RedTeam Lab: l'Enseignement par la CyberAttaque.

Kevin ARNASSALOM, Joel GROUFFAUD et Tahiry RAZAFINDRALAMBO
IUT de Saint-Pierre - Université de la Réunion
40 avenue de Soweto - Terre Sainte - 97455 Saint-Pierre
kevin.arnassalom@rt-iut.re joel.grouffaud@rt-iut.re tahiry@rt-iut.re

***Abstract*— La cybersécurité est au centre de l'attractivité de nos filières. L'enseignement des protocoles réseaux, de la théorie et des langages de programmation, de la théorie et des systèmes d'exploitation ou des mathématiques et de la cryptographie pour ne citer que ceux là. Dans ce contexte il est important de repenser l'approche de l'enseignement des matières fondamentales de nos filières pour les rendre plus attractives. Dans cet article nous nous intéressons à l'enseignement de la cybersécurité par l'attaque. Cette approche que nous proposons est une approche *top-down* dans laquelle le point de départ de chaque enseignement est la vulnérabilité puis l'attaque de ce système vulnérable et enfin la théorie sous-jacente. Nous adossons ces enseignements à un laboratoire dans lequel des vulnérabilités sont insérées pour permettre une mise en pratique immédiate. Cet article décrit cette méthode d'enseignement que nous voulons mettre en place et la description du laboratoire nommmé : RedTeam Lab.**

I. INTRODUCTION

"*Faire de la cybersécurité une culture nationale*" : le Ministre de l'Intérieur, Gérard Colomb annonce la couleur dans l'avant-propos d'un rapport, intitulé "État de la menace liée au numérique en 2018" [1], qui lui a été remis le 20 juin 2018. Cette étude, coordonnée par la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), présente un panel exhaustif des diverses menaces et attaques que peuvent subir un particulier ou un système d'information. Elle fait référence à une autre étude, éditée par le Club des Experts de la Sécurité de l'Information de du Numérique (CESIN) qui indique que près de 80 % des entreprises ont été touchées par au moins une cyberattaque en 2017, alors que la cybersécurité représente moins de 5 % du budget IT pour deux tiers des entreprises. Un point important à noter pour nos formations réseaux et télécommunications : cette étude met en avant les nombreuses menaces portées par l'Internet des objets.

Quantité d'autres études faisant référence dans le monde de la cybersécurité (Cisco [2], ANSSI [3]) parviennent aux même conclusions : les attaques sont de plus en plus nombreuses, et toujours plus sophistiquées, et nécessite en retour, une expertise de plus en plus pointue dans le champ de la sécurité défensive. La firme de recherche Cybersecurity Ventures [4] fournit quelques chiffres vertigineux : le marché mondial de la cybersécurité a augmenté d'un facteur 35 ces treize dernières années, et attend une croissance à deux chiffres pour la période 2017-2021, avec un chiffre d'affaire cumulé supérieur à 1000 milliards de dollars. Dans le même temps, ce cabinet s'attend à la création de 3,5 millions d'emplois (au niveau mondial) d'ici 2021. A titre d'exemple, le Ministère de l'Intérieur français annonce la création de 800 postes, ce qui n'est pas, tout le monde le sait, la tendance lourde de la fonction publique. Cet état des lieux confère aux organismes de formation (initiale ou FTLV), et en premier lieu évidemment les départements Réseaux et Télécommunications des IUT, une reponsabilité particulière, et ouvre un domaine immense à explorer.

II. ÉTAT DES LIEUX DE L'ENSEIGNEMENT DE LA CYBERSÉCURITÉ A L'IUT DE SAINT-PIERRE

A. En DUT RT

Le PPN de 2013 a "relégué" la sécurité au sein de modules complémentaires. A Saint-Pierre, nous proposons dans notre maquette le module M4210C "Infrastructures de sécurité". Au regard des enjeux exposés dans notre introduction, c'est clairement insuffisant. Ceci d'autant plus que de nombreux lycéens sont attirés par notre département sur des thématiques de cybersécurité. Certes, certains arrivent chez nous avec une vision biaisée de ces notions, forgée par les médias, les films ou les jeux vidéo. Le discours "vous verrez ça quand vous serez plus grands", "il faut d'abord étudier les technologies et les protocoles" ne les satisfait pas, et nous verrons dans la partie suivante que nous avons instillé, dès que possible, et parfois dès le premier semestre, des notions de cybersécurité.

B. En licence professionnelle MRIT

En licence professionnelle, les enjeux sont différents. Les bases sont solides, après le DUT ou le BTS. Pour les parcours ASUR et RIMS de notre licence MRIT, nous avons saisi l'opportunité de la labellisation SecNumEdu de l'ANSSI pour faire de la cybersécurité une notion ubiquitaire du programme, comme le demande le cahier des charges du label.

III. LA PÉDAGOGIE PAR L'ATTAQUE

A. La meilleure défense, c'est l'attaque !

Cet adage n'est pas à prendre au pied de la lettre, comme au football ou dans le domaine militaire. Simplement, et c'est presque une évidence, on protège un système d'information comme on protège une maison en recherchant les points de fragilité, et ensuite en renforçant ce qui semble être suceptible de favoriser une intrusion.

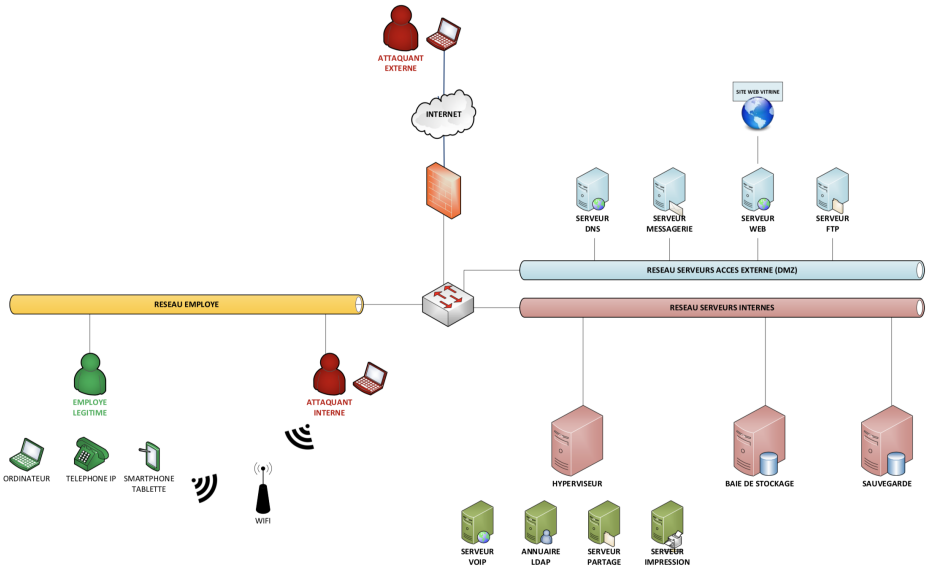

Fig. 1. L'architecture du Red Team Lab

B. *La cyberattaque, une compétence recherchée*

La cybersécurité est souvent vue, dans les programmes d'enseignement, sous l'angle défensif, les aspects offensifs semblant être évoqués à titre culturel. Néanmoins, les compétences de hacking deviennent de plus en plus recherchées, par les sociétés de tests d'intrusion (pen-testing) notamment. En particulier, les nouvelles offres de cyberassurance intègrent un volet "prévention" qui passera par des audits de sécurité et des tests d'intrusion.

C. *L'approche red-team*

Dans cette partie, nous développerons la notion d'approche "red team" (l'équipe des attaquants) par opposition à l'approche "blue team" (les défenseurs).

D. *Un apprentissage plus efficace*

Pour des jeunes férus de jeux vidéo, la sécurité offensive, qui passe par l'apprentissage des techniques de hacking, est un argument de choix pour s'orienter vers nos filières.

Dans cette partie, nous montrerons que l'enseignement des techniques de hacking n'est pas un argument publicitaire. Il s'intègre dans une vraie démarche pédagogique, en trois temps :

1) Présentation et étude d'un protocole (exemple : DHCP)
2) Présentation et mise en oeuvre d'une attaque (exemple : DHCP starvation, DHCP rogue)
3) Présentation de la contre-mesure associée (exemple : DHCP snooping)

Les étudiants comprennent l'intérêt de l'étude du protocole, au delà de sa simple mise en oeuvre, au moment de la phase 2. Ainsi, expliquer le rôle des différents flags de l'entête TCP peut être austère, pour les étudiants et aussi pour l'enseignant. Néanmoins, lors d'un scan de ports (avec l'outil nmap par exemple), il est essentiel de maîtriser le fameux *three way handshake* de TCP. L'avantage collatéral de cette approche est que les étudiants s'intéressent aux RFCs !

IV. LES PHASES D'UNE ATTAQUE

Dans cette partie, nous rappellerons les différentes phases d'une attaque, telles que définies dans la certification Ethical Hacking (CEH) [5].

V. LE RED TEAM LAB

Le point de départ de notre démarche a été la connaissance d'une session de formation CEH organisée à la Réunion, en janvier 2018. Sachant que l'autoformation n'est pas la méthode la plus efficace dans ce domaine, au vu de la sophitication des moyens mis en oeuvre par les hackers, et malgré le coût élevé, pour un département d'IUT (près de 4000 euros par participant), nous avons choisi d'inscrire les trois auteurs de cet article à cette formation.

Pour accompagner cette pédagogie par l'attaque, et armés de la conviction que la pratique est la méthode la plus efficace, nous avons planifié, sur l'année 2018, l'installation, au sein du département, un laboratoire de pen-testing, nommé **Red Team Lab**. Il s'agit d'un système d'information grandeur réelle, totalement indépendant de l'intranet de l'IUT.

Ce laboratoire sera bien entendu utilisé dans le cadre des enseignements en DUT et en licence professionnelle, et à l'occasion d'un Diplôme Universitaire Cyberattaque Cyberdéfense, validé par les instances de l'IUT et de l'Université, et dont une première session est programmée en 2019. Nous souhaitons même insufler l'esprit Fablab, en laissant un accès libre aux étudiants et aux partenaires extérieurs de l'IUT.

Nous présenterons dans cet article l'architecture de ce laboratoire, dont un premier synoptique est fourni sur la figure 1.

REFERENCES

[1] "La cybersécurité une culture nationale," 2018. [Online]. Available : http ://riteproject.eu/2014/10/23/slow-internet-more-bandwidth-is-not-the-answer/

[2] CISCO, 2017. [Online]. Available : https ://www.cisco.com/c/fr_fr/products/security/security-reports.html

[3] ANSSI, 2017. [Online]. Available : https ://www.ssi.gouv.fr/actualite/lannee-2017-un-tournant-pour-la-securite-numerique-en-france/

[4] CybersecurityVentures, 2018. [Online]. Available : https://cybersecurityventures.com/

[5] CEH, 2018. [Online]. Available : https ://www.eccouncil.org/programs/certified-ethical-hacker-ceh/