# PROJET SECURITE RESEAU

## Groupe Analyse

## Comité d'Audit S.T.R.I.

ETUDIANTS :

Jonathan Blanc
David Gerbaulet
Julien Manuel
David Nembrot
Simon Pachy
Dimitri Tsiopoulos

# SOMMAIRE

# I. Introduction

## a. Situation

Dans le cadre du cours de sécurité des systèmes d'information, il a été mis en place plusieurs approches métiers concernant cette dernière.

Trois groupes de six personnes ont été formé avec pour chacun d'eux des buts différents ; tout se base sur la mise en place d'un réseau sécurisé par le groupe Défense, sur lequel le groupe Attaque tente de s'infiltrer, de récupérer des données ou de créer des dénis de service. Parallèlement à cela, le groupe Audit, met en place une supervision en étroite collaboration avec le groupe Défense afin de prévenir toute intrusion et de pouvoir réagir.

C'est ce dernier groupe que nous formons et que nous allons vous présenter tout ce qui a été mis en place et a été effectué dans le cadre de notre mission.

## b. Objectif

Notre groupe d'Analyse s'est fixé quelques grandes lignes à suivre afin d'évoluer de façon cohérente, notamment de manière à atteindre les objectifs inhérents à une supervision de réseau.

Ces derniers ont été amené à évoluer tout au long du projet en raison du manque de vision sur un domaine qui nous été encore quelque peu inconnu.

Dans un premier temps les critères de réussite que nous nous sommes fixés étaient :

- ✓ Prouver qu'avec un groupe hétérogène du point de vue technique, social et d'un point de vue du management, on était capable de fournir un travail clair, propre et sans erreur, ou du moins limitées.
- ✓ Faire preuve d'une grande communication, coordination afin de gommer cette hétérogénéité.

Sur le plan plus technique :

- ✓ Savoir prédire les failles du système de sécurité mis en place par la défense.
- ✓ Dégager les responsabilités, les objectifs et les moyens mis en œuvre en les explicitant dans un contrat détaillé et exhaustif.

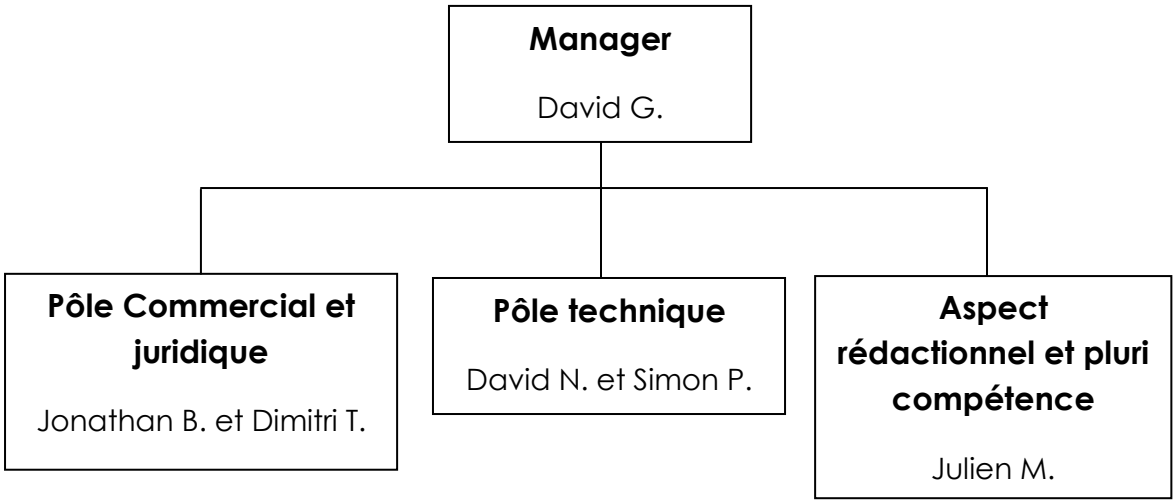
- ✓ Déchiffrer très clairement les logs des différents systèmes de supervision mis en place afin d'exposer les grandes lignes au groupe de Défense.

Suite à cela se sont vu ajoutés :

- ✓ Réagir au plus vite suite à un déni de service et savoir en informer le groupe défense sans perdre de temps afin d'allier nos forces pour éviter que cela ne se reproduise.

# III. Distribution des tâches :

## a. ***Diagramme organisationnel***




**Généralités :**

Des référents ont été désignés dans chaque pôle. Il n'était pas figé et pouvait être modifié à tout moment sur accord de chaque protagoniste. Toute modification devait être reportée à l'ensemble de l'équipe.

Jonathan et David N. ont été les référents sur les pôles Commercial et Technique.

## b. ***Rôles***

- ***Manager : David G.***

- Définir les objectifs de chacun, essayer d'établir la charge de travail nécessaire à chaque tâche (Diagramme de Gantt) et d'organiser et mettre en relation tous les acteurs du projet (Aussi bien de notre équipe Analyse que de l'équipe Défense),

- Cerner tous les éléments (commercial, juridique et technique) du projet afin que, même en l'absence des différents experts, il y ai une redondance des informations et la possibilité d'avoir au moins un interlocuteur compétent face aux demandes de l'équipe Défense.

- Se pencher sur les différentes méthodes d'audit

- Tenir informer l'équipe Analyse des dates de réunions, des sujets, des participants, des objectifs et faire transiter les informations.

- Participer à l'épluchage des logs après les confrontations.

### ➢ *Pôle Commercial et Juridique : Jonathan B. et Dimitri T.*

- Etablir un cadre juridique et commercial entre les deux parties (Contrat entre la Défense et Analyse)

- Vérifier l'application de la politique de sécurité au jour le jour et rapporterez, à l'ensemble de notre équipe ainsi qu'à l'équipe Défense, les vices de procédures s'il y en a,

- Rédiger des avenants signés par les deux parties pour régulariser la situation si besoin.

- Participer à l'épluchage des logs après les confrontations.

### ➢ *Pôle techniques : David N. et Simon P.*

- Rôles clés de l'équipe. En effet, Il n'existe pas d'audit performant sans des experts techniques tout aussi performant.

- Installer la sonde et les outils adéquats.

- Identifier les différentes failles de l'équipe Défense et les attaques réalisés par l'équipe Attaque. Ensuite, les notifier (Date, Type d'attaque, Heure..) à l'ensemble de notre équipe ainsi qu'à l'équipe Défense.

- Etablir les procédures nécessaires à l'obstruction des failles et des procédures de reprise sur incidents au cas où le système défendu venait à être touché.

### ➢ **Aspects rédactionnel et pluri-compétence : Julien M.**

- Définir un mini-cahier des charges par rapport à la demande de l'équipe Défense.

- Rôle de « volant » susceptible d'être appelé pour différentes tâches d'où une compréhension globale de tous les aspects du projet.

- Gère le rédactionnel de l'équipe pour décharger les pôles et leurs permettre de ne pas perdre de temps sur la mise en forme de leurs travaux.

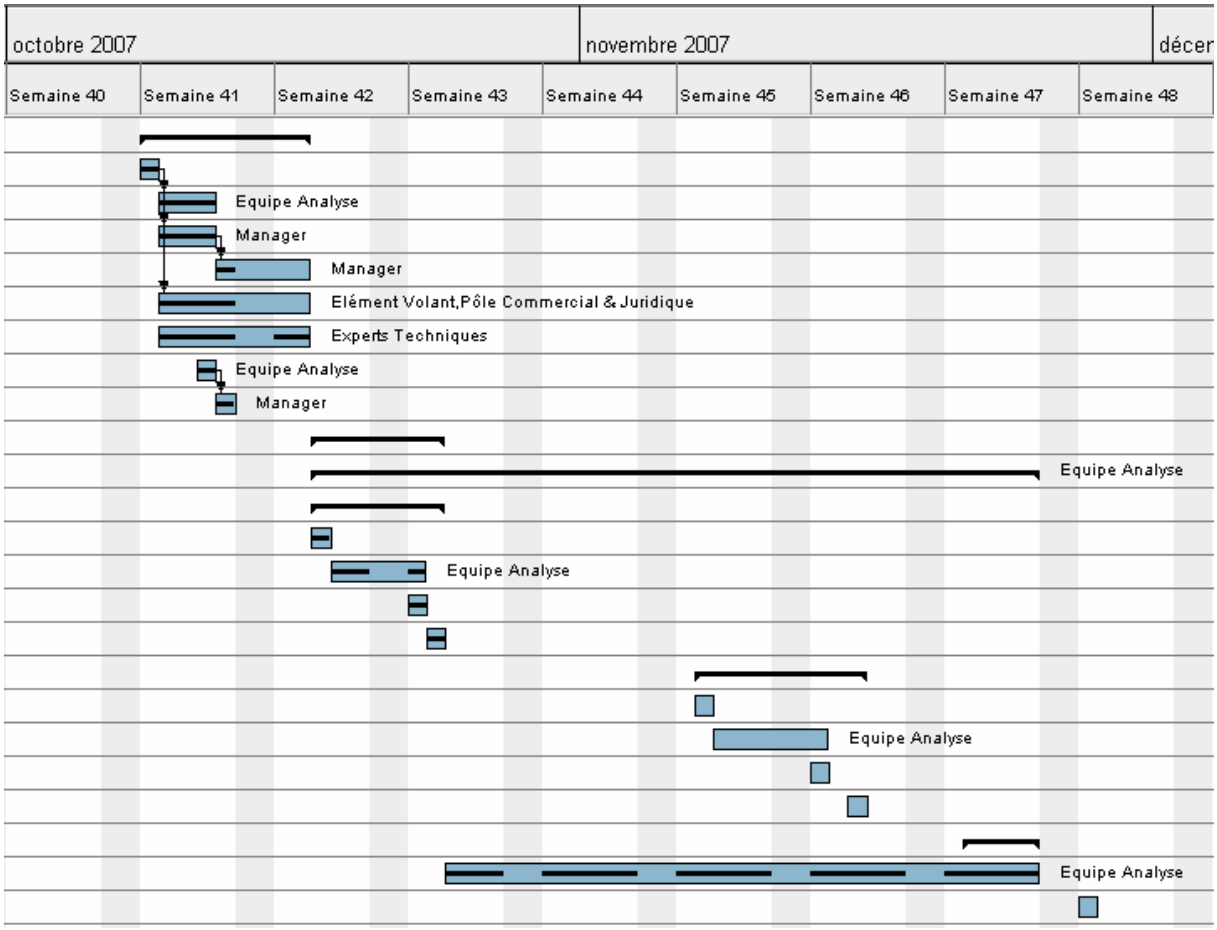
- Participer à l'épluchage des logs après les confrontations.

## c. ***Planning***

Le Diagramme de Gantt ci-dessous montre le planning des activités tel qu'il était prévu au début du projet. Cependant, la grève et le blocage du bâtiment U2 ont perturbé notre planning.

Nous n'avons pu faire que deux confrontations avec l'équipe Attaque (le 17/10/07 et le 04/12/07) et la date de remise du rapport a été reportée au 17 décembre 2007.

| Nom | Date de... | Date de ... | Durée |
|---|---|---|---|
| Phase de mise en route | 08/10/07 | 17/10/07 | 7 |
| Répartition des roles | 08/10/07 | 09/10/07 | 1 |
| Etude des rapports des années précédentes | 09/10/07 | 12/10/07 | 3 |
| Etude des differentes methodes d'audit | 09/10/07 | 12/10/07 | 3 |
| Choix de la Méthode d'Audit MEHARI et prise ... | 12/10/07 | 17/10/07 | 3 |
| Etude contrat et cahier des charges | 09/10/07 | 17/10/07 | 6 |
| Etude sur les outils logiciel d'audit | 09/10/07 | 17/10/07 | 6 |
| Réunion avec l'équipe Défense | 11/10/07 | 12/10/07 | 1 |
| Compte rendu de réunion | 12/10/07 | 13/10/07 | 1 |
| Partie n°1 du Projet | 17/10/07 | 24/10/07 | 5 |
| Confrontation | 17/10/07 | 24/11/07 | 28 |
| Second TP Réseau | 17/10/07 | 24/10/07 | 5 |
| Analyse en temps réel de la confrontation | 17/10/07 | 18/10/07 | 1 |
| Analyse des logs | 18/10/07 | 23/10/07 | 3 |
| Remise du rapport de logs à la Défense | 22/10/07 | 23/10/07 | 1 |
| Réunion Equipe | 23/10/07 | 24/10/07 | 1 |
| Troisième TP Réseau | 06/11/07 | 15/11/07 | 7 |
| Analyse en temps réel de la confrontation | 06/11/07 | 07/11/07 | 1 |
| Analyse des logs | 07/11/07 | 13/11/07 | 4 |
| Remise du rapport de logs à la Défense | 12/11/07 | 13/11/07 | 1 |
| Réunion Equipe | 14/11/07 | 15/11/07 | 1 |
| Quatrième TP Réseau | 20/11/07 | 24/11/07 | 4 |
| Rapport d'AUDIT 2007/08 | 24/10/07 | 24/11/07 | 23 |
| EXAMEN du Projet | 26/11/07 | 27/11/07 | 1 |




## d. ***Mise en place et démarrage de l'activité***

Dans un premier temps nous nous sommes investis sur certains points particuliers, tout cela supervisé par David Gerbaulet:

- La mise en place du contrat nous liant au Groupe Défense, tâche affectée à Jonathan Blanc et Dimitri Tsiopoulos,
- La mise en place des systèmes de supervision, tâche affectée à David Nembrot et Simon Pachy,
- La mise en place du cahier des charges, tâche affectée à Julien Manuel,
- La recherche d'une méthode d'audit pour essayer de la calquer sur notre projet, tâche affectée à David Gerbaulet.

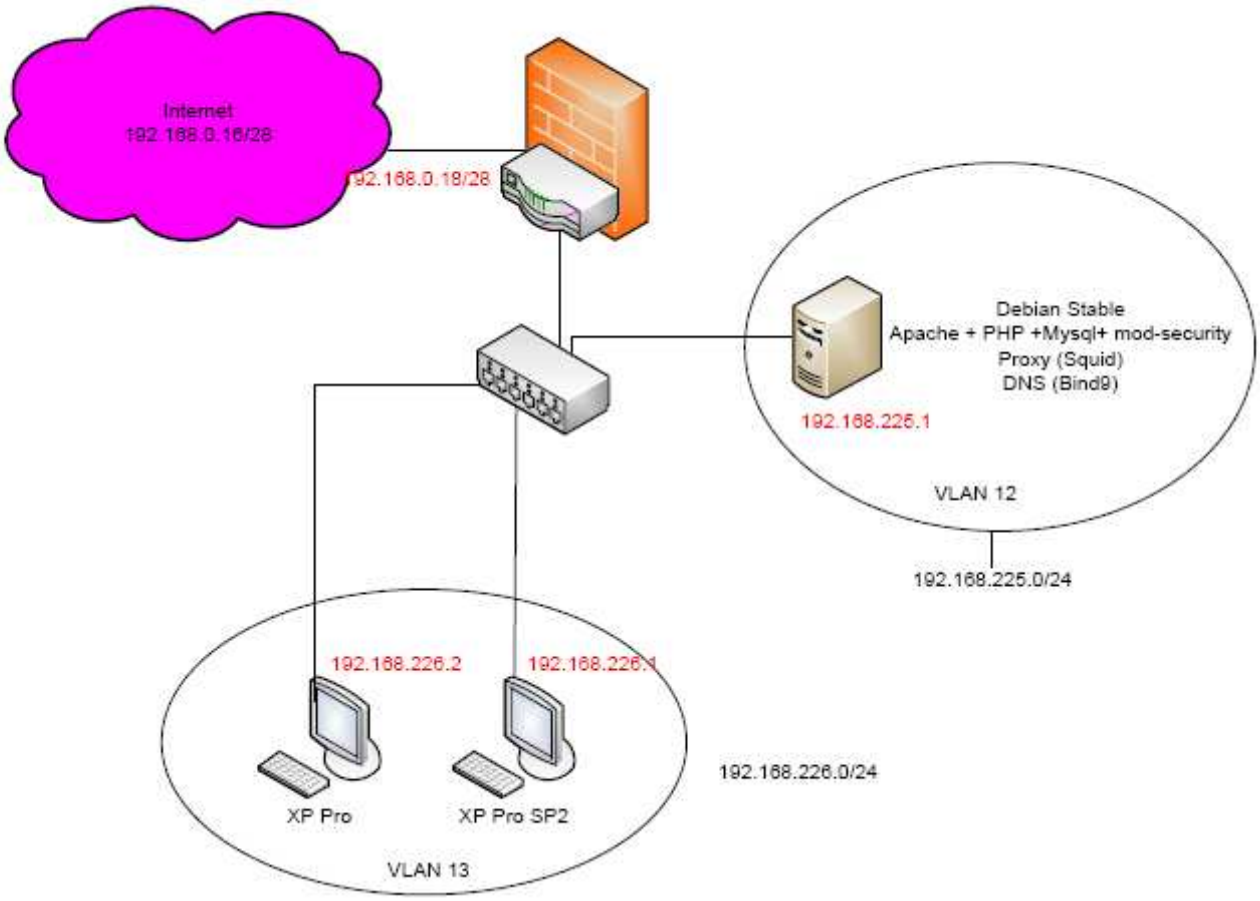
Une fois la sonde mise en place et la configuration pour récupérer les logs effectuée, Julien Manuel s'est penché sur les logs pour « s'habituer » au bruit de fond constant et ainsi permettre une réaction plus rapide lors des tentatives d'intrusion ultérieures.

Par la suite est venu la première confrontation qui a entraîné un peu de travail supplémentaire :

- ✓ L'analyse en temps réel des évènements sur le réseau du groupe Défense
- ✓ L'observation des demandes de manipulation du groupe Attaque et des éventuels déni de services
- ✓ L'analyse a postériori des logs remontés par les différents systèmes (la sonde, le serveur…) répartie entre tous les membres du groupe.

# III.Partie AUDIT

## a. ***Présentation brève de l'architecture cliente :***




Ce modèle d'architecture est assez sommaire puisque seul le pare-feu du routeur et le serveur, configurés par la défense par application de règles iptables, permet d'assurer une sécurité minimale du système.

Néanmoins, la configuration des vlans a permis de bien cloisonner le réseau et de segmenter les périmètres serveurs et clients.

Le réseau audité se compose donc d'un serveur APACHE avec les modules PHP5 et mod-security ainsi que 2 postes clients Windows XP Pro et XP Pro SP2.

La mise en place ultérieure d'un serveur DNS et d'un proxy web ont permis de compléter la sécurité des échanges de données avec le monde extérieur.

Enfin, les techniciens de la défense ont pu rapidement exporté tous les logs système vers notre sonde.

## *b. Tâches et Réalisations :*

### ▪ Contrat

(voir annexe 1 : Contrat d'audit)

Objectifs :

- Délimiter le périmètre d'action du groupe d'Analyse et du groupe Défense.
- Définir les besoins en termes d'informations et d'accessibilité au réseau pour une analyse complète et efficace.
- Poser les notions de confidentialités, de rémunération et de rapports périodiques

Les moyens mis en œuvre pour établir ce contrat ont été d'une part, une profonde recherche sur les éléments à traiter dans un contrat dans le domaine de la sécurité de réseau informatique et d'autre part, un appui sur l'expérience de nos prédécesseurs.

Le contrat a été établi dans les temps mais nous avons eu quelques difficultés au niveau de la mise en forme pour que ce document soit clair et que les éléments traités ne se recoupent pas les uns les autres.

### ▪ Cahier des charges

(voir annexe 2 : cahier des charges 1iere et 2ieme confrontation)

Objectifs :

- Connaître l'organisation de l'équipe défense, ainsi que le rôle de chacun au sein de cette équipe afin de faciliter la communication.
- Nous spécifier les droits d'accès sur le réseau de la défense.
- Définir l'architecture du réseau de la défense pour la première confrontation, ainsi qu'un aperçu des évolutions envisagées pour la deuxième confrontation.
- Définir les attentes de l'équipe défense vis-à-vis de notre équipe d'audit.
- Enfin, communiquer le calendrier des confrontations élaborées entre les différentes parties.

Les cahiers des charges nous ont été fournis par l'équipe défense. Le premier avant la première confrontation, le second avant la deuxième pour nous signaler d'éventuels changements dans l'architecture du réseau.

Ces échanges ont eu lieu avec le pôle communication de l'équipe Défense.

## c. Mise en place de la Méthode MEHARI

*(voir annexe 3 : Méthode Mehari)*

Objectifs :

- Essayer de prendre en main un outil complet d'analyse.

Cette méthode est très complète voir trop pour le cadre de notre projet. C'est pourquoi nous nous sommes limités à la définition de l'existant, à un questionnaire adapté et à une rapide analyse en fonction des recommandations de la norme ISO 17999:2005, référence sur la gestion de la sécurité informatique.

Ci-dessous, les principales méthodes d'audit :

**Les principales méthodes d'audit de sécurité**

| Nom | Signification | Origine | Caractéristiques |
|---|---|---|---|
| **Cobit** | Control objectives for information and technology | ISACA | Méthode accessible à tous, dans un langage simple. Les outils fournis permettent la mesure des performances mais la méthode est aujourd'hui davantage assimilée à une méthode de gouvernance des SI. |
| **Ebios** | Expression des Besoins et Identification des Objectifs de Sécurité | DCSSI | Notamment déployée au sein de l'administration française, cette méthode comprend une base de connaissances et un recueil de bonnes pratiques. Elle est téléchargeable sur le site de la DCSSI et s'accompagne d'un logiciel. |
| **Feros** | Fiche d'Expression Rationnelle des Objectifs de Sécurité | SCSSI | Pas une méthode à proprement parler mais un document permettant à une autorité donnée (secteur secret défense notamment) de définir le niveau d'engagement de sa responsabilité dans l'application d'une politique de sécurité. |
| **Marion** | Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux | CLUSIF | Fonctionne par questionnaires débouchant sur 27 indicateurs répartis en 6 catégories. 2 phases (audit des vulnérabilités et analyse des risques) permettent la définition et la mise en œuvre de plans d'actions personnalisés. |
| **Mehari** | Méthode Harmonisée d'Analyse de Risques | CLUSIF | Succède à la méthode Marion. S'articule autour de 3 plans. Permet désormais d'apprécier les risques au regard des objectifs "*business*" de l'entreprise. |

Nous avons choisi la méthode MEHARI car d'une part, elle est l'évolution de la méthode MARION et d'autre part, elle est gratuite.

La première étape a été de définir avec Mr BOSCARI, Chef de projet de la Défense, et Mr ABOUZEID, Responsable de la Communication, les différents domaines d'activités et les processus sensibles

Nous avons ensuite demandé aux responsables quel serait l'impact sur « l'entreprise » en cas de dysfonctionnements d'un des processus.

Il a fallu ensuite définir les seuils de gravité pour chaque critère d'impact sachant que :

- Seuil 1 : Sans dommage significatif
- Seuil 2 : Dommage important
- Seuil 3 : Grave dommage
- Seuil 4 : Dommage extrêmement grave

Nous avons ensuite recensé et classifier les ressources suivant trois critères :

- Disponibilité
- Intégrité
- Confidentialité
-

Les notes sont comprises entre 1 et 4 sachant que, plus le critère paraissait important, plus la note était élevée.

Une fois ces classifications terminées, nous nous sommes appuyés sur les questionnaires de la méthode MEHARI, basé sur 12 scénarii, pour modeler un questionnaire d'environ 400 questions, découpé en six domaines et pour donner un léger aperçu de ce que pourrait être un audit.

Voici les six domaines identifiés :

- **Domaine d'Organisation**

- **Domaine des Locaux**

- **Domaine du Réseau Local (LAN)**

- **Domaine de l'Exploitation des Réseaux**

- **Domaine de la sécurité des Systèmes et de leur architecture**

- **Domaine de la Protection de l'Environnement de Travail**

Pour chaque question, le responsable devait répondre par « oui » ou par « non ».

A la suite de ça, nous nous sommes penchés sur les réponses négatives pour mettre en lumière les non-conformités par rapport à la norme ISO 17999: 2005 et proposés, quand cela était possible, quelques améliorations.

Ce que l'on peut retenir :

L'analyse aurait pu être plus approfondie avec le calcul de différents indicateurs tels que la métrique de risque, de dissuasion, de potentialité, etc.

Néanmoins, cela nous paraissait inutile car la base de questionnaire ayant été modifiée, les calculs qui en découlent se trouvent biaisés. De plus, compte tenu du nombre important de projets que nous avions à réaliser, nous n'aurions pas eu le temps de rentrer plus amplement dans les détails.

Quoiqu'il en soit, on a donc pu voir, par cette méthode, que le point le plus critique du projet était le domaine des locaux.

Pour conclure, il était intéressant d'essayer de prendre en main une méthode d'audit malgré la difficulté inhérente. Les cabinets d'audits étant de plus en plus convoités par les entreprises pour obtenir une évaluation de leur système informatique, on sera peut être amené, dans un futur proche, à travailler au sein d'un de ces cabinets ou à faire appel à l'un d'eux.

Il devient donc avantageux de connaitre les méthodes et démarches utilisé.

## d. Mise en place de la Sonde :

Objectifs :

- Installer physiquement la sonde sur le réseau de la Défense
- Définir les règles de sécurité sur la sonde pour éviter qu'elle soit compromise
- Installer les logiciels permettant la supervision du trafic
- Penser à une future évolution de la supervision (tests de failles, attaques…)

En premier lieu, nous avons remplacé le daemon telnetd par sshd afin d'améliorer la sécurité concernant l'accès à distance. Nous avons ensuite monté le serveur Web en installant la dernière version d'Apache avec les modules nécessaires à nos besoins : php5, php5-mysql et mod-security principalement...

Une fois le serveur Web mis en place, nous nous sommes attelé à déployer une base de données locale en installant les paquets mysql-server et php-myadmin. SCette base servant de système d'archives pour les outils de détection d'intrusion SNORT et de visualisation ACIDBASE, installés après beaucoup plus de difficultés: les scripts automatiques de remplissage de la base de données ne se sont pas exécutés du premier coup.

Après validation des configurations système (droits de chaque utilisateur, partage des droits, purge des services inutiles, etc), nous avons défini un formulaire d'informations réseau que la défense a du mal à nous retransmettre rapidement. Au final, nous avons quand même pu intégré notre sonde au réseau de l'équipe

Défense. Enfin, pour apporter une gestion de vlan, nous avons du installer le paquet éponyme pour configurer des interfaces virtuelles.

A terme, nous avons monté un serveur de logs qui recueille tous les logs système des hosts du réseau local. La configuration de syslog-ng n'a pas été de tout repos, mais avec l'intercession de Mr LATU et la collaboration active de Mr PY, nous avons pu finaliser la centralisation de logs assez rapidement. Le but étant d'avoir une trace de tout événement système afin de mieux prévenir les failles et de comprendre les éventuelles démarches d'intrusion.

Côté supervision, nous avons mis en place l'outil Ntop qui restitue graphiquement l'activité réseau en live. Cet outil nous a beaucoup servi dans la mesure où il propose un niveau de précision très intéressant. Par exemple, il est possible de surveiller un host au niveau port avec une gestion de NetFlow. On voit donc aisément qui essaie de se connecter, qui communique avec qui.

De façon plus globale, on peut aussi observer la distribution des protocoles utilisés par chaque machine, apprécier les statistiques au niveau de la taille des trames relatives et avoir une idée chronologique des transactions de données sur le réseau interne et externe vu que Ntop analyse aussi les machines qui sont régulièrement impliquées dans le trafic local.

Ensuite, nous avons essayé de déployer un autre outil de monitoring réseau: Hobbit ie BB4.

Cet outil en complément de Ntop, permet de connaître les états de connexion des équipements en temps réel. Ainsi, il est très facile de visualiser sur l'interface Web la saturation d'une machine et de déduire la bande passante réseau utilisée, afin de prendre les dispositions nécessaires pour éviter les dénis de service. Malheureusement, nous n'avons pas réussi à configurer correctement cet outil.

Tout comme l'outil MRTG qui demandait une implémentation SNMP au sein du réseau: par manque de temps et de ressources nécessaires aux recherches, nous n'avons pas pu concrétiser cette idée.

Par contre, nous avons réussi à installer N3ssus sur la sonde. Après l'interminable mise à jour de ses 17838 modules de sécurité, nous avons procédé à des tests assez poussés de vulnérabilités sur le réseau local afin de conseiller au mieux l'équipe défense vis-à-vis des failles de sécurité trouvées.

Des rapports ont été envoyés à l'équipe défense avec la plus grande priorité et ont su être traités rapidement.

Les tâches suivantes font suite aux informations recueillies pendant ou ultérieurement aux confrontations entre la Défense et l'Attaque. Les principales tâches qui découlent de ces confrontations sont l'analyse des logs et l'établissement

des rapports périodiques pour le groupe Défense, leurs objectifs et les moyens mis en œuvre sont les mêmes quelque soit la phase du projet et sont les suivants :

- **L'analyse de logs :**

Objectifs :

- Identifier les tentatives/réussites d'intrusion sur le réseau
- Retracer les actions de l'équipe Attaque

Afin de collecter le plus grand nombre de logs possibles, nous avons installé un deuxième disque dur dédié pour laisser un peu plus de marge à l'outil de sniffeur réseau TSHARK.

Principalement, lors des confrontations, nous lancions à travers un système de fenêtrage virtuel (cf. paquet screen) une capture intégrale de paquets réseau. Un fichier destination.pcap correspondant au trafic spécifique à un protocole particulier sur un vlan précis.

Concernant l'analyse en elle-même, la répartition des logs fraîchement récoltés et l'assignation des tâches se faisaient le soir même. Une connexion SFTP distante permettant de rapatrier tous les fichiers désirés et de les redistribuer au sein de l'équipe.

Lors des confrontations, le chef de projet a pris des notes chronologiques, servant par la suite de base commune à la lecture analytique des fichiers de logs. Nous avons principalement utilisé Wireshark pour les fichiers.pcap et le Ctrl-F pour les autres fichiers système.log *(oh malheureux ! Un bon coup de grep serait tellement plus approprié ;)*

- **Synthèses et rédactions des rapports :**

Objectifs :

- Synthétiser le contenu des logs et l'exploitation faite par les différents membres de notre groupe Audit
- Proposer des solutions pour éviter de rencontrer de nouveaux les mêmes problèmes

La lecture des centaines de Mégaoctets de logs a permis de comprendre en détail la méthodologie des attaquants. Nous avions une idée précise des outils utilisés pour alourdir les attaques par dictionnaire sur le port SSH, ou par débordement de pile sur le port HTTP. De nombreuses remarques en interne ont

permis de recouper les événements critiques et de confirmer les accès frauduleux au système.

De plus, le serveur syslog qui écoutait en permanence sur le port 514 et qui recueillait des logs bufférisés nous a permis d'avoir des feedbacks sur les erreurs et de mieux comprendre l'impact des attaques sur le réseau.

Après chaque confrontation, un scan N3ssus établissait l'état de santé de la sonde et du serveur de la défense. Ce qui permettait d'apprécier à chaud les vulnérabilités résultantes.

Un rapport bien fourni en commentaires et précisions techniques était adressé à l'équipe Défense dans la semaine suivant la confrontation.

Concernant les rapports, nous avons tenu à présenter les événements chronologiques un peu comme une intrigue avec des remarques et des annotations qui rendent le côté technique moins rébarbatif. L'attention du lecteur étant de ce fait beaucoup plus articulée au fil de la lecture.

Notez que les résultats et les réactions ont été différents en fonction des phases, dus en partie à une plus grande maîtrise des outils utilisés par l'équipe attaque et à une faible évolution de l'architecture et des moyens de sécurité du groupe Défense.

### e. ***Première Phase***

#### ▪ Objectifs visés

A première vue, le but était de se familiariser avec les outils déployés par les techniciens, de comprendre ce qui se passait et comment ça se passait, à l'aide des outils d'audit.

La prise en main n'a pas été facile dans la mesure où les techniciens étaient plus préoccupés à finaliser la centralisation des logs avec la défense alors que le reste de l'équipe audit essayait d'analyser à chaud les actions des attaquants.

Au final, le chef de projet a bien pu noter l'ensemble des événements chronologiques, ce qui a grandement facilité la lecture post-attaque des logs.

## ▪ Observations durant la confrontation

Sous la tutelle du chef de projet, les collaborateurs du CASTRI ont pu suivre grossièrement le déroulement de la première attaque:

**16h35** Tous les protagonistes sont prêts. L'opération « Attaque Soviétique » est lancée.

**16h48** NTOP signale une nouvelle activité TCP et HTTP.

**16h57** L'outil *Nikto* est utilisé par les attaquants.
*Dénis de service du serveur défense. Temporairement.*

**17h05** Second Denis de Service avec un trafic HTTP et TCP encore plus intense.
*Les attaquants semblent avoir utilisé* **python-urllib**.

**17h07** L'équipe Attaque n'arrive pas à pénétrer le réseau et demande à la Défense d'atteindre l'URL : **192.168.0.20/accueil.htm**
***Sans succès***

**17h10** Les attaquants utilisent un hôte de la salle 213.
La sonde audit est victime d'une attaque majeure:

- flooding ICMP et attaques des services *(bruit de fond)*
- attaque SSH par dictionnaire *(charge utile)*

*Dénis de service de la sonde audit quasi immédiat mais temporaire.*
***Un torrent de plus de 700 paquets par seconde est identifié !!!***

**17h45** La décision est prise : suite à une demande de l'équipe attaque, la défense permet une grosse faille dans le code PHP *(# include..)*.

**17h51** La faille est vérifiée et le serveur défense est sous pression.

*Les logs de la sonde audit rapportent une vaste attaque SSH par dictionnaire et des tentatives d'injection de code dans les formulaires du site web de la défense.*

**18h00** A la demande de l'équipe attaque, l'URL faussée est rechargée de nouveau.

*On se rend compte à cet instant que la sonde est visée*

**18h15** Un processus nommé « a.exe » est détecté sur le poste client non mis à jour provoquant l'ouverture de pages web. Il est aussitôt détruit.

*Le routeur rapporte une erreur ICMP à la sonde : le poste client XP tente d'accéder au périmètre services.*

**18h17** Les attaquants ont accès au site web du serveur défense.
Tous les fichiers du site sont récupérés et archivés.

**18h18** La sonde audit est à bout de souffle.

Une activité encore plus intense est constatée sur le port 22 et elle ne répond plus. Une déconnexion physique est décidée pour éviter le pire.

**18h20** L'équipe audit arrive à retrouver un accès distant à la sonde depuis une nouvelle machine de la salle.

**18h23** Elle établit un premier bilan des services et des outils.

**18h25** L'opération « Attaque Soviétique » est officiellement terminée.

*Le lendemain, de nouvelles attaques ont été découvertes:*
*- bad_checksum portscan en bruit de fond*
*- tentative d'injection de scripts CGI via VPN*

## ▪ Résultats de l'analyse de log et conseils à la défense

Suite à une interception douteuse d'échanges de clés du serveur SSH de la Défense, nous avons préconisé un changement complet des mots de passe.

Autrement, cette première attaque n'a pas vraiment causé de dégâts conséquents à l'échelle du réseau grâce à un bon cloisonnement inter-vlans.

## ▪ Implémentation de nouveaux outils :

Après le première confrontation, une cellule de recherche a été organisée afin de disposer d'éléments nouveaux en matière de :

- ✓ monitoring réseau à travers les outils Hobbit et MRTG,
- ✓ bouclier du serveur Web Apache (Logcheck et mod-security principalement),
- ✓ scans réseau avec N3ssus et les autres outils de défense offensive permettant d'identifier les vulnérabilités du réseau mis en place (metasploit, SSL2open, DNS-bruteforce),
- ✓ pénétration réseau en faisant fi du pare-feu installé à l'aide des outils Firewalk et Itrace.

## f. ***Seconde Phase :***

### ▪ Objectifs visés

Premièrement, notre but était d'avoir un contrôle temps réel du réseau. Grâce à l'interface Ntop, une partie de l'équipe était capable d'avertir les techniciens rapidement d'un transit suspect, d'une nouvelle connexion, tout en surveillant « les flux normaux ». De même via AcidBase, qui est censé renseigner très rapidement les tentatives d'intrusion.

Deuxièmement, nous voulions réagir très vite en rajoutant des règles iptables à la volée, en manipulant dynamiquement certains services critiques et en avertissant l'équipe défense au plus vite lorsqu'ils étaient pris pour cible.

### ▪ Observations durant la confrontation

**15h** Tous les protagonistes sont prêts. L'attaque est lancée.

*Les règles iptables draconiennes déployées sur le routeur racine,*
*sur le serveur défense et sur la sonde ont considérablement*
*ralenti les tentatives d'intrusion des attaquants.*

**16h00** L'outil NTOP présente des dysfonctionnements d'affichage.
Le rafraîchissement de l'interface ne livre plus d'informations temps-réel.

```
Dec  4 16:07:35 sonde-analyse ntop[16391]:   **WARNING** free of NULL pointer @ http.c:3588
Dec  4 16:07:35 sonde-analyse ntop[16391]:   **ERROR** EPIPE during sending of page to web client
[... ... ...]
Dec  4 16:51:56 sonde-analyse ntop[16391]:   **ERROR** EPIPE during sending of page to web client
```

**16h25** Les attaquants utilisent désormais les outils AcuneTix *(scanner de vulnérabilités, SQL injection / Cross site scripting testing)* et IngresLock *(mise en place de backdoor)* afin d'alourdir les attaques par flooding entamées sur le port 80 des serveurs audit et défense.

*On a observé que le serveur attaque a tenté des injections*
*de code SQL et Java et a envoyé une quantité énorme*
*de requêtes GET sur les deux instances de phpMyAdmin,*
*La principale cible étant la page web site/etudiant_action.php*

**16h30** Les premières requêtes authentifiées apparaissent sur la sonde.

Un GET suivi d'un POST avec le mot de passe admin leur ouvre un accès complet sur le port 8080 de la sonde.

*Les attaquants continuent leur flood sur le port 80 de la défense,*
*et s'attaquent à la page site/prof_action.php*

**16h35** Les attaquants commencent à exploiter le serveur mail.
Postfix signale à la sonde la présence de mails en attente d'expédition pour *james.patagueul@truc.com*

**16h45** L'outil SNORT est compromis. Son intégrité est mise à mal et la consultation des intrusions via Acidbase ne marche plus *(port 8080)*.

**16h48** Les attaquants pénètrent le SGBD de la sonde audit et ont désormais accès à la structure de la base de données snort.

*Quelques minutes plus tard, on a découvert une requête POST sur la page phpmyadmin/import.php contenant du code SQL* ***DROP DATABASE*** *suivie d'une deuxième pour vérifier d'effacement via* ***SELECT * FROM ...***

**16h52** Via phpMyAdmin, une attaque est lancée depuis un poste de la salle 212. Il tente un débordement de pile sur le site web défense:
*/site/index.php?page=http%3A%2F%2F192.168.0.20%{...}*

**16h59** Toujours via phpMyAdmin, les attaquants envoient un nombre encore plus impressionnant de requêtes GET/POST au serveur défense sur les pages *inscrit.php & inscription.php*

*Les daemons* ***mysqld, squid et spamd*** *de la défense*
*redémarrent suite à une erreur de socket.*

**17h00** Le protocole gIFT *(graphic Internet File Transfer)* est utilisé par l'attaque. Une requête ***ResetStats*** est envoyée périodiquement à la sonde, vraisemblablement pour effacer les logs des outils de monitoring.

*Le port 3000 de la sonde se met à délirer sérieusement.*
*Les logs montrent des communications suspectes*
*(envoi périodique du signal* ***ResetStats*** *?!?)*

***L'activité SYSLOG est à son apogée : la sonde récolte***
***près de 30 Mo de logs provenant de la défense... en 11 sec !!!***

*De nombreuses pertes ultérieures de segments TCP*
*ont été observées sur le périmètre serveurs.*

**17h05** Le service mail envoit un log d'alerte : il rapporte l'initialisation du service SSL imaps en loopback, suivie d'une mauvaise authentification avec comme message d'erreur:
*'' Command: stream end of file, while reading line user=defense2 host=localhost [127.0.0.1]\n ''*

**17h10** L'équipe défense découvre l'installation du Linux KeyLogger sur plusieurs ordinateurs de la salle 213 via la commande:

*find / -name ' *lkl* '*

*Notamment sur le poste utilisé par Dawid pour se connecter à distance sur la sonde. L'équipe attaque a donc eu accès aux mdp système.*

*Pour preuve, le changement des mdp de la sonde fait apparaître instantanément des messages ' AUTHENTICATION FAILURE' dans le fichier /var/log/user.log:*

*Dec 4 17:10:15 sonde-analyse sshd[26203]: Accepted password for sysadmin from 172.16.80.86 port 1385 ssh2*
*Dec 4 17:10:15 sonde-analyse sshd[26216]: pam_unix(ssh:session): session opened for user sysadmin by (uid=0)*
*Dec 4 17:10:35 sonde-analyse su[26236]: Successful su for root by sysadmin*
*Dec 4 17:10:35 sonde-analyse su[26236]: pam_unix(su:session): session opened for user root by sysadmin(uid=1000)*
*Dec 4 17:12:27 sonde-analyse passwd[26240]: pam_unix(passwd:chauthtok): **password changed for root***
*Dec 4 17:12:34 sonde-analyse su[26236]: pam_unix(su:session): session closed for user root*
*Dec 4 17:14:37 sonde-analyse passwd[26273]: pam_unix(passwd:chauthtok): **password changed for sysadmin***
*Dec 4 17:15:38 sonde-analyse su[26306]: pam_unix(su:auth): **authentication failure**; logname=sysadmin uid=1000 euid=0 tty=pts/1 ruser=sysadmin rhost= user=root*
*Dec 4 17:15:40 sonde-analyse su[26306]: pam_authenticate: Échec d'authentification*
*Dec 4 17:15:40 sonde-analyse su[26306]: FAILED su for root by sysadmin*
*Dec 4 17:16:05 sonde-analyse su[26328]: pam_unix(su:auth): **authentication failure**;*
*Dec 4 17:16:38 sonde-analyse su[26340]: pam_unix(su:auth): **authentication failure**;*
*Dec 4 17:17:04 sonde-analyse su[26341]: pam_unix(su:auth): **authentication failure**; logname=sysadmin uid=1000 euid=0 tty=pts/1 ruser=sysadmin rhost= user=root*
*Dec 4 17:17:06 sonde-analyse su[26341]: pam_authenticate: Échec d'authentification*
*Dec 4 17:17:06 sonde-analyse su[26341]: FAILED su for root by sysadmin*
*Dec 4 17:17:32 sonde-analyse sshd[26346]: **Bad protocol version identification from 192.168.0.20***
*Dec 4 17:18:03 sonde-analyse su[26345]: pam_unix(su:auth): **authentication failure**;*

**17h15** L'équipe défense change eux aussi les mdp de leur serveur et le redémarre.

Après le redémarrage, le service mail annonce la couleur:

mail : postfix/local[19593]: table hash:/etc/aliases(0,lock|no_proxy|no_unauth) has changed – restarting\n

De plus, il envoi à la sonde un buffer de données qu'il stockait depuis quelques heures. Les logs ont ainsi montré plusieurs tentatives d'accès au service en fin de matinée:

Message: Dec 4 11:41:21 mail : spamc[3435]: connection attempt to spamd aborted after 3 retries\n
Message: Dec 4 11:42:02 mail :connect(AF_INET) to spamd at 127.0.0.1 failed : Connection refused\n

**17h18** Les logs montrent des activités très suspectes du serveur défense:

Message: Dec 4 17:18:22 srv-web apache_error : **Not all processes could be identified.**\n
Message: Dec 4 17:18:22 srv-web apache_error : **Connecting to 192.168.0.20:80**... connected.\n
Message: Dec 4 17:18:22 srv-web apache_error : (59.72 MB/s) - **`zap2.c' saved** [1995/1995]\n
Message: Dec 4 17:18:22 srv-web apache_error : (6.15 MB/s) - **`hihi' saved** [73716/73716]\n
Message: Dec 4 17:18:22 srv-web apache_error : **Connecting to packetstormsecurity.org:80**... ready.\n

DAEMON.ERR: Dec 4 17:18:40 srv-web mysqld[2283]: InnoDB: Started; log sequence number 0 43655\n
DAEMON.ERR: Dec 4 17:18:41 srv-web mysqld[2283]: [Note] /usr/sbin/mysqld: ready for connections.\n
DAEMON.ERR: Dec 4 17:18:41 srv-web mysqld[2283]: socket: '/var/run/mysqld/mysqld.sock' port: 3306\n
DAEMON.INFO: Dec 4 17:18:45 srv-web /etc/mysql/debian-start[2348]: Checking for crashed MySQL tables.\n
MAIL.INFO: Dec 4 17:18:46 srv-web spamd[2345]: logger: removing stderr method\n

**17h19** Côté défense, de nombreux accès aux dossiers /proc, /dev, /etc, /usr, /var ont été refusés ainsi que des tentatives de zip:

Message: apache_error : tar: /etc/lvm/backup: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/mysql/debian.cnf: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/passwd-: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/shadow: Cannot open: Permission denied\
Message: apache_error : tar: /etc/squid/squid.conf: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/ssh/ssh_host_dsa_key: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/ssh/ssh_host_rsa_key: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/ssl/private: Cannot open: Permission denied\n

**17h20** L'équipe Attaque continue d'exploiter le serveur mail de la défense. En utilisant une session www-data, ils arrivent à créer des nouveaux mails dans la file d'attente de postfix:

| | | |
|---|---|---|
| *attack@attack.attack* | *pouet@pouet.piouff* | *hihi@hoho.haha* |
| *py@gnole.com* | *daweed@gmail.com* | *jeremy.py@gmail.com* |
| *aziz@wanadoo.fr* | *galy@stri.net* | *aoun@irit.fr* |
| *torguet@irit.fr* | *desprats@cict.fr* | *...* |

Le tout imbriqué dans une boucle !!

**17h23** Les attaquants lancent un puissant flood SSH et HTTP sur la sonde, et provoque un Déni de Service meurtrier.

*Tshark a montré que les attaquants ont floodé la sonde avec les bits RST et ACK à 1.*

*Les attaquants semblent avoir eu accès à la sonde vu qu'ils ont réussi à inhiber le firewall interne mis en place.*

*Par mesure de sécurité, tous les mots de passe de la sonde sont modifiés et un rechargement du script iptables permet de retrouver un état opérationnel.*

*La configuration d'Apache est modifiée à travers la régression des capacités limites de traitement des instances.*

**17h40** Les attaquants demandent à l'équipe défense de connecter un poste client à l'adresse publique de leur serveur: *http://192.168.0.20/*

*Le navigateur utilisé pour cette manipulation a planté et on a découvert l'exécution du processus ''dumprep.exe'' qui a pour but de tracer les erreurs logicielles au format texte.*

*Malheureusement, aucune détection de spyware n'a été confirmée...*

**18h00** L'attaque est officiellement terminée.

- **Résultats de l'analyse de log**

Les firewalls configurés ont permis de bien protéger l'architecture existante. Sans la présence du keylogger, les attaquants auraient eu beaucoup plus de mal à pénétrer le réseau interne.

La centralisation des logs vers la sonde a été beaucoup plus importante que la première confrontation, qui a d'ailleurs grandement facilité les recoupements d'informations lors de la rédaction du rapport d'audit (même si la lecture du GigaOctet de logs a été éprouvante...).

Les envois bufferisés de logs ont surtout permis d'avoir des feedbacks et donc de revenir sur des points antérieurs d'activité réseau de façon plus précise.

La sonde d'audit a été fortement dévastée. La compromission du SGBD a empêché l'outil SNORT de remonter les intrusions, la présence du keylogger a divulgué bon nombre d'informations confidentielles avant de permettre aux attaquants de provoquer notamment la désactivation du firewall interne, le déni de service complet et le crash du serveur SQL.

Le serveur défense a été le plus éprouvé dans l'histoire même s'il a bien tenu le choc. Le remplissage de la base MYSQL et l'écriture continue des logs système ont saturé l'espace disque et bon fonctionnement de la machine.

Aucun diagnostic n'a pu être fait en profondeur par manque de temps et de ressources consacrés à ce projet.

- **Implémentation de nouveaux outils :**

De façon optimale, s'il y avait eu une autre confrontation, nous pourrions prévoir un meilleur blindage des outils de monitoring pour éviter les requêtes provenant de l'extérieur. Et surtout une vérification systématique de l'intégrité des machines utilisées...

# IV. Bilan

## a. Bilan de l'action auprès de la Défense

Les rapports avec l'équipe Défense ont été très bon. Il convient néanmoins de relever une petite friction qui s'est produite pendant la première analyse des logs où les bonnes adresses IP avait été transmise un peu tard par l'équipe Défense.

Nous avons nous même eu du retard dans la livraison du rapport d'analyse des logs pour la deuxième confrontation.

Bref, chaque partie a apprécié la qualité du travaille fournit par l'autre équipe.

## b. Bilan de notre organisation

Plutôt que de finir par un bilan global, il était plus intéressant de laisser la parole à chaque pôle pour que chacun puisse pouvoir s'exprimer.

- **Management**

« En ce qui me concerne, le projet a été une expérience enrichissante, notamment en gestion des ressources humaines. J'ai pu voir qu'il était parfois laborieux de gérer un groupe de six personnes. Il a fallut faire en fonction des qualités et de l'investissement de chacun.

Je me suis beaucoup appuyé sur un pôle technique performant et compétent qui représentait la clef de voûte du projet.

Il est aussi intéressant de remarquer que, sans aucune indication préalable, tout le monde s'est placé dans un cadre professionnel en s'envoyant des e-mails toujours très formels. C'est peut être aussi pour ça que le partenariat avec l'équipe Défense a si bien fonctionné. »

- **Pôle Commercial et Juridique**

« Ce projet, de manière général, donne je pense, une bonne idée de ce que peut être la vie en entreprise et la réalisation de projet complexe au sein d'une organisation avec une hiérarchie.

L'organisation du travail s'est avérée très efficace en début de projet en raison de pas mal de temps libre de chacun des membres ; que ce soit le contrat, le cahier des charges, la méthode MEHARI ou la mise en place de la sonde, toutes ces

opérations ont été réalisées sans problème vis-à-vis des délais que nous nous étions fixées.

Cependant, on a vite remarqué qu'avec une équipe déjà supérieure à trois membres, nous étions beaucoup dépendants des à côté de chacun d'entre nous.

Les contraintes temporelles ont à quelques moments été dépassées mais le résultat du travail est tout de même resté de bonne qualité.

La grosse difficulté de ce projet a été ce respect des délais que nous nous étions fixé et sans relance de notre manager, il y aurait eu des répercussions de la qualité du travail fourni. »

- **Pôle Technique**

« J'ai apprécié le contexte général du projet. Cette mise en situation concrète a été tellement rare que je me suis donné à fond afin de me réconcilier avec Linux et mettre à profit tous mes acquis des cours de Mr Latu.

Mon affectation à la direction technique m'a garanti d'avoir une vision globale sur le projet avec un interfaçage direct avec le chef de projet, mais aussi de me rendre compte de l'importance des choix d'orientation technique pour notre machine.

Au début, il a été difficile de devenir opérationnel mais au fur et à mesure que le projet avançait, nous prenions à force de nuits blanches, une longueur d'avance afin d'anticiper et d'avoir une démarche de sécurité offensive.

Les interactions avec l'équipe Défense a été efficace coté technique. Leur directeur technique a été conciliant et très disponible (seul).

La grève nous a mis au chômage technique mais bon, vu le travail à gérer en parallèle, les ressources consacrées n'aurait peut être pas été suffisantes... »

- **Pôle Aspect rédactionnel et pluri compétence**

« J'ai pour ma part pris goût à ce projet, mon poste était particulièrement intéressant car pluri disciplinaire. J'ai en effet participé aux étapes de discutions avec l'équipe défense, aux aspects rédactionnels, mais aussi à l'analyse, beaucoup plus technique, des logs remontés de la sonde pendant les phases de confrontation.

L'aspect relationnel avec l'équipe défense ma conforté dans l'idée que la communication peut être un point délicat qui peut entrer des erreurs d'interprétation. Notamment si les documents, tel que les cahiers des charges par exemple, ne possèdent pas de numéro de version. Difficile de s'y retrouver par la suite ! »

**NOTES**

# V. Annexes

# Annexe 1 : Contrat d'audit

# Contrat d'audit informatique

La collaboration entre les équipes « défense » et « analyse » doit faire l'œuvre d'un contrat permettant de fixer les limites d'actions auprès de Candide S.A. Ce contrat aura pour but d'assurer le bon déroulement de la mission d'audit de sécurité, à savoir la validation des moyens de protections mis en œuvre sur les plans organisationnels, procéduraux et techniques, au regard de la politique de sécurité rédigé par les soins de la défense.

Nous avons donc convenu après négociation avec la défense, des clauses suivantes :

Article1 - Informations sur le Réseau :

L'audité, ayant confié à l'équipe d'analyse le soin d'assurer un audit complet des systèmes d'information de Candide S.A, s'engage à fournir le recensement détaillé de l'ensemble des éléments qui constituent ce système. L'auditeur pourra réaliser l'état des lieux et des objectifs de sécurité, à savoir :

- Réglementation interne, procédures, organigramme du personnel, charte d'utilisation des ressources.
- Sécurité physique : Normes de sécurité, protection des accès (équipements, infrastructure câblée, etc.), redondance physique, plan de maintenance.
- Exploitation et administration : sauvegarde et archivage des données, continuité de service, journalisation.
- Réseaux et télécoms : architecture réseau (topologie, plan d'adressage), matériels (modems, routeurs, commutateurs, pare-feux), contrôle des accès logiques.
- Systèmes : poste de travail (gestion des droits), serveurs et les services qu'ils délivrent, applications, solutions antivirales.

Article2 - Périmètre d'actions de l'audit :

Ayant connaissance des éléments composant le système d'information, l'auditeur pourra définir le périmètre de l'audit et planifier ses interventions et ses entretiens avec les personnes à interviewer au sein de la défense. L'équipe d'analyse sera responsable de l'organisation des réunions avec l'équipe auditée et devra, à l'issue de celles-ci, proposer des recommandations pour la mise en place de mesures organisationnelles et techniques.

Article3 - Mise en place des outils de supervision:

L'audité conviendra avec l'auditeur d'un droit accès physique au système pour la mise en place d'outils d'analyse et de détection (analyse des logs, scans, sondes). Sur autorisation explicite de la défense, l'auditeur pourra effectuer des tests d'intrusions selon des scénarios potentiels d'attaque, afin de déterminer les vulnérabilités et les failles de sécurité.

Article4 - Compte-rendu :

Chaque phase d'analyse et d'évaluation réalisée par les soins de l'équipe d'analyse devra faire l'œuvre d'un rapport complet présentant de manière explicite les vulnérabilités détectées sur le système audité, et proposant des améliorations techniques et organisationnelles pouvant entraîner une revue de la politique de sécurité.

A son tour la défense devra informer l'auditeur de toute modification ou évolution de son système de sécurité.

Article5 - Confidentialité :

L'organisme d'audit, à savoir l'ensemble des personnes qui interviendra pour la mission d'audit de sécurité, s'engage, sous sa responsabilité exclusive, à considérer confidentielles toutes informations transmises par la défense, de façon orale ou écrite, et par conséquent à ne pas les divulguer à un tiers. Une clause de confidentialité sera établie à l'initiative de la défense et devra faire l'objet d'une signature par l'ensemble des membres composant l'équipe d'analyse.

L'organisme d'audit est entièrement responsable de la sécurisation de la sonde et de l'accès au réseau de la défense par celle-ci ou par éventuelle adresse IP donnée pour cette même sonde.

De la même manière, les différents droits octroyés à l'organisme d'audit sont sous leur entière responsabilité.

En cas de violation volontaire ou négligente de cette clause, la ou les personnes responsables devront répondre de sanctions négociées au préalable avec la défense.

Article6 - Cadre juridique :

L'organisme audité doit être conscient de la législation concernant les systèmes d'informations. Les responsables de sécurité ont une obligation de moyens pour que leur système de sécurité rentre en conformité juridique. Ils doivent être vigilants au respect de la protection des données privées des employés. L'organisme responsable doit également sensibiliser ses employés sur le cadre d'utilisation d'internet. Un usage abusif sortant du cadre professionnel pouvant induire des problèmes de sécurité et mettre en cause la responsabilité civile ou pénale de l'entreprise et de l'employé.

A cet effet une charte d'utilisation de l'informatique et des télécommunications devra être établie à l'initiative de la défense.

Article7 - Financier :

Par ce contrat la défense s'engage à prendre en charge la totalité des frais matériels indispensables à la mise en place d'une supervision efficace. Une fois l'installation effectuée, une rémunération mensuelle sera versée à l'organisme d'audit pour le travail fourni. Une déduction sur cette rémunération pourra être effectuée en cas de responsabilité de l'organisme d'audit dans un quelconque déni de service portant atteinte aux activités de l'entreprise Défense.

Au terme des actions entreprises par l'équipe d'attaque durant le temps imparti aux trois séances de TP, et après établissement du rapport d'analyse, un bilan organisationnel et technique de la mission accomplie par les deux équipes en collaboration permettra d'évaluer la part de responsabilité de la défense et de l'audit.

**L'équipe ayant le plus failli à sa mission aura l'honneur d'inviter l'autre équipe au restaurant de son choix.**

Article8 - Modification de Contrat :

Pour des éventuelles modifications de contrat des Avenants seront produits et devront être obligatoirement signés par les deux partis que ce soit pour une modification mineure ou majeure afin que tout compromis soit évité.

Article9 - Intégrité physique :

L'audit se dégage de toute responsabilité dans l'éventualité d'une attaque de niveau physique, le matériel étant hébergé dans les locaux clients ; La défense prendra donc en charge l'intégrité physique du matériel de supervision.

Article 10 - Facilité de supervision :

Lors d'une connexion à distance par le VPN mis à disposition à l'équipe défense, une signalisation de cet accès doit être effectuée à M David NEMBROT par mail, afin que la lecture des logs en soit facilitée.

Signatures des deux parties (précédées de la date et de la mention « lu et approuvé ») :

| | |
|---|---|
| Pour le groupe Défense, | Pour le groupe Analyse, |
| M. David BOSCARI | M. David GERBAULET |
| Le ..... | Le |

# Annexe 2 : cahier des charges 1iere et 2ieme confrontation

# Annexe 3 : Application de la méthode MEHARI