MAJEURE SRS

Présentation du programme 2020

Référence : 2020_SRS_PROGRAMME_MAJEURE_191031.docx
Le Kremlin-Bicêtre octobre 2019
Ce document comprend 20 pages.

EPITA – Direction des Études	

Mises à jour				
Indice	***Date***	***Nom***	***Mise à jour***	
			Page	*Nature*
1 (initial)	***31/10/19***	Christian Dujardin		

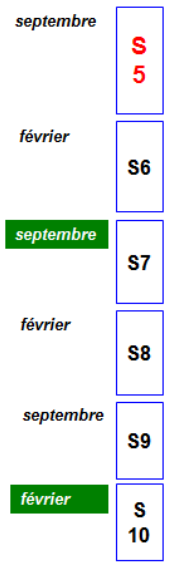
SOMMAIRE

1. MAJEURE SRS DU CYCLE INGENIEUR DE L'EPITA

1.1. REMARQUE

Ce document présente le programme de la majeure Système Réseau et Sécurité (SRS) du cycle ingénieur en cursus initial.

1.2. SITUATION DE LA MAJEURE SRS DANS LE CURSUS



La majeure SRS :

- Débute en semestre S8 (ING2)
- Continue en semestre S9 (ING3)
- Et se termine en semestre S10 (ING3) via le stage de fin d'études. Le stage de fin d'études (6 mois) est réalisé en entreprise dans le domaine de la sécurité.

1.3. ORGANISATION DU CURSUS DE L'ÉCOLE EPITA

Un semestre est décomposé en UE (Unités d'enseignement) thématiques

Une UE regroupe des activités d'une même thématique :

- Cours magistraux
- Projets
- Conférences
- Travaux Pratiques

Chaque activité est évaluée selon les modes suivants :

- Examen en salle (Devoir sur Table)
- Contrôle continu (durant les cours)
- Rapport et soutenance
- Rendu de projets

La suite de ce document présente :

- Le cursus (libellé des activités et volume horaire)
- Les résumés des activités pédagogiques connexes à la sécurité

2. PROGRAMME DES 450H DU SEMESTRE S8 (ING2)

Heures représentant des heures de face à face pédagogiques (Cours, TP, TD, Conférences)

UE	Code-COUR	INTITULE	Total
[SYS1]-Système et Sécurité	ACDA	Windows Active Directory	40
	ADLIN	Administration Linux Avancée, automatisation et orchestration	12
	HTS	Harmonisation Technologique Système	36
	NSE1	Noyau et Systèmes d'exploitation [1]	12
	R_SR1	Rush 1 : Infrastructure haute-disponibilité	12
			112
[RSS1]-Réseaux et sécurité	CLAN	LAN concepts	12
	CMAN	MAN concepts	12
	CRYPA	Cryptologie Moderne pour l'Ingénieur	12
	FNSA	Network and Security [Mise en œuvre technologie FORTINET]	12
	IAM	Identity & Access Management	15
	TATT	Sécurité : Analyses et Défenses Générales	18
	WAN	WAN : concepts	12
			93
[SOR1]-Sécurité Organisationnelle	ARS2	Management de la Cybersécurité et de la Cyberdéfense	18
	DACE	Datacenter : Infrastructure et services	12
	MOSE	Mobilité & Sécurité Applications Mobiles	12
	POLSR	Politique de Sécurité (majeure SRS)	12
	SCCO	Sécurité et conduite du changement dans les organisations	12
	SECUP	Sécurité dans les projets et Audit de Sécurité	12
	SIDU	Sécurité des systèmes industriels	12
	SOC	Sécurité opérationnelle (SOC, CERT, etc)	12
			102
[MCE4]-Management et Connaissances pour l'Entreprise	ARS1	Cybersécurité et Cyberdéfense	15
	DBRE	Droit des propriétés intellectuelles	12
	DRIN	Droit de l'Internet	12
	ENAC4	Sport, Communication, vie associative et entrepreneuriat [3]	
	NMSS	Normes et Méthodologies dans la Sécurité Numérique	15
	P_INMA	Projet Inter-majeure [SIGL-SRS-TCOM]	12
	R_DEFNET	Exercice Défense Nationale	8
	RE_S4	Conférences Technologiques (S8)	21
			95
[SG4]-Sciences Générales	ANDO	Analyse de données	12
	CRYPI	Principes mathématiques pour la Cryptologie	12
	ROST	Recherche Opérationnelle Stochastique	12
	TEC1	Tests classiques 1	*12*
			48
		Total général	***450***

Les descriptifs des activités sont présentés dans le chapitre 4 dans la suite de ce document.

3. PROGRAMME DES 450H DU SEMESTRE S9 (ING3)

Heures représentant des heures de face à face pédagogiques (Cours, TP, TD, Conférences)

UE	Code-COU	INTITULE	Total
[SOR2]-Sécurité Organisationnelle	ARS3	Cybersécurité et Cyberdéfense [niveau avancé]	24
	ELSI	Signature Electronique	15
	IESE	Intelligence Economique et protection du patrimoine informatic	12
	VVRI	Veille en vulnérabilité et Réponses aux incidents	12
			63
[RSS2]-Réseaux et sécurité	IPAV	IP-TCP-Avancé	42
	MWAV	Réseaux MAN/WAN avancé	12
	MXAN	Management et mise en pratique MAN/WAN (Business & IT)	12
	R_SR2	Rush 2 : Développement SAN	18
	TATT2	Sécurité : Analyses et Défenses Réseau et Web	24
	VIRO	De la Virologie aux Malwares	42
	WSEC	Windows et Sécurité (niveau avancé)	35
			125
[SYS2]-Sécurité des Systèmes & Système d'information	FIBI	Sécurité & Reverse Engineering	12
	FIBI2	Sécurité & Reverse Engineering [niveau avancé]	12
	IBMZ1	zSeries Academic Initiative - 1	12
	IBMZ2	zSeries Academic Initiative - 2	12
	NSE2	Noyau et Systèmes d'exploitation : Aspect Virtualisation	42
	SDNE	Architecture SDN	12
	VIRLI	Architectures de Virtualisation (légère / conteners)	24
			96
[MCE5]-Management et projets transversaux	BIWI	Business Week (simulation de création d'entreprise)	30
	ENAC5	Sport, Communication, vie associative et entrepreneuriat [4]	
	FIC_D	Organisation et préparation du challenge FIC (Lille)	30
	P_INMA	Projet Inter-majeure [SIGL-SRS-TCOM]	15
	RE_S5	Conférences Technologiques et Forum (S9)	24
	RE_SFE	Soutenances des Stages de Fin d'études	12
	SYNTH_SRS	Synthèse compétences acquises en majeure	4
	TMS	Technologies, Offres et marché de la sécurité	15
	MINEURE	Mineure [en libre choix]	36
			166
Mineure générique [CE]	DRTR	Droit du travail	
	LCE_EPICE_	Libre choix d'un cours dans la liste LCE_Cex	
	LCE_EPICE_	Libre choix d'un cours dans la liste LCE_Cex	
Mineure de création d'entreprise	EPISTART	Mineure Entrepreneuriat	
Mineure d'Intelligence Economique	IEAN	Intelligence Economique : Analyser	
	IEINF	Intelligence Economique : Intervenir et dimensionner le terrain	
	IEREP	Intelligence Economique : Répondre et Influencer	
Mineure Finances	MAFI3	Mathématiques & Finances de marché	
	PROFI	Produit Financiers	
	SIBOT	Système d'Information Bancaire et Outils Technologiques	
Mineure e-santé et imagerie médicale	EPISANTE	Mineure e-santé et imagerie médicale	
Total Mineure e-santé et imagerie médicale			
[LCE_CEx] Liste des matières électives	ANFI	Analyse Financière des Entreprises	
	BUWI	Business Writing	
	CEDU	Comprendre le développement durable	
	DRCO	Droit des contrats	
	DRIN	Droit de l'Internet	
	ECO1	Macro Economie (niveau 1)	
	EGEA	Internet Geopolitics	
	MKGR	Modélisation économique et modèles de marchés	
	RSE	Responsabilité Sociétale des Entreprises	
	SAME	Sales and Marketing for Engineers	
		Total général	450

Les descriptifs des activités sont présentés dans le chapitre 4 dans la suite de ce document.

4. RÉSUMÉ DES ACTIVITÉS CONNEXES À LA SÉCURITÉ

4.1. [ACDA] ACTIVE DIRECTORY & WINDOWS 2008 (NIVEAU AVANCÉ)

A la fin de ce cours, les étudiants devront maîtriser l'implémentation et la configuration des services de domaine Active Directory dans un environnement d'entreprise de dimension internationale.

Plan :

A] Configuration et sécurisation d'un serveur Windows [12h00]

B] Paramétrage et sécurisation du service DNS sous Windows [6h00]

C] Paramétrage et sécurisation du service DHCP sous Windows [1h30]

D] Paramétrage et sécurisation du service NTP sous Windows [0h30]

E] Kerberos – Les bases [0h30]

F] AD – Les bases [3h00]

G] AD - Structure logique [6h30]

H] AD - Structure physique [2h00]

I] AD – Authentification [4h00]

J] AD – Gestion de la sécurité [3h00]

K] Contrôle d'accès sur les objets [1h00]

4.2. [ACMA] ACCESS MANAGEMENT

L'objectif est de parcourir l'ensemble des méthodes d'authentifications considérées comme standards et d'analyser les infrastructure techniques associées. A la fin du cours les étudiants doivent être capables de choisir en fonction des cas la meilleure solution d'authentification et d'en comprendre l'impact sur le système d'information.

Plan :

- Acces Management,
- Infrastructure d'authentification,
- TP de 4h.

4.3. [ADLIN] ADMINISTRATION LINUX AVANCÉE

Maîtrise, par la pratique, ludique, de la ligne de commande et des outils pour l'administration système et réseau avancée des machines Unix.

L'étudiant est notamment amené à :

- appréhender les techniques de démarrage d'une distribution GNU/Linux (bootloader),
- découvrir, s'insérer puis modifier un réseau IP existant,
- installer et configurer sa distribution pour un usage serveur,
- savoir administrer un nom de domaine.

Une part importante des acquis concernent tout particulièrement la sécurité relative aux points abordés (notamment face aux problèmes de sécurité physique ou lié aux configurations installées) ; ainsi qu'une introduction aux principes de DevOps.

En complément : sensibilisation à la messagerie sécurisée (PGP) et à la veille technologique dans le domaine.

4.4. [ARS1] CYBERSÉCURITÉ ET CYBERDÉFENSE

Introduction à la SSI (Sécurité des Systèmes d'Information) et aux contrôles des accès logiques en entreprise.

Connaissance des technologies d'authentification centralisée, de gestion d'identités, PKI, SSO, méthodologie de classification de l'information, gestion des habilitations...

Sensibilisation d'un point de vue RSSI et/ou MOA sécurité

Plan :

- Introduction à la sécurité
- Introduction à l'authentification centralisé
- Introduction au SSO + PKI
- PKI
- Gestion des identités et des habilitations

Chaque cours est suivi d'un dossier à réaliser permettant l'approfondissement d'une technologie.

4.5. [ARS2] MANAGEMENT DE LA CYBERSÉCURITÉ ET DE LA CYBERDÉFENSE

Cette partie permet aux élèves d'effectuer des recherches en groupe et de présenter à la promotion par des exposés un état de l'art sur leur sujet.

Les cours présentent d'un point de vue entreprise les concepts suivants :

1. Introduction à la lutte antivirale et des vulnérabilités
2. Architecture et organisation des raccordements extérieurs (Tierce Maintenance, filiale, architecture mail, proxy, …)
3. Audit et contrôle de l'infrastructure
4. Modèle formel de la sécurité

A l'issue de ce cours l'élève connaitra le panorama des problématiques de sécurité (technique et juridique) classiques d'un grand compte

4.6. [ARS3] GESTION OPÉRATIONNELLE DE LA SÉCURITÉ EN SSI.

Connaissance en SSI sur l'organisation de la gestion opérationnelle de sécurité

Présentation du cadre juridique français pour la mise en place de solution de sécurité entreprise.

L'étudiant devra pourvoir à l'issu de ce cours choisir des solutions de sécurité adaptées à l'entreprise d'un point de vue organisationnel et juridique.

Plan :

- Cadre juridique de la Cybersurveillance
- Organisation de l'anticipation (veille menaces et des vulnérabilités)
- Organisation et traitements des incidents (malveillance ou abus)
- Organisation de la gestion de crise

4.7. [CLAN] LAN CONCEPTS

Donner aux étudiants les connaissances techniques sur les divers composants entrant dans une architecture de réseaux locaux de type immeubles, building, usines ou autres.

Plan :

- Introduction
- Les divers protocoles de réseaux locaux
- Les ponts et la commutation
- Architecture building
- Introduction aux wireless Lan et aux Pan

4.8. [CMAN] MAN CONCEPTS

Donner aux étudiants les connaissances techniques sur les divers composants entrant dans une architecture de réseaux métropolitains au sein d'une agglomération.

Plan :

Introduction

- Historique des réseaux métropolitains
- Les principes de base d'une architecture réseau locale

Les divers protocoles

- PDH
- SDH
- WDM
  - C-WDM
  - D-WDM

Les accès opérateurs

- Types d'interfaces
- Niveau de disponibilité
- Les contraintes

Les offres constructeurs d'équipements MAN

- Nortel / Cisco / Ciena etc

Comment choisir son opérateur MAN

4.9. [CPCSA] CHECK POINT CERTIFIED SECURITY ADMINISTRATOR

Notre partenaire, la société CheckPoint organise dans l'école une adaptation de son offre de formation destinée à sa cible entreprise :-

- Installation d'un Firewall + Management Check Point, configuration système, manipulation/commandes du clish
- Création et Mise en place de politiques de sécurités (règles, objets, etc…)
- Utilisation des outils de Monitoring et le Logs
- Mise en place et configuration de la NAT sur les objets (Static NAT, Hyde NAT, etc..)
- Création et mise en place de règles de sécurité par rapport à des utilisateurs d'un AD
- Les Labs seront entrecoupés de Présentations Techniques des fonctionnalités.

4.10. [CRYAP] CRYPTOLOGIE APPLIQUÉE

Comprendre et appliquer les mécanismes de sécurité fournis par la cryptographie

- Rappel de cryptographie (définitions, historique, familles d'algorithmes et primitives cryptographiques)
- Cryptographie appliquée et cas d'usage courant (confidentialité du courrier électronique, tunnels VPN, authentification, vérification d'intégrité, etc.)
- Les infrastructures de gestion de clés et les réseaux de confiance (x.509 et PGP) :
- Protocoles sécurisés : SSH
- Protocoles sécurisés : SSL/TLS

4.11. [CRYPA] CRYPTOLOGIE MODERNE POUR L'INGÉNIEUR

Plan :

- La cryptographie asymétrique : RSA pour le chiffrement et la signature , Rabin, Diffie-Hellman pour l'échange et la mise en accord de clés, introduction aux courbes elliptiques.

- Le reste du cours est consacré à des cCompléments : SSL/TLS, quelques cryptanalyses de RSA ou comment calculer une « bonne » clé RSA, PGP, les problèmes de OpenSSL depuis 10 ans, derniers problèmes récents de la cryptographie, stéganographie et watermarking, « géocryptographie » : comprendre les problèmes juridiques de l'usage de la cryptographie dans le monde réel (cas BERNSTEIN /ITAR).

4.12. [CRYPI] PRINCIPES MATHÉMATIQUES POUR LA CRYPTOLOGIE

Plan :

- Une courte histoire de la cryptographie (âge artisanal (<1918), âge technique (1919-1975), âge paradoxal (>1976)

- Bases mathématiques et algorithmiques (Groupes, anneaux et corps, nombres premiers et factorisation, PGCD et PGCD étendu, théorème de Bézout, petit théorème de Fermat (et d'Euler), inversion modulaire, théorème des restes chinois, les problèmes : factorisation et logarithme discret, tests de primalité probabilistes et déterministes, exponentiation modulaire rapide, multiprécision, générateurs de nombres pseudo-aléatoires)

- La cryptographie sans secret (fonctions à sens unique, fonctions de hachage)

- La cryptographie symétrique : de DES/2DES/3DES à l'AES, authentification par MAC

4.13. [DACE] DATACENTER : INFRASTRUCTURE ET SERVICES

Les applications sont aujourd'hui le cerveau de nombreuses entreprises. Leur disponibilité est primordiale. Les données qu'elles traitent sont de plus en plus critiques. Leur volume augmente continuellement.

Les infrastructures et services associés à ces applications (serveurs, stockage, sauvegarde, virtualisation, hébergement, réseau…) sont en constante évolution. L'hébergement et le socle IT représentent des éléments primordiaux pour la performance, l'agilité et la sécurité des applications.

Le présent module a pour objectif de présenter, au travers de plusieurs cours, ces problématiques.

4.14. [DRIN] DROIT DE L'INTERNET

Aspects juridiques de la cybersécurité

Objectifs : Donner aux ingénieurs en cybersécurité le cadre légal dans lequel leur activité s'exercera.

Compétences :

- Vérifier la prise en compte des contraintes liées à la réglementation sur la protection des données à caractère personnel

- Connaître les atteintes aux systèmes de traitement automatisé de données et les sanctions associées

- Mettre en œuvre les exigences issues de la loi de programmation militaire

- Comprendre les enjeux juridiques de la cybercriminalité

4.15. [EGEA] INTERNET GEOPOLITICS

Architecture d'Internet
- Historique
- Gouvernance
- E-economie
- Argent sur Internet
- Comment les lois des états impactent Internet
- Les états impliqués dans le développement d'Internet
- E-mafia
- Internet et la Démocratie

4.16. [ELSI] SIGNATURE ELECTRONIQUE SÉCURISÉE

Ce cours propose d'appréhender les difficultés inhérentes à la mise en œuvre de la signature électronique au sein de projets réels à grande échelle.

L'un des objetifs est de faire prendre conscience aux élèves de la complexité des aspects organisationnels, juridiques et culturels d'une mise en œuvre effective de la signature électronique, malgrè son niveau de sécurité technique théorique (cryptographique).

Dans un premier temps, et après quelques rappels cryptographiques, la finalité ainsi que les principes techniques et organisationnels de la signature électronique sont présentés. On expose ensuite le corpus réglementaire menant à la signature électronique sécurisée en y détaillant l'ensemble des aspects organisationnels (autorité, politique et prestataire de certification) et techniques (HSM, SSCD, nomes, application de vérification de signatures, RGS, autres).

Les apports concrets proposés aux éléves sont la présentation du caractère complexe et vulnérable des mises en œuvres (travaux pratiques), l'utilisation d'un corpus normatif riche mais peu connu, la synthèse des textes principaux et surtout la prise de conscience d'une méconnaissance généralisée de ce que représente l'intérêt de la signature électronique au sein des entreprises elles-mêmes.

4.17. [FIBI] SÉCURITÉ & REVERSE ENGINEERING

L'objectif de ce module est de sensibiliser les étudiants aux techniques statiques et dynamiques utilisées pour l'analyse de fichiers binaires.

Cette connaissance permettra aux étudiants d'appréhender plus facilement les domaines tels que le forensics, l'analyse de malware, la protection logicielle et l'analyse de programme.

- Asm x86
- Format PE (COFF Microsoft)
- IDA Pro 5.0 (Hexrays)
- Debugging
- Hooking/Injection de code

4.18. [FIC_D] ORGANISATION ET PRÉPARATION DU CHALLENGE FIC (LILLE)

Travaux de groupe pour le challenge forensic du FIC

1) élaboration de scénarii d'attaque réalistes

2) recherche sur des vulnérabilités, des thématiques et des technologies imposées par les professeurs

3) mise en place du système d'information cible, réalisation de l'exploitation des vulnérabilités retenues (environ 5 par scénario)

4) récupération des éléments de compromission pour permettre aux participants de reconstituer l'agression par des analyses forensics

Les étudiants aborderont des aspects complexes d'intrusion, de forensic pour permettre la résolution du challenge et aussi de mesures anti-forensic pour compléter la difficulté de l'exercice ainsi préparé.

Les sujets de forensics explorés concernent (liste non exhaustive) les technologies suivantes :

Malware / Radio / Base de données / Firmware industriel / Browser add-on / Android / USB / RAT / Virtualisation / Social engineering / Bigdata / Firmware matériel embarqué (routeur, imprimante, caméra, …) / Web

4.19. [GRIC] GESTION DES RISQUES ET GESTION DE CRISES

Comprendre les méthodes d'analyse et de gestion des risques, aborder les aspects de la gestion de crises.

-Notions de base,

-Outils d'identification des risques,

-Méthodes d'évaluation des risques,

-Outils de traitement des risques,

-Les Systèmes d'Information de Gestion des Risques (SIGR).

-Les clés de la gestion de crise.

4.20. [IAM] IDENTITY MANAGEMENT

Introductions à l'exposition et la consommation sécurisées d'API avec les protocoles OAuth2, OpenID Connect, et les briques fonctionnelles d'API Management et d'Access Management

Plan :

- Rappels élémentaires sur les API REST
- Présentation des moyens historiques de s'authentifier auprès d'une API et de leurs limites
- Introduction aux failles les plus courantes (Top10 de l'OWASP) et leurs conséquences type
- Utilisation d'une API Gateway en tant que policy enforcement point
- Délégation d'autorisations via les protocoles OAuth2 et OpenID Connect, et au travers d'une brique d'Access Management

4.21. [IEAN] INTELLIGENCE ECONOMIQUE : ANALYSER

A]- Introduction Méthodologique

1) Accélération du changement

2) Approche classique de la stratégie vs. intelligence économique

3) Comprendre les changements (economiques, politiques et sociaux) qui s'opèrent depuuis 15 ans

4) Prendre la mesure de l'insuffisance des outils classiques d'analyses stratégique en matière d'analyse de l'environnement

B]- Analyser

1) comprendre des multiplicités des parties prenantes

2) comprendre les jeux d'acteurs

3) initier une réflexion stratégique

4) savoir réaliser une cartographie relationelle et une cartographie de positionnement

4.22. [IEINF] INTELLIGENCE ECONOMIQUE : INTERVENIR ET DIMENSIONNER LE TERRAIN

Comprendre le rôle central de l'intelligence économique et de la réputation pour la stratégie des entreprises, savoir cartographier les parties prenantes et analyser les risques et enjeux, comprendre les mécanismes de la formation de l'opinion, connaître les techniques d'influence et leurs supports.

Plan :

Présentation: intelligence économique et réputation de l'entreprise

I – Analyser

Cartographier les risques internes et externes de l'entreprise

II – Influencer

La réputation : un actif immatériel majeur pour les entreprises (histoire, définition, coût/valeur)

La formation de l'opinion : connaissance du fonctionnement des « key opinion leaders » : medias, réseaux sociaux, ONG, whistleblowers

Les techniques d'influence & la gestion de situations sensibles ou de crise : stratégie, méthodologie, actions, supports…

4.23. [IEREP] INTELLIGENCE ECONOMIQUE : RÉPONDRE ET INFLUENCER

Mettre en action la réponse opérationnelle conçue dans le cours IEINF :

A- Définir les 7 grandes familles d'opérations possibles

B- Méthodologies et cycle de vie d'une cyber-opération

B.1. Objectif

B.2. Analyse de risque

B.3. Méthode d'action (manoeuvre)

B.4. Chronologie (timeline)

B.5. BDA - MOE (mesure d'efficacité et des dommages éventuelles)

B.6. Définition des GO/No Go

B.7. Compte rendu et RETEX / Debriefing

C. Approfondir le risque (stratégique et tactique)

D. Concept de base d'une Cyber-Ops

E. Mise en application avec des machines virtuelles en organisant un jeu avec 2 équipes

4.24. [IESE] INTELLIGENCE ECONOMIQUE ET SÉCURITÉ

Introductions aux thématiques de l'Intelligence Économique (IE) en entreprise.
- Différents concepts liés à l'Intelligence Économique,
- Utilité pour les entreprises
- Cas concrets
- Travaux de recherche pour une cellule de veille

4.25. [IPAV] IP-TCP-AVANCÉ

Donner aux étudiants une connaissance pointue sur les aspects réseaux des technologies Internet, Extranet et Intranet.
- Comportement de IP sur les réseaux ATM (LANE, Classical IP)
- CIDR, VLSM
- SNMP V1/V2/V3
- Le multicast IP : IGMP, DVMRP, PIM D/SM
- Sécurité des réseaux IP : risques et parades
- QoS IP : DiffServ vs IntServ
-Les VPN IP (L2TP, PPTP, IPSec, MPLS), introduction à VPLS (L2 VPN sur IP MPLS)
- Mobile IPv4
-IPv6
-Mobile IPv6

4.26. [KSTO] COURS MICRO NOYAU SYSTÈME

Cours (sous forme exclusivement de projets) d'implémentation de noyau.
Il est composé 4 petits projets d'implémentation dans un noyau simplifié permettant de mettre en valeur les problématiques vues en cours :
* Projet 1 : Protection Mémoire
* Projet 2 : Events et Interruptions
* Projet 3 : Virtualisation mémoire et pagination
* Projet 4 : Scheduling et support userland

4.27. [KSTO2] COURS MICRO NOYAU SYSTÈME (#2)

Cours (sous forme exclusivement de projets) d'implémentation de noyau.
Il est composé 4 petits projets d'implémentation dans un noyau simplifié permettant de mettre en valeur les problématiques vues en cours :
* Projet 1 : Protection Mémoire
* Projet 2 : Events et Interruptions
* Projet 3 : Virtualisation mémoire et pagination
* Projet 4 : Scheduling et support userland

4.28. [MOSE] MOBILITÉ & SÉCURITÉ APPLICATIONS MOBILES

Introduction à la sécurité des usages mobiles en entreprise (ouverture du SI, enjeux sécurité, accès distants VPN, gestion de flotte, plateformes MDM/MAM/EMM, déploiement BYOD/COPE etc.) et des plateformes mobiles (modèle de sécurité Android/iOS, malware, développement sécurisé et distribution des applications, Top 10 OWASP mobile etc.).

4.29. [MWAN] RÉSEAUX MAN/WAN AVANCÉ

Donner aux étudiants une connaissance à la fois des divers besoins fonctionnels auxquels doit répondre une architecture WAN, mais aussi le pourquoi de l'évolution des réseaux WAN vers des réseaux du type MPLS et/ou Ethernet.

4.30. [NMSS] NORMES ET MÉTHODOLOGIES EN SSII

Afin d'aider l'Entreprise à gérer le cyber-risque qui pèse sur ses métiers, ses processus, son pa-trimoine informationnel, le cours s'attache à mettre en évidence l'apport INDISPENSABLE des Normes, Standards, Méthodologies, Bonnes Pratiques dans la constitution des POLITIQUES de SÉCURITÉ permettant la maîtrise de ses risques.

Après un positionnement de l'apport et des limites de ce matériel, le cours en présente un panel représentatif et en propose l'analyse.

L'ingénieur, et particulièrement en cybersécurité, est concerné par la sécurité des systèmes d'information qu'il peut être amené à concevoir, à évaluer, à administrer, à utiliser, à faire évoluer, à contrôler.

Le futur professionnel de la sécurité des SI doit disposer de la culture sécurité lui permettant d'aider à ap-préhender les risques et d'être force de réflexion et de proposition en la matière vis à vis des différents acteurs intervenant sur le système d'information de l'entreprise.

Il doit savoir présenter ces risques et en argumenter les moyens de les encadrer, il doit convaincre de l'impérative nécessité de formaliser des politiques pour les maîtriser. Ceci est particulièrement prégnant dans le monde Internet où la menace évolue rapidement et où les enjeux liés aux innovations sont primor-diaux induisant une forte exigence d'agilité

4.31. [NSE] NOYAU ET SYSTÈMES D'EXPLOITATION [1+2]

Le cours de Noyaux et Systèmes d'Exploitation présente en déetails les concepts fondamentaux mis en oeuvre pour le fonctionnement des noyaux modernes, depuis la gestion du matéeriel jusqu'à la communication inter-processus, en passant par la distribution des ressources.

Suite du cours d'ING1 (SYS). Ce cours approfondi les notions vues dans le premier cours, en examinant l'implémentation dans des noyaux de systèmes d'exploitation modernes.

La liste de notions abordées sont:

- Processus, threads et taches
- Algorithmes et problématiques de scheduling
- Virtualisation mémoire
- Problématiques de storage et block layer

Les points abordés sont les aspect de design des api, tant d'un point de vue de sûreté d'exécution que d'un point de vue sécurité.

Ce cours sert de support théorique pour les projets des activités KSTO1 et KSTO2.

4.32. [R_DEFNET] EXERCICE DÉFENSE NATIONALE

Entrainement et participation au challenge DEFNET organisé par le Ministère de la Défense.

4.33. [R_SR1] RUSH 1 : INFRASTRUCTURE HAUTE-DISPONIBILITÉ

Identifier et éliminer les points individuels de défaillance (SPOF) potentiels d'une architecture minimaliste mais fonctionnelle de type « application web »

Apprendre à choisir et utiliser des techniques de répartition de charge et haute-disponibilité de la couche réseau à la couche applicative le tout sous forme de rush encadré en équipe.

Le sujet du rush est rédigé de manière à faire travailler les étudiants de façon autonome. Pour chaque étape, des pointeurs leurs sont donnés, mais ils sont libre de l'ordre de réalisation de chaque tâche.

4.34. [R_SR2] RUSH 2 : DÉVELOPPEMENT SAN

A partir de spécifications fonctionnelles volontairement floues et ouvertes, concevoir et développer une solution de stockage de type Cloud distribuée et à haute-disponibilité, le tout sous forme de rush encadré en équipe.

Le but secondaire est de mettre en application pratique les concepts étudiés en cours magistraux de réseau (Multicast, IPv6, etc.)

4.35. [SADI] SÉCURITÉ EN ENVIRONNEMENT ACTIVE DIRECTORY

L'objectif de ce cours est de permettre axu étudiants de maîtriser les aspects sécurité de l'annuaire Active Directory.

Plan du cours :

- Mécanismes fondamentaux et composants clés d'Active Directory
- Comptes Active Directory
- Mécanisme d'authentification
- Principales faiblesses du modèle (pass the ticket, etc.)
- Relation d'approbation inter et intra domaines
- Les stratégies de groupes (GPO)
- Principes de sécurisation d'une forêt Active Directory
- Nouvelles fonctionnalités Active Directory

4.36. [SCCO] SÉCURITÉ ET CONDUITE DU CHANGEMENT DANS LES ORGANISATIONS

Chaque éléve-ingénieur sera confronté à des situations de changement où il devra appliquer des nouvelles directives autant qu'il aura à en donner. Le cours s'intéresse à l'accompagnement du changement dans les organisations, la performance opérationnelle et sociale, et ses liens avec la sécurité informatique.

Le cours propose d'étudier les facteurs humains et organisationnels pour la sécurité industrielle. Le but est d'amener les élèves-ingénieurs à mieux se représenter l'activité réelle de travail et le fonctionnement global des organisations pour comprendre (et anticiper) les effets des décisions de changement, quel que soit le niveau d'impact. Le cours vise donc à sortir d'une vision du changement exclusivement technique et/ou centrée sur le « comportement individuel » pour le replacer (aussi) dans le système complexe de l'entreprise en considérant les rôles et les responsabilités de chacune des parties prenantes (management, individus, collectifs de travail,…).

4.37. [SDNE] COURS ET PROJET EN ARCHITECTURE SDN

SDN and Security : OpenFlow-enabled SDN offers a wide range of benefits for security implementation and management.

- Fine-grained enforcement and control of multiple simultaneous security policies throughout the network.
- Rapid response to threats, with the ability to rapidly steer or quarantine flows based on real-time network conditions.
- Incorporation of a trust model with live rule-conflict detection and resolution at the controller layer.
- Synchronization of distributed policy insertion and removal.
- Optimization of secure flow routing in a highly dynamic environment.
- Provision of a mechanism for auditing and audit trails

4.38. [SECUP] SÉCURITÉ DANS LES PROJETS

Intégration de la sécurité dans les projets : Gagner en maturité en gérant ses risques SSI tout au long du cycle de vie du projet.

Plan :

ISP : Activités Sécurité, de l'analyse et du suivi des risques aux recettes et tests de sécurité

ISP : Intégration des activités SSI dans la démarche Projet

ISP : Méthodologie et Normes (Standard ISO, OWASP, Guides ANSSI, …)

ISP : Cas particulier des externalisations (Plans d'Assurance Sécurité - Cloud Computing,…)

4.39. [SIDU] SÉCURITÉ DES SYSTÈMES INDUSTRIELS

Introduction à la cybersécurité des SI industriels, leurs spécificités et actions clefs pour les sécuriser.

Panorama de leurs vulnérabilités et techniques d'audit de composants industriels (automates)

Plan :

1) SI industriels : historique et évolution

2) Définition et grands principes

3) Spécificités des SI industriels (par rapport à un système d'information d'entreprise/de gestion)

4) Évolution de la règlementation

5) Exemples d'attaques, déroulement et impacts

7) Atelier participatif : démonstration d'attaques sur maquette SI industriel

6) Les grandes familles de risques, les vulnérabilités et comment protéger un SI industriel

7) Panorama des normes et guides de sécurité- Panorama des normes et guides de sécurité

4.40. [SOC] SÉCURITÉ OPÉRATIONNELLE (SOC, CERT, ETC)

Nulle entreprise, administration ou état ne peut ignorer la menace cyber et le fait qu'elle est peut-être déjà, ou sera tôt ou tard, la cible d'hacktiviste, de la cybercriminalité ou de groupes d'actions adverses.

Face à cette prolifération de menaces dotées d'un arsenal en perpétuel évolution et s'adaptant sans cesse, les approches historiques de la sécurité sont peu efficaces. La cyberdéfense doit s'adapter en conséquence en s'axant non pas uniquement sur la recherche de signatures mais également sur la détection de comportements représentatifs d'activités potentiellement malveillantes afin d'y réagir le plus rapidement possible. Ce sont là les principales missions d'un Centre Opérationnel de Sécurité (SOC).

Au travers de cas concret issus d'expériences professionnelles réelles, nous aborderons les thèmes suivants :

Le besoin de cyberdéfense ;

Les métiers de la cyberdéfense dans l'écosystème de la cybersécurité ;

Les conditions nécessaires pour défendre efficacement : s'organiser, connaître le théâtre d'affrontement et connaître ses ennemis ;

Les objectifs de la détection ;

L'élaboration d'une stratégie de détection ;

Les méthodes de détection d'une présence ennemi potentielle ou avérée ;

Les outils nécessaires au développement d'une capacité de détection ;

Les éléments clefs d'une réaction rapide et efficace ;

L'analyse d'une alerte ;

Le traitement d'un incident de sécurité ;

Les principes de gestion d'une crise cyber d'ampleur

4.41. [STORM] SÉCURITÉ ET PARE-FEU STORMSHIELD

Notre partenaire, la société Stormshield organise dans l'école une adaptation de son offre de formation destinée à sa cible entreprise :

conférence "Traitement haute performance de paquets réseaux dans un Firewall/IPS sous FreeBSD" (2h)

Master Class par le directeur Marketing Produit de Stormshield (2h)

Lancement du projet de certification CSNA (3h)

accompagnement sur les labs CSNA (3h)

Coaching sur certification labs CSNA (2h)

4.42. [TATT] SÉCURITÉ : ANALYSES ET DÉFENSES GÉNÉRALES

Donner aux étudiants un état de l'art sur les technologies utilisées pour réaliser des attaques informatiques, afin de pouvoir rendre plus robustes les infrastructures qu'ils devront déployer.

-Les failles les plus courantes sur les systèmes Unix et leur exploitation

-L'écriture de shellcodes et les techniques associées pour contrer les systèmes de détection

-Les attaques de type buffer overflow, heap overflow, int overflow, string format (explication et mise en pratique)

-Les failles web courantes (include PHP, injection SQL, XSS)

-Les rootkits sous Linux et Windows

-Les Outils disponibles sur internet pour réaliser ces attaques et les techniques à mettre en oeuvre pour les détecter.

4.43. [TATT2] SÉCURITÉ : ANALYSES ET DÉFENSES RÉSEAU ET WEB

Les objectifs de ce cours sont les suivants :

- Comprendre et distinguer les problématiques liées à la sécurité réseau d'une façon concrète
- Connaître l'état de l'art sur les techniques récentes en matière d'exploitation réseau et web
- Mettre en pratique de ces techniques
- Étudier des protections existantes

4.44. [TMS] TECHNOLOGIES, OFFRES ET MARCHÉ DE LA SÉCURITÉ

Mettre en adéquation les technologies de la sécurité avec son marché. Confronter la théorie (la technique pure) et la réalité du terrain (le marché).

Passer en revue des technologies-clés de la sécurité et analyser leurs origines, leurs évolutions et, aujourd'hui, leur place sur le marché : qui les vend ? Comment ? Pourquoi les entreprises les achètent (ou pas...). Qui sont les principaux acteurs sur chaque technologie abordée ? (origine des produits, rachats des technologies, etc...)

Préparer les élèves à réalité de l'écosystème de la sécurité, et les aider à y évoluer à leur arrivée sur ce marché : au delà des développeurs et des ingénieurs, le marché de la sécurité s'articule autour de nombreux autres rôles-clés, qui sont autant de débouchées potentielles pour les élèves ingénieurs.

Par ailleurs, chaque cours fera l'objet d'une discussion libre autour de l'actualité de la sécurité de la semaine écoulée

4.45. [VIRLI] VIRTUALISATION LÉGÈRE

Appréhender les notions de virtualisation légère. Mettre en œuvre des conteneurs applicatifs dans les environnements dérivés d'UNIX (GNU/Linux, FreeBSD), maîtriser les différentes méthodes de virtualisation réseau, connaître les limitations techniques et les problématiques de sécurité associées.

Plan:

-Historique

- Focus sur GNU/Linux

- Réseaux

4.46. [VIRO] De la Virologie au Malware

Présentation des principales techniques lutte antivirale.

Plan :

-Les virus d'exécutables (COM, EXE, PE).

-Les macro-virus et les virus de documents.

-Les vers.

-Les virus de boot.

-Les techniques de lutte antivirale.

-Scripts de détection et de désinfection.

4.47. [VVRI] Veille en vulnérabilité et Réponses aux incidents

Notre partenaire, la société LEXSI organise dans l'école un projet de recherche de Vulnérabilité et de Réponse à Incident :

- Une VM est données aux étudiants
- Cette VM contient des applications et un disque virtuel contenant les contexte d'un retour d'incident
- Les étudiants doivent détecter les vulnérabilités et pour chacune d'entre elles tenter de générer un "exploit"
- Les étudiants doivent réaliser une analyse Forensic de l'incident
- l'évaluation est réalisée via le rapport et les codes d'exploitation.

4.48. [WSEC] Windows et Sécurité

• Acquérir une connaissance approfondie du système d'exploitation Windows, en particulier les mécanismes liés à la sécurité, afin de pouvoir apporter une expertise technique sur le système ou sur un projet basé sur un système Windows

• Maitriser les concepts des systèmes d'exploitation communs aux familles Unix/Windows/BSD et ceux plus spécifiques à l'environnement Windows en insistant sur les impacts en termes de sécurité

• Savoir développer des logiciels élémentaires sous Windows répondant à des besoins précis (tester une librairie d'authentification, comprendre et reproduire des codes malveillants, …)

• Connaitre et savoir utiliser les outils les plus courants, en particulier ceux liés à la sécurité ou à l'analyse du système.