Retour d'expérience : enseignement de la cybersécurité dans les formations d'officiers à l'École de l'air et de l'espace

Charles-Edmond Bichot, Alain Menelet

***Abstract*—L'école de l'air et de l'espace a décidé ces dernières années de renforcer et homogénéiser l'enseignement de la cybersécurité dans ses formations d'élèves officiers car le cyberespace est devenu un enjeu sécuritaire majeur et une menace importante pour la sécurité de la France. Il a ainsi été créé un socle de formation commun en cybersécurité, des cours ont été transformés pour intégrer dans leur domaine des notions de cybersécurité et des options en cybersécurité ont été ajoutées à certaines formations.**

Afin d'accompagner les enseignements théoriques par des travaux pratiques réalistes et collant à une réalité en perpétuelle mutation, il a été nécessaire de mettre en oeuvre une plateforme supportant des architectures hétérogènes. Deux solutions complémentaires ont été mises en place afin de faciliter la création, le déploiement et l'exploitation de topologies ainsi que la création d'environnements cohérents de type attaque défense. La première solution s'appuie sur Hynesim et permet de créer des architectures hybrides via une interface adaptée et intuitive et la seconde s'appuient sur des technologies de création d'infrastructures personnalisables et automatisables à base de catalogues.

I. Introduction et contexte

L'ÉCOLE de l'air et de l'espace (EAE) a pour mission première la formation des futurs officiers de l'armée de l'air et de l'espace française (AAE). Il existe cinq grandes catégories d'admission d'élèves officiers français à l'EAE [1] :

1) Les élèves des classes préparatoires aux grandes écoles (CPGE) ayant passé le concours commun INP (instituts nationaux polytechniques) et étant admis à l'EAE (environ 70 places). Ils recevront une formation d'ingénieur de trois ans ;
2) Les étudiants titulaires d'une licence ayant été sélectionnés aux concours "sciences politiques" (environ 4 places) ou "sciences" (environ 2 places). Les premiers recevront une formation en sciences politiques amenant au grade de master, en partenariat avec l'institut d'études politiques d'Aix-en-Provence, les seconds suivront la formation d'ingénieur avec les élèves issus de CPGE ;
3) Les candidats titulaires d'un diplôme de niveau master et admis sur titres à l'EAE (environ 6 places). Ils recevront une formation d'un an en grande partie au sein de la formation d'ingénieur ;
4) Les militaires non officiers possédant soit une licence, soit un baccalauréat général ou technologique. Il s'agit le plus souvent de sous-officiers (environ 50 places). Ils suivent une scolarité de deux ans amenant au grade de licence ;
5) Les candidats recrutés en tant qu'officiers sous contrat. Ils recevront une formation, principalement militaire, de quelques semaines.

Les lauréats issus des quatres premières catégories d'admission deviendront officiers de carrière. Les officiers sous contrat pourront intégrer pendant leur carrière, au choix, les officiers de carrière. Tous rejoindront l'un des trois corps d'officier de l'AAE : officiers de l'air, officiers mécaniciens de l'air, officier des bases de l'air.

Les cursurs de l'EAE que suivent les candidats admis[1] sont :

- Cours de master de l'EAE qui se divise trois parcours :
  - parcours ingénieur (admissions 1 et 2)
  - parcours sciences politiques (admission 2)
  - parcours titre (admission 3)
- Cours de licence de l'EAE qui se divise en trois parcours (admission 4) :
  - parcours systèmes informatiques et logiciels
  - parcours systèmes aéronautiques et spatiaux
  - parcours management public
- Formation des officiers sous contrat (admission 5).

À l'issu de ces formations, les élèves officiers lauréats intégreront l'AEE en tant qu'officier de l'air, mécanicien ou basier dans l'un des 25 métiers recensés. Ces derniers sont répartis dans 8 domaines d'activité : opérations aériennes, systèmes aéronautiques, sécurité, renseignement, SIC, logistique, administration, communication. Comme on peut le constater, le spectre d'emploi des élèves officiers formés à l'EAE est très large. Ceci explique le nombre des parcours de formation proposés alors que la population formée est peu nombreuse.

Au vu de la diversité des formations, mais aussi des métiers dans lesquels devront travailler les élèves officiers, il est aisé de comprendre le défi qu'a consisté la création d'un socle de formation en cybersécurité à l'EAE qui soit à la fois transverse aux formations, mais aussi adaptée aux exigences de chacune d'entre elles.

Charles-Edmond Bichot était maître de conférences à l'École de l'air et de l'espace pendant la mise en place de la réforme, il est maintenant maître de conférences à l'École centrale de Lyon

Alain Menelet était enseignant-instructeur à l'École de l'air et de l'espace pendant la mise en place de la réforme, il est maintenant officier de l'Armée de l'air et de l'espace

[1]Il s'agit des cursus des années 2018 à 2020 pendant lesquels l'enseignement en cybsersécurité à l'EAE a été réformé

Le dernier livre blanc de la défense [2] prévoyait la création du commandement de la cyberdéfense des armées. Il a particulièrement insisté sur la prise en compte de la menace cyber au sein des armées et a mis en avant l'importance d'une bonne formation de ces dernières. La revue stratégique de défense [3] a confirmé ces deux points tout en insistant sur la finalité opérationnelle de la formation.

Tous ces éléments ont amené à une prise de conscience progressive au sein de l'EAE sur l'importance d'un enseignement de la cybersécurité à la fois dans toutes les formations de l'école et adapté à celles-ci. L'enseignement de la cybersécurité a donc progressivement évolué au sein de l'EAE pour aboutir au format que nous allons vous présenter dans les prochaines sections, d'abord pour la formation au niveau licence, puis au niveau ingénieur. La quatrième section présentera la plateforme hybride mise en place pour mettre en oeuvre les travaux pratiques.

II. Formation à la cybersécurité des élèves officiers au niveau licence

Le cours de licence de l'EAE forme à la fois les élèves officiers issus du rang — principalement des sous-officiers — et les cadets étrangers venant de pays possédant des relations fortes avec la France, au niveau d'une licence professionnelle, en deux ans. La première année de formation est acquise par VAE (validation des acquis de l'expérience) et mise à niveau avant le début de la formation. Comme décrit plus haut, il existe trois parcours de formation.

Afin de garantir un niveau homogène de compétence en cybersécurité des futurs officiers, il a été décidé de construire une action de formation commune aux trois parcours de licence avec des adaptations ponctuelles en fonction du niveau des élèves au niveau des travaux pratiques (TP).

Cette action de formation transverse a été construite à la fois en se basant sur les cours de cybersécurité préexistants à l'EAE, car cette discipline est logiquement enseignée depuis longtemps à l'EAE, mais aussi sur les excellents supports de formation de l'association CyberEdu et avec les conseils de l'ANSSI en termes de contenus.

L'association CyberEdu[2] permet la labellisation des formations du supérieur qui ne sont pas spécialisées en cybersécurité. Elle met aussi à disposition de nombreux supports de formation et des guides pour la construction des actions pédagogiques pouvant inclure de la cyber.

Il est important de mettre en avant que la construction du parcours de formation en cybersécurité au niveau licence s'est faite à la fois par la création d'une action de formation transverse, mais aussi par une réflexion, dans chacun des modules de formation pouvant s'y prêter, de la façon dont la cybersécurité pouvait être abordée. Ceci a bien évidement été particulièrement vrai pour la licence systèmes informatiques et logiciels. Cependant, cela a été aussi vrai pour les autres licences. Par exemple, dans la licence de management public, un module de formation a été restructuré pour y introduire la géopolitique du cyberespace ainsi qu'une introduction à la protection des données.

L'action de formation commune en cybersécurité est divisée en trois parties : une introduction magistrale aux notions de base en cybersécurité et cyberdéfense de 8 heures ; une mise en application des concepts étudiés est réalisée sous la forme d'un TP de 4 heures où nous insistons sur la diversité des attaques cyber et leur facilité de mise en œuvre en nous appuyant sur la plateforme Hynesim présentée plus loin ; un retour d'expérience de militaires et d'industriels pendant 6 heures de conférences.

III. Formation à la cybersécurité des élèves officiers au niveau ingénieur

Le cursus d'ingénieur de l'EAE forme en trois ans des élèves issus des classes préparatoires aux grandes écoles, souvent effectuées dans des lycées militaires. Toujours dans le but de garantir un niveau homogène de compétences en cybersécurité des futurs officiers, il a été décidé que l'action de formation d'introduction à la cybersécurité du cursus ingénieur allait être calquée sur celle donnée aux licences avec quelques ajustements liés au niveau plus avancé des élèves. Ainsi les cours magistraux et les travaux pratiques vont un peu plus loin dans le cadre du cycle ingénieur.

Il est important de noter que la formation d'ingénieur de l'EAE n'a pas pour vocation de former des spécialistes en informatique, encore moins en cybersécurité. En effet, comme précisé plus haut, la diversité des métiers qu'exerceront les futurs officiers nécessite que la formation d'ingénieur soit assez générale. Ainsi, il n'a pas été retenu que la formation soit labellisée SecNumEdu[3] par l'ANSSI, même si le contenu pédagogique exigé a été une source d'inspiration pour faire évoluer les enseignements [4], [5], [6], [7].

L'EAE a créé en 3ème année du cursus ingénieur une option dédiée à la cybersécurité. Cette option de 60 heures d'enseignement en face à face permet aux élèves officiers de se spécialiser dans le domaine. Elle aborde la cybersécurité avec une approche de pédagogie inversée [9] orientée vers le *learning by doing* en initiant aux pratiques d'attaque pour mieux savoir défendre. Sont abordés dans cette option la cryptographie, les normes, le forensic, la cyberdéfense et les tests d'intrusion. La plateforme Hynesim sert de support aux enseignements dispensés dans cette formation.

IV. Plateformes pédagogiques mises en oeuvre pour l'enseignement de la cybersécurité

La cybersécurité est transverse à de nombreuses disciplines (réseaux, développement, modes opératoires, normes) et son enseignement doit prendre en compte cette diversité. L'EAE est membre de la CISCO networking Academy. À ce titre, elle propose des certifications CCNA ainsi que le CCNA security aussi bien dans le cadre du cursus licence et que celui d'ingénieur. Les formateurs sont au préalable certifiés par CISCO afin d'accompagner au mieux les étudiants. La certification pour les formateurs consiste à passer le même examen que les élèves, mais avec un critère de réussite plus strict.

[2]https://www.cyberedu.fr

[3]https://www.ssi.gouv.fr/entreprise/formations/secnumedu/

La nécessité d'une plateforme permettant de simuler des environnements complexes s'est avérée très rapidement au cœur des préoccupations. Il fallait offrir un enseignement pratique au plus près de la réalité permettant à chaque élève de mettre en pratique les enseignements reçus [8] sur des situations opérationnelles en minimisant le temps d'adaptation. Cette plateforme devait respecter un cahier des charges précis tel que la mise à disposition d'infrastructures hydrides (permettant de connecter des matériels physiques et virtuels), d'infrastructures facilement évolutives (à base de provisionning afin de gagner du temps sur la mise en place des environnements d'apprentissage) et ayant une approche de construction ne nécessitant que peu de prérequis (interface de création simple, ergonomique et intuitive).

Notre infrastructure est composée deux ensembles, répondant chacune à des besoins précis.

A. Plateforme Hynesim

Le premier ensemble s'appuie sur Hynesim[4] dans sa version cybertraining center (HNS). Il s'agit d'une solution de virtualisation d'infrastructure orientée sur la pédagogie avec une attention portée sur l'interface utilisateur et les actions possibles par simple glisser-déposer. Proposé et maintenu par la société DIATEAM, Hynesim existe en une version open-source qui n'est plus maintenue depuis 2018 et en une version pro payante. Cette dernière est installée à l'EAE, mais également à l'école de formation des sous-officiers de l'Armée de l'air. L'EAE, au travers de son contrat, possède une version continuellement mise à jour pour la sécurité (MCS), les conditions opérationnelle (MCF) et l'évolution des fonctionnalités (maintenance évolutive). Hynesim s'appuie sur de nombreux hyperviseurs dont le couple KVM/Qemu.

L'infrastructure simulée est constituée d'une ou plusieurs topologies, préalablement préparée, qui vont permettre à l'apprenant de se focaliser sur l'essentiel. Celles-ci se composent d'objets (poste client, équipements actifs de type switch ou routeur, serveur) qui peuvent être déplacés à partir d'un catalogue et connectés entre eux par des liens virtuels. La création de ces topologies se fait via une interface intuitive en s'appuyant principalement sur des glisser-déposer facilitant ainsi la mise en place d'ensembles complexes tout en s'affranchissant d'actions sans plus-value pédagogique. Les topologies pourront être déployées et répliquées à la demande permettant au corps enseignant de s'adapter facilement. Le catalogue de poste client et serveur comprend aussi bien des systèmes GNU/Linux que des systèmes sous Microsoft Windows.

Un des éléments ayant appuyé le choix de cette plateforme est la possibilité de créer des interfaces dites hybrides. Elles offrent la possibilité de connecter la topologie à des équipements physiques afin de profiter des infrastructures CISCO et des compétences obtenues par les élèves lors du passage des certifications.

De nombreux TP sont facilités :

- chaque élève à sa topologie
- duplication facilitée
- prélèvement mémoire de masse et mémoire vive via simple clic
- glisser-déposer

Les concepts fondamentaux sont expliqués en cours théoriques et mis en pratique en TP/TD. Il s'agit donc pour tous les élèves de rapidement pouvoir créer leur topologie en choisissant les éléments demandés via un catalogue préalablement mis en place et maintenu par le corps enseignant. Chaque poste client possède son système d'exploitation. Ce dernier est accessible via un double clic sur l'icône correspondant, offrant ainsi un système de bureau à distance via le protocol Spice[5].

B. Plateforme Terraform–Parker

Le second ensemble est complémentaire au premier. Il s'appuie sur les solutions libres Terraform/Packer. Il s'agit d'un hyperviseur VMware ESX sur lequel nous avons implémenté la création de machines virtuelles dédiées à des scénarios d'attaque/défense en nous appuyant sur la solution Packer[6]. Cet outil permet la création des images personnalisées qui seront manipulées lors de la création des architectures. Un catalogue interne est maintenu pour être au plus proche de la réalité.

Terraform est publié en open-source par la société HashiCorp. Il s'agit d'un environnement open source d'infrastructure as code ou IaC. Il permet d'automatiser la construction d'une infrastructure (réseau, ressources, poste client et serveur). La personnalisation des images s'appuie sur la solution open source Packer également publié par la société HashiCorp. Il s'agit de créer des images (.box) à destination d'une plateforme cible (Vmware, Azure ...), dans notre cas le serveur terraform/ESX. Elle s'appuie sur des templates écrit en HCL/JSon et permet d'exécuter des scritps lors de l'installation.

Prenons l'exemple d'un TP où les étudiants travaillerons sur la vulnérabilité CVE-2019-0708. Elle permet l'exécution d'un RCE (Remote Code Execution) sur des postes Windows principalement Windows 7 et Windows Server 2008. Nous procédons à la création via Packer d'une image s'appuyant sur une version de Windows vulnérable à laquelle nous ajoutons également un agent de monitoring tel que Sysmon. Cette image sera disponible dans un catalogue et accessible à tous les étudiants. Le poste client sur la plateforme Hynesim sera équipé du framework Metasploit afin de procéder à l'exploitation de cette vulnérabilité. Toutes ces images réalisées par Packer seront déployées et connectées grâce à la solution Terraform[7]. L'un des avantages de cette approche est de n'avoir à maintenir que des fichiers de configuration. Une fois ces éléments démarrés, nous pouvons connecter cette solution à Hynesim offrant ainsi un cadre complet aux étudiants.

L'intérêt de cette solution est multiple :

[4]https://www.hynesim.org/

[5]https://spice-space.org/

[6]https://www.packer.io/

[7]https://www.terraform.io/

- Facilité d'installation (simple client coté administrateur et accès ssh coté ESX)
- Elle s'appuie sur des fichiers à plat (langage HCL) simple à appréhender et à maintenir.
- Un simple répertoire avec des fichiers de quelques ko est suffisant pour maintenir nos architectures
- Une fois le TP fini, l'infrastrucuture peut être mis en pause ou bien supprimée
- Une nouvelle instance d'un TP va simplement consister à relancer l'installation des machines et leur configuration
- Un dépôt local permet de gagner du temps en ne téléchargeant à nouveau pas tout à chaque fois
- Une banque d'images (iso ou images personnalisées) qui permet de gagner du temps, une fois l'image conforme au TP, elle sera réutilisable autant de fois que nécessaire.

Cet ensemble est installé sur un serveur IBM Lenovoa M5 avec 256 Go de RAM. Un lab composé d'un frontal web, un active directory et de deux clients windows 10 est monté en 25 minutes.

C. Cas d'utilisation :

La figure ci-dessous présente un scénario intervenant dans le cadre d'un TP introduisant l'analyse des évènements de sécurité au sein d'un centre des opérations de sécurités (SOC).

Les élèves se connectent à HNS puis suivent les instructions présentes dans un support de TP. Ils procèdent à la création d'une topologie par déplacement et instanciation des éléments composants cette dernière. Chaque topologie est connectée via une interface hybride sur un équipement actif physique de type routeur. Les services vulnérables tels qu'un frontal web ou bien un Active Directory sont instanciés sur l'ESX et mis à disposition des élèves via les postes clients Hynesim.

Chaque poste vulnérable possède un agent qui a pour fonction de transformer et normer les fichiers de logs au format Json. Ces logs sont ensuite envoyés vers un système de gestion des événements et des informations de sécurité (SIEM) par exemple Splunk ou bien QRadar. Dans le cadre de ce TP, nous utilisons Splunk comme SIEM et splunkforwarder comme agent.

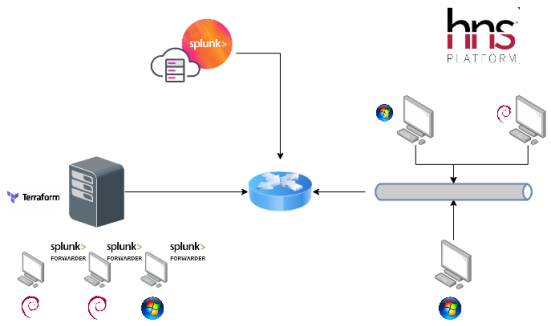

Fig. 1. Infrastucture hybride HNS / Terraform dans le cadre d'un TP introduisant l'analyse des évènements de sécurité au sein d'un SOC.

Les élèves réalisent donc le TP en exploitant les vulnérabilités présentes. La partie attaque finie, ils ont accès via le SIEM à l'ensemble des fichiers de logs propres à leurs attaques et peuvent désormais se mettre du côté des défenseurs et comprendre comment ils pourraient être détectés.

Cet exemple illustre une réflexion menée par les équipes enseignantes sur la mutualisation des efforts. En effet, ces fichiers de logs sont au cœur de nombreux cours et le travail réalisé à tout intérêt à être réutilisé. L'exemple ci-dessus va générer des logs qui pourront être utilisés dans le cadre du cours sur l'apprentissage automatique (sous couvert de quelques modifications), les postes sous Hynésim et sur ESX seront analysés lors du cours sur l'investigation numérique après prélèvement des mémoires vives et mémoire de masse.

V. Conclusion

L'évolution et la réorganisation de l'Armée française lui permettant de mieux appréhender la menace cyber, avec notamment la création du commandement de la cyberdéfense, s'est décliné au niveau de l'École de l'air et de l'espace par une transformation de l'enseignement de la cybersécurité aux élèves officiers et la création d'un socle de formation commun aux différentes formations. Nous avons montré dans cet article quels étaient les enjeux de cette transformation malgré la diversité des futurs métiers des élèves officiers ainsi que l'hétérogénéité de leurs origines. Nous avons aussi explicité les modalités de cette transformation pour les formations de niveau licence et ingénieur. La déclinaison de l'enseignement théorique en travaux pratiques nous a obligé à étudier plusieurs options possibles. Nous avons présenté dans les grandes lignes comment nous avons mis en oeuvre une plateforme de cybersécurité évolutive nous permettant une grande flexibilité dans la mise en oeuvre de scénarios pédagogiques basée sur Hynesim et Terraform.

Toutes ces évolutions ont permis à l'École de l'air et de l'espace de se mettre au niveau des exigences rendues nécessaires par la formation d'élèves officiers dont certains travailleront au sein du commandement de la cyberdéfence des armées ou au sein d'unités dédiées aux systèmes d'information ou à la lutte informatique défensive, sachant que tous pourront être confrontés à une attaque cyber dans leur environnement de travail immédiat.

References

[1] Ministère de la défense, *Décret n° 2008-943 du 12 septembre 2008 portant statut particulier des corps des officiers de l'air, des officiers mécaniciens de l'air et des officiers des bases de l'air*, Journal officiel de la république française, n°0216 du 16 septembre 2008.
[2] République française, *Livre blanc sur la défense et la sécurité nationale*, 15 juillet 2013.
[3] Ministère de la défense, *Revue stratégique de défense et de sécurité nationale*, La documentation française, 13 octobre 2017.
[4] ANSSI, *Fiches pédagogiques sur l'authentification*, février 2017.
[5] ANSSI, *Fiches pédagogiques sur la sécurité des systèmes d'exploitation*, février 2017.
[6] ANSSI, *Fiches pédagogiques sur la sécurité des réseaux*, février 2017.
[7] ANSSI, *Fiches pédagogiques sur la sécurité des logiciels*, février 2017.
[8] AUSTIN, Greg (ed.) *Cyber Security Education: Principles and Policies. Routledge*, p26 ,2020.
[9] Marcel Lebrun et Julie Lecoq, *Classes inversées. Enseigner et apprendre à l'endroit !*, 2015.