Projet étudiant : mise en place et administration tout au long de l'année d'une salle informatique adoptant une architecture réaliste d'un SI

Sylvain Lesage
Département Sécurité et Technologies Informatiques
INSA Centre Val de Loire
88 boulevard Lahitolle CS 60013 18022 Bourges cedex
sylvain.lesage@insa-cvl.fr

***Résumé*—Cet article présente un module d'enseignement intitulé "*Architecture système et réseau*" dans lequel des étudiants[1] fraîchement arrivés en 3ème année de cycle ingénieur mettent en place une salle informatique adoptant une architecture réaliste d'un SI d'entreprise. Tous les autres enseignements qui leur sont prodigués se font dans cette salle et ils l'administrent tout au long de l'année académique.**

I. Introduction

Le module s'adresse aux 24 étudiants de l'option *Architecture, Administration, Audit et Analyse de Sécurité* (4AS) du département *Sécurité et Technologies Informatiques* (STI) de l'INSA Centre Val de Loire. Le département STI est une filière d'ingénieurs en informatique spécialisée en cybersécurité. L'option de 3ème année de cycle ingénieur 4AS se focalise sur l'acquisition de compétences en cybersécurité à tous les stades de la vie des systèmes d'information : la conception de leur architecture, leur administration, leurs audits et analyses, y compris post-mortem le cas échéant. Ceci requiert à la fois un bagage théorique et une certaine expérience pratique.

Après quasiment 5 années d'études dont 3 dans une spécialité informatique, les futurs ingénieurs ont un bagage académique conséquent, et ont déjà pu faire des projets dans des domaines spécifiques : développement, chiffrement, réseau, ...

Toutefois, dans leur futur poste, ils ne seront plus dans un environnement "de test" protégé, mais dans un écosystème où ils devront certes mobiliser leurs connaissances, mais surtout faire preuve d'initiative, savoir communiquer et travailler au sein d'une équipe, mettre en œuvre des outils maintenables, comparer différentes solutions pour répondre à une expression de besoin, ainsi que tenir compte du contexte financier et technique de la structure où ils évoluent.

Ce module a justement pour objectif de leur laisser carte blanche pour construire, mettre en œuvre et maintenir des solutions techniques répondant à une expression de besoins qui va les forcer à se répartir le travail, communiquer, prendre toute leur place dans un écosystème, rechercher des solutions adaptées à la demande, intégrer dans leur réflexion la résilience de leur projet : en bref fournir un produit comme s'ils étaient en entreprise.

Afin de leur permettre de quitter momentanément le monde académique, ils disposent d'une part d'un environnement particulier (qui sera décrit juste après), mais surtout un scénario leur est présenté, qui va leur permettre de donner du sens à leur travail et leur permettre de comprendre le sujet plus vaste que la simple démonstration technique.

Ce scénario se base sur un fait réel : le Centre de Formation des Appentis (CFA) de la région Centre Val de Loire qui, lors de la réforme de l'apprentissage, est sorti du périmètre de responsabilité de la région et a dû construire rapidement un nouvel environnement réseau, un nouveau système d'information, recruter des ingénieurs et trouver des prestataires.

Il est donc expliqué aux étudiants que d'une part ils font partie d'une Direction du Système d'Information nouvellement créée dont l'intervenant est le DSI, à tout le moins le maître d'ouvrage, et d'autre part qu'ils doivent penser leurs solutions afin de permettre à différentes populations (administratifs, enseignants, étudiants) de travailler sur site ou en mobilité, sur un campus constitué de plusieurs bâtiments. Bien évidemment les notions de sécurité, de segmentation, de sauvegarde, de passage à l'échelle, et de maintenabilité sont évoqués.

Le fonctionnement et la scénarisation du module pour les faire travailler autour d'une structure d'enseignement virtuelle, proche tout à la fois du fonctionnement d'un CFA et de l'INSA Centre Val de Loire est aussi dû au parcours de l'intervenant : l'actuel RSSI et responsable de la DSI de l'INSA CVL qui gère aujourd'hui 3 équipes : gestion de parc, infrastructures et applicatifs de gestion, soit 10 personnes, pour servir une population d'environ 1700 étudiants et 230 personnels administratifs, techniques et enseignants.

II. Environnement et contexte

Ce module est installé dans une salle entièrement dédiée à l'option 4AS qui en accueille tous les enseignements. De plus, la salle est accessible toute l'année aux étudiants sur de larges créneaux horaires, ils peuvent donc utiliser cette salle et le matériel mis à disposition à loisir.

1. Pour alléger le document, le masculin est utilisé à titre épicène.

FIGURE 1. La salle 4AS

Le matériel présent est constitué de plusieurs serveurs hétérogènes, des switchs de niveau 3 manageables, du câblage, 24 postes clients récents, des bornes wifi, d'armoires réseau et de divers périphériques. Un accès Internet avec peu de filtrage est accessible.

Le matériel n'est pas modifiable, sauf à demander à la DSI (la vraie) quelques pièces détachées : lorsque les étudiants seront dans le milieu professionnel, ils devront faire avec les installations existantes. Charge aux étudiants de s'organiser entre eux.

Les étudiants trouvent le matériel *"as is"*, encore configurés de l'année précédente. Ils sont libre d'étudier ce qui a été fait les années précédente pour s'en inspirer, ou tout refaire.

D'un point de vue logiciel, les étudiants peuvent faire des choix Open-Source, ou utiliser les outils VmWare et Microsoft mis à disposition par les accords cadres nous liant à ces deux entreprises (Microsoft Azure, Vmware OnTheHub), qui leur permette de télécharger les systèmes et licences d'outils de production (Windows Server, VmWare vSphere) le cas échéant.

Dès la première séance, les étudiants sont répartis arbitrairement dans les différents groupes thématiques : on ne choisi pas ses collègues, on fait avec.

Juste après, l'intervenant leur explique l'objectif : construire à partir du matériel présent dans la salle les couches réseau, infrastructures, services numérique nécessaires pour qu'un établissement d'enseignement puisse remplir ses missions dans toute ses dimensions : pédagogie, administration, industrialisation des processus, documentation, protection du système d'information, résilience des services, mobilité,...

Enfin, ils sont placés dans le contexte d'une DSI, l'intervenant jouant le rôle du responsable de la DSI, avec un rôle de pilotage et d'arbitrage, chaque groupe constituant une "équipe" spécialisée et responsable.

III. OBJECTIFS DU MODULE

Les objectifs du module sont :

— de leur faire appréhender le travail au sein d'une équipe ou entreprise, de les imprégner de la nécessité de mettre en œuvre des outils et technologies sécurisés, stables et communicants avec le reste de l'écosystème, de leur permettre de comparer les solutions commerciales et libres (avantages/inconvénients), de la nécessité de produire des solutions durables, de documenter leur travail, le support client,...

— de leur faire manipuler, démonter, modifier, relier des matériels informatiques de production qu'ils n'ont en général jamais réellement approché, ce qui a l'air d'intéresser grandement les étudiants. Une séquence est d'ailleurs entièrement dévolue au démontage d'un serveur afin de leur montrer les différences avec le matériel grand public : cartes de monitoring iDrac, cartes RAID, organisation des ventilateurs, double alimentation,...

FIGURE 2. Armoires serveurs et switchs dans la salle

Enfin, tout au long du module, et en fonction des questions, remises en questions, remarques des étudiants, l'intervenant replace la question dans le contexte de leur école : capacité de l'équipe en place et compétences liées aux agents, difficultés de passage à l'échelle de certaines solutions, population diverse de 2000 personnes, acceptation des arrêts de service, perte de données, ...

Afin de maintenir un esprit pratique et opérationnel à ce module, les réponses aux échanges et aux questions sont formulées sous formes de retours d'expériences liés à la DSI de l'INSA, ou sous formes d'anecdotes qui permettent de d'ancrer le retour formulé dans la réalité du terrain.

IV. PÉDAGOGIE ET MÉTHODOLOGIE

Comme abordé précédemment, la salle est dédiée aux étudiants de 5ème année de l'option 4AS, et ce toute l'année.

Ils y accèdent à leur convenance grâce à un accès par badges. Il est juste interdit d'y manger, d'y boire, et d'y dormir !

La salle devant servir à d'autres cours et notamment aux projets d'approfondissement -qui mettent en jeu des technologies de sécurité et virtualisation plus complexes-, le module a lieu en tout début d'année. Cette année le choix a été fait de mener ce module sur 1 mois, 6 séances d'une demi-journée avec l'intervenant étant planifiées à raison de 2 séances par semaine : l'une en début de semaine pour fixer les objectifs et l'autre en fin de semaine pour voir l'état d'avancement et faire les réorientations si nécessaire.

L'intégralité de la période sur laquelle se déroule ce module est sanctuarisée, très peu d'autre cours sont planifiés sur cette période afin de permettre aux étudiants de consacrer leur temps à construire les solutions techniques dans la salle même, en dehors des séances avec l'intervenant.

Sur toute la durée du module, et un peu après, les étudiants doivent utiliser "Teams" pour communiquer aux autres équipes les problèmes, avancées, questions. Le même outil permet de contacter l'intervenant en dehors des séances programmées sur plusieurs semaines.

La première séance est la plus importante, elle contient plusieurs séquences :

- Présentation de l'intervenant et de l'organisation de la DSI de l'INSA Centre Val de Loire,
- Présentation du scénario (le CFA, un peu mixé avec l'organisation de l'INSA),
- La répartition des étudiants dans les groupes
- La présentation du matériel
- Un rappel sur les sous-réseaux IP (indispensable)
- Une séance de brainstorming par groupe, afin de les faire travailler ensemble afin qu'ils fassent des propositions d'orientation dès l'issue de la journée

Par la suite, les séances commencent en général par une 1/2 heure ou plus de discussion pour que les différents groupes puissent faire état de leurs questions, avancées et problèmes. L'intervenant peut soit répondre à partir de son expérience, soit faire intervenir le groupe. Cette initialisation de la séance permet surtout de faire communiquer les groupes entre eux, ce qui n'est pas naturel au premier abord.

Sur la séance, l'intervenant fait un tour groupe par groupe pour vérifier l'avancement des travaux, éventuellement évoquer des sujets non abordés devant tout le monde, et orienter les étudiants.

L'aspect le plus important de ce module reste d'offrir aux étudiants la possibilité de manipuler tout un ensemble de matériel. Cet aspect pratico-pratique est particulièrement apprécié des étudiants.

La séquence concernant l'observation de l'anatomie d'un serveur rackable DELL de production a beaucoup plu car les étudiants ignoraient toute la complexité ne technique et mécanique d'un tel appareil, par exemple la possibilité de changer des alimentation à chaud, la redondance des ventilateurs, l'évacuation de la chaleur, la présence d'une carte iDrac permettant de contrôler la machine à distance. Cette séquence a été réalisée à froid, mais il faudra prévoir de faire des expérimentation à chaud sur le sous-système RAID par exemple.

V. La répartition en groupes thématiques

Le sujet étant la construction intégrale d'un système d'information sécurisé, en tout cas la partie infrastructures, le sujet est divisé en thématiques. Chaque groupe doit pouvoir disposer d'un sujet cohérent, mais reste interdépendant des autres groupes (toujours la communication, plus la notion de service client). Les thématiques et réalisations de chaque groupe sont synthétisé ci-après.

Réseau

- Mettre en œuvre la communication dans la salle et vers l'extérieur
- Réalisations : Coté réseau ; design réseau de la salle, routage, segmentation en VLAN, agrégation de liens, ACL, dhcp-snooping, port-mirroring, affectation automatique de VLAN relié à un RADIUS. Côté système ; installation d'un DNS public en DMZ avec redondance, installation d'un DHCP redondant.

Sécurité :

- Mise en place d'un firewall et ses règles
- Réalisations : déploiement d'un firewall pfSense, d'une patte interne, un patte DMZ et une patte dédiée à l'IDS. Paramétrage des règles pour les services accessibles depuis Internet. Déploiement d'un VPN authentifié relié à l'active directory pour le travail en dehors de la salle.

Infrastructures et virtualisation

- Mettre en place un serveur de virtualisation propre à accueillir les différents serveurs des autres groupes
- Réalisations : installation d'un serveur vmware ESXi ainsi que d'un contrôleur vSphere, paramétrage des interfaces réseau en agrégation de liens sur différents VLAN, imports des machines virtuelles (VM) des groupes, pré-paramétrage de VM, sauvegarde des VM.

Gestion des identités

- Mettre en œuvre un annuaire centralisé et les services associés, ainsi qu'un système de fichiers, le tout avec un minimum de sécurité
- Réalisations : annuaire Active Directory sous Windows Server 2019, contrôleur de domaine secondaire, serveurs de fichiers Windows : homeDirectory et répertoires partagés, gestion des groupes, gestion des droits, GPO, serveur RADIUS sous Windows, stratégies de mots de passe, accès bureau à distance sur les postes clients par GPO.

Déploiement

- Déploiement de windows et linux sur les postes clients de la salle. Automatisation des process d'installation et de mise à jour.
- Réalisations : installation d'un système d'industrialisation de la gestion de parc OPSI, développement de packages d'installations logiciels (workstation, OpenOffice, wireshark), déploiement de Windows, paramétrage et déploiement en masse des logiciels sur l'ensemble des postes clients, activation de licences Windows sur le parc

clients. Installations d'outils Linux (PXE, TFTP) pour autoriser un boot réseau sur une image LiceCD de Linux si les postes clients Windows sont dysfonctionnels.

WIFI

— Déploiement d'un portail captif et d'une authentification sécurisée 802.1x, (plus installation d'un puit de logs).
— Réalisations : déploiement d'un portail captif pfSense, paramétrage de plusieurs bornes de marques différentes (panne de la borne d'origine), configuration d'une authentification 802.1x wifi liée à un RADIUS (FreeRadius puis active directory). Configuration d'un puit de logs et d'un interface graphique associée, tests de clients Windows pour alimenter les journaux d'évènements des postes clients.

D'autres thématiques sont possibles, selon la taille des groupes ou l'avancement de ces derniers : messagerie sécurisée, sauvegarde automatisée, service de fichiers en mobilité…

VI. Une salle vivante toute l'année

À la fin du module, la salle est entièrement fonctionnelle et simule une mini-école. L'ouverture vers les projets d'approfondissement a alors lieu, en présence des intervenants de cette seconde partie. Les projets d'approfondissements continueront dans la salle installée et maintenue par les étudiants. Ces projets incluent l'installation d'une plateforme Kubernetes, le déploiement d'une PKI, la gestion des identités SSO, et le scan de code, mais aussi des projets dans la continuité de l'installation de la salle : Honeypot, serveur proxy, Windows Hardening.

Les étudiants ont la responsabilité du "maintien en conditions opérationnelles" de la salle sur le reste de l'année académique. Les services installés et les postes clients doivent rester opérationnels, et leur paramétrage adapté en fonction des besoins des intervenants qui auront à utiliser cette salle.

VII. Évaluation

L'évaluation se fait par groupes, de façon légèrement empirique. Les notes vont dépendre de la présence des étudiants, de leur implication dans le projet confié, des interactions dont ils ont fait preuve, de l'atteinte des objectifs (sachant de l'erreur est acceptée car participant à la connaissance).

Une petite partie de la notation est liée à la documentation qui leur est demandée à la fin du module. Ils doivent reformuler la demande qui leur a été faite, expliquer ce qu'ils ont proposé et en quoi leur réponse répond à l'expression des besoins, et expliquer à minima les jalons de leurs projet. Il s'agit d'un embryon de documentation de leurs travaux de 4 à 10 pages. Ils indiquent aussi comment ils se sont répartis les tâches au sein du groupe.

VIII. Feedback et feuille de route du module

Un sondage anonyme a été mis en place cette année pour permettre aux étudiants de fournir leur ressenti sur le module. Il était proposé de noter de 1 (mauvais) à 6 (excellent) : le module en général (Q1) ; son apport sur la capacité à appréhender la réalité professionnelle du management d'un SI d'un point de vue organisationnel et interpersonnel (Q2) et technique (Q3) ; l'utilisabilité, la stabilité et la maintenabilité de la salle résultante (Q4) ; le degré d'autonomie laissé (Q5). 18 des 24 (75%) étudiants concernés ont répondu, le résultat étant présenté dans le tableau I. Notons qu'un étudiant n'a pas souhaité répondre à la question 2 (Q2).

Question	**Appréciation**						**Appréciation**
	1	**2**	**3**	**4**	**5**	**6**	**moyenne**
Q1 global	0	0	1	0	14	3	5.1
Q2 réalité humaine	0	0	1	9	5	2	4.5
Q3 réalité technique	0	1	0	5	6	6	4.9
Q4 résultat	0	0	1	1	10	6	5.2
Q5 autonomie	0	0	0	0	4	14	5.8

TABLE I
APPRÉCIATION DES ÉTUDIANTS DE 1 (MAUVAIS) À 6 (EXCELLENT)

Outre un outlier ayant attribué trois 3 et un 2, toutes les évaluations sont positives sur toutes les dimensions avec une appréciation moyenne allant de 4.5 pour Q2 à 5.8 pour Q5. On peut donc raisonnablement estimer que les étudiants ont beaucoup apprécié ce modèle de mise en situation réaliste. Quelques axes d'amélioration ont été détectés, de la part de l'intervenant ou des étudiants qui ont été interrogés sur leur ressenti :

— Les groupes de 4 sont trop gros dans certains groupes. Il faudra penser à des groupes de 2 à 3 maximum,
— Il est nécessaire d'accentuer les aspects sécurité dans chacun des groupes (chiffrement, certificats),
— Les étudiants qui ont travaillé essentiellement autour de ce projet durant 1 mois désirent pouvoir faire un retour de leur expérience devant leurs camarades,
— Le démarrage dans une salle non fonctionnelle (c'est le but du jeu) est un peu complexe. Il faudra pouvoir permettre aux différents groupes d'avancer plus efficacement en attendant que les parties réseau et virtualisation soient opérationelles.
— Les étudiants apprécieraient de pouvoir choisir leur thématique. Cela pose un challenge vis à vis de la nécessité de leur imposer des co-équipiers.

IX. Conclusion

En conclusion, le module est apprécié par les étudiants et en adéquation avec les objectifs de l'option orientée administration système et sécurité. Les étudiants ont été motivés par la possibilité de construire en synergie un ensemble somme toute complexe, sur des matériels professionnels, avec une forte responsabilité sur le maintien de conditions opérationnelle sur l'année scolaire.

Il est à noter que la coloration "Direction du Système d'Information" cette année est liée au parcours de l'intervenant. Précédemment, les cours étaient assurés par le responsable support à la Recherche et RSSI de l'Université Paris 13, et le profil de l'intervenant faisait que les thématiques, même si elles étaient identiques, étaient abordées sous un angle plus technique.