MOOC Sécurité des réseaux : un apprentissage massif de la sécurité par la théorie et la pratique

Maryline Laurent[1], Olivier Paul[1], Grégory Blanc[1], Bruno Carron[2], Nicolas Charbonnier[3], Isabelle Chrisment[4], Jérôme François[5], Damien Hotz[2], Philippe Jaillon[6], Rida Khatoun[7], Christophe Kiennert[1], Marwan Lazrag[1] et Souha Masmoudi[1] [*]

May 17, 2019

Abstract

Le MOOC Sécurité des Réseaux, destiné à l'apprentissage massif à distance de la sécurité dans les réseaux informatiques, s'adresse à un public ayant des prérequis légers en informatique et des prérequis plus solides en réseaux (DNS, adressage, routage, ARP, ICMP). Il vise sur 5 semaines, à raison de 5h par semaine environ, à connaître, comprendre, pratiquer, mettre en oeuvre et/ou configurer plusieurs aspects clés de la sécurité dans les réseaux, telles que les menaces, les attaques réseaux, les techniques de filtrage, les VPNs, la détection d'intrusions, les architectures de sécurité, l'analyse de risques, les textes réglementaires, les normes, l'audit, etc. Grâce aux nombreux travaux pratiques proposés dans une machine virtuelle (environnement Docker sous GNU/Linux), les apprenants sont amenés à expérimenter les menaces (ex : ICMP redirect, ARP spoofing, détournement de session TCP), et à configurer plusieurs mécanismes de sécurité classiques (filtrage, VLAN, NAT, IPsec, TLS, IDS/IPS, certificats électroniques).

L'originalité de ce MOOC tient dans le champ thématique restreint à la sécurité des réseaux, un niveau d'expertise élevé pour un apprentissage à distance, et l'offre conséquente de TPs proposés.

1 Introduction

Le MOOC Sécurité des Réseaux se positionne sur la thématique étroite de la sécurité dans les réseaux, et s'appuie sur des prérequis en informatique et en réseaux, ce qui lui permet d'être plus ambitieux sur le niveau d'expertise attendu comparativement à d'autres MOOCs portant sur la sécurité informatique et/ou réseaux (ex. *Computer security* sur Coursera).

Le programme est construit sur 5 semaines et un travail personnel à fournir évalué à 5h par semaine. En première semaine de cours, les apprenants se familiarisent avec les menaces et les vulnérabilités propres aux couches protocolaires, puis les deux semaines qui suivent sont dédiées aux mécanismes de filtrage et de VPN. La quatrième semaine est une semaine de synthèse où peu de nouvelles notions sont introduites, mais où les apprenants sont amenés à réfléchir vis-à-vis d'une menace, à faire les bons choix de mécanismes et à configurer les mécanismes en TP. La cinquième semaine apporte deux dimensions supplémentaires : les architectures de sécurité pour une meilleure compréhension de la place de chaque mécanisme dans un réseau et la dimension méthodologique qui permet d'ouvrir sur d'autres facettes indispensables de la sécurité des réseaux.

[*1] M. Laurent, O. Paul, G. Blanc, C. Kiennert, S. Masmoudi et M. Lazrag de Télécom SudParis, `prénom.nom at telecom-sudparis.eu`

[†2] B. Carron et D. Hotz d'Airbus Defense and Space, `prénom.nom at airbus.com`

[‡3] N. Charbonnier de l'ANSSI, `nicolas.charbonnier at ssi.gouv.fr`

[§4] I. Chrisment de Télécom Nancy, `isabelle.chrisment at loria.fr`

[¶5] J. François de l'INRIA Nancy Grand-Est, `jerome.francois at inria.fr`

[‖6] P. Jaillon de l'Ecole Nationale Supérieure des Mines de St-Etienne, `jaillon at emse.fr`

[**7] R. Khatoun de Télécom Paris, `rida.khatoun at telecom-paristech.fr`

Le MOOC alterne à des fins pédagogiques entre plusieurs types de supports : des vidéos de cours calibrées entre 8 et 15 minutes, des TPs en environnement Docker sous GNU/Linux (Ubuntu), des interviews, un bureau d'études, et l'évaluation au travers de quiz. Les quiz ont pour fonction d'évaluer le niveau de compréhension de l'apprenant, de lui apporter des explications complémentaires au cours, de le/la guider dans la réalisation des TPs, ainsi que de tester qu'il/elle a bien réalisé la manipulation demandée. Les apprenants ont par ailleurs la possibilité d'interagir entre eux et avec l'équipe enseignante au travers du forum mis à disposition sur la plate-forme FUN.

Le MOOC s'appuie sur une équipe pédagogique issue de plusieurs écoles et centres de recherche et sur l'expertise terrain d'Airbus Defense & Space et l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Il bénéficie de financements obtenus de l'ANR au travers du projet FLIRT (Formations Libres et Innovantes Réseaux & Télécom) et de la Fondation Patrick et Lina Drahi.

Le MOOC sera disponible fin 2019 en français sur la plate-forme FUN et devrait être disponible en anglais par la suite. Une première session MOOC devrait être lancée fin 2019 pour ensuite partir sur un rythme de 2 sessions par an.

2 Public visé

Le MOOC a pour cible les étudiants en enseignement supérieur et des professionnels en entreprise [administrateurs réseaux, intégrateurs, techniciens supérieurs Réseaux expérimentés].

3 Prérequis

Les prérequis en informatique consistent à savoir manipuler un ordinateur sous Windows, Linux, Macintosh ou autre pour pouvoir installer le logiciel de TP, à gérer des fichiers, exécuter des commandes, à connaître la pratique en ligne de commandes Linux.

Les prérequis en réseaux sont plus pointus. Il est nécessaire de : connaître la pile TCP/IP et le fonctionnement des principaux services de l'Internet (DNS, BGP, etc.), et maîtriser les principes des réseaux, à savoir les adresses IP/MAC, la notion de flux (numéros de port, TCP/UDP), les entités réseaux (commutateurs, routeurs), les tables de routage, les protocoles ARP et ICMP, les notions de passerelles par défaut (default gateway) et de masque. Notez que ce MOOC fait partie d'une collection de MOOCs disponibles et diffusés par l'Institut Mines-Télécom et que les apprenants peuvent s'appuyer dessus pour acquérir les connaissances nécessaires. Les autres MOOCs de la collection d'intérêt sont : A la découverte des télécommunications, Principes des réseaux de données, Routage et qualité de service dans l'Internet, Comprendre le coeur d'internet : les réseaux d'opérateurs, Les Réseaux Locaux, Supervision de Réseaux et Services, Objectif IPv6.

4 Compétences attendues en fin de MOOC

Les compétences qui doivent être acquises sont les suivantes :

- connaître les principales menaces contre les réseaux informatiques et les vulnérabilités sur chaque couche/protocole ;
- comprendre les principes d'exploitation des vulnérabilités ;
- connaître les différents mécanismes de filtrage, les protocoles de sécurité (IPsec, TLS, Wi-Fi), et les VLANs ;
- être capable de configurer des règles de filtrage, des VLANs et des VPNs IPsec ;
- appréhender les outils de scan et d'analyse réseau (nmap, wireshark), d'interception et d'altération de trames (ettercap, shijack) et les outils suivants sous GNU/Linux : curl / netfilter / iptables / conntrack / ndpi / ebtables / ipsec-tool / racoon / macchanger et mod_security (apache) ;
- savoir positionner de façon pertinente sur une architecture de réseaux les fonctions de sécurité de base.

5 Contenus

Le MOOC est structuré de la façon suivante. La semaine 0 est consacrée au test de connaissances des apprenants et à la mise en place de l'environnement des TPs.
La semaine 1 porte sur les menaces liées aux

réseaux. Elle comprend 4 vidéos de cours sur les menaces de couche MAC, IP, transport et applications et 3 TPs permettant d'expérimenter les menaces suivantes : ICMP redirect, ARP spoofing, détournement de session TCP (*session hijacking*). Un dernier TP permet d'appréhender les menaces applicatives (vol de cookies HTTP) dans un scénario plus global, allant du scan de machines dans un réseau à l'exploitation des informations dérobées à la victime.
La semaine 2 porte sur les mécanismes de filtrage. Elle inclut 6 vidéos de cours sur le NAT et les différents types de filtrage – couche réseau, avec/sans état, applicatif, DPI – et 4 TPs permettant de tester et configurer les différents filtres, les VLANs, les proxys.
La semaine 3 traite des VPNs et des protocoles de sécurité. Elle comprend 5 vidéos de cours sur les éléments protocolaires et cryptographiques utiles, les certificats électroniques et infrastructures à clé publique (PKI), ainsi que les protocoles de confidentialité TLS et IPsec. 3 TPs permettent d'expérimenter les certificats électroniques et de configurer des VPNs.
La semaine 4 effectue la synthèse des semaines précédentes pour permettre d'aider à comprendre quels mécanismes permettent de contrer quelles menaces. Au delà de la synthèse, elle introduit les mécanismes IDS/IPS et la notion de supervision de réseaux. Deux vidéos de cours sont prévues, 2 interviews sur la supervision de réseaux et le rôle des CERT[1], ainsi qu'un TP plus long permettant de valider les acquis.
La semaine 5 porte sur les architectures de sécurité et sur les aspects méthodologies propres à la sécurité des réseaux. 2 vidéos de cours présentent les architectures traditionnelles et avancées ; 1 bureau d'étude permet aux apprenants de construire une architecture de sécurité et de comprendre de façon non approfondie la méthodologie de sécurité, à savoir : la réglementation, les normes, l'analyse de risque, les politiques de sécurité et l'audit.
La dernière semaine prévoit également une dernière évaluation portant sur l'ensemble du contenu du MOOC.

6 Environnement de TP retenu : Labtainers

Bien qu'il existe aujourd'hui une grande variété d'outils de simulation permettant l'apprentissage de la sécurité et des réseaux par la pratique, notre choix s'est porté sur Labtainers[2] et la distribution de l'environnement de TP par une machine virtuelle, ceci pour les raisons suivantes :

- **Machine virtuelle**. Labtainers ne fonctionne actuellement que sous GNU/Linux, ce qui nous a conduit à distribuer notre environnement de TP dans une machine virtuelle afin de permettre une utilisation dans d'autres systèmes d'exploitation. Ce mode de distribution, permet de limiter les difficultés d'adaptation aux systèmes hôtes.

- **Conteneurs**. Les conteneurs utilisés par Labtainers s'appuient sur Docker. Ceci permet de créer des architectures de réseau relativement complexes comprenant des dizaines de noeuds dans lesquelles les conteneurs peuvent jouer les rôles de commutateurs, routeurs, serveurs, terminaux et passerelles de différents niveaux protocolaires avec des ressources réduites.

- **GNU/Linux**. GNU/Linux inclut un grand nombre d'outils d'attaque et de protection, il permet donc une grande variété de scénarios de TPs.

- **Vivier de TPs existants**. Labtainers comprenait par défaut une quarantaine de TPs qui pour certains nous ont inspirés.

- **Instances locales**. L'utilisation d'instances locales des outils permet de réaliser les TPs hors ligne, ce qui n'est pas possible lorsque ces instances s'exécutent dans un cloud. Par ailleurs, comme en dehors de la diffusion de l'environnement de TP, les ressources utilisées sont celles de l'apprenant, le coût d'exécution du MOOC est beaucoup plus restreint pour ses organisateurs. En contrepartie, l'utilisation locale demande une adaptation de l'environnement diffusé à la machine de l'apprenant ce qui peut se traduire par des incompatibilités et un coût non négligeable en termes de support à l'installation et à l'utilisation. La mise à disposition d'outils

[1] CERT pour *Computer Emergency Response Team*
[2] https://my.nps.edu/web/c3o/labtainers

utilisables à distance en particulier dans le cadre d'un MOOC orienté sécurité pose par ailleurs le problème du contrôle des actions des utilisateurs et de la responsabilité de celles-ci.

- **Solutions libres**. Les solutions libres sont généralement plus adaptables et sont moins coûteuses que les solutions propriétaires, même si certaines solutions propriétaires sont gratuites (GNS3, Packet-tracer).

- **Evaluation automatisée**. Labtainers fournit un support à l'évaluation des actions des apprenants permettant d'intégrer les travaux pratiques dans des activités notées. Cependant, nous n'utilisons pas cette fonctionnalité actuellement.

- **Eventail de TPs à enrichir par la communauté**. Nous comptons enrichir l'éventail de TPs disponibles dans Labtainers au bénéfice de la communauté scientifique.

Labtainers a un point faible, celui d'être une solution pour le moment uniquement orientée texte. Nous n'avons pas jugé ce point là comme problématique étant donné que le MOOC s'adresse à des utilisateurs ayant déjà des acquis en informatique et en réseau.

7 Conclusions

L'Institut Mines-Télécom et ses écoles commencent à diffuser des parcours certifiants, en particulier en Afrique. Le MOOC Sécurité des Réseaux contribuera à enrichir l'offre, l'objectif étant d'aller jusqu'à une licence télécom en ligne.

8 Remerciements

L'équipe du MOOC remercie l'Agence Nationale de la Recherche, les coordinateurs du projet ANR FLIRT (Formations Libres et Innovantes Réseaux & Télécom) et la Fondation Patrick et Lina Drahi pour leur soutien financier, et leurs conseils.