédits ECTS

Période : octobre – janvier

Objectifs du cours et compétences acquises :
À la fin du module, les étudiants peuvent :
— dégager une problématique associée à un sujet ;
— analyser l'état de l'art associé à cette problématique ;
— apporter une réponse d'ingénieur à cette problématique ;
— concevoir et réaliser un prototype répondant à cette problématique ;
— présenter de manière écrite et orale (sous la forme d'un rapport, d'un poster et d'une présentation orale) les résultats obtenus.

Contenu détaillé du cours :
Après une présentation des projets, les étudiants disposent d'un volume horaire important pour développer leur sujet et faire une restitution écrite et orale.

Les sujets sont proposés soit par des enseignants-chercheurs, soit par des industriels, qui jouent le rôle de tuteurs du projet pendant la durée du module.

Voici quelques exemples de projets :
— démonstrateur de canaux cachés réseau ;
— étude des normes et standards de la détection d'intrusion ;
— mise en œuvre d'un protocole basé sur du zero-knowledge dans la sécurisation d'une messagerie ;
— analyse de la sécurité NFC en pratique ;
— étude des attaques sur le réseau GSM avec OpenBTS ;
— étude de la résistance aux attaques des claviers virtuels javascript ;
— évaluation de la sécurité d'une application web ;
— analyse comportementale de malwares et génération de signatures.

Méthodes et/ou moyens pédagogiques : Projet en binôme

Modalités d'évaluation : Rapport + soutenance