

Fiches pédagogiques sur la sécurité des réseaux

CyberEdu



Table des matières

| | | |
|---|---|----|
| 1 | Fiche 1 : capture de données sur un réseau | 5 |
| 2 | Fiche 2 : attaque sur un réseau | 7 |
| 3 | Fiche 3 : pare-feux et proxys | 11 |
| 4 | Fiche 4 : systèmes de détection d'intrusion | 14 |
| 5 | Fiche 5 : IPSec | 17 |
| 6 | Fiche 6 : SSH | 20 |
| 7 | Fiche 7 : SSL/TLS | 23 |

Introduction

Objectifs

Les fiches pédagogiques présentées dans ce guide ont pour objectif de mettre en avant les éléments fondamentaux de la sécurité des réseaux qui peuvent être présentés à des étudiants de l'enseignement supérieur non-spécialistes du domaine. Les fiches apportent à l'enseignant des repères pédagogiques mais ne peuvent constituer à elles seules un support d'apprentissage pour l'enseignant. Les fiches pédagogiques peuvent typiquement être utilisées pour illustrer un cours sur les fondamentaux des réseaux informatiques.

Prérequis pour les étudiants

Chacune des sept fiches indique les prérequis nécessaires à sa compréhension. Les prérequis portent sur les connaissances fondamentales en réseaux informatiques : structures d'un réseau local, dispositifs sur le réseau (routeur, concentrateur, commutateur) ainsi que les protocoles TCP/IP. La maîtrise de la cryptographie n'est pas nécessaire, mais elle permet d'approfondir certains concepts présentés dans les fiches 5 à 7.

Prérequis pour les formateurs

Les fiches apportent des repères pédagogiques aux enseignants, en présentant de manière structurée et concise les sujets importants de la sécurité des réseaux qui peuvent être présentés à des étudiants durant un cours sur les fondamentaux des réseaux informatiques. Ces fiches ne constituent pas un cours complet sur la sécurité des réseaux. Il n'est pas demandé à l'enseignant de parfaitement maîtriser le domaine de la sécurité, mais il devra se renseigner sur les sujets présentés pour pleinement exploiter les fiches pédagogiques. Une parfaite maîtrise des réseaux est fortement conseillée.

Utilisation du guide pédagogique

Ce document contient sept fiches pédagogiques à destination des enseignants en réseaux informatiques dans l'enseignement supérieur. Chaque fiche permettra à l'enseignant d'illustrer son cours de réseaux avec des notions de sécurité. Typiquement, l'enseignant consacra une quinzaine de minutes à la sécurité à la fin de chacun de ses chapitres. Les fiches peuvent être présentées en tout ou partie, dans l'ordre approprié à l'enseignement et aux étudiants visés. Les fiches sont toutefois présentées dans ce document en suivant un ordre logique qu'il est recommandé de suivre.

Des liens vers des documents en français ou en anglais sont fournis. Les fiches incluent des références vers des livres, articles et sites web permettant d'approfondir les sujets abordés. Deux supports sont régulièrement référencés dans ce document, à savoir le livre « Sécurité informatique, cours et exercices corrigés » de Gildas Avoine, Pascal Junod et Philippe Oechslin (éd. Vuibert, 2010), ainsi que les diapositives du cours de sécurité des réseaux de Gildas Avoine disponibles à l'adresse : <http://www.avoine.net/cyberedu/>. Ces diapositives sont régulièrement mises à jour et peuvent être utilisées librement par tout enseignant.

Ci-dessous figure un récapitulatif des sujets abordés, ainsi que le temps recommandé pour présenter les sujets et les prérequis correspondants.

| Numéro | Sujet | Durée (min) | Prérequis |
|---------|-----------------------------------|-------------|----------------------|
| Fiche 1 | Capture de données sur un réseau | 15 | Modèle ISO ou TCP/IP |
| Fiche 2 | Attaques sur un réseau | 15 | TCP/IP, DHCP, HTTP |
| | Déni de service | 15 (*) | TCP/IP, ARP, DNS |
| | Usurpation d'identité | 15 (*) | TCP/IP, HTTP |
| | Vol de session | 15 (*) | |
| Fiche 3 | Pare-feux et proxys | 15 | LAN |
| | Notions fondamentales | 15 (*) | LAN |
| | Règles de filtrage | 15 (*) | LAN, proxy |
| | Architectures des pare-feux | 15 (*) | |
| Fiche 4 | Systèmes de détection d'intrusion | 20 | LAN |
| Fiche 5 | IPsec | 20 | LAN, TCP/IP |
| Fiche 6 | SSH | 10 | LAN |
| | Authentification du serveur | 10 (*) | Cryptographie |
| | Protocoles cryptographiques | 5 | |
| | Authentification du client | 10 (*) | TCP/IP |
| Fiche 7 | Redirections de ports | 10 (*) | |
| | SSL/TLS | 15 | Client-serveur |
| | Fondements de SSL/TLS | 15 (*) | Cryptographie |
| | Mécanismes cryptographiques | | |

(*) Les durées marquées d'un astérisque correspondent à des activités complémentaires qui permettent d'étendre le sujet principal d'une fiche.

1 Fiche 1 : capture de données sur un réseau

1.1 Sujet d'étude

Capture de données sur un réseau.

1.2 Durée recommandée

15 minutes.

1.3 Objectifs pédagogiques

L'objectif de cette activité est de sensibiliser les étudiants à la facilité de capturer des données sur un réseau informatique, en particulier la capture de mots de passe qui transitent en clair.

1.4 Prérequis

Cette activité s'intègre dans un cours de réseaux et peut être présentée dès que les étudiants maîtrisent les différentes couches protocolaires d'un réseau informatique. Elle permet aux étudiants de confronter la connaissance acquise avec la pratique. Cette activité peut être présentée sous forme d'une démonstration d'environ 15 minutes faite par l'enseignant ou sous forme d'une séance de travaux pratiques. Dans ce dernier cas, il faudra prévoir une séance de une à deux heures de travaux pratiques. L'enseignant pourra profiter de cette activité pour rappeler aux étudiants qu'écouter un réseau informatique n'est pas anodin et peut conduire à des poursuites lorsque cette activité est réalisée à des fins non justifiées et sans le consentement explicite des personnes concernées.

1.5 Notions abordées

- Présentation de l'outil Wireshark.
- Capture de mots de passe POP, FTP, Telnet, HTTP, etc.
- HTTP et *cookies*.
- Concentrateur (hub) et commutateur (switch).

1.6 Description

L'enseignant présentera l'outil Wireshark aux étudiants en leur montrant les protocoles des différentes couches de communication. Il mettra notamment en avant le three-way handshake du protocole TCP et les numéros de séquence. Au niveau applicatif, il prendra quelques exemples de protocoles qui envoient des mots de passe en clair : POP, FTP et Telnet. Il pourra également prendre l'exemple de l'authentification « *basic* » du serveur web Apache. Si les notions fondamentales de la cryptographie ont été abordées avec les étudiants, alors l'enseignant pourra montrer la différence entre l'authentification « *basic* » où le mot de passe est envoyé en clair, et l'authentification « *digest* » où un protocole d'authentification par défi avec question/réponse (*challenge-response authentication protocol*) est utilisé, ce qui évite que le mot de passe ne soit envoyé en clair.

L'enseignant pourra expliquer le fonctionnement de HTTP. Il pourra notamment mettre en avant le concept de « *cookie* » et montrer à l'aide de Wireshark que le cookie est envoyé par le client dans les réponses au serveur. L'enseignant pourra ensuite expliquer le principe fondamental que seul le serveur (identifié par son nom de domaine) qui a déposé le cookie peut y avoir accès ultérieurement. Il pourra expliquer que les cookies permettent de chaîner les transactions et donc de simuler une session au niveau HTTP, et qu'il serait difficile aujourd'hui de se passer des cookies, notamment pour les sites de vente en ligne. L'enseignant pourra également souligner les effets pervers des cookies, notamment la traçabilité des internautes entre plusieurs sites qui font appel à une même régie publicitaire. Un internaute peut ainsi se voir proposer des offres d'achat de voitures sur un site d'information parce qu'il a précédemment consulté des annonces de vente d'automobiles sur un autre site.

L'enseignant présentera la différence majeure d'un point de vue technique entre un concentrateur (« *hub* ») et un commutateur (« *switch* »). Il pourra alors expliquer la différence entre ces deux dispositifs du point de vue de la capture de trafic (la compromission de tables ARP qui permet à un adversaire de contourner la difficulté apportée par le commutateur sera abordée dans la fiche n°2). L'enseignant pourra également aborder le filtrage par adresses MAC grâce au serveur DHCP pour réduire les intrusions sur le réseau, mais il devra alors mettre en avant sans ambiguïté les limites de cette approche : nécessité pour l'administrateur d'enregistrer les adresses MAC de tous les utilisateurs, mais surtout la possibilité pour un intrus d'usurper l'adresse MAC d'une machine autorisée.

Références

- [1] *Tele-Lab Internet Security*, http://telelab.aimcy.eu/pluginfile.php/36/mod_resource/content/1/3.%20Eavesdropping.pdf
- [2] LAURA CHAPPELL, *Wireshark 101 : Essential Skills for Network Analysis*, 370 pages, 2013, Laura Chappell University, (978-1893939721)
- [3] GILDAS AVOINE, *Network Sniffing*, <http://www.avoine.net/cyberedu/>

2 Fiche 2 : attaque sur un réseau

2.1 Sujet d'étude

Attaques sur un réseau.

2.2 Durée recommandée

- 15 minutes (déni de service) ;
- 15 minutes (usurpation d'identité) ;
- 15 minutes (vol de session).

2.3 Objectifs pédagogiques

L'objectif pédagogique de cette activité est de présenter aux étudiants quelques attaques élémentaires qu'il est possible de réaliser sur un réseau informatique : déni de service, usurpation d'identité et vol de session.

2.4 Prérequis

Cette activité s'intègre dans un cours de réseaux et peut être présentée dès que les étudiants maîtrisent les protocoles TCP/IP. La connaissance du fonctionnement du protocole ARP est également nécessaire pour présenter l'attaque par compromission de tables ARP et ses contre-mesures.

2.5 Notions abordées

- Les attaques sur les couches suivantes du modèle OSI
 - 2 (liaison de données) ;
 - 3 (réseau) ;
 - et 4 (transport).
- Les dénis de service (le ping de la mort, l'inondation de paquets SYN, l'attaque par rebond, le déni de service distribué, l'épuisement des adresses du serveur DHCP), les usurpations d'adresses et les vols de sessions (TCP et HTTP).
- Les contre-mesures correspondantes : *SYN cookies*, analyse des messages ARP.

2.6 Description

L'enseignant présentera lors de cette activité trois grands types d'attaques sur les réseaux, à savoir le déni de service (*denial of service*), l'usurpation d'identité (*spoofing*) et le vol de session (*hijacking*), ainsi que quelques contre-mesures usuelles. Si l'enseignant ne dispose pas d'assez de temps pour présenter les trois types d'attaques, il pourra se concentrer sur le déni de service.

Déni de service. En ce qui concerne le déni de service [1, 2, 3], l'enseignant pourra démarrer son cours avec l'exemple historique du « *ping de la mort* » (*ping of death*) qui est facile à comprendre. Cette attaque consiste à rendre inutilisable un service (routeur, serveur, imprimante, etc.) en lui

envoyant un paquet « *ping* » mal formé (datagramme IP de longueur supérieure à la longueur maximale autorisée). Bien que les systèmes soient résistants au « *ping* de la mort » depuis la fin des années 90, cette attaque permet à l'enseignant de souligner l'importance de vérifier la taille des données fournies en entrée à un système et l'importance de s'attendre à des comportements non spécifiés, inattendus.

L'enseignant pourra ensuite présenter l'attaque par inondation de paquets TCP SYN (*SYN flooding*) qui consiste pour un attaquant à noyer sa cible avec des demandes fictives d'établissement de connexion TCP. En envoyant un paquet TCP SYN mais en ne répondant pas au paquet TCP SYN ACK du serveur, le client (c'est-à-dire l'attaquant) laisse une connexion TCP semi-ouverte du côté du serveur et peut ainsi provoquer un déni de service dès que la file de connexions semi-ouvertes du serveur a atteint sa limite maximale. Il est alors intéressant de présenter une contre-mesure efficace : les *SYN cookies* [4].

Le parallèle avec les cookies HTTP pourra être fait : dans les deux cas, l'idée est que le protocole soit sans mémoire (stateless) pour le serveur. L'enseignant pourra éventuellement présenter le déni de service par « paquets kamikazes » (*Kamikaze Packets* ou *Christmas Tree Packets*), c'est-à-dire des paquets TCP dont les bits URG, PSH et FIN sont activés [5]. Envoyés en grand nombre, ces paquets malformés peuvent provoquer un comportement inattendu du routeur, par exemple un redémarrage inopiné.

L'enseignant pourra ensuite présenter rapidement l'attaque DHCP Starvation, qui consiste pour un attaquant à générer de nombreuses requêtes DHCP pour épuiser les adresses IP disponibles au niveau du serveur DHCP : les utilisateurs légitimes ne peuvent alors plus se connecter au réseau.

Enfin, si le principe du protocole BGP est connu des étudiants, alors il est possible de leur présenter l'attaque dite « attribut 99 » sur BGP. Cette attaque, qui consiste à transmettre des informations de routage erronées à un routeur BGP, peut provoquer un déni de service important sur une partie significative d'Internet et a pour origine une expérience utilisant une valeur d'attribut réservée [6, 7, 8].

L'enseignant pourra ensuite montrer comment accentuer l'impact d'une attaque par déni de service. Il pourra pour cela présenter l'approche par rebond (*smurf attack*) où un amplificateur de trafic est utilisé : par exemple un paquet « *ping* » envoyé sur une adresse de *broadcast* [9, 10]. L'enseignant pourra alors parler des règles élémentaires pour limiter cette attaque, qui consistent à interdire de propager ou de répondre à des requêtes envoyées sur une adresse de broadcast. Il pourra également présenter l'approche par déni de service distribué (DDoS) [11]. L'architecture typique d'une attaque par déni de service distribué pourra être décrite en introduisant le concept de « réseau de zombies » (*botnet*). Quelques exemples récents d'attaques réelles permettront d'illustrer le concept. La facilité d'une telle attaque pourra également être mise en avant en donnant des exemples de sites web qui offrent la possibilité de louer des réseaux de zombies. En parallèle à cela, des exemples de condamnations de loueurs de tels réseaux permettra de rappeler aux étudiants les risques légaux encourus avec de telles pratiques.

Usurpation d'identité. L'enseignant pourra avant tout présenter les attaques par usurpation DNS qui consistent à répondre à une requête DNS plus rapidement que le serveur DNS lui-même. Cette attaque, facilitée par l'usage du protocole UDP, sera ensuite complétée par l'empoisonnement de cache DNS (*DNS cache poisoning*), qui consiste pour un attaquant à envoyer de fausses informations à un serveur DNS en se faisant passer lui-même pour un serveur DNS [12]. L'enseignant pourra mettre en avant l'absence de sécurité dans le protocole DNS et indiquer qu'il existe DNSSEC, un protocole obligeant les serveurs DNS à fournir des données signées.

L'enseignant pourra ensuite présenter les attaques par usurpation d'adresse IP (*IP Spoofing*). L'in-

térêt de cette attaque (c'est-à-dire usurper l'adresse IP d'une machine de confiance) sera présenté, puis les deux cas de figure possibles seront décrits : machine usurpatrice et machine usurpée sont situées sur le même LAN (cas simple) ou sur des LAN interconnectés par un commutateur (*switch*). Dans le second cas, la machine usurpatrice n'est pas en mesure de voir la réponse à son paquet TCP SYN et ne peut alors pas déterminer le numéro de séquence initial (ISN) du serveur victime de l'attaque. L'exemple de l'attaque de Kevin Mitnick contre Tsutomu Shimomura permettra d'illustrer l'attaque et de faire le lien avec l'attaque par inondation de requête TCP SYN : l'attaquant met hors service la machine usurpée pour éviter qu'elle ne réponde au serveur avec un paquet TCP RST. Plutôt que de présenter explicitement l'exemple de l'attaque de Kevin Mitnick, il est possible et pédagogiquement intéressant de fournir aux étudiants la trace complète de l'attaque [13] et de leur demander d'expliquer ce qui se passe en identifiant les différentes parties de l'attaque.

L'attaque par compromission de tables ARP (*ARP Poisoning*) [14] pourra ensuite être présentée. Pour aborder l'attaque par compromission de tables ARP, il est important que les étudiants soient à l'aise avec le modèle de communication en couches. En général, ils connaissent assez bien la conversion « nom de domaine » vers « adresse IP » grâce au DNS, mais la compréhension de la conversion « adresse IP » vers « adresse MAC » est généralement beaucoup moins bien maîtrisée. Il est alors important de rappeler les fondements du protocole ARP et ses lacunes en termes de sécurité : la table ARP gérée par le système d'exploitation mémorise généralement la dernière réponse ARP reçue, même si la machine n'a pas généré elle-même la requête ARP. L'enseignant pourra également donner quelques exemples pertinents d'utilisation de cette attaque pour usurper l'identité d'une imprimante, de la passerelle d'un réseau local ou d'un serveur DHCP. Il est important d'insister sur le fait que l'attaque ARP est facile à mettre en œuvre sur la majorité des systèmes. L'enseignant pourra faire une démonstration en utilisant par exemple l'outil « arpspoof ». Sans nécessairement entrer dans les détails, l'enseignant pourra expliquer qu'il existe des contre-mesures au niveau des commutateurs récents pour éviter cette attaque : configuration des commutateurs (mécanisme pVLAN ou équivalent), inspection dynamique des paquets ARP (*Dynamic ARP Inspection*) et détection de faux serveurs DHCP (*DHCP Snooping*).

Vol de session. L'enseignant pourra enfin présenter les attaques de type « vol de session » en mettant l'accent sur la différence fondamentale avec l'usurpation : dans le cas de l'usurpation, l'attaquant démarre une session en utilisant l'identité de la victime. Dans le cas du vol de session, l'attaquant attend que la victime démarre une session pour la lui voler. L'attaquant attend typiquement que la victime se soit authentifiée avant de lui voler sa session. Deux exemples pourront être donnés : vol de session TCP (TCP hijacking) et vol de session HTTP. Dans le premier cas, l'attaquant utilise par exemple une des techniques décrites pour usurper l'identité d'un client légitime ; l'enseignant analysera avec les étudiants l'impact d'injecter des paquets IP dans une session existante.

Dans le second cas, l'enseignant reviendra sur les connaissances de la fiche 1 en montrant que les *cookies* et les URL personnalisées permettent de constituer des « sessions » HTTP mais que cela constitue aussi une faiblesse dès que ces approches sont utilisées pour authentifier le client. L'enseignant pourra demander aux étudiants ce qui se passe si, par exemple, un client se fait voler un *cookie* du site web Amazon et qu'il a renseigné son numéro de carte bancaire dans le système d'Amazon (on ne parle pas des canaux sécurisés à ce stade).

Références

- [1] DANY FERNANDES, PAPA AMADOU SARR, *La protection des réseaux contre les attaques DOS*, http://www.mi.parisdescartes.fr/~osalem/Projects/Fernandes_Sarr.pdf, mai 2010
- [2] HOTTE MARION, LUTUN QUENTIN-EDOUARD, ASCOET THOMAS, *Protection contre les attaques de déni de service dans les réseaux IP*, http://www.mi.parisdescartes.fr/~osalem/Projects/Hotte_LUTUN_ASCOET.pdf
- [3] CERTA *Note d'information : Dénis de service — Prévention et réaction*, <http://cert.ssi.gouv.fr/site/CERTA-2012-INF-001/index.html>, 14 janvier 2013
- [4] D. J. BERNSTEIN, *TCP/IP SYN cookies*, <http://cr.yp.to/syncookies.html>
- [5] *Christmas Tree Attack — CompTIA Security+ SY0-401 : 3.2*, <https://www.youtube.com/watch?v=bVrxL2AL4yQ>
- [6] FRANÇOIS CONTAT, SARAH NATAF, AND GUILLAUME VALADON, *Influence des bonnes pratiques sur les incidents BGP*, http://www.ssi.gouv.fr/IMG/pdf/Influence_des_bonnes_pratiques_sur_les_influences_BGP_article.pdf
- [7] STÉPHANE BORTZMEYER, *BGP et le désormais célèbre attribut 99*, <http://www.bortzmeyer.org/bgp-attribut-99.html>
- [8] *RIPE NCC and Duke University BGP Experiment*, <https://labs.ripe.net/Members/erik/ripe-ncc-and-duke-university-bgp-experiment/>
- [9] *Securing Cisco Routers with No IP Directed-Broadcast*, <http://learn-networking.com/network-security/securing-cisco-routers-with-no-ip-directed-broadcast/>
- [10] *Changing the Default for Directed Broadcasts in Routers*, <http://tools.ietf.org/html/rfc2644/>
- [11] CERTA *Note d'information : Le déni de service distribué*, <http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-001/>, 19 juin 2000
- [12] *DNS Cache Poisoning Attack*, <https://www.checkpoint.com/defense/advisories/public/dnsvideo/index.html>
- [13] *Technical details of the attack described by Markoff in NYT*, <http://www.cs.berkeley.edu/~daw/security/shimo-post.txt>
- [14] ROY ABU BAKAR *ARP Poisoning Attack and Mitigation for Cisco Catalyst*, <http://www.royabubakar.com/blog/2013/11/04/arp-poisoning-attack-and-mitigation-for-cisco-catalyst/>, 4 novembre 2013
- [15] GILDAS AVOINE, PASCAL JUNOD, PHILIPPE OECHSLIN, *Sécurité informatique, cours et exercices corrigés, 2e édition*, 10, 304 pages, Vuibert (978-2711748600)
- [16] GILDAS AVOINE, *Network Attacks*, <http://www.avoine.net/cyberedu/>

Enfin, l'enseignant pourra illustrer son cours avec des condamnations récentes de dénis de service en recherchant « déni de service condamnation » sur un moteur de recherche.

3 Fiche 3 : pare-feux et proxys

3.1 Sujet d'étude

Mécanismes et architectures des pare-feux (*firewalls*) et des serveurs proxys.

3.2 Durée recommandée

- 15 minutes (notions fondamentales) ;
- 15 minutes (règles de filtrage) ;
- 15 minutes (architectures).

3.3 Objectifs pédagogiques

L'objectif pédagogique de cette activité est de présenter aux étudiants

1. les notions fondamentales (principes et fonctionnalités) des pare-feux ;
2. les règles de filtrage et la méthodologie pour les définir et
3. les architectures usuelles des pare-feux et des serveurs (*proxys*).

3.4 Prérequis

Cette activité s'intègre dans un cours de réseaux et peut être présentée dès que les étudiants maîtrisent les protocoles TCP/IP. La connaissance de la couche 2 (liaison de données) n'est pas nécessaire. L'enseignant décidera de présenter les activités correspondant aux objectifs pédagogiques (1), (1, 2) ou (1, 2, 3) en fonction du temps disponible.

Il est important de ne pas restreindre ce cours à des pare-feux spécifiques (commerciaux ou non). L'approche pédagogique devra au contraire mettre en avant les concepts fondamentaux et pérennes des pare-feux. L'enseignant pourra toutefois présenter des exemples de pare-feux spécifiques (iptables pour Linux, Checkpoint, Sonic Wall, etc.) à la fin de l'activité et montrer que les connaissances théoriques acquises peuvent être directement exploitées sur ces pare-feux largement répandus.

3.5 Notions abordées

- Principes fondamentaux de la protection des réseaux
- Techniques des pare-feux
- Serveur *proxys*
- Attaques par usurpation d'adresses IP et par inondation de requêtes TCP SYN

3.6 Description

Cette fiche est constituée de trois parties : les notions fondamentales (principes et fonctionnalités) des pare-feux, puis les règles de filtrage et la méthodologie pour les définir, et enfin les architectures usuelles des pare-feux et des serveurs *proxys*.

Notions fondamentales. L'enseignant présentera et expliquera les principes fondamentaux à appliquer pour assurer la protection d'un réseau :

- le principe du moindre privilège ;
- la défense en profondeur ;
- la mise en place d'un point de contrôle obligatoire ;
- l'identification et renforcement du maillon le plus faible ;
- l'interdiction comme politique par défaut (par opposition au concept de liste noire). Tout ce qui n'est pas autorisé est donc interdit ;
- l'implication des utilisateurs ;
- la simplicité.

Afin de renforcer la compréhension, l'enseignant illustrera ces principes par des cas concrets. Par exemple, il pourra illustrer le principe du point de contrôle obligatoire (qui consiste à obliger tout le trafic entrant et sortant du réseau à passer par un point de contrôle unique) en présentant des architectures de réseaux qui respectent (ou ne respectent pas) ce principe. La participation des utilisateurs pourra quant à elle être illustrée par des expériences personnelles de l'enseignant où des utilisateurs ont contourné des mesures de sécurité car leurs besoins n'avaient pas été suffisamment pris en compte. Citons par exemple l'utilisation d'un téléphone en mode relais pour télécharger un logiciel sur son lieu de travail à partir d'un site bloqué par le pare-feu de l'entreprise.

Les fonctionnalités les plus importantes des pare-feux pourront ensuite être décrites, en particulier le filtrage des paquets entrants et sortants à l'aide de règles d'interdiction et d'autorisation. L'enseignant pourra aussi aborder les fonctionnalités additionnelles (qui ne sont pas des fonctionnalités intrinsèques des pare-feux mais qui sont généralement réalisées au niveau de celui-ci) comme la traduction (dynamique et statique) d'adresses IP (NAT), la détection de virus, le chiffrement du trafic, etc.

Expliquer les fonctionnalités des pare-feux permet également aux étudiants de mieux comprendre le fonctionnement de leur point d'accès à Internet situé à leur domicile. Il est, en effet, facile de montrer aux étudiants l'importance du sujet abordé car ils y sont confrontés eux-mêmes dans leur vie personnelle. L'apprentissage peut être renforcé par des travaux pratiques encadrés, mais l'enseignant peut aussi suggérer aux étudiants d'étudier le fonctionnement de leur point d'accès personnel et de mettre en pratique certains des concepts abordés comme le filtrage et la traduction (dynamique et statique) d'adresses IP.

Règles de filtrage. Les règles de filtrage pourront être présentées plus en détails, en particulier dans les cursus où les étudiants se destinent éventuellement au métier d'administrateur informatique. L'enseignant pourra avant tout présenter le filtrage avec des pare-feux sans mémoire (*stateless*) et mettre en avant les limites de tels pare-feux. Il pourra dans un second temps introduire les pare-feux avec mémoire (*stateful*) en indiquant leurs avantages, sans oublier de mentionner que le fait d'utiliser beaucoup de ressources (mémoire et CPU) pour suivre l'état de toutes les connexions ouvre la porte à des attaques par déni de service.

Afin de faire participer les étudiants, il est possible de présenter des scénarios et de leur demander d'écrire les règles de filtrage correspondantes. L'enseignant pourra faire le lien avec la fiche 2 en expliquant comment les pare-feux agissent pour éviter les attaques par inondation de requêtes TCP SYN.

Architectures des pare-feux. Pour approfondir les connaissances des étudiants, les principales architectures de pare-feux pourront être présentées, en indiquant pour chacune d'entre elles les fonctionnalités usuelles ainsi que les cas d'usage :

- pare-feux personnels ;

- pare-feux avec filtrage et NAT ;
- pare-feux avec zone démilitarisée ;
- pare-feux (en sandwich).

Il sera important de souligner que choisir une architecture de pare-feux doit prendre en compte les compétences de l'équipe qui sera chargée de l'administrer.

Le concept de serveur *proxy* (direct et inverse) sera introduit en mettant en avant les avantages des serveurs *proxys* en termes de sécurité, notamment dans une architecture avec des pare-feux (en sandwich) où il devient facile d'imposer les *proxys* comme point de passage obligatoire où une politique de sécurité peut-être appliquée. L'enseignant pourra passer en revue les principaux *proxys* existants : HTTP, HTTPS, FTP, DNS, SOCKS. L'enseignant insistera sur le risque potentiel que constitue un serveur *proxy* générique de type SOCKS. Il est également possible de parler du problème des serveurs *proxys* ouverts (*open relays*) en insistant sur l'impact négatif que de tels serveurs *proxys* peuvent avoir sur une infrastructure, ainsi que les règles fondamentales à appliquer pour éviter qu'un serveur interne ne se transforme malencontreusement en serveur *proxy* ouvert.

Références

- [1] GILDAS AVOINE, PASCAL JUNOD, PHILIPPE OECHSLIN, *Sécurité informatique, cours et exercices corrigés*, 2e édition, 10, 304 pages, Vuibert (978-2711748600)
- [2] GILDAS AVOINE, *Network Attacks*, <http://www.avoine.net/cyberedu/>
- [3] ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, http://www.ssi.gouv.fr/IMG/pdf/NP_Politique_pare_feu_NoteTech.pdf

4 Fiche 4 : systèmes de détection d'intrusion

4.1 Sujet d'étude

Systèmes de détection d'intrusion (IDS).

4.2 Durée recommandée

20 minutes.

4.3 Objectifs pédagogiques

L'objectif pédagogique de cette activité est de présenter aux étudiants les systèmes de détection d'intrusion pour les réseaux, en mettant en avant les atouts, mais aussi les limites de tels dispositifs.

4.4 Prérequis

Cette activité s'intègre dans un cours de réseaux et peut être présentée dès que les étudiants ont une vision globale de l'architecture d'un réseau local. Il n'est pas nécessaire dans ce cours de maîtriser les protocoles de communication, bien que la connaissance de ceux-ci aidera à comprendre la construction de signatures d'attaques.

4.5 Notions abordées

- Systèmes de détection d'intrusion (IDS) sur un réseau.
- Détection par signature d'attaques.
- Détection par caractérisation du trafic (approche comportementale).
- IDS *Snort*.

4.6 Description

Pour introduire les systèmes de détection d'intrusion (IDS), l'enseignant pourra expliquer la différence entre les notions de protection (on se protège en installant par exemple un pare-feu ou un logiciel anti-virus) et de défense (on réagit face à une attaque). Les IDS sont donc des outils de défense. Les grandes familles d'IDS seront présentées, en prenant garde à distinguer les IDS de réseaux (*Network Intrusion Detection System*, NIDS) des IDS systèmes (*Host Intrusion Detection System*, HIDS). Bien que l'enseignant concentrera ses explications sur les IDS de réseaux, en particulier ceux qui effectuent une analyse en temps réel du trafic, le schéma ci-après permet de replacer ce type d'IDS dans le contexte plus global de la détection d'intrusion.

| | Analyse en temps réel | Analyse <i>a posteriori</i> |
|-----------------|--|--|
| IDS de réseaux | Capture et analyse du trafic sur le réseau | Analyse des traces et des configurations des dispositifs sur le réseau |
| IDS de systèmes | Inspection des interruptions du système | Analyse des traces enregistrées dans le système |

Les IDS de réseaux par analyse en temps réel sont essentiellement constitués d'un outil pour capturer le trafic sur le réseau et d'un moteur qui analyse ce trafic selon des règles prédéfinies utilisant les champs des paquets de différents protocoles. Lorsque le trafic du réseau active une règle de l'IDS, alors l'IDS exécute une action. Les actions usuelles pourront être passées en revue par l'enseignant : journaliser l'événement, alerter l'administrateur (message électronique, interface web, texto, etc.), ou réagir (mettre fin à une connexion, modifier les règles du pare-feu, etc.). Lorsque l'IDS peut réagir lui-même à une attaque, on parle alors généralement de système de prévention d'intrusion (*Intrusion Prevention System*, IPS), qui constitue alors à une mesure de protection et non plus de défense selon la terminologie employée.

Deux types d'IDS de réseaux par analyse en temps réel seront vus plus en détails :

- IDS par caractérisation du trafic sur le réseau.
- IDS par reconnaissance de signatures d'attaques.

IDS par caractérisation du trafic sur le réseau.

- Des statistiques réalisées sur le trafic du réseau permettent de détecter un comportement anormal du trafic. Par exemple, la quantité de données téléchargées sur Internet est significativement supérieure aux limites usuelles.
- Faux négatifs :
 - Un tel IDS peut reconnaître de nouvelles attaques, mais il peut aussi ne pas les reconnaître.
- Faux positifs :
 - Un tel IDS peut aussi détecter une attaque alors qu'il n'y en a pas. Dans l'exemple précédent, la quantité inhabituelle de données téléchargées est peut-être due au téléchargement par de nombreux employés d'une nouvelle version de leur système d'exploitation.
- Le fort taux de faux positifs rend ces IDS peu populaires.

IDS par signatures.

- L'IDS possède une base de signatures d'attaques connues. Par exemple une requête HTTP contenant une URL d'une longueur supérieure à 2 000 caractères pourra être considérée comme une tentative d'attaque par débordement du tampon de stockage.
- Un IDS par signatures ne reconnaît pas les nouvelles attaques, ce qui nécessite de mettre à jour la base de signatures régulièrement.
- Faux négatifs :
 - Il est difficile de reconnaître des attaques ciblées car l'attaquant peut éventuellement modifier le code de l'attaque pour qu'il ne corresponde plus à la signature originale.
 - Les signatures sont parfois trop restrictives, ce qui empêche de détecter les variantes proches de l'attaque.
- Faux positifs :
 - Les faux positifs n'existent *a priori* pas avec les IDS par signatures, mais les attaques détectées ne sont pas toujours pertinentes pour le réseau considéré : par exemple une attaque sur le système Windows est détectée alors que le réseau ne contient que des ordinateurs utilisant Linux.

L'enseignant pourra ensuite discuter de l'IDS le plus répandu, *Snort*, et montrer quelques exemples de signatures (*rules*). L'enseignant pourra éventuellement expliquer le concept de pot de miel (*honeypot*) qui permet de récupérer des signatures d'attaques, mais parler de pots de miel à forte ou faible interaction conduirait l'enseignant à aller trop en profondeur dans la matière.

Enfin, il est important que l'enseignant fasse le point sur les avantages et inconvénients des IDS. Il pourra notamment aborder les points suivants : Les IDS par caractérisation du trafic ne sont pas très efficaces (taux de faux positifs élevé). La majorité des attaques détectées par un IDS par signatures peuvent être contrées par une mise à jour du système ou du pare-feu dès qu'elles sont connues. La portée de l'IDS est donc limitée aux cas où le système ne peut pas être mis à jour et aux cas où la signature peut être installée plus rapidement que la mise à jour du système (la publication de la mise à jour peut prendre plusieurs jours) ou du pare-feu. Il peut néanmoins s'agir d'un bon mécanisme de défense en profondeur. Il ne faut considérer l'installation d'un IDS que si les mesures de protection usuelles (mise à jour des logiciels, pare-feu, anti-virus, etc.) sont déjà mises en place et maîtrisées. Il n'est, en effet, pas suffisant d'installer un IDS : il faut savoir comment réagir en cas d'alerte.

Références

- [1] GILDAS AVOINE, *IDS*, <http://www.avoine.net/cyberedu/>
- [2] ALEXANDRE MARTIN, JONATHAN BRIFFAUT, *Les IDS et IPS Open Source*, <http://cosy.univ-reims.fr/~fnolot/Download/Cours/reseaux/m2pro/SESY0708/ids-ips.pdf>
- [3] JONATHAN KRIER, *Les systèmes de détection d'intrusions*, <http://dbprog.developpez.com/securite/ids/>

5 Fiche 5 : IPSec

5.1 Sujet d'étude

IPsec.

5.2 Durée recommandée

20 minutes.

5.3 Objectifs pédagogiques

L'objectif pédagogique de cette activité est de présenter aux étudiants les concepts des réseaux privés virtuels (VPN) en leur expliquant comment ces VPN peuvent protéger les communications. Les protocoles et primitives cryptographiques utilisés pour les VPN nécessitent des prérequis importants en cryptographie et ne sont donc pas présentés dans cette activité.

5.4 Prérequis

Cette activité s'intègre dans un cours de réseaux et peut être présentée dès que les étudiants maîtrisent les protocoles TCP/IP. Il est intéressant de présenter IPsec (Fiche 5), TLS (Fiche 6) et SSH (Fiche 7) pour montrer la variété des outils disponibles pour créer des tunnels, et mettre en avant les avantages et inconvénients de chacun de ces outils. Présenter les trois fiches permet également aux étudiants de bien associer les protocoles IPsec, TLS et SSH aux couches correspondantes de la communication.

5.5 Notions abordées

- Réseaux privé virtuel (Virtual Private Network), VPN
- IPsec
- Modes transport et tunnel
- Méthodes de sécurisation AH et ESP
- Traduction d'adresses (*Network Address Translation*), NAT

5.6 Description

L'enseignant pourra démarrer l'activité en décrivant l'objectif fondamental des réseaux privés virtuels, qui est d'étendre un réseau local (LAN) à des machines distantes tel que ces machines agissent comme si elles étaient dans le LAN. Du point de vue de la sécurité, les communications (généralement à travers Internet) depuis le LAN vers les machines distantes, et réciproquement, doivent être aussi sécurisées que les communications entre les machines à l'intérieur du LAN. Le principe est que les communications entre les machines distantes et le LAN passent à travers un tunnel sécurisé. En pratique, les paquets subissent des transformations cryptographiques pour assurer leur authenticité, intégrité et éventuellement leur confidentialité. Dans certaines configurations, les paquets peuvent être entièrement encapsulés dans de nouveaux paquets pendant leur transport à travers Internet.

Afin de motiver les VPN, l'enseignant pourra présenter deux cas typiques d'usage : (1) un employé nomade veut se connecter au LAN de son entreprise pour accéder à des services qui ne sont accessibles qu'au sein de ce LAN, et (2) deux sites distants d'une même entreprise souhaitent être connectés à travers un tunnel sécurisé.

L'enseignant présentera ensuite le protocole le plus utilisé pour créer des VPN au niveau de la couche IP : IPsec.

Les deux modes d'IPsec seront détaillés : le mode transport qui protège le contenu des paquets sans modifier l'entête IP d'origine, et le mode tunnel qui encapsule intégralement les paquets dans de nouveaux paquets. L'enseignant pourra demander aux étudiants quel mode est le plus adapté lorsque (1) le tunnel est de bout en bout, c'est-à-dire établi entre les deux machines qui souhaitent communiquer, et (2) le tunnel est établi par deux routeurs intermédiaires, de manière totalement transparente pour les deux machines qui souhaitent communiquer. Un dessin facilitera la compréhension des étudiants.

À partir du dessin, l'enseignant pourra préciser que les machines (ou routeurs) aux deux extrémités du canal utilisent une base de données de politiques de sécurité (Security Policy Database, SPD) définie par l'administrateur du VPN pour décider **quoi** protéger. Les règles de cette politique de sécurité peuvent être par exemple :

- sécuriser tout le trafic ;
- sécuriser les paquets destinés au serveur de virements bancaires ;
- sécuriser le trafic UDP ;
- sécuriser le trafic TCP sauf le trafic protégé par TLS.

Si le temps le permet, l'enseignant pourra introduire le concept d'associations de sécurité (*Security Association*, SA) qui permettent de mettre en œuvre les règles mentionnées, c'est-à-dire décider **comment** protéger la connexion. Il y a ainsi une SA définie pour chaque flux unilatéral de données. Il y a donc une SA par triplet adresse de destination, type de protocole (TCP, UDP, etc.) et numéro de port. La SA contient en particulier les paramètres pour sécuriser le flux (algorithmes et clefs cryptographiques à utiliser, date de validité des clefs, numéros de séquence, etc.). L'enseignant pourra indiquer que les SA sont établies entre les machines en utilisant un protocole spécifique d'échanges de clefs (*Internet Key Exchange*, IKE), mais la description en profondeur de IKE est plus appropriée à un cours de sécurité qu'à un cours de réseaux.

L'enseignant pourra ensuite introduire la méthode de sécurisation AH (*Authentication Header*) qui permet d'assurer l'authenticité et l'intégrité des communications et la méthode ESP (*Encapsulated Security Payload*) qui permet d'assurer en plus la confidentialité. L'enseignant pourra montrer, pour chaque méthode (AH et ESP) et mode (transport et tunnel) quelles informations dans le paquet sont authentifiées et lesquelles sont chiffrées. Si les étudiants ont suivi un cours de cryptographie, il est alors possible de leur indiquer plus précisément les algorithmes utilisés pour assurer l'authenticité et la confidentialité. Notons que la méthode AH n'est plus utilisée en pratique, sauf cas particuliers. Si l'enseignant n'a pas assez de temps pour présenter AH et ESP, il est alors préférable de se concentrer sur ESP.

Si les étudiants sont familiarisés avec la traduction d'adresses (NAT), il est possible de proposer un exercice sur la compatibilité entre le NAT d'une part, et les modes (transport et tunnel) et méthodes de sécurisation (AH et ESP) d'autre part, en montrant l'incompatibilité de certaines combinaisons en raison, notamment de la violation de couches entre IP et TCP. En effet, le contrôle d'erreur du protocole TCP prend en compte dans son calcul les adresses figurant dans l'entête IP. Lorsqu'un paquet subit une traduction d'adresse IP, le contrôle d'erreur dans l'entête TCP doit être modifié en conséquence. Si l'adresse IP du paquet est modifiée par le NAT alors que IPsec a authentifié ou

chiffré la valeur du contrôle d'erreur du protocole TCP, le NAT ne peut pas adapter cette valeur pour prendre en compte la nouvelle adresse IP, ce qui génère une erreur. Seul ESP en mode tunnel est alors compatible avec le NAT car c'est la seule configuration où un nouvel entête IP non-authentifié est ajouté.

Références

- [1] GILDAS AVOINE, *IPSec*, <http://www.avoine.net/cyberedu/>
- [2] GILDAS AVOINE, PASCAL JUNOD, PHILIPPE OECHSLIN, *Sécurité informatique, cours et exercices corrigés, 2e édition*, 10, 304 pages, Vuibert (978-2711748600)
- [3] NAGANAND DORASWAMY ET DAN HARKINS, *IPSec, The New Security Standard for the Internet, Intranets, and Virtual Private Networks, second edition*, 2003, Prentice Hall (978-0130461896)
- [4] STEVE FRIEDL, *An Illustrated Guide to IPsec*, <http://unixwiz.net/techtips/iguide-ipsec.html> présentation du protocole IPsec de manière très didactique avec de nombreuses références vers les RFC liées à IPsec.

6 Fiche 6 : SSH

6.1 Sujet d'étude

Secure SHell (SSH).

6.2 Durée recommandée

- 10 minutes (authentification du serveur) ;
- 10 minutes (optionnel, protocoles cryptographiques) ;
- 5 minutes (authentification du client) ;
- 10 minutes (optionnel, redirection de ports).

6.3 Objectifs pédagogiques

L'objectif pédagogique de cette activité est de présenter aux étudiants le protocole SSH, en mettant l'accent sur :

- l'importance de vérifier l'authenticité de la clef publique du serveur ;
- la possibilité d'authentifier le client en utilisant une clef publique/privée ;
- l'avantage de la confidentialité persistante (*forward secrecy*) ;
- la possibilité de réaliser des redirections de ports.

6.4 Prérequis

Cette activité s'intègre dans un cours de réseaux et nécessite peu de prérequis. La maîtrise de TCP/IP n'est pas nécessaire, mais la notion de port doit être connue pour la quatrième partie de l'activité sur la redirection de ports.

La description de SSH est découpée dans cette fiche en quatre parties :

1. authentification du serveur ;
2. protocoles cryptographiques (optionnel) ;
3. authentification du client ;
4. redirections de ports (optionnel).

Les parties 1 et 3 constituent les connaissances fondamentales sur SSH. La partie 2 peut être abordée si les étudiants ont des connaissances fondamentales en cryptographie à clef publique. La partie 4 n'est pas nécessaire à la compréhension des autres parties mais elle montre les possibilités souvent ignorées de SSH de faire de la redirection de port.

Mettre en place des travaux pratiques sur SSH peut permettre d'en approfondir la compréhension et démystifier auprès des étudiants la possibilité offerte au client de réaliser une authentification par clef publique/privée.

6.5 Notions abordées

- *Secure SHell* (SSH)
- Confidentialité persistante (*forward secrecy*)

- Redirection de ports (*port forwarding*)

6.6 Description

L'enseignant pourra démarrer l'activité en décrivant l'objectif de SSH, qui est de réaliser des tunnels sécurisés (confidentialité, authenticité, intégrité) à travers des réseaux non sûrs. Il est important de comparer SSH aux autres techniques permettant de réaliser des tunnels sécurisés. Selon l'ordre choisi pour présenter les fiches 5, 6 et 7, l'enseignant pourra comparer SSH à IPsec (Fiche 5) et SSL/TLS (Fiche 7), en mettant notamment en avant la couche dans laquelle l'outil considéré opère. L'enseignant pourra notamment souligner que lorsque l'on veut permettre l'accès à un service donné sur un serveur, il est préférable d'utiliser SSL/TLS (car l'accès est limité à un port particulier) plutôt que d'utiliser IPsec.

Il est également important de replacer SSH dans le contexte historique : SSH a été créé en 1995 avec pour objectif de remplacer, entre autres, telnet, rlogin, rsh et ftp qui ne procurent pas de sécurité. La philosophie de son concepteur était d'avoir un outil facile d'utilisation et prêt à l'emploi.

Authentification du serveur. Pour vérifier l'authenticité du serveur, il est important d'expliquer aux étudiants comment réagir lorsqu'ils se connectent pour la première fois sur le serveur. Même dans une classe de master en informatique, la grande majorité des étudiants cliquent sur « oui » lorsqu'ils reçoivent un message affichant l'empreinte cryptographique de la clé du serveur sans s'interroger sur ce que cela signifie et implique. L'enseignant pourra également mettre en avant le problème de l'intégrité de la base de clés publiques gérée par le client et expliquer l'impact que la compromission de la base de clés publiques peut avoir.

Protocoles cryptographiques. Si les étudiants possèdent les connaissances fondamentales de la cryptographie, l'enseignant pourra présenter les grandes étapes de SSH :

- Le serveur et le client négocient les protocoles cryptographiques à utiliser.
- Le serveur et le client se mettent d'accord sur une clé symétrique en utilisant le protocole de Diffie-Hellman.
- Le serveur signe les informations échangées en utilisant sa propre clé privée.
- Le serveur envoie sa clé publique au client, qui doit en vérifier l'authenticité.

Les premières étapes peuvent être facilement « montrées » aux étudiants en écoutant une connexion SSH entre un client et un serveur à l'aide de Wireshark¹. L'enseignant devra mettre en avant le fait que l'utilisation du protocole de Diffie-Hellman permet d'assurer la confidentialité persistante (*forward secrecy*). Cette propriété fondamentale assure que si la clé privée du serveur est compromise, la confidentialité des communications antérieures reste garantie. L'enseignant pourra utiliser cette opportunité pour préciser que la confidentialité persistante est seulement optionnelle dans IPsec (Fiche 5).

Authentification du client. L'enseignant présentera ensuite les moyens possibles pour authentifier le client, à savoir par mot de passe ou par clé publique/privée, en décrivant les avantages et inconvénients de chacune des deux approches. L'authentification par clé publique/privée est recommandée mais l'authentification par mot de passe est parfois plus facile à mettre à œuvre lorsque les utilisateurs se connectent à partir de machines sur lesquelles leur clé publique n'a pas été copiée.

1. Wireshark. <https://www.wireshark.org/>

Lorsque l'authentification du client se fait par clef publique/privée, il est également recommandé de protéger la clef sur l'ordinateur du client par un mot de passe. L'enseignant pourra montrer aux étudiants la simplicité en pratique pour un client de générer une clef publique/privée.

Redirection de ports. L'enseignant présentera la copie de fichiers à distance par SSH (SCP) mais surtout la possibilité de rediriger des ports, souvent ignorée des étudiants. Les étudiants sont généralement impressionnés par l'étendue des possibilités offertes par la redirection de ports dans SSH. L'enseignant pourra dessiner des scénarios au tableau et montrer quelle configuration de SSH est alors la plus appropriée. Deux exemples simples peuvent permettre aux étudiants de comprendre les possibilités de SSH, et l'impact sur la sécurité du système d'information : ouvrir un tunnel SSH avant de quitter son bureau pour ensuite accéder à son ordinateur professionnel à partir de son domicile (redirection inverse de ports) lorsque le pare-feu du bureau n'autorise pas de connexion directe. L'enseignant mettra également en avant les possibles problèmes de sécurité que cela engendre. Ouvrir une connexion SSH sur un ordinateur distant avec l'option « -X » (redirection inverse de ports) pour que le contenu de la fenêtre graphique distante s'affiche localement. Montrer ensuite que cette approche, simple à mettre en œuvre mais nécessitant une bande passante importante, est souvent inappropriée. Lorsque l'on utilise cette approche pour naviguer sur Internet avec l'adresse IP de la machine distante, il est alors préférable d'utiliser le serveur SSH distant comme un relais (*proxy*) SOCKS. Enfin, l'enseignant pourra mettre en avant un problème de sécurité majeur avec l'option -X : en autorisant la machine distante à accéder à l'interface graphique de la machine locale, elle autorise également l'administrateur de cette machine distante à récupérer des informations locales liées à l'interface graphique, notamment ce qui est affiché à l'écran et ce qui est saisi au clavier.

Références

- [1] GILDAS AVOINE, *SSH*, <http://www.avoine.net/cyberedu/>
- [2] GILDAS AVOINE, PASCAL JUNOD, PHILIPPE OECHSLIN, *Sécurité informatique, cours et exercices corrigés, 2e édition*, 10, 304 pages, Vuibert (978-2711748600)
- [3] DANIEL J. BARRETT, RICHARD E. SILVERMAN ET ROBERT G. BYRNES, *SSH, The Secure Shell, The Definitive Guide, Second Edition*, 2005, O'Reilly Media, 670 pages (978-0596008956)
- [4] BRIAN HATCH, *SSH Port Forwarding*, <http://www.symantec.com/connect/articles/ssh-port-forwarding>
- [5] WIKIPÉDIA, *Comparison of SSH clients*, http://en.wikipedia.org/wiki/Comparison_of_SSH_clients, présentant une liste très fournie de clients SSH pour des systèmes d'exploitation variés

7 Fiche 7 : SSL/TLS

7.1 Sujet d'étude

SSL/TLS.

7.2 Durée recommandée

- 15 minutes ;
- 15 minutes (optionnel, présentation des mécanismes cryptographiques).

7.3 Objectifs pédagogiques

L'objectif pédagogique de cette activité est de présenter aux étudiants le protocole SSL/TLS, en mettant l'accent sur :

- l'importance de chiffrer les communications, en particulier lorsque des mots de passe sont échangés ;
- le fait que le serveur est obligatoirement authentifié par certificat avec SSL/TLS, alors que le client n'est qu'optionnellement authentifié ;
- l'importance de vérifier le certificat du serveur ;
- l'importance d'utiliser le protocole de DIFFIE-HELLMAN pour assurer la confidentialité persistante (*forward secrecy*).

7.4 Prérequis

Il est assez difficile d'aborder le protocole SSL/TLS avec des étudiants qui n'ont pas de connaissances en cryptographie. Il est donc proposé de diviser cette activité en deux parties. La première partie présentera les fondements de SSL/TLS et les notions de clé publique/privée, certificat et signature. La seconde partie présentera les mécanismes cryptographiques utilisés dans SSL/TLS (DH, RSA) pour les étudiants qui ont déjà des connaissances dans ce domaine.

7.5 Notions abordées

- *Secure Sockets Layer / Transport Layer Security* (SSL/TLS)
- Clefs publiques/privées, signatures, certificats
- Diffie-Hellman (DH), Rivest-Shamir-Adleman (RSA)
- Confidentialité persistante (*forward secrecy*)

7.6 Description

Fondements de SSL/TLS. Dans la première partie de cette activité, l'enseignant décrira l'objectif de SSL/TLS, à savoir de réaliser des tunnels sécurisés (confidentialité, authenticité, intégrité) à travers des réseaux non sûrs, au-dessus de la couche 4 (transport) du modèle OSI. SSL/TLS est utilisé en mode client-serveur pour ne donner a priori accès aux clients qu'à un seul service, par exemple HTTP, SMTP ou IMAP. L'enseignant pourra également fournir un bref historique de

SSL/TLS et expliquer pourquoi on parle souvent de SSL et de TLS indifféremment : SSL est le protocole développé par Netscape en 1995, alors que TLS est la version de SSL normalisée par l'IETF en 2001. On ne devrait plus parler de SSL, mais la bibliothèque la plus connue qui implémente TLS s'appelle OpenSSL, ce qui rajoute de la confusion. Il est alors commun de parler de SSL/TLS.

L'enseignant insistera sur le fait que la confidentialité et l'intégrité sont assurées. Ainsi, contrairement aux protocoles basiques tels que HTTP, FTP et POP3, qui transportent les informations (notamment les mots de passe) en clair, les informations sont chiffrées lorsqu'elles transitent dans un tunnel SSL/TLS.

L'enseignant insistera ensuite sur le fait que l'authentification du serveur (par certificat) est obligatoire dans l'immense majorité des cas d'usage, alors que l'authentification du client (également par certificat) est optionnelle et rarement utilisée. À la place, une authentification du client au niveau applicatif par mot de passe est généralement préférée.

L'enseignant devra ensuite décrire quelques fondamentaux de la cryptographie. À ce stade, dire aux étudiants qu'un mécanisme de signature numérique repose sur deux clefs, dont l'une est publique et l'autre privée peut être suffisant, en précisant que chacun utilise sa propre clef privée pour signer un document, et que tout le monde peut utiliser la clef publique du signataire pour vérifier cette signature. Il faut toutefois ensuite décrire le concept de certificat, ce qui peut se résumer à dire qu'il s'agit d'un document signé par une autorité pour lier l'identité d'une personne à la clef publique de cette personne.

L'enseignant décrira ensuite les étapes nécessaires pour vérifier un certificat, et donc vérifier l'authenticité du serveur SSL/TLS avec qui le tunnel est établi. En résumé, il faut vérifier que :

- l'identité incluse dans le certificat est bien celle qui est attendue (par exemple l'adresse du site web visité) ;
- le certificat est en cours de validité ;
- le certificat n'a pas été révoqué ;
- la signature de l'autorité de certification est correcte, ce qui nécessite pour cela de connaître et faire confiance au certificat de l'autorité de certification.

Pour montrer l'importance de vérifier le certificat, l'enseignant pourra décrire une attaque de type « l'homme au milieu » (*man in the middle*) sur un client qui se connecte à un serveur avec SSL/TLS.

Mécanismes cryptographiques. La seconde partie de cette activité aborde de manière plus détaillée les mécanismes cryptographiques utilisés par SSL/TLS. Il serait illusoire de présenter l'intégralité des mécanismes cryptographiques de SSL/TLS aux étudiants en quelques minutes. L'enseignant pourra donc se concentrer sur l'échange de clefs, qui permet d'aborder la notion de confidentialité persistante (*forward secrecy*), et l'authentification, qui permet quant à elle de mettre l'accent sur le fait que DH seul n'assure pas l'authentification de l'échange de clefs.

L'enseignant pourra par exemple capturer l'établissement d'une connexion SSL/TLS avec Wireshark et expliquer l'une ou l'autre des combinaisons cryptographiques proposées par le client dans son premier message, par exemple « TLS_RSA_WITH_AES_256_CBC_SHA » et « TLS_DHE_RSA_WITH_DES_CBC_SHA ». Après une description plus ou moins avancée en fonction des connaissances des étudiants en cryptographie, l'enseignant pourra présenter plus en détails les protocoles DH (Diffie-Hellman) et RSA (Rivest-Shamir-Adleman). Dans la configuration TLS_RSA, le client choisit une clef symétrique et la chiffre avec la clef publique RSA du serveur. Seul le serveur pouvant déchiffrer cette clef symétrique, RSA permet dans cette configuration d'assurer en même temps l'échange de clef et l'authentification du serveur. Dans le cas TLS_DHE_RSA, le client et le serveur se mettent d'accord sur une clef symétrique en utilisant le protocole DH, et le serveur signe avec

RSA les informations envoyées au client durant l'exécution du protocole DH. Dans ce cas-ci, DH assure donc l'échange de clef et RSA l'authentification du serveur.

Si l'enseignant capture l'établissement d'une connexion SSL/TLS avec Wireshark, il est possible qu'il observe deux configurations concernant DH proposées par le client, à savoir TLS_DHE et TLS_DH. TLS_DHE est la version qui doit être utilisée car le secret du serveur est éphémère, c'est-à-dire détruit à l'issue de la communication. Cela permet d'assurer la confidentialité persistante. Avec TLS_DH, le serveur possède un secret statique et l'information publique correspondante est intégrée au certificat du serveur (il s'agit alors d'un certificat DH et non plus RSA). Cette configuration n'assure pas la confidentialité persistante. Même si certains clients SSL/TLS continuent de proposer la configuration TLS_DH, elle n'est jamais acceptée en pratique par les serveurs.

Références

- [1] GILDAS AVOINE, *SSL/TLS*, <http://www.avoine.net/cyberedu/>
- [2] GILDAS AVOINE, PASCAL JUNOD, PHILIPPE OECHSLIN, *Sécurité informatique, cours et exercices corrigés*, 2e édition, 10, 304 pages, Vuibert (978-2711748600)
- [3] OLIVIER LEVILLAIN, *SSL/TLS : état des lieux et recommandations.*, http://www.ssi.gouv.fr/IMG/pdf/SSL_TLS_etat_des_lieux_et_recommandations.pdf, 2012
- [4] OLIVIER LEVILLAIN, *SSL/TLS : 3 ans plus tard.*, http://www.ssi.gouv.fr/uploads/2015/06/SSTIC2015-Article-ssl_tls_soa_reloaded-levillain_c0bDbqp.pdf, 2015

Ce document a été rédigé par un consortium regroupant des enseignants-chercheurs, des professionnels du secteur de la cybersécurité ainsi que l'ANSSI.



L'ensemble des documents est distribué sous licence ouverte Etalab V1.