Rapport de stage technique du cycle ingénieur ESIEA

4e année

Intégration d'une plate-forme d'auto enregistrement au portail ALCASAR

Laboratoire de Cryptologie et de Virologie opérationnelles
38 Rue des Docteurs Calmette et Guérin
53 000 Laval

Tél. : 02 43 59 24 24

Étudiant :	Tuteur ESIEA :	Maître de stage :
Nicolas AUBRY	**Richard REY**	**Franck BOUIJOUX**

Résumé

Le sujet de ce stage traite en de l'intégration d'une plate forme d'auto-enregistrement au portail captif ALCASAR (Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau). Ce portail est un outil libre (sous licence GNU GPLv3) et gratuit permettant aux particuliers ou aux professionnels d'offrir un réseau de consultation Internet, tout en respectant les aspect légaux éxigés en France. Cette protection est basée sur l'imputabilité des connexions assurée par un système de journalisation des connexions et des authentifications.

Avant la réalisation de ce stage, la création des comptes utilisateur n'était possible que par un administrateur. Le but de ce stage a donc consisté à la mise en place d'un module d'auto-enregistrement exploitant la technologie GSM, et plus précisément, le système de Short Message Service (SMS). L'utilisateur souhaitant obtenir un accès au réseau envoie son mot de passe par SMS à un modem GSM (clé 3G/4G) branché sur le serveur ALCASAR, entraînant ainsi la création du compte. Le login étant le numéro de téléphone. Le mot de passe étant le contenu du SMS.

Une fois l'intégration de ce module faite, mon travail s'est orienté vers l'intégration d'un module permettant la visualisation des flux Internet sur une carte du monde. Ce module se base sur la collecte des flux effectuée par la sonde Netflow, et l'exploitation de ces flux par NfSen (Netflow Sensor).

Pour finir, cette nouvelle version d'ALCASAR ne repose plus sur la distribution Mageia 2 mais sur la distribution Mageia 4. Cela engendre donc une phase de correction d'erreurs et de bugs, à laquelle j'ai pu participer lors de ce stage.

Abstract

The first goal of this internship was the integration of an auto registration platform to the ALCASAR portal.
This portal is a free and open source software (under GNU GPLv3) which uses the Network Access Control. This portal is a bridge between a consultation network and the Internet. It authenticates, attributes and protects users' access regardless their connected equipments.
Moreover this portal incorporates a filtering solution, in order to protect minor at school or people in public places.

Before this internship, the only way to create an account was by the administrator of the portal. But during this internship, I create an auto registration module for the user. This module uses the GSM technology. The user must send his password by SMS to a modem connected on the ALCASAR server. The login is the phone number, and the password is the content of the SMS.

After this first work, I incorporated a plugin which show the flows on a world map. This plugin uses a Netflow probe and the NfSen interface (Netflow Sensor).

At the end, this new version of ALCASAR is based on the last version of Mageia (Mageia 4), while the previous version of ALCASAR is based on Mageia 2. I was able to participate in the correction of few of them.

Table des matières

Remerciements

Je tiens en premier lieu à remercier l’ensemble du laboratoire CVO² qui m’a permis de travailler dans de très bonnes conditions.

Je tiens à remercier plus particulièrement Monsieur Richard REY et Monsieur Frank BOUIJOUX, qui m’ont suivi tout au long de ces 4 mois, me poussant à faire mieux chaque jour.

Je tiens aussi à remercier le docteur Rick HOFTEDE pour toute l’aide apportée sur le module SurfMap.

L’ensemble de toutes ces personnes a contribué à rendre mon stage dynamique, intéressant et riche en connaissances.

Introduction

a) Présentation de l'entreprise

L'intégralité de mon stage a eu lieu au sein du laboratoire de Cryptologie et Virologie Opérationnelles (CVO²), implanté dans les locaux de l'École Supérieur d'Informatique, Électronique et automatique (ESIEA) sur le site de LAVAL. Ce laboratoire traite des domaines de la lutte informative défensive et offensive, la recherche dans les domaines de la sécurité informatique, la virologie et la cryptologie.
L'approche théorique et pratique faite au sein de ce laboratoire lui permet de rester actif et lui donne ainsi des capacités pour anticiper les menaces (approche défensive) et donne aussi des outils dans le domaine offensif.

Illustration 1: Logo CVO²

Ayant un fort héritage militaire, le laboratoire travaille en étroite collaboration avec différents ministères de l'État français : ministère de la Défense, ministère de la Justice et ministère de l'Intérieur. Actuellement, le laboratoire prend part au développement du Démonstrateur d'Antivirus Français et Internationaux (DAVFI), projet qui vise à créer le premier antivirus libre français qui permettrait à l'état français d'obtenir une indépendance au niveau de la protection contre les malwares.

Pour finir, l'implantation du laboratoire CVO² au sein des locaux de L'ESIEA permet un partage de connaissances entre les membres du laboratoire et les étudiants en cursus d'Ingénieur ESIEA. Une intégration au laboratoire (statut « espoir recherche ») est même possible pour certains d'entres-eux, leur permettant de travailler sur des projets concrets.

b) Projet ALCASAR

L'Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau (ALCASAR) est un projet libre et gratuit permettant à une personne de mettre à disposition son réseau de consultation Internet, tout en respectant les obligations légales françaises. Ce NAC (Network Access Control/Contrôleur d'accès au réseau) permet d'imputer et tracer tout utilisateur connecté au réseau.

Illustration 2: Logo ALCASAR

Illustration 3: Page d'Interception

La connexion au réseau de consultation se fait par login/mot de passe, permettant ainsi d'avoir une traçabilité des activités réalisées par les utilisateurs. Ces traces conservées pendant un an (selon l'article 3 du Décret n° 2011-219 du 25 février 2011), peuvent être chiffrées afin de préserver la vie privée des utilisateurs et empêcher toute fraude. L'exploitation directe de ces traces est rendue impossible dans ALCASAR. Seules les autorités compétentes ont le droit d'effectuer un agrégat de ces données pour imputer les échanges. ALCASAR protège aussi les utilisateurs contre les oublis de fermetures de session (utilisation d'un watchdog) et donne la possibilité à l'utilisateur de modifier à tout moment son mot de passe.

ALCASAR intègre aussi des modules ayant pour but de protéger les utilisateurs. Un pare-feu et un antivirus protègent les utilisateurs ainsi que les équipements du réseau. Une protection interne est aussi mise en place afin d'empêcher l'usurpation de session. Un système de filtrage est également proposé, permettant de bloquer l'accès à certains sites (blacklist), ou d'en autoriser l'accès qu'a une liste restreinte (whitelist).

Illustration 4: Accès refusé

D'un point de vue matériel, ALCASAR ne requiert pas une importante infrastructure (un simple ordinateur avec deux cartes réseau est suffisant). S'installant sur une distribution Linux (Mageia), la mise en place de ce NAC est possible par tous, que ce soit dans les écoles, dans les espaces publics, les chaînes d'hôtel, les bibliothèques, ou même de plus grosses organisations.

Pour finir, une partie « administration » complète permet de manipuler, gérer et surveiller le serveur ALCASAR. La consultation et la gestion des utilisateurs sont possibles via ce panel d'administration. L'exportation des logs archivés est aussi possible.

D'un point de vue technique, ALCASAR va se placer entre un réseau de consultation et Internet. Tous les flux du réseau interne vers Internet vont transiter par ALCASAR et, suivant le niveau de filtrage des usagers, vont être traités ou redirigés.

c) Problématique du stage

Jusqu'à aujourd'hui, la création de comptes utilisateur n'était possible que par les deux méthodes suivantes :

- via l'interface d'administration (création au cas par cas ou génération de tickets)
- via un annuaire externe (LDAP ou A.D)

Cependant, certains organismes utilisant ALCASAR ne peuvent se permettre d'avoir un administrateur à temps plein pour créer les comptes utilisateurs.

L'idée de créer un système d'auto enregistrement a donc vu le jour. Elle doit permettre à l'utilisateur de créer lui même son compte. La première piste, qui est exploitée par de nombreux sites web ou forums, utilise une adresse e-mail pour créer un compte. Cette solution, bien que simple, n'est pas compatible avec les exigences d'ALCASAR vis-à-vis du droit français. En effet, ayant pour objectif de tracer et d'imputer les traces de connexion, une simple adresse e-mail ne peut constituer un élément fiable d'identification.
La solution d'adresse e-mail n'étant pas retenue, mes recherches se sont orientées sur l'utilisation de SMS. Le principe étant d'envoyer son mot de passe par SMS à une clé 3G/4G connecté sur ALCASAR. Cette solution respecte bien les idées d'imputabilité et de traçabilité : en effet, la loi française impose qu'une ligne de téléphonie mobile ne puisse être ouverte qu'avec les coordonnées réelles du client. C'est-à-dire qu'en cas de litige, il y a possibilité, via l'opérateur téléphonique, de remonter jusqu'au client.

Plate forme d'auto enregistrement

a) Approche

Le but de cette plate forme, comme énoncé précédemment, est de permettre à un utilisateur de se créer un compte pour pouvoir accéder au réseau de consultation. De façon à rendre le procédé simple, cet utilisateur n'aura que son mot de passe à envoyer au numéro de téléphone de la clé 3G/4G connectés au serveur ALCASAR, cf. Illustration 5: Module SMS et ALCASAR.

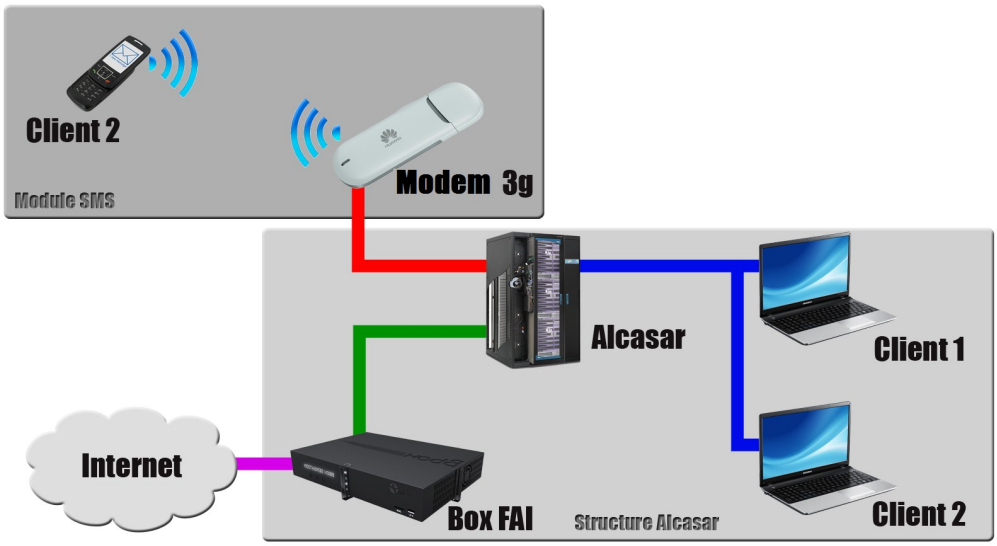


Illustration 5: Module SMS et ALCASAR

b) Les commandes AT

Pour communiquer avec les modems, il est nécessaire d'utiliser le jeu de commandes AT.

Ces commandes sont une évolution des commandes Hayes développées en 1981, qui permettaient de communiquer avec le modem Hayes Smartmodem 300.
Elles permettent de faire un grand nombre de choses, de la composition d'un numéro de téléphone à l'envoi de SMS, en passant par l'interrogation sur l'état du modem.

La syntaxe de ces commandes suit le schéma suivant :

- **AT+commande** [1]
  Les deux premiers caractères (AT) sont l'abréviation du mot 'ATtention'. Ils permettent d'avertir le modem, afin qu'il prenne en compte la commande qui suit.

- **AT^commande** [2]

Ce type de commande est classé dans les commandes AT étendues. Ce sont des commandes implémentées par les constructeurs de modems/adaptateurs GSM. Certaines ne sont reconnues que par une famille ou marque de modem.

Le nombre de ces commandes est assez important. On ne trouve qu'un nombre réduit de celles-ci sur Internet. Exemple :

État de la carte SIM

AT+CPIN?	Interrogation sur l'état de la carte SIM (ready, sim pin, simpuk …)
AT+CPIN="0000"	Permet de rentrer le code PIN (ici, 0000)

Information Système

AT+CGMM	Requête sur le model du modem
AT^SYSINFO	Requête sur les informations système
AT+COPS?	Requête sur l'opérateur du modem

Lecture et écriture des SMS

AT+CMGF=y	On sélectionne le mode opératoire | 1=text et 0=PDU
AT+CPMS?	On sélectionne la mémoire de stockage
AT+CMGL="ALL"	Affiche tous les messages
AT+CMGR=y	Lis le message d'index y
AT+CMGD=y	Supprime le message d'index y
AT+CMGS="0102030405"	Envoi un SMS au 0102030405. Ctrl+z pour valider le message.

On listes plus complètes sont disponibles sur Internet, que ce soit des commandes génériques, ou des commandes étendues.

c) Le projet GAMMU et son fonctionnement

Afin de pouvoir mettre en place un tel module, il a été nécessaire de rechercher une solution permettant d'exploiter les SMS reçus par le modem GSM connecté au serveur ALCASAR.

La solution retenue se nomme GAMMU. Ce projet open source, développé en langage C et dérivé de Gnokki, permet de communiquer avec un grand nombre de modems GSM (du modem au téléphone mobile). Outre le fait de gérer les SMS, ce que nous recherchons, ce projet permet :

- d'exploiter les MMS reçus (compatible avec certains périphériques)

- récupérer les informations du périphérique et du réseau
- gérer ses contacts et lancer des appels

Le projet GAMMU fonctionne de la manière suivante : une fois que le périphérique GSM est branché, on renseigne dans la configuration de GAMMU le port d'écoute (ex : /dev/ttyUSB0), et on indique toutes les informations utiles concernant la vitesse de transfert utilisée lors de la connexion, l'emplacement du stockage des SMS (base de données ou fichier log), ou encore le code PIN.
Dans le cadre d'ALCASAR, le stockage des SMS exploite une base de données. J'utiliserai le SGBD « MariaDB » déjà fonctionnel sur ALCASAR. GAMMU va donc faire office de liaison entre le modem GSM et la base de données.

Une fois lancé, GAMMU va vérifier à intervalle régulier la présence de SMS dans la carte SIM du modem GSM. Si au moins un SMS est en attente, ce dernier va être copié dans la base de données, puis être supprimé de la carte SIM. Les échanges effectués entre GAMMU et le modem GSM sont réalisés à l'aide de commandes AT.

Une fois stockés en base, le ou les SMS sont facilement exploitables.

d) Les modems 3g

Afin de pouvoir recevoir les SMS, j'ai effectué une étude de différentes clés 3g/4g. Afin d'intégrer ce module d'auto enregistrement au projet ALCASAR. J'ai travaillé avec des modems n'étant pas soumis à un blocage opérateur afin de rester le plus généraliste possible. Ce travail à été effectué sur deux catégories de modems :

- Les modems de développement,
- les modems commerciaux.

Illustration 6: Wavecom Q2303A USB

Les modems de développement ne possèdent aucune restriction opérateur, ce qui les rend plus aptes à effectuer la tâche recherchée. Leur prix oscille entre 40 € et 60 €. Cette catégorie de modems a été d'une grande fiabilité pendant les différentes phases de test. Ces tests ont ciblé deux modems de cette catégorie. L'un utilisait une connexion USB, alors que l'autre utilisait une connexion série (RS232). Un adaptateur Série-USB a permis de contourner l'absence de port série le serveur ALCASAR de test.

Les modems commerciaux quant à eux sont plus abordables (~ 30 €). Le constructeur *Huawei* est l'un des plus représentés dans le monde avec un nombre important de modèles. Une phase de test a été réalisée avec les modèles « E220 » et « E180 ».
Un problème est rapidement apparu avec ces modems. En effet, ils intègrent une mémoire interne (gérée comme une clé USB) contenant les pilotes Windows. La gestion de cette mémoire interne provoque un gel du modem après un certain temps d'utilisation. Le modem bascule automatiquement du mode « modem GSM » au mode « clé USB »


Illustration 7: Huawei E220

(mass storage). À la suite de nombreuses recherches de contournement, j'ai découvert le projet **USB_ModeSwitch**[3] qui a permis de résoudre le problème. L'utilisation d'une ligne de commande exécutée au branchement d'un modem de marque *Huawei* (via le module udev), permet de figer le modem dans le mode que l'on souhaite.

Suite à ces deux séries de tests, le fonctionnement de quatre modems est assuré. Cependant, le projet GAMMU est compatible avec un grand nombre de modems et téléphones[4]. Il est donc possible de faire fonctionner le module d'auto enregistrement avec d'autres périphériques.

Les différents modems testés ne possèdent pas la même vitesse de connexion. Il a donc fallu mettre en place une option permettant à l'administrateur de choisir la vitesse de connexion du modem qu'il branche à son serveur ALCASAR. Ces vitesses varient de 9600 bit/s à 115200 bit/s.

e) Le module d'auto-enregistrement

Après avoir étudié les différents éléments de ce module, je me suis intéressé sur la réalisation de la partie logicielle.

Avant de réaliser ce module, il a fallu répondre à plusieurs questions :

1. Comment traiter le SMS reçu ?
2. Comment gérer les utilisateurs déjà inscrits ?
3. Comment gérer les envois abusifs ?
4. Comment gérer le service (mode cron, daemon ou script)

Le projet GAMMU intègre deux « hooks » (ce qui permet par exemple l'appel d'un script lors d'un événement précis), un sur la réussite de stockage de SMS et l'autre sur l'échec. Ce système de « hook » m'a permis de répondre à la quatrième question, permettant ainsi de ne pas alourdir le système avec une tâche de fond (DAEMON).

Une fois la méthode de gestion de SMS trouvée, l'idée de mettre en place un système de blocage m'a permis de répondre aux deux dernières questions. Ce système de blocage a été pensé pour prévenir en premier lieu l'envoi abusif de SMS au serveur ALCASAR, permettant ainsi de réduire la charge de traitement lors de l'exécution du script, puis gérer les utilisateurs déjà inscrits. Ce système de blocage est géré par deux tables en base de données : l'une regroupant les numéros bloqués (comptes déjà créés ou envois abusifs), appelés « table de blocage fort» dans la suite de ce rapport et l'autre permettant de gérer le nombre d'essais permis pour chaque numéro (que j'appellerai « table de blocage temporaire » par la suite).

Comme énoncé précédemment, le contenu du SMS ne doit contenir qu'un seul mot, afin de respecter la structure d'un mot de passe classique. Une fois que le script est appelé par le « hook », ce dernier commence déjà par vérifier si le numéro de l'expéditeur du SMS n'est pas bloqué. Si ce numéro est soumis à un « blocage fort», le script s'arrête, sinon, un contrôle du mot de passe est effectué : dans le cas où le contenu du SMS est vide ou comporte deux mots ou plus, le numéro est

inscrit dans la table de blocage temporaire. Dans le cas où le contenu du SMS est valide, ce dernier est chiffré, puis la création d'un compte est lancée (dans la table « radcheck » de la base RADIUS [cf. Liste des Annexes]). Le numéro est ensuite ajouté à la table de blocage fort. Dans le cas où un utilisateur a envoyé plus de SMS que le nombre autorisé, son numéro se retrouve alors ajouté dans la table de blocage fort pour cause d'envois abusifs. La migration des blocages temporaire en blocage fort est réalisée à la fin du script lors de chaque exécution.

Partie administrative

Tout ce qui précède est géré par le serveur ALCASAR. Une interface a été mise au point afin de permettre à l'administrateur de gérer ce module. Cette administration est rendue possible dès qu'un modem (dont le constructeur fait partie des modems testés) est branché (et est reconnu) à ALCASAR.

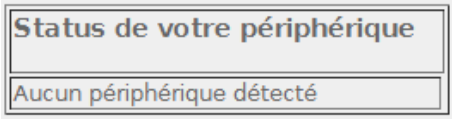


Illustration 8: Modem absent

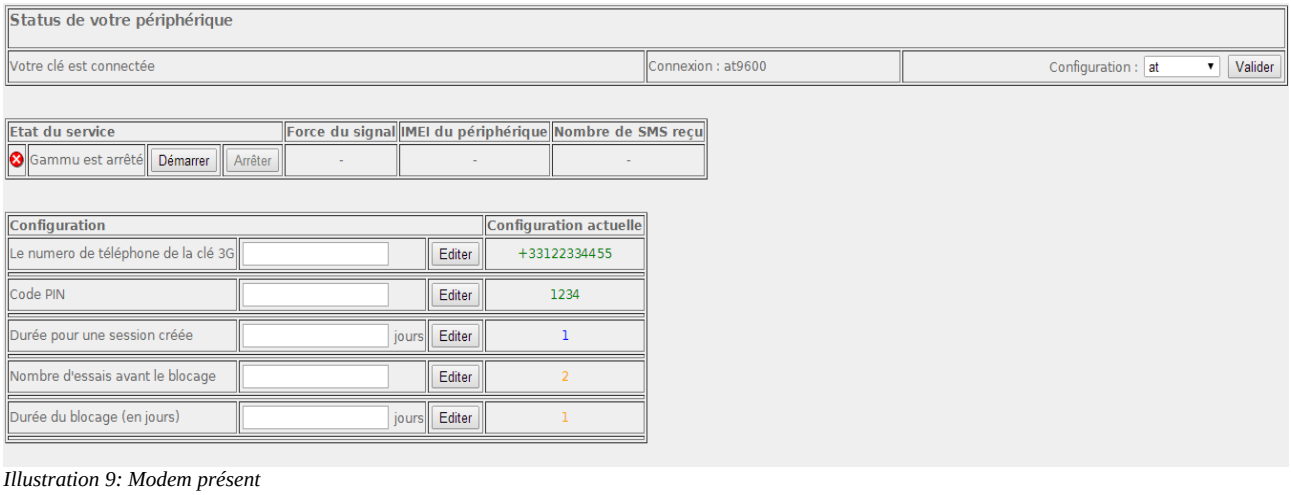


Illustration 9: Modem présent

Une fois le modem connecté et reconnu, le panneau d'administration (cf. Illustration 9: Modem présent) apparaît et offre la possibilité de configurer le module :

- L'administrateur a la possibilité de renseigner le numéro de téléphone associé à la carte SIM, insérée dans le modem GSM. Ce numéro sera par la suite affiché sur une page d'aide à la création de comptes auto enregistrés pour les utilisateurs ;
- L'édition du code PIN (code qui permet de protéger le contenu et l'accès aux fonctions de communication de la carte SIM) ;
- Ce module ne fonctionnant pas comme la création manuelle de comptes, il n'est pas possible de bloquer la date d'expiration des comptes auto créés par une date fixe. C'est pour cela que l'administrateur a la possibilité de renseigner la durée en jour de validité du compte. Cette variable sera récupérée lors de l'exécution du script puis additionnée à la date d'exécution du script.
- Concernant la politique pour empêcher l'abus d'envois de SMS, l'administrateur à la

possibilité d'indiquer le nombre d'essais disponible par usagers avant le blocage du numéro.
- Et toujours concernant cette politique, la durée en jours de ce blocage est aussi éditable.

Une fois la configuration faite, l'administrateur peut lancer le module, et obtient le tableau suivant :

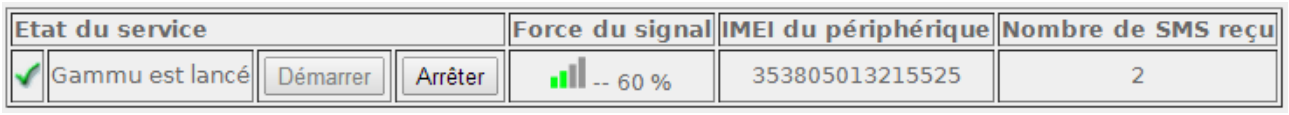


Illustration 10: Service lancé

Ce tableau permet de visualiser certaines informations, comme la force du signal du réseau GSM, ainsi que le nombre de SMS reçu depuis que le service est activé (relancer le service remet à zéro le compteur).

Chaque compte créé ou bloqué sera affiché sur la page d'administration. Cette liste (cf. Illustration 11: Comptes bloqués) permet à l'administrateur de connaître la raison du blocage et, le cas échéant, de débloquer un usager. Il est cependant utile de dire que débloquer un usager ayant un compte encore valide supprime ce compte.

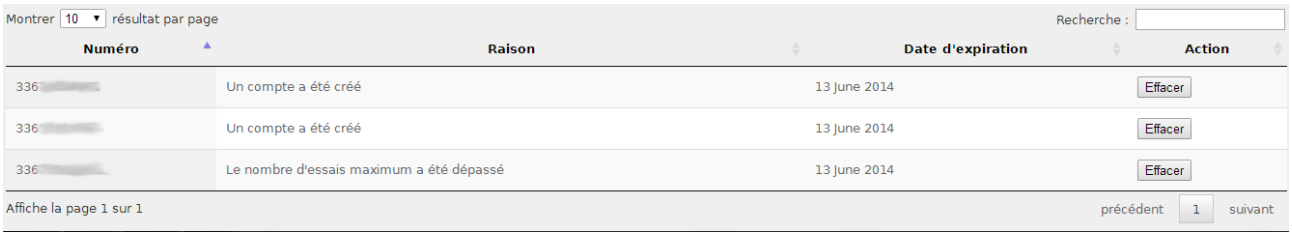


Illustration 11: Comptes bloqués

Pour finir sur la partie administration, un groupe « sms » a été spécialement créé afin de pouvoir affecter les attributs ALCASAR (débit, filtrage, durée de connexion ...) aux comptes « auto-inscrits ». Chaque nouvel utilisateur est automatiquement associé à ce groupe. Cette volonté de créer un groupe est née du fait que seuls le login, le mot de passe et la date d'expiration du compte sont insérés dans la base de données lors de la création du compte.

Partie publique

Une fois le module lancé, une page d'aide à l'auto-enregistrement fait son apparition sur la page d'interception.

La page d'aide indique aux utilisateurs la procédure à suivre pour obtenir un compte.
On retrouve sur cette page le numéro de téléphone renseigné en partie administration. Les utilisateurs peuvent aussi avoir une information sur l'état de blocage de leur numéro. Ils doivent effectuer une recherche en indiquant les 5 derniers chiffres du numéro de téléphone. Ces numéros étant accessibles par tous, seule une partie des chiffres sont visibles dans un tableau récapitulatif.

Illustration 12: Page auto-enregistrement public

Plugin SURFmap

a) Principe

À la suite de la création du module d'auto-enregistrement, une nouvelle tâche m'a été confiée. La version 2.8 d'ALCASAR s'est vu doter d'une sonde NETFLOW exploitée par le projet NfSen [5]. Cette sonde permet de collecter les flux transitant par ALCASAR, qui sont par la suite interprétés graphiquement par NfSen. Cela permet donc à l'administrateur d'avoir un visuel statistique sur les ports réseau utilisés ou encore, voir de façon graphique le nombre de paquets qui transitent par ALCASAR (à un moment déterminé, ou sur une période). Toutes ces données sont stockées sous forme de fichier de capture par un daemon Nfcapd : les flux sont stockés temporairement, puis copiés dans des fichiers exploitables toutes les 5 minutes. Le fichier temporaire est alors supprimé.

Un module, nommé SURFmap [6], offre la possibilité d'avoir une représentation réelle des flux qui transitent. Ce module récupère et géolocalise les adresse IP consultés par les utilisateurs du réseau de consultation, puis les relie par un lien de couleur au point d'origine (c'est à dire le point représentant le serveur ALCASAR).

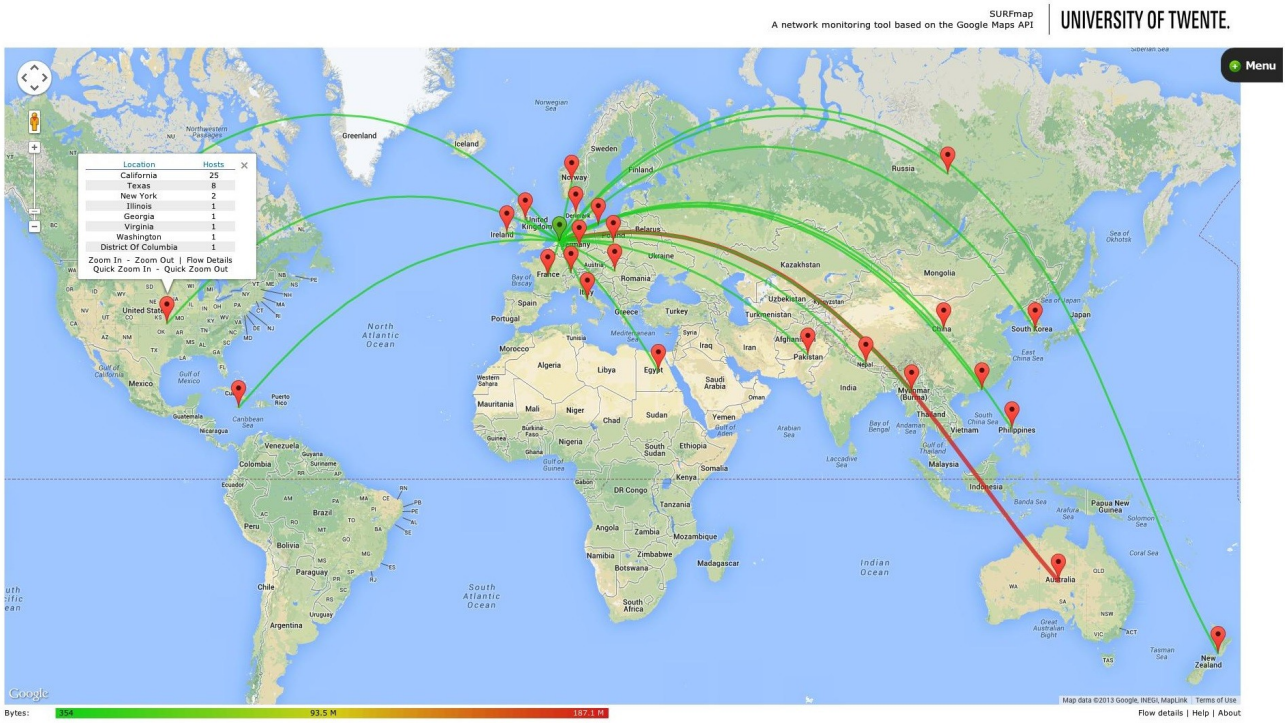


Illustration 13: SURFmap — Représentation

Comme on peut le voir sur Illustration 13: SURFmap — Représentation, la représentation des flux suit un code couleur permettant de distinguer les trafics forts. Plus la couleur tend vers le rouge, plus le nombre de flux est important.
Un « Menu » permet d'affiner les recherches : choix d'un intervalle, date fixe, nombre de flux

affichés, échelle de la carte, champs pour différents filtres (affichage spécifique à une IP), auto rafraîchissement...

b) Les problèmes rencontrés

Concernant l'installation de ce module, aucun problème n'a été rencontré. Cependant lors de l'utilisation, certaines fonctionnalités n'étaient pas opérationnelles. Ces problèmes m'ont poussé à entrer en contact avec le docteur Rick HOFTEDE, créateur de SURFmap, afin de lui proposer des pistes d'amélioration.

Lors de nos échanges, nous avons pu corriger les problèmes suivant :

- choix d'un intervalle d'affichage défectueux,
- géolocalisation du point d'origine changeant en fonction du niveau de zoom,
- génération d'une erreur si le fichier de capture est inexistant.

Suite aux modifications, ce module a été entièrement intégré à ALCASAR.

c) Les limites du module

En fonction des options choisies dans le « Menu », et suivant la capacité de calcul du serveur, le traitement et l'affichage des données varient fortement. En effet, à l'exécution de la page, les flux que l'on souhaite afficher vont être récupérés dans les fichiers de capture. Ils sont traités afin de générer la carte (cf. Illustration 13: SURFmap — Représentation). Ce traitement devient très lourd si l'administrateur sélectionne plus de 1500 flux. À titre d'exemple, la visualisation d'un téléchargement de fichiers via « bittorrent », nécessite le traitement de plus de 2000 flux. Ce traitement aboutit au bout de 10 minutes.
Certaines adresses IP sont localisées dans les centres des villes ou pays, donnant ainsi une approximation et non la localisation précise de celles-ci.

Ce module reste un outil très intéressant pour pouvoir observer statistiquement vers quels pays vont les requêtes du réseau de consultation.

Phase de débug

Comme dit précédemment, le changement majeur de cette nouvelle version d'ALCASAR est l'évolution de la version de Mageia.
Cela a donc engendré de nombreux problèmes et donc de diagnostiques lors de l'intégration de mon travail.

a) NfSen

L'un de ces problèmes bloquait le script d'installation au niveau du bloc NfSen. L'installation entrait dans une boucle sans fin, causée par le fait que NfSen ne démarrait pas lorsque l'on indiquait l'expiration des captures de 62 jours. Cette expiration a été mise en place afin de permettre une libération de mémoire.

b) Fail2ban

Un second problème majeur empêchait le démarrage de Fail2Ban.

Fail2Ban est outil qui consulte les logs de différents services, et en fonction d'une ou plusieurs « expressions rationnelles » (chaînes de caractère ou motifs), bloque les adresses IP à l'aide de règles iptables. Cet outil est généralement utilisé pour détecter les tentatives d'authentification par fuzzing sur des services comme SSH, FTP, WEB…

Dans mon cas, Fail2Ban était paramétré pour accéder à un fichier inexistant généré par Apache. Or, apache ayant été mis à jour récemment, sa structure interne a légèrement changé, ce qui m'a poussé à adapter Fail2Ban.

J'ai donc édité les paramètres de Fail2Ban pour ne lire que dans un seul fichier, dont l'existence est assurée. J'ai modifié les expressions rationnelles afin de les adapter à ce nouveau fichier de log.

Conclusion

J'ai donc effectué ces quatre mois de stage au sein du laboratoire CVO², en menant à bien les missions qui m'ont été confiées. Ces différentes missions m'ont permis de mettre en pratique certaines connaissances acquissent lors de ma quatrième année à l'ESIEA.

De plus, le cadre professionnel du laboratoire fut très enrichissant, que ce soit humainement, ou techniquement.

Mon application dans un projet collaboratif comme ALCASAR est une grande première pour moi. L'ajout de fonctionnalités, la correction de certaines autres, le respect de la philosophie du projet sont, à mon sens, très intéressant et riche en expériences. En effet, le fait d'être à plusieurs à travailler sur le même projet m'a poussé à être à l'écoute des autres, et à apprendre le travail en collaboration afin de trouver une solution qui soit la plus travaillée et réfléchie possible, tout en ne freinant pas le travail des autres collaborateurs.

Pour finir, je reste disponible afin de répondre aux hypothétiques problèmes qui surviendraient à la sortie d'ALCASAR 2.9.

Webographie

1. ActiveXperts software - SMS Component.
   http://www.activexperts.com/sms-component/at/etsi/

2. Huawei - UMTS Datacard Modem AT Command Interface Specification.
   http://www.net139.com/UploadFile/menu/HUAWEI%20UMTS%20Datacard%20Modem%20AT%20Command%20Interface%20Specification_V2.3.pdf

3. USB_ModeSwitch
   http://www.draisberghof.de/usb_modeswitch/

4. Base de connaissances Gammu
   http://fr.wammu.eu/phones/

5. NfSen
   http://nfsen.sourceforge.net/

6. SURFmap
   http://sourceforge.net/projects/surfmap/

Glossaire

GSM : Global System for Mobile Communications, anciennement **G**roupe **S**pécial **M**obile.

SMS : **S**hort **M**essage **S**ervice

MMS : **M**ultimedia **M**essage **S**ervice

PIN : **P**ersonal **I**dentification **N**umber, Numéro d'Identification Personnel

SIM : **S**ubscriber **I**dentity **M**odule

USB : **U**niversal **S**erial **B**us, bus universel en série.

Connexion série : C'est une interface entrée sortie permettant un échange entre l'ordinateur et un périphérique extérieur. La norme utilisée est : RS-232. Le terme « série » traduit le type la transmission des données qui a lieu dans cette liaison.

NfSen : **N**et**f**low **Sen**sor est une interface web graphique exploitant les données recueillies par la sonde Netflow.

IP : **I**nternet **P**rotocol, niveau 3 (réseau) du modèle OSI, permet l'adressage de périphériques.

OSI : **O**pen Systems **I**nterconnection, est une norme définie pour une infrastructure réseau, et les équipements qui le composent.

NAC : **N**etwork **A**cces **C**ontrol, ou Contrôleur d'accès au réseau, est une solution permettant de donner accès à un réseau sous la réserve d'une identification.

SSH : Secure Shell

Apache : Apache est un projet de serveur HTTP

FTP: File Transfert Protocol, est un protocole de transfert de fichiers.

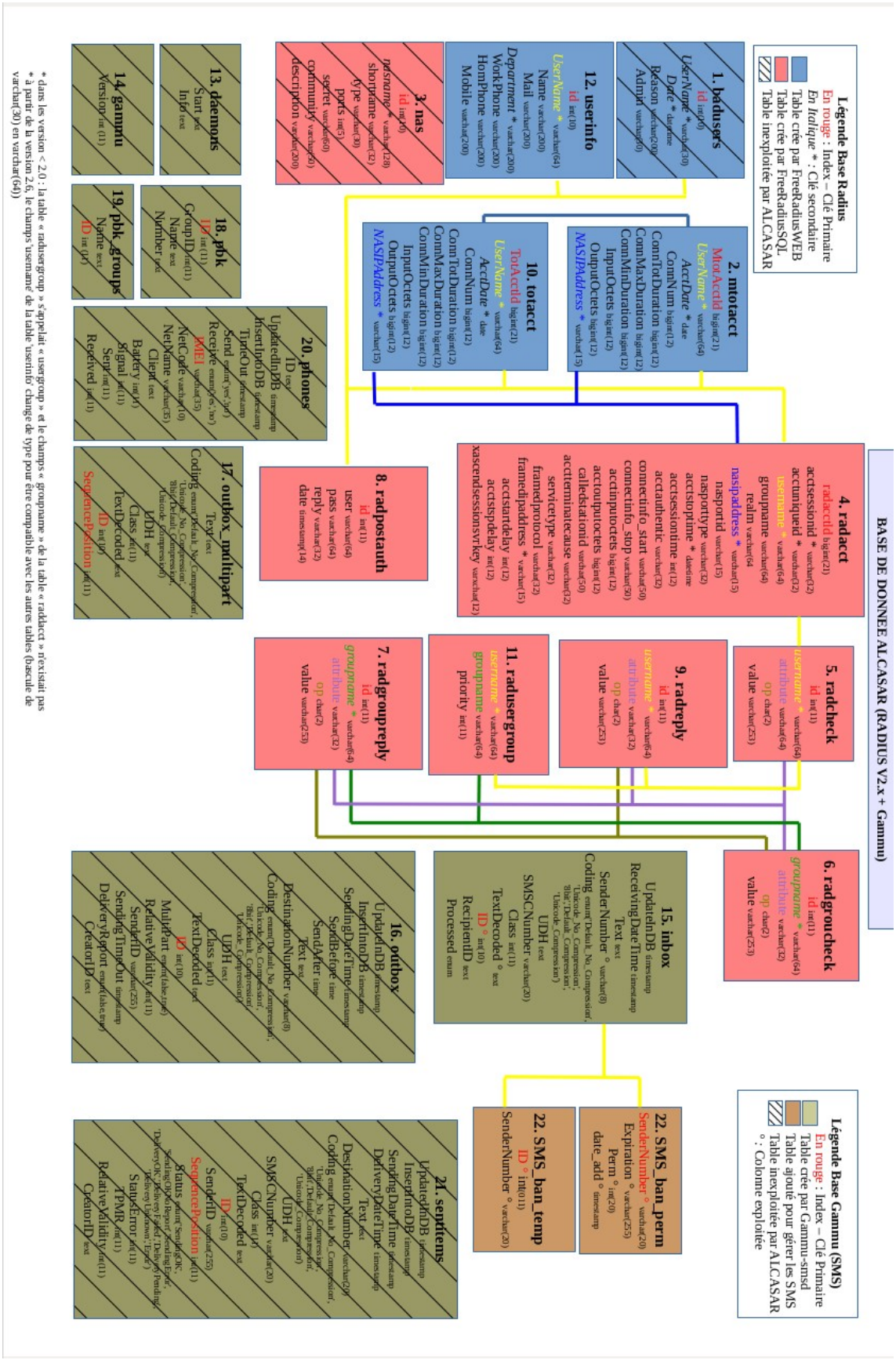
LDAP : Lightweight Directory Access Protocol

A.D : Active directory

Liste des illustrations

Liste des Annexes

Annexe 1 *– Base de données ALCASAR*



* dans les version < 2.0 : la table « radusergroup » s'appelait « usergroup » et le champs « groupname » de la table « radacct » n'existait pas
* à partir de la version 2.6, le champs 'username' de la table 'userinfo' change de type pour être compatible avec les autres tables (bascule de varchar(30) en varchar(64))

Fiche d’évaluation