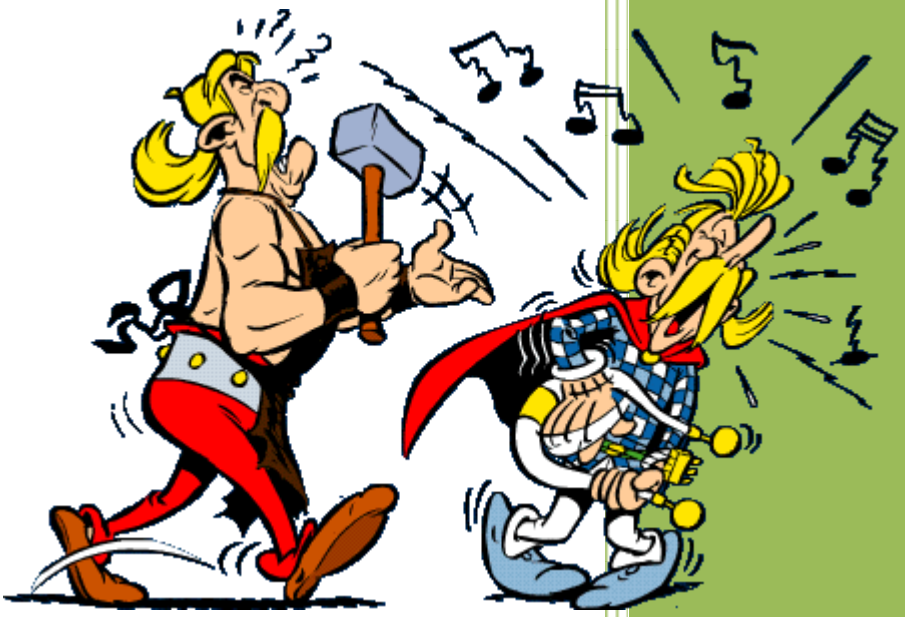
STRI
| Télécoms & Réseaux |

Rapport du projet de sécurité



Lise BANQUET
Kenza BENGELLOUN
Goulven BUREL
Alexandre CLAMART
Tristan DELGRANGE
Christophe DUBOS
Romain LAVERNHE
Alexandre LACOURTE
Pierre-Michel LEBOULC'H
Nyaka LELO
Gwendal RAISON
Bastien TEIL
Maxime VIAUD
Médéric VIGROUX

Société Assurancetourix

13/12/2010

Tables des matières

Introduction

Fidèle aux années précédentes, les étudiants de master 2 STRI sont soumis à une « paranoïa soudaine » durant quelques semaines. En effet, afin d'illustrer nos connaissances en sécurité informatiques acquises durant les cours nous avons pris part au projet de sécurité mené par Mr LATU.

Notre promotion est alors divisée en trois groupes de projets afin d'offrir trois approches des sécurités des systèmes d'informations :

- Le groupe Défense ➔ le but est de mettre en place un système d'information que l'on peut retrouver dans une entreprise et offrir le maximum de sécurité et de protection pour ses services et données.

- Le groupe Attaque ➔ l'objectif est de mettre à mal l'infrastructure du système d'information du groupe défense

- Le groupe Audit ➔ ce dernier groupe doit travailler en étroites collaboration avec le groupe de défense afin de lui offrir un grand nombre de service leurs permettant d'assurer la sécurité des systèmes d'informations.

A travers ce document, nous vous expliquerons notre organisation au sein de notre société d'audit **AssuranceTourix** ainsi que les différents outils mis en place afin de superviser détecter les intrusions éventuelles sur le réseau de la société AeroDef.

I. La société d'audit Assurancetourix

1. Présentation d'Assurancetourix

Assurancetourix est une jeune entreprise d'audit en réseau et télécom. Elle emploie 14 personnes dans la région Toulousaine.

Assurancetourix annonce la réussite à la certification ISO 27001:2005 pour ses prestations d'audits de sécurité des systèmes d'information.

RAISON SOCIALE	Assurancetourix France
STATUT	SAS au capital de 1 €
SIEGE SOCIAL	Université Paul Sabatier, Bât U3, IUP STRI, 118 Route de Narbonne 31062 Toulouse Cedex 9
EFFECTIF	14 personnes
HISTORIQUE	Septembre 2010 : création d'Assurancetourix en France

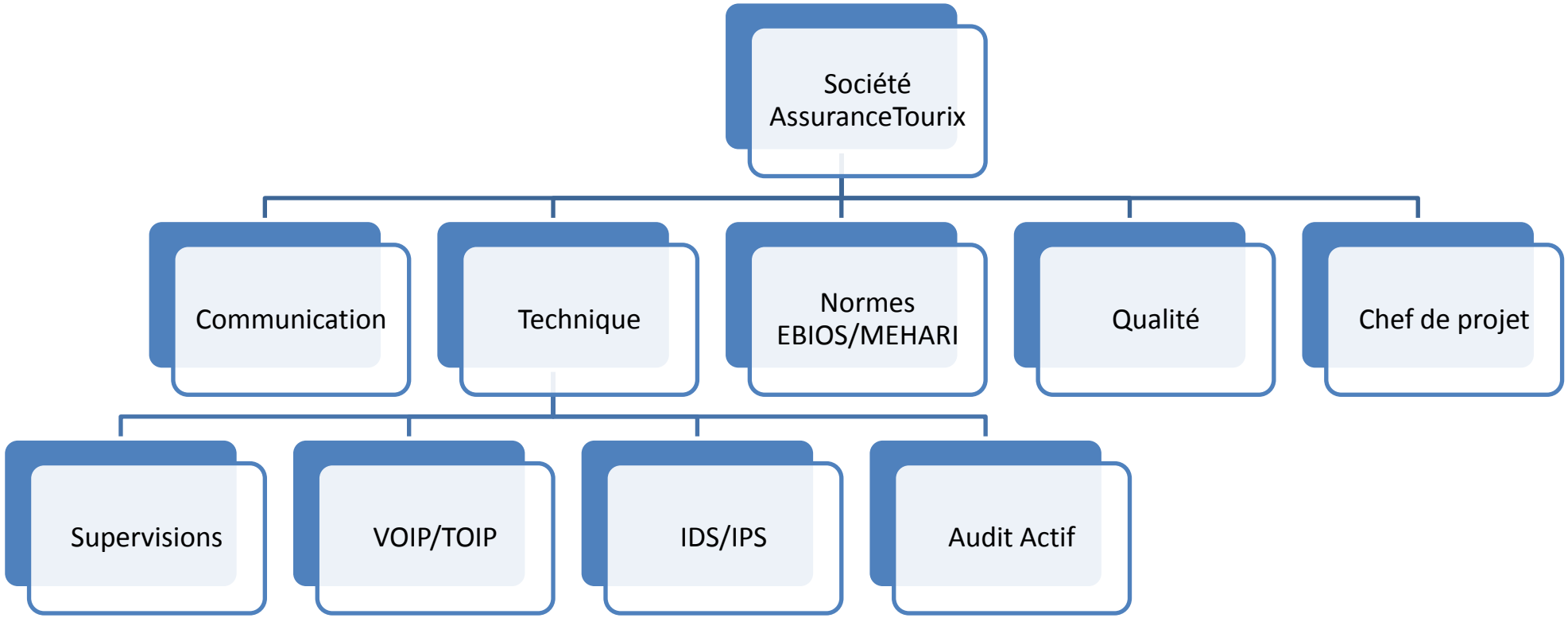
Concrètement, pour une société d'audit comme Assurancetourix, cela signifie que la manipulation des données relatives aux audits de sécurité chez ses clients s'effectue avec le niveau de protection requis, ces données étant effectivement sensibles.

La certification ISO 27001 garantit qu'elle met en œuvre un système de management et des mesures de sécurité organisationnelles et techniques. Cela signifie qu'un cercle vertueux a été enclenché pour une amélioration continue.
En septembre 2010, l'offre audit d'Assurancetourix a été auditée et certifiée ISO 27001 par l'organisme LSTI1, accrédité par le COFRAC2.

2. Organisation de la société

Notre organisation au sein de l'entreprise nous permettant d'avoir un poste technique mais également un poste plus bureaucratique. Chaque personne occupait donc 2 rôles.

Nous avons plusieurs pôles d'expertise :


Société AssuranceTourix
Communication
Technique
Normes EBIOS/MEHARI
Qualité
Chef de projet
Supervisions
VOIP/TOIP
IDS/IPS
Audit Actif

a. Communication

Le but de cette entité consiste à la relation avec notre client et la communication au sein d'AssuranceTourix.

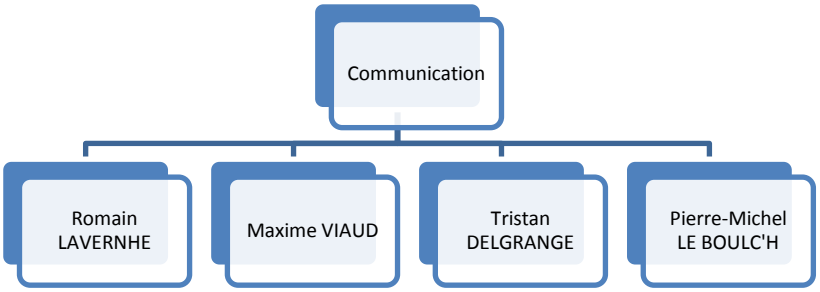


Figure 1 - Organisation du groupe communication

b. Administration, organisation et qualité

Les objectifs de ce groupe est de valider et de s'assurer que les documents émis par la société que ce soit pour notre client ou en interne soit conforme et correct aux différentes règles appliqué dans la diffusion de l'information au sein de la société.

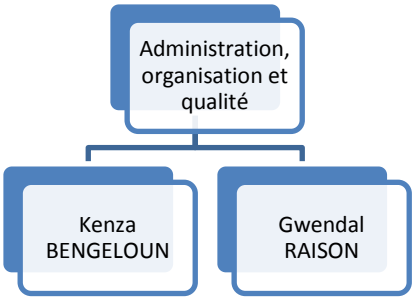


Figure 2 - Organisation du groupe d'administration, organisation et qualité

c. Norme EBIOS/Mehari

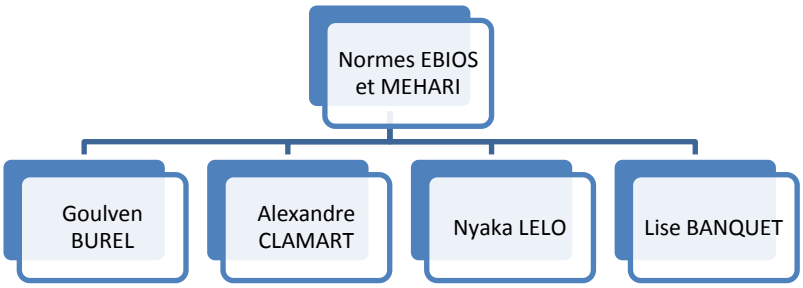


Figure 3 - Organisation du groupe EBIOS et MEHARI

d. Supervision

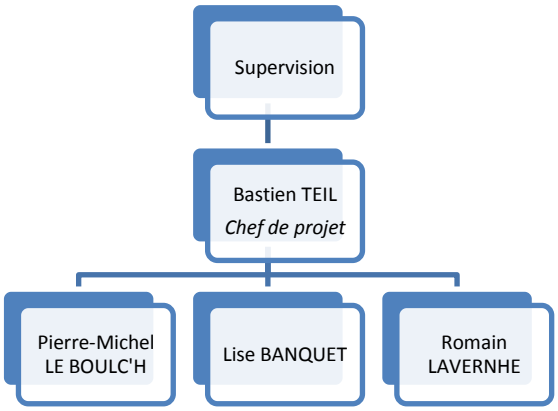


Figure 4 - Organisation du groupe supervision

e. VOIP/TOIP

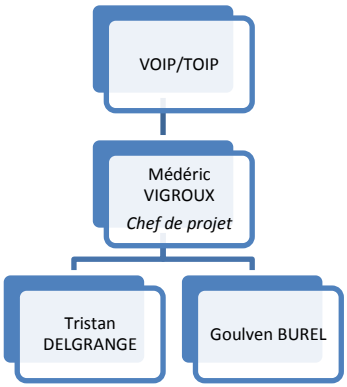


Figure 5 - Organisation du groupe VOIP/TOIP

f. Audit Actif

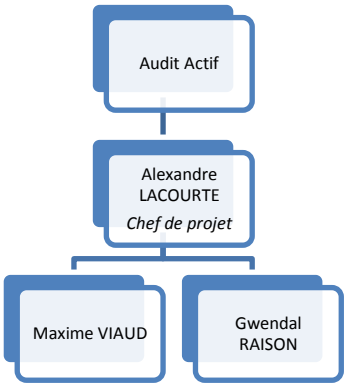


Figure 6 - Organisation du groupe d'audit actif

II. Contexte du projet

1. Processus « Appel d'offre – RAO – contrat »

Nous allons voir dans cette partie le processus de création des contrats nous liant avec la société Aérodef. En effet, cette entreprise avait émis deux appels d'offres. Un concernant la supervision de leur système d'information et un autre pour la VoIP – ToIP.

Pour les mettre en place, nous avons étudié ces appels d'offres et rédigé une réponse à appel d'offre (RAO) pour la supervision et une pour la VoIP - ToIP. Ces réponses décrivaient l'ensemble des services que nous pouvions fournir au client.

Voici la structure de la RAO de supervision :

I. Présentation d'Assurancetourix :
- *A. Assurancetourix*
- *B. La mission*
- *C. Les qualifications et certifications*
- *D. La répartition des services*
- *E. La fiche d'identité*

II. Le projet d'audit actif :
- *A. Introduction du projet d'audit actif*
- *B. Outils mis en place*
  1. *Nessus*
  2. *Netflow - Métrologie*
  3. *Gestion des logs*
  4. *Analyse complémentaire*
- *C. Coûts et investissements*

III. Le projet supervision :
- *A. Introduction du projet supervision*
- *B. Choix techniques*
- *C. Fonctions*
- *D. Intégration à l'architecture du client*
- *E. Estimation des coûts*
- *F. Déroulement et mise en place*
- *G. Recommandations et remarques*

IV. Le projet IDS/IPS :
- *A. Introduction du projet IDS/IPS*
- *B. Projet*
- *C. Coûts et investissements*

Annexe

Vous trouverez la RAO de supervision en annexe 1.
Et celle de la VoIP – ToIP :

I. Présentation d'Assurancetourix :
- *A. Assurancetourix*
- *B. La mission*
- *C. Les qualifications et certifications*
- *D. La répartition des services*
- *E. La fiche d'identité*

II. Présentation du projet Toip/Voip :
- *A. Choix techniques*
- *B. Intégration à l'architecture du client*
- *C. Estimation des coûts*
- *D. Déroulement et mise en place*
- *E. Recommandations et remarques*

Annexe

Vous trouverez la RAO de VoIP - ToIP en annexe 2.

La société Aérodef nous avait donné deux dates différentes concernant les RAO. Une première pour la supervision (07/10/2010) et une deuxième pour la VoIP – ToIP (20/10/2010).

Une fois la RAO supervision émise, nous pensions que l'entreprise Aérodef l'aurait tout simplement consulté et annoté les points sur lesquels ils étaient d'accord et ceux où ils ne l'étaient pas. Mais ils ont préféré rédiger un contrat synthétisant cette RAO.

Nous avons donc été surpris de cette décision puisque le contrat de supervision ne contenait que les grandes actions que nous étions censés mettre en place. Nous leur avons donc fait part de notre volonté de mettre en annexe du contrat cette RAO.

Comme ils n'étaient pas d'accord avec tous les points décrits, nous l'avons modifié jusqu'à ce qu'ils l'approuvent et qu'ils acceptent de la mettre en annexe. Cela était aussi valable pour la RAO de VoIP – ToIP.

Voici comment se compose le contrat de supervision établit entre nos deux sociétés :

Article 1 – Partage des informations
Article 2 – Clause de confidentialité
Article 3 – Moyens mis à disposition au Prestataire pour la supervision et utilisation de ces moyens
Article 5 – Frais
Article 6 – Communication
Article 7 – Modification du contrat

Vous trouverez le contrat complet de supervision en annexe 3.

Voici la composition du contrat de VoIP – ToIP :

Article 1 – Partage des informations :
Article 2 – Clause de confidentialité :

Article 3 – Moyens mis à disposition au Prestataire pour le projet ToIP/VoIP
Article 5 – Frais
Article 6 – Communication
Article 7 – Modification du contrat

Vous trouverez le contrat complet de VoIP-ToIP en annexe 4.

Après avoir vu la partie présentant la mise en place des contrats entre la société Assurancetourix, nous allons nous intéresser aux outils de communication et de sécurisation mis en place.

2. Nos objectifs

Aujourd'hui, le réseau est au cœur du système d'information des entreprises et constitue un de ses éléments les plus sensibles. C'est sur la fiabilité et les performances de son infrastructure de réseaux que repose l'ensemble des échanges internes et externes de l'entreprise, ainsi que le bon fonctionnement de ses applications métier. Dans le même temps, le développement des réseaux et de l'utilisation d'Internet s'accompagnent d'un besoin croissant de la part des entreprises en outils pour optimiser et sécuriser ces réseaux. Assurancetourix répond à l'ensemble de ces demandes et fournit à ses clients, un service de haut niveau, grâce à une connaissance pointue de leurs besoins et une approche adaptée à chacun d'eux.

Nos objectifs internes étaient au début du projet les suivants avant la signature du contrat et l'appel d'offre :

Sous-groupe VOIP :

Déploiement d'Asterisk ainsi que 2 soft phones XLITE. ⌊ court terme

Possibilité de réaliser des communications en externe (accès internet) ⌊ long terme

Audit sur les éventuelles attaques ⌊ long terme

Sous-groupe IDS:

Déploiement de l'outil PRELUD (surcouche de SNORT) ⌊ court terme

Migration et centralisation vers OSIM ⌊ long terme

Sous-groupe Audit Actif :

Déploiement de Nessus ⌊ court terme

Simulation des flux malveillants pour détéction\ court terme

Utilisation de TOOL KIT \ long terme

Audit de machines et d'équipements réseaux (en négociation)\ long terme

Migration et centralisation vers OSIM \ long terme

Sous-groupe Supervision :

Déploiement de l'outil de supervision FAN \ court terme

Remonter d'alertes pertinentes et intégration dans le SI d'Aerodef (email, téléphone,…)\ long terme

Migration et centralisation vers OSIM \ long terme

Pour la majorité des groupes, le travail effectué durant le projet ne correspond en rien à celui fixé dans nos objectifs. Cette évolution est due à la difficulté de rendre opérationnel certains outils ou que la société AeroDef ne souhaitait pas que cela se fassent en particulier pour le groupe audit actifs. De ce fait, ce groupe a pris en charge la gestion complète du serveur de l'audit mais également certains outils d'analyse qui nous détaillerons par la suite.

3. Architecture de la société AeroDef

Voici l'architecture de la société AeroDef qui nous a été fourni. Il a pourtant été spécifié a de nombreuses reprises qui nous fallait plus ample détails mais aucune suite n'a été donnée. Nous avions l'impression d'évoluer dans un environnement réseau que nous ne métrisions pas !

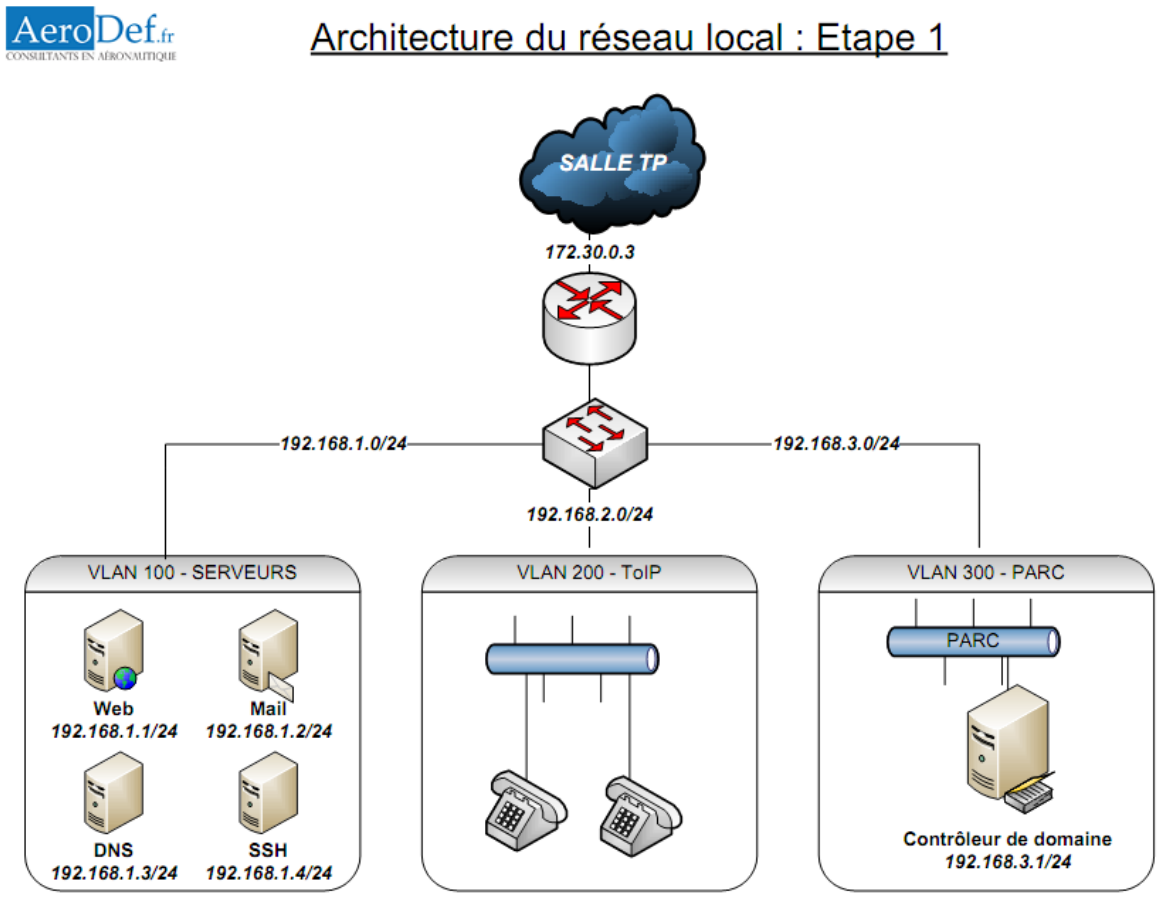


Figure 7 - Architecture de la société interne

4. MEHARI

MEHARI est la *Méthode Harmonisée d'Analyse des Risques*. Elle a été développée et proposée par le CLUSIF (Club de la Sécurité de l'Information Français). C'est une méthode complète d'évaluation et de management des risques liés à l'information, ses traitements et les ressources mise en œuvre.

L'utilisation de la méthode est gratuite et sa distribution est réalisée selon les dispositions du logiciel libre (Open Source). La dernière version de MEHARI a été présentée par le CLUSIF le 28 Janvier 2010.

a. Présentation de MEHARI

Objectifs

L'objectif premier de MEHARI est de fournir une méthode d'analyse et de gestion des risques et, plus particulièrement pour le domaine de la sécurité de l'information, une méthode conforme aux exigences de la norme ISO/IEC 27005 :2008, avec l'ensemble des outils et moyens requis pour sa mise en œuvre.

A cet objectif premier s'ajoutent deux objectifs complémentaires :

- Permettre une analyse directe et individualisée de situations de risques décrites par des scénarios de risques
- Fournir une gamme complète d'outils adaptée à la gestion à court, moyen et long terme, de la sécurité, quelle que soit la maturité de l'organisme en matière de sécurité et quelques soient les types d'actions envisagés.

Compte tenu de ces objectifs, MEHARI propose un ensemble méthodologique cohérent, faisant appel à des bases de connaissances adaptées, et capable d'accompagner les responsables d'entreprise ou d'organisme et les responsables de la sécurité dans leurs différentes démarches et actions de gestion des risques.

Concepts

MEHARI se décompose en cellules, les 8 types de cellules sont :

- L'entité
- Le site
- Les locaux
- Les applicatifs
- Les services offerts par les systèmes et l'infrastructure
- Le développement
- La production informatique
- Les réseaux et les télécoms.

MEHARI propose des modules d'analyse pour chacune de ces cellules. Les modules de MEHARI peuvent être combinés, en fonction de choix d'orientation ou de politiques d'entreprise, pour bâtir des plans d'action ou, tout simplement, pour aider la prise de décision concernant la sécurité de l'information.

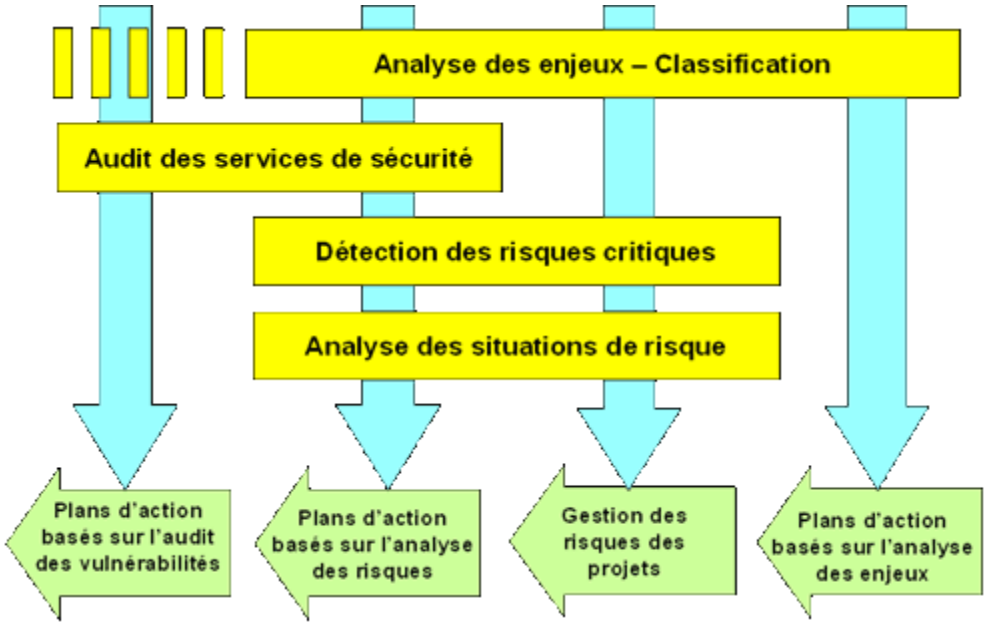


Figure 8 - Concepts MEHARI

Analyse des enjeux

Dans MEHARI, on appelle "Analyse des enjeux de la sécurité" :

- L'identification des dysfonctionnements potentiels pouvant être causés ou favorisés par un défaut de sécurité,
- L'évaluation de la gravité de ces dysfonctionnements.

Il s'agit d'une analyse totalement focalisée sur les objectifs et attentes des "métiers" de l'entreprise, et, de ce fait pérenne. Elle met à contribution les décideurs et le haut management de l'entreprise ou de l'entité dans laquelle elle est menée.

Cette analyse se traduit par :

- Une échelle de valeurs des dysfonctionnements potentiels, document de référence centré sur les impacts " business ",
- Une classification formelle des informations et ressources du système d'information.

Il ne s'agit en aucun cas d'un audit des dysfonctionnements réels qui pourraient être constatés, mais d'une réflexion sur les risques majeurs auxquels l'entité est exposée et sur le niveau de gravité de leurs conséquences éventuelles.

Cette analyse des enjeux vise, le plus souvent, à :

- Etre sélectif dans les moyens à mettre en œuvre pour la sécurité de l'information et ne pas engager de dépenses là où les enjeux sont faibles,
- Éviter des contraintes inutiles aux utilisateurs,

- Définir les priorités,
- Répondre à l'inévitable question d'un décideur en face d'un budget de sécurité : " est-ce bien nécessaire ? ".

Dans cette analyse, MEHARI apporte :

- Une démarche centrée sur les besoins du business et une implication des managers et dirigeants,
- Un guide de mise en œuvre et des livrables types,
- Des liens directs vers l'analyse détaillée des risques correspondants.

Analyse des vulnérabilités

L'analyse des vulnérabilités revient à identifier les faiblesses et les défauts des mesures de sécurité. En pratique, il s'agit d'une évaluation quantitative de la qualité de mesures de sécurité. Les mesures de sécurité évaluées sont, en fait, des services de sécurité, décrits et documentés dans une base de connaissance développée et maintenue par le CLUSIF.

Dans MEHARI, cette analyse couvre :

- L'efficacité des services de sécurité,
- Leur robustesse,
- Leur mise sous contrôle.

Cette analyse des vulnérabilités permet de :

- Corriger les points faibles inacceptables par des plans d'action immédiats.
- Évaluer l'efficacité des mesures mises en place et garantir leur efficience.
- Préparer l'analyse des risques induits par les faiblesses mises en évidence.
- Se comparer à l'état de l'art ou aux normes en usage.

Analyse des risques

Dans MEHARI, "l'analyse des risques" couvre :

- L'identification des situations susceptibles de remettre en cause un des résultats attendus de l'entreprise ou de l'organisme.
- L'évaluation :
    - de la probabilité de telles situations,
    - de leurs conséquences possibles,
    - de leur caractère acceptable ou non.
- La mise en évidence des mesures susceptibles de ramener chaque risque à un niveau

acceptable.

Cette analyse des risques vise, le plus souvent, à :

- Définir les mesures les mieux adaptées au contexte et aux enjeux.
- Mettre en place un management des risques et garantir que toutes les situations de risques critiques ont été identifiées et prises en compte
- Analyser et gérer les risques d'un nouveau projet.

L'analyse des risques proposée par MEHARI peut être vue comme suit :

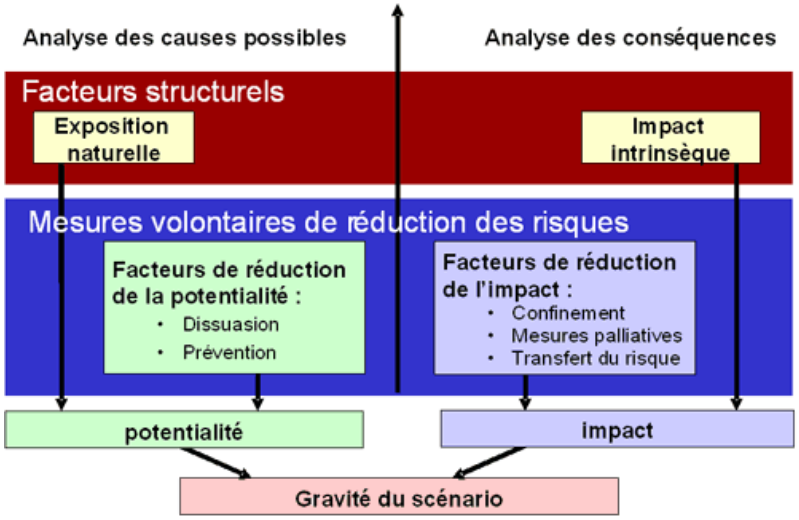


Figure 9 - Analyse des risques dans MEHARI

Pilotage de la sécurité

Le "pilotage de la sécurité" demande :

- Un cadre structurant pour définir les objectifs annuels ou les étapes de plans d'action,
  - Des indicateurs permettant de comparer les résultats obtenus aux objectifs : en termes qualitatifs et quantitatifs ainsi qu'en termes de délais
- Des références externes permettant un "benchmarking" (référenciations, étalonnage)

Dans ce domaine, MEHARI apporte :

- Un cadre adapté à différentes démarches et différentes sortes de management de la sécurité avec une variété d'indicateurs et de synthèses :
  - Niveaux de vulnérabilités et de risques,
  - Centres d'intérêt de sécurité (16 thèmes, dont contrôle d'accès, plan de secours,…), relatifs aux points de contrôles ISO 17799:2005 (repris dans ISO 27001),
  - Tableau de bord des risques critiques.

b. Mise en œuvre

Voici dans un premier temps les différents modules de diagnostics définis par Méhari :

- Module d'analyse de risques
- Module d'analyse des enjeux
- Module de diagnostic de l'état de la sécurité

La méthode d'analyse des situations des risques correspond aux questions suivantes :

- ✓ A quels risques l'organisme est exposé ?
- ✓ Sont-ils acceptables ?

La représentation se fait soit sur documents Excel ou sur le logiciel « *RISICARE* ».

Le diagnostic de sécurité est basé sur un questionnaire qui s'appuie sur les mesures de sécurité et l'évaluation du niveau de qualité des mécanismes et solution mise ne place pour la réduction des risques.

L'analyse des enjeux correspond aux questions suivantes :

- ✓ Que peut-on redouter ?
- ✓ Serait-ce grave si cela devait arriver ?

Les résultats retenus permettront ainsi d'élaborer d'un côté une échelle de valeurs des dysfonctionnements du système d'information d'où leurs descriptions, la définition des paramètres influant sur la gravité des dysfonctionnements et l'évaluation des seuils de criticité qui font varier les niveaux de gravité de ceux-ci.
D'un autre côté, la classification des infos et des actifs du SI basé sur la Disponibilité, l'Intégrité et la Confidentialité des indicateurs représentatifs de la gravité d'une atteinte au SI.

- Traitement des risques

Plan d'action mise en place pour la réduction des risques.

Ce plan d'action consiste en une analyse de chaque scénario de risque et à prendre des décisions conséquentes.
En pratique, l'organisation de ce travail se fait de manière structurée et en envisageant plusieurs approches :

*travail par familles de scénarios ayant le même type d'actif et le même impact : Pour chaque famille de scénarios est proposée des plans d'action (feuille Plan d'action) regroupant différents services pertinents pour la famille.

*travail par projets fédérateurs avec des services de finalités (contrôle d'accès physique, gestion des droits et des habilitations,..) : Ils permettent de faire des simulations à différentes époques et de définir ainsi un tableau de bord des risques.

*travail par services en fonction des notions de besoin de service : Définir un indicateur de besoin de service en fonction du nombre de scénarios faisant appel à un service donné, de la gravité de ces scénarios et de l'efficacité dans les plans d'action de ces services

On répertorie les différentes menaces d'attaques dans un tableau et on cherche des solutions pour nuire à celles-ci.

Tableau des événements : types et exposition naturelle						
Type	*Code type*	*Événement*	*Code*	*Exposition naturelle standard CLUSIF*	*Exposition naturelle décidée*	*Exposition naturelle résultante*
Absence accidentelle de personnel	AB.P	Absence de personnel de partenaire	AB.P.Pap	3		3
		Absence de personnel interne	AB.P.Per	2		2
Absence ou indisponibilité accidentelle de service	AB.S	Absence de service : Énergie	AB.S.Ene	3		3
		Absence de service : Climatisation	AB.S.Cli	2		2
		Absence de service : Impossibilité d'accès aux locaux	AB.S.Loc	2		2
		Absence de maintenance applicative ou maintenance applicative impossible	AB.S.Mas	3		3
		Absence de maintenance système ou maintenance système impossible	AB.S.Mas	2		2
Accident grave d'environnement	AC.E	Foudroiement	AC.E.Fou	2		2
		Incendie	AC.E.Inc	2		2
		Inondation	AC.E.Ino	3		3
Accident matériel	AC.M	Panne d'équipement	AC.M.Equ	3		3
		Panne d'équipement de servitude	AC.M.Ser	3		3
Absence volontaire de personnel	AV.P	Conflit social avec grève	AV.P.Gre	2		2
Erreur de conception	ER.L	Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne)	ER.L.Lin	3		3
Erreur matérielle ou de comportement du personnel	ER.P	Perte ou oubli de document ou de media	ER.P.Peo	3		3
		Erreur de manipulation ou dans le suivi d'une procédure	ER.P.Pro	3		3
		Erreur de saisie ou de frappe	ER.P.Prs	3		3
Incident dû à l'environnement	IC.E	Dégât dû au vieillissement	IC.E.Age	2		2
		Dégât des eaux	IC.E.De	3		3
		Surcharge électrique	IC.E.Se	2		2
		Dégât dû à la pollution	IC.E.Pol	2		2
Incident logique ou fonctionnel	IF.L	Incident d'exploitation	IF.L.Exp	3		3
		Bug bloquant dans un logiciel système ou un progiciel	IF.L.Lsp	2		2
		Saturation bloquante pour cause externe (ver)	IF.L.Ver	3		3
		Virus	IF.L.Vir	4		4
Malveillance menée par voie logique ou fonctionnelle	MA.L	Attaque en blocage de comptes	MA.L.Blo	2		2
		Effacement volontaire ou pollution massive de configurations systèmes	MA.L.Cfg	2		2
		Effacement volontaire direct de supports logiques ou physiques	MA.L.Del	2		2
		Captation électromagnétique	MA.L.Ele	3		3
		Falsification logique (données ou fonctions)	MA.L.Fal	3		3
		Création de faux (messages ou données)	MA.L.Fau	3		3
		Rejeu de transaction	MA.L.Rej	2		2
		Saturation malveillante d'équipements informatiques ou réseaux	MA.L.Sam	3		3
		Destruction logique totale (fichiers et leurs sauvegardes)	MA.L.Tot	2		2
		Détournement logique de fichiers ou données (téléchargement ou copie)	MA.L.Vol	3		3
Malveillance menée par voie physique	MA.P	Manipulation ou falsification matérielle d'équipement	MA.P.Fal	2		2
		Terrorisme	MA.P.Ter	2		2
		Vandalisme	MA.P.Van	2		2
		Vol physique	MA.P.Vol	2		2
Procédures non conformes	PR.N	Procédures inadéquates	PR.N.Apl	2		2
		Procédures inappliquées par manque de moyens	PR.N.Nas	2		2
		Procédures inappliquées par méconnaissance	PR.N.Nam	2		2
		Procédures inappliquées volontairement	PR.N.Nav	2		2

- Guide analyse des enjeux et classification

L'échelle de valeur des dysfonctionnements est le résultat principal de l'analyse des enjeux de la sécurité.

Les mécanismes employés dans l'appréciation et la gestion des risques nécessitent que ces dysfonctionnements soient traduits en termes techniques relatifs à des ressources de toute nature du Système d'information qu'on appelle les « actifs » (Exemple : perte de la confidentialité de telle base des données applicative ou de l'indisponibilité de tel serveur,…)

Ces actifs classifiés doivent se référer aux besoins des organisations que l'on classe dans trois catégories :

*les services (informatiques, télécommunications et généraux),

*les données nécessaires au fonctionnement des services,

*les processus de gestion de la sécurité ou de la conformité des référentiels

Ainsi on sera amené au remplissage des tableaux ci-dessous l'un des services et l'autre des données :

Tableau T1	CLASSIFICATION DES DONNÉES																																		
Processus métier, domaine applicatif ou domaine d'activité Services communs à particulariser	Données applicativ. (bases de données)			Données applicati. boîtes aux lettres, Messages			Fichiers bureaut. Partagés			Fichiers bureaut. Personnels			Docum. Person.		Lotus notes imprim.	Courrier électronique			Courrier postal / fax			Archives docum.		Archives informat.			Données publiées (web ou intrane)					
	D	I	C	D	I	C	D	I	C	D	I	C	D	C	C	D	I	C	D	I	C	D	C	D	I	C	D	I	C	D	I	C
Nom de colonne pour formules Classif	D01	I01	C01	D02	I02	C02	D03	I03	C03	D04	I04	C04	D05	C05	D06	D07	I07	C07	D08	I08	C08	D09	C09	D10	I10	C10	D11	I11	C11						
Processus métiers																																			
Domaine 1 : Ressources Humaines	2	3	2	2	3	2	1	1	3	1	1	3	2	1	2	1	1	2	1	1	2	2	1	1	1	3	1	1	2						
Domaine 2 : Gestion commerciale	2	2	4	2	2	4	1	3	3	1	3	3	1	3		3	2	4	3	2	4	1	3	1	3	3	3	2	4						
Domaine 3 : Plan stratégique							2	2	3	2	2	3	1	3	3	2	3	3	2	3	3	1	3	2	2	3	2	3	3						
Domaine 4 : Domaine financier et comptable	2	2	3	2	2	3				2	2	3	3	2								3													
Domaine 5	2	3	1	2	3	1	2	3	1	2	3	1												2	3	1									
Domaine 6 : CAO	3	3	3	3	3	3	3	3	3	3	3	3												3	3	3									
Domaine 7 : Site Webcommercial	3	3	1	3	3	1	1	1	1	1	1	1												1	1	1									
../...																																			
Domaine N	2	2	1	2	2	1	2	2	1	2	2	1					1			1				2	2	1			1						
Processus transverses																																			
Administration/ politique d'ensemble			3	3												2			2															
Classification	3	3	4	3	3	4	3	3	3	3	3	3	3	3	3	3	3	4	3	3	4	3	3	3	3	3	3	3	4						

Tableau T1 Classification des actifs

Tableau T2	CLASSIFICATION DES SERVICES																							
Processus métier , application ou domaine applicatif Services communs	Services du réseau étendu		Services du réseau local		Services applicatifs			Services bureaut. communs		Equipem. mis à la dispos. des utilisateurs		Services systèmes Communs (Systèmes, ports, etc.)		Services de publication sur siteweb		Services généraux environ. de travail		Services télécom	
	D	I	D	I	D	I	C	D	I	D	I	D	I	D	I	D	I	D	I
Nom de colonne pour formules Classif	R01	R01	R02	R02	S01	S01	S01	S02	S02	S03	S03	S04	S04	S05	S05	G01	G01	G02	G02					
Processus métiers																								
Domaine1 : Ressources Humaines	1	1	2	3	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1					
Domaine 2 :Gestion commerciale	2	2	2	2	2	2	4	1	3	1	3	3	2	3	2	3	1	3	2					
Domaine3 : Plan stratégique			2	2				2	2	2	2													
Domaine4 : Domaine financier et comptable	2	2	2	2	2	2	3																	
Domaine 5	2	3	2	3	2	3	1	2	3	2	3													
Domaine6 : CAO	3	3	3	3	3	3	3	3	3	3	3													
Domaine7 : SiteWeb commercial	3	3	3	3	3	3	1	1	1	1	1													
../...																								
Domaine N																								
Processus transverses																								
Administration/ politique d'ensemble			3	3										2										
Classification	3	3	3	3	3	3	4	3	3	3	3	3	2	3	2	3	1	3	2					

Tableau T2 Classification des services mis en œuvre

En bas des tableaux T1 et T2 existe une ligne de politique générale permettant d'indiquer un jugement global, indépendant de divers secteurs d'activité.

- Evaluation de la qualité des services de sécurité
  Les services de sécurité peuvent avoir des niveaux de performances très variés selon les mécanises et les processus employés.

La mesure de cette qualité est facteurs de trois paramètres à savoir : l'efficacité du service, sa robustesse et les moyens de contrôle du maintien dans le temps de caractéristiques précédentes.

Une de ces bases de connaissances de cette qualité consiste en une base d'audit des services de sécurité sous la forme d'un questionnaire et d'un système de pondération des réponses. Ces questions sont axées sur l'efficacité des mesures de sécurité (par exemple : fréquence de sauvegardes, types de contrôle d'accès physique : lecteur de carte, digicode,…) et des questions axées sur la robustesse des mesures de sécurité (par exemple : localisation et protection d'accès au lieu de stockage des sauvegardes, protection du système de détection d'incendie,…) et, généralement, une ou deux questions sur le contrôle ou l'audit des fonctionnalités attendues du service.

*Types de questionnaires

Il s'agit des questionnaires spécialisés par domaines techniques correspondants à des interlocuteurs différents

*Système de pondération des questions

Les questions à se poser au sujet d'un service de sécurité sont relatives à des mesures liées au service. On distingue les mesures majeures ou suffisantes et les mesures indispensables. Le tableau ci-dessous est réservé pour la réponse aux questions (1 pour OUI et 0 pour NON) avant la colonne indiquant le poids de chaque question

Questionnaire d'audit : Domaine des Systèmes (07)			
Service : A. Contrôle d'accès aux systèmes et applications **Sous-service : A02. Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)**			
N° Question	**Libellé de la question**	**Rép.**	**Poids**
07A02-01	La procédure d'attribution des autorisations d'accès nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ?	0	4
07A02-02	Les autorisations sont-elles attribuées nominativement en fonction du seul profil des utilisateurs ?	1	2
07A02-03	Le processus d'attribution (ou modification ou retrait) effectif d'autorisations à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? *Un contrôle strict requiert une identification formelle du demandeur (reconnaissance de sa signature, signature électronique, etc.), que la matérialisation des profils attribués aux utilisateurs (par exemple sous forme de tables) soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.*	1	4
07A02-04	Y a-t-il un processus de remise à jour systématique de la table des autorisations d'accès lors de départs de personnel interne ou externe à l'entreprise ou de changements de fonctions ?	0	2
07A02-05	Y a-t-il un processus strictement contrôlé (voir ci-dessus) permettant de déléguer ses propres autorisations, en tout ou en partie, à une personne de son choix, pour une période déterminée (en cas d'absence) ? *Dans ce cas les autorisations déléguées ne doivent plus être autorisées à la personne qui les a déléguées. Cette dernière doit cependant avoir la possibilité de les reprendre, en annulant ou en suspendant la délégation.*	0	4
07A02-06	Peut-on contrôler à tout moment, pour tous les utilisateurs, les habilitations, autorisations et privilèges en cours ?	1	1
07A02-07	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des profils ou des autorisations attribués aux utilisateurs et des procédures de gestion des profils attribués ?	0	1

Problèmes rencontrés

Après étude du tableau 2010 de Méhari, on se rend rapidement compte qu'il est assez complexe et long à étudier.
En effet, il est composé de 14 questionnaires classés par thème. Les voici :

- Organisation de la sécurité
- Sécurité des sites
- Sécurité des locaux
- Sécurité
- Réseau étendu intersites
- Réseau Local
- Exploitation des réseaux
- Production Informatique
- Sécurité applicative
- Sécurité des projets et développements applicatifs
- Protection des postes de travail utilisateurs
- Exploitation des télécommunications
- Processus de gestion
- Gestion de la sécurité de l'Information

Les 14 questionnaires sont uniquement composés de questions fermées. Il faut répondre seulement par « *Oui* », « *Non* » ou « *Sans réponse* ».
Chaque questionnaire est composé de plus de 100 Questions. Au total, il faut répondre à plus de 2300 questions environ !
Nous avons transmis ce questionnaire à la défense afin qu'ils y répondent.

En effet, on n'était incapable de répondre par nous même aux questionnaires. La défense ne nous a transmis pratiquement aucune information concernant son réseau ainsi que sur sa politique de sécurité. Ils étaient donc très difficile pour nous de répondre à toutes les questions.

Nous avons obtenu une réponse négative de leur part car ils estimaient qu'ils n'avaient pas assez de temps pour répondre à l'ensemble du questionnaire.

Au final, pour réaliser une étude Mehari à l'aide du tableur, il faut consacrer beaucoup de temps à la réponse du questionnaire. La réponse aux différents questionnaires demande un gros investissement en termes de temps mais également en termes d'analyse (Recensement de la sécurité du réseau, état du réseau, emplacement des locaux etc…)

III. Communications au sein d'Assurancetourix

La communication est un élément primordial du projet compte tenu de l'importance des groupes. En effet une mauvaise communication interne et/ou externe peut faire apparaitre des problèmes de tout genre. Il était donc important de gérer au mieux ce processus.

La communication d'Assurancetourix s'articule autour de deux axes : la communication interne et la communication avec ses clients, ici, Aérodef. Dans un premier temps, cette partie va s'attacher à décrire les outils de communication mis à disposition de ses collaborateurs ainsi que les usages souhaités de son système d'information. Dans un second temps, cette partie décrira les moyens et les solutions choisis afin de communiquer avec le client.

1. La communication interne

c. La chartre de l'utilisateur du SI

La charte des utilisateurs est l'un des documents essentiels d'une entreprise. Elle permet de décrire les comportements, les règles ainsi que les recommandations que se doivent de respecter l'ensemble des utilisateurs du système d'information afin de limiter, au maximum, la perte ou le vol d'informations.

Assuranretourix est une entreprise au service de ses clients, lesquels détiennent des informations sensibles et hautement confidentielles. C'est pourquoi, le service communication d'Assurancetourix a édité une charte des utilisateurs, garante du professionnalisme de l'entreprise.

Voici, ci-dessous, un résumé des consignes élémentaires décrites par la charte de l'utilisateur du système d'information :

- Privilégier l'utilisation de votre ordinateur personnel.
- Verrouiller sa session avant de s'éloigner de son ordinateur.
- Construire des mots de passes complexes associant des majuscules/minuscules et des caractères spéciaux.
- Ne jamais écrire son mot de passe.

Cette charte des utilisateurs a été soumise à l'ensemble des utilisateurs du système d'information, lesquels avaient pour obligation de la lire et de signaler leur accord en envoyant un mail au service communication.

L'ensemble des consignes de la charte de l'utilisateur du système d'information est disponible à **l'annexe 5**.

d. La communication par email

La communication entre les collaborateurs d'une entreprise est un point sensible. En effet,

de nombreuses informations plus ou moins confidentielles transitent par l'intermédiaire des mails. Cependant, cet outil bien qu'essentiel pour la communication entre les collaborateurs n'est absolument pas sécurisé.

Vous viendrez-t-il à l'idée d'écrire des informations sensibles sur une carte postale sans enveloppe, c'est-à-dire lisibles de tous les intervenants de la livraison (trieurs de courrier, facteurs…) ? Bien sûr que non ! C'est pourquoi Assurancetourix a décidé de mettre en place une communication par mails signés et chiffrés.

Avant de décrire la mise en place des mails chiffrés au sein d'Assurancetourix, nous avons créé des adresses mails pour tous les collaborateurs. Toutes les adresses ont été créées à l'aide d'un générateur IKEA qui permet de transcrire le prénom d'un collaborateur en celui d'un pseudo-meuble IKEA. A noter que toutes les adresses mails d'Assurancetourix ont été créées chez Gmail.

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

Figure 10 - Adresses mails d'Assurancetourix

Passons maintenant aux outils utilisés par tous les collaborateurs afin de permettre la communication via des mails chiffrés. Une procédure de mise en place des mails chiffrés a été créée, disponible en **annexe 6**, afin d'expliquer à chacun les procédures à suivre.

Nous avons choisi d'utiliser le client Thunderbird comme client de messagerie couplé avec l'extension Enigmail afin de permettre le chiffrement/déchiffrement des mails. Chaque collaborateur a aussi dû utiliser GnuPGP afin de permettre la génération de ses clefs privée et publique. Nous avons, par ailleurs, choisi d'utiliser le protocole POP afin de supprimer les mails sur Gmail, une fois leur transfert effectué sur Thunderbird. Bien que les mails soient chiffrés, cela permet en cas de vol du mot de passe de messagerie de ne pas pouvoir exploiter les informations des mails contenus sur le webmail Gmail. En effet, il faut noter que les expéditeurs, les destinataires et l'objet du mail sont en clair et que seul le contenu est chiffré.

Ainsi, seuls les mails non encore rapatriés sont stockés sur le webmail. Après leur

rapatriement, ils sont supprimés de la webmail et disponible sur le client Thunderbird en local.

Afin de permettre l'utilisation des mails chiffrés, chaque collaborateur doit envoyer sa clef publique aux personnes avec lesquelles il souhaite communiquer et réciproquement.

e. Partage des documents via l'outil GoogleDocs

Lors de ce projet de nombreux documents et procédures ont été créés aussi bien en interne qu'à destination du client.

Afin de permettre une gestion des documents plus aisée pour chacun, en comparaison à l'envoi des documents par mail, et une mise à disposition permanente des documents, nous avons décidé d'utiliser l'outil fourni, pour l'ouverture d'une boite Gmail, appelé GoogleDocs. Pour se faire, nous avons également créé une procédure disponible en **annexe 7**.

Chaque collaborateur possède alors un droit en lecture sur tous les dossiers d'Assurancetourix et un droit en écriture sur les groupes auxquels il appartient.

Il faut noter que notre client ne possède pas d'accès à cet espace de partage de documents. La communication avec le client est décrite ci-après.

2. La communication externe

a. Les réunions

De nombreuses réunions ont eu lieu entre AssuranceTourix et Aérodef particulièrement concernant le contenu des contrats et des moyens de communication entre les deux entreprises. Toutes les réunions ont fait l'objet d'un compte-rendu de réunion.

b. La communication formelle

La communication externe et plus particulièrement celle avec notre client s'est effectué de la manière suivante :

- Toutes les communications devant être effectuées avec le client, avant l'établissement des contrats, se sont faites par l'intermédiaire des services communication des deux entreprises. Ces communications sont faites via des mails chiffrés.
- Après signature des contrats, le client nous a fourni une liste de contacts techniques avec lesquels pouvaient communiquer nos équipes. Ces communications se sont effectuées par

l'intermédiaire de mails non-chiffrés.

Malgré notre instance à vouloir utiliser obligatoirement des communications, entre services techniques, par l'intermédiaire de mails chiffrés, le client n'a pas voulu entendre raison. Ce dernier nous a fourni différentes raisons à la non-utilisation de mails chiffrés :

- Trop contraignant puisqu'il faut utiliser l'ordinateur disposant du client de messagerie.
- Trop difficile à mettre en place.

Devant leur réticence et malgré nos nombreux contre-arguments, nous avons cédé et permis la communication entre services technique par l'intermédiaire de mails non-chiffrés. En contrepartie, nous avons demandé au client de porter la responsabilité des conséquences, en cas d'interception de ces communications non-chiffrées, chose qu'il a accepté.

c. *La communication informelle*

Il est intéressant de noter les différences qu'il existe entre la communication formelle et la communication informelle. La communication formelle regroupe les différents éléments cités précédemment s'inscrivant dans un processus de communication officiel. La communication informelle, quant à elle, s'inscrit plutôt dans un processus officieux dit de « conversation de machine à café ».

Au travers de ce projet, nous avons usé de ces deux types de communications en privilégiant au départ une communication par les canaux officiels. Cependant, nous n'arrivions pas, la plupart du temps, à nos fins. Ainsi, au fur et à mesure du projet, nous avons usé des canaux officieux qui procurent des résultats plus que convaincants.

A titre d'exemple, il était bien plus aisé de s'entretenir directement avec le responsable des « ouvertures de ports » afin que ce dernier nous débloque certains ports. Les ouvertures de ports s'effectuaient alors très rapidement. A contrario, si nous étions intervenus par le canal officiel cela aurait pris plusieurs jours sans forcément aboutir.

3. Problèmes rencontrés

En lisant les rapports des années précédentes, on s'aperçoit très rapidement que les difficultés sont les mêmes d'années en années.

En début de projet l'équipe défense est prise d'une paranoïa excessive et voit dans certaines de nos démarches une volonté de nuire à leur système. Du moins c'est ainsi que nous le percevons. De notre côté, nous avons tendance à juger un peu promptement les décisions du groupe défense. Ces réactions sont logiques, le groupe défense a la volonté de bien faire et par conséquent restreint un maximum l'accès à leur système et aux informations, l'audit quant à lui veut prouver son utilité, il se sent donc forcé de démontrer l'inefficacité des actions de la défense pour pouvoir en proposer de meilleures.

Ces réactions logiques entravent toutefois la communication entre les 2 groupes. Comme mentionné dans le paragraphe précédent, au début de ce projet l'accès aux informations de la défense fut laborieux. Or ces informations étaient nécessaires pour réfléchir aux solutions que nous comptions proposées. Le fait de devoir passer obligatoirement par le groupe communication de la défense pour s'entretenir avec un responsable a également ralenti considérablement nos actions.

Malgré tout, après avoir fait remonter ces problèmes au groupe défense, on a pu noter, en fin de projet, un assouplissement de toutes ces règles ce qui nous a permis de travailler plus efficacement sans toutefois mettre en danger l'architecture de la défense.

IV. Serveur d'audit

Au sein de ce projet, nous avions à disposition un seul serveur physique. Afin de faciliter la gestion de ce dernier nous avons opté pour la virtualisation de serveurs et d'éléments réseaux de niveau 2.

1. Environnement virtualisé

L'architecture de notre système d'audit se compose d'un serveur physique qui virtualise aussi bien des équipements réseaux que des serveurs. Il se compose de :

- Un pool de serveur
- Un switch permettant la gestion des VLAN
- Un pont entre l'interface physique et le switch virtuel

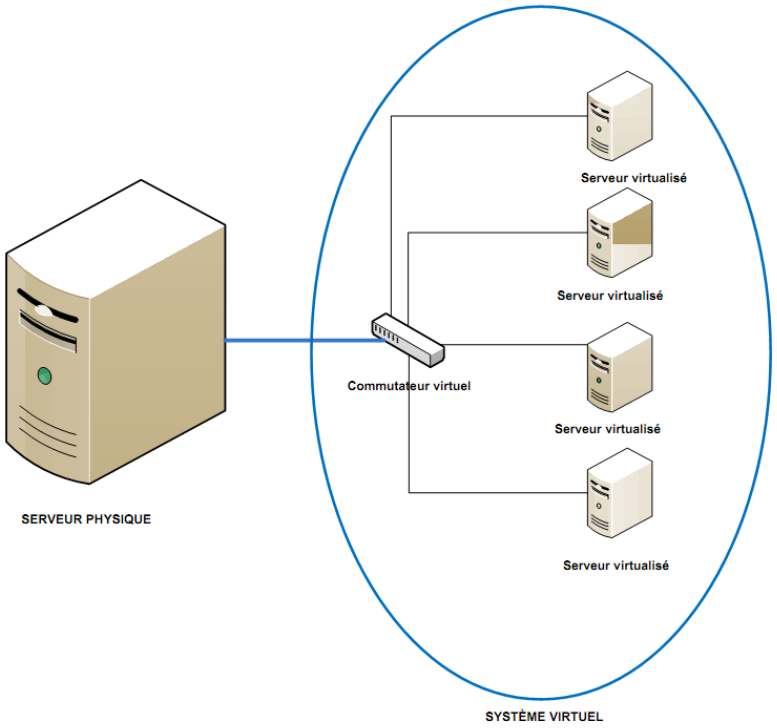


Figure 11 - Architecture de notre serveur d'audits

Afin de réaliser l'implémentation de ce système, nous avons déployé la solution KVM qui est permet d'exécuter le système d'exploitation invité de manière native sans modification. Avec cette technique, la virtualisation n'a aucun impact sur l'exécution du noyau du système virtualisé. En revanche, la virtualisation complète sacrifie les performances au prix de la compatibilité. En effet, il est plus difficile d'obtenir de bonnes performances lorsque le système invité ne participe pas au processus de virtualisation et doit traverser une ou plusieurs couches d'émulation avant d'accéder aux ressources matérielles.

Côté matériel, les développements récents sur les processeurs ont tendance à diminuer les écarts de performances entre paravirtualisation et virtualisation complète. Qu'il s'agisse d'Intel™ (VT : Intel® Virtualization Technology) ou d'AMD™ (AMD-V : Industry Leading Virtualization Platform Efficiency) les derniers processeurs disposent de fonctions matérielles pour la virtualisation.

Avec le noyau Linux, l'objectif de la solution Kernel Based Virtual Machine ou KVM est d'ajouter des capacités de virtualisation à un noyau standard. Il est ainsi possible de tirer parti de toutes les fonctions de réglage fin dèjà intégrées au noyau et de bénéficier des nouveaux avantages apportés par les environnements virtualisés.

Avec le modèle KVM, chaque machine virtuelle est un processus standard du noyau Linux géré par l'ordonnanceur (scheduler). Un processus normal de système GNU/Linux peut être exécuté selon deux modes : noyau (kernelspace) ou utilisateur (userspace). Le modèle KVM ajoute un

troisième mode : le mode invité qui possède ses propres modes noyau et utilisateur.

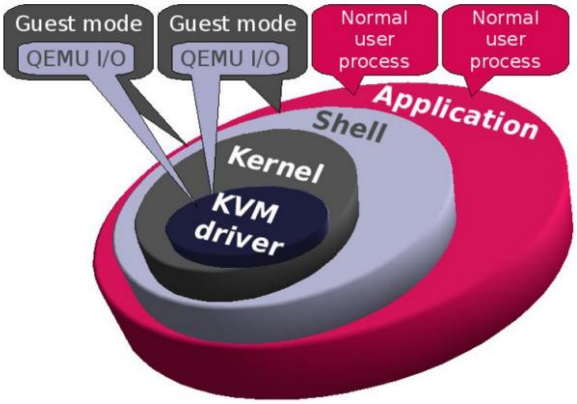


Figure 12 - KVM dans le noyau Linux

2. Mise en place

g. *Partie réseau*

La virtualisation de la partie réseau se fait en 4 étapes :

- Activation du routage
- Création d'une interface virtuelle « TAP »
- Création d'un bridge BR0 reliant le TAP à l'interface physique du serveur
- On raccorde le TAP au VDE-switch

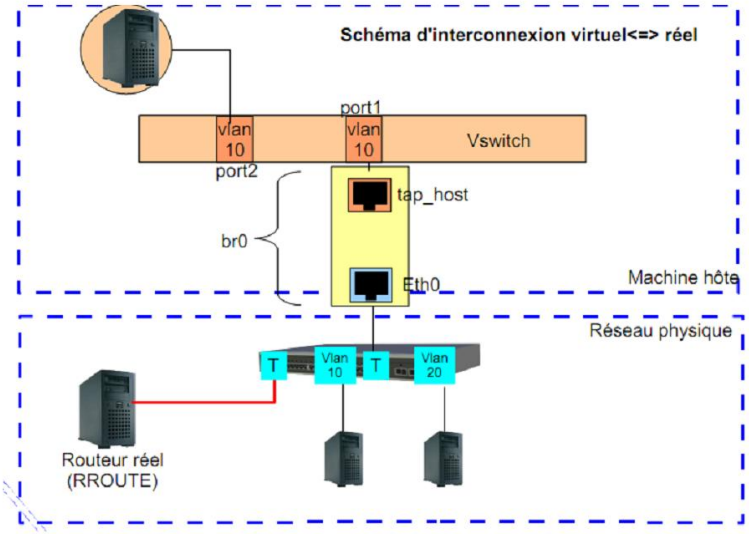


Figure 13 - Schéma de principe d'interconnexion

h. Partie système

Pour la partie système tout est gérer par KVM. La première étape est de créer un disque virtuel puis de démarrer la machine avec KVM.

Lors du démarrage des machines, on passe un ensemble de paramètre comme :

- L'adresse MAC,
- Le port de connexion sur le switch VDE
- Le disque dur associé à la machine
- La mémoire attribuée à la machine,…

Le démarrage des machines a été scripté afin de facilité le démarrage des machines. Afin de rendre stable et facile à configurer, nous avons une instruction dite « post-up » dans le fichier /etc/network/interface. Cette commande exécutée un script (cf. Annexe n°8) reprenant les étapes présenter dans la partie réseau pour la mise en place du commutateur.

3. Plan de reprise

Dès le début du projet, nous nous sommes positionnés comme étant une cible potentielle pour l'attaque. De ce fait, nous avons mis en place un système de reprise de service en cas de coupure du serveur (physique ou virtuel).

En cas d'infiltration ou destruction d'un serveur virtuel, nous disposions de copies des disques à chaque étape du projet et du déploiement d'application. Cette copie est réalisée sur l'ordre des chefs de projets en cas d'avancer significative de la mise en place des services. Nous pouvions donc en quelques minutes remettre un serveur virtuel en état de marche dans l'état où nous le souhaitions. Les sauvegardes pouvant être redéployées à distance.

Dans le cas où ce soit le serveur physique qui soit ciblé, nous disposions d'une sauvegarde complète comprenant également les sauvegardes de disques virtuelles sur un serveur appartenant à Mr LATU. Afin de remettre en état le serveur, nous devions utiliser le même principe que celui utiliser en salle de TP3 ; c'est-à-dire booter le serveur sur un CD qui récupère par la suite l'image du disque. Le temps de reprise si nous étions sur place était d'une dizaine de minutes.

V. Application d'audits – Système d'informations

1. NetFlow – Analyse de flux

Netflow est un protocole propriétaire Cisco s'appuyant sur la notion de flux et permettant de centraliser les informations relatives au trafic réseaux. C'est un protocole permettant de simplifier l'analyse des compteurs des équipements réseaux.

Pour fonctionner, ce protocole a besoin de 2 entités. La première sera présente sur chaque équipement réseaux et permettra de gérer le cache Netflow et d'exporter celui-ci vers le centralisateur. La seconde est présente sur le centralisateur et permet d'enregistrer toutes les informations provenant des équipements réseaux.

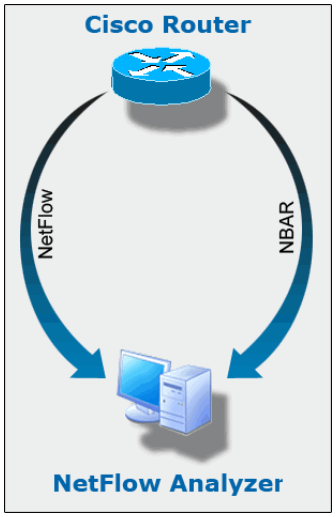


Figure 14 - Principe de NetFlow

Un routeur sur lequel Netflow est activé possède en cache (cache Netflow) une table des flux actifs. Celui-ci permet de compter le nombre de paquets et d'octets reçus pour chaque flux. Ainsi, à chaque paquet reçu le routeur met à jour le cache soit en créant une nouvelle entrée soit en incrémentant les compteurs d'une entrée existante.

Lorsqu'un flux expire, il est supprimé du cache et les informations sont envoyées vers la machine de collecte.

Contexte du projet :

La Défense utilise un routeur Cisco dans son infrastructure réseaux. Nous leur avons donc demandé d'utiliser Netflow (cf annexe 10) afin de nous remonter des informations vers notre collecteur.

Pour cela nous avons choisi le couple de logiciel nfdump et nfsen :

-**nfdump** est le daemon permettant d'enregistrer les informations récoltées

-**nfsen** est une interface graphique utilisant les statistiques enregistrées sous forme de graphique sur une interface WEB.

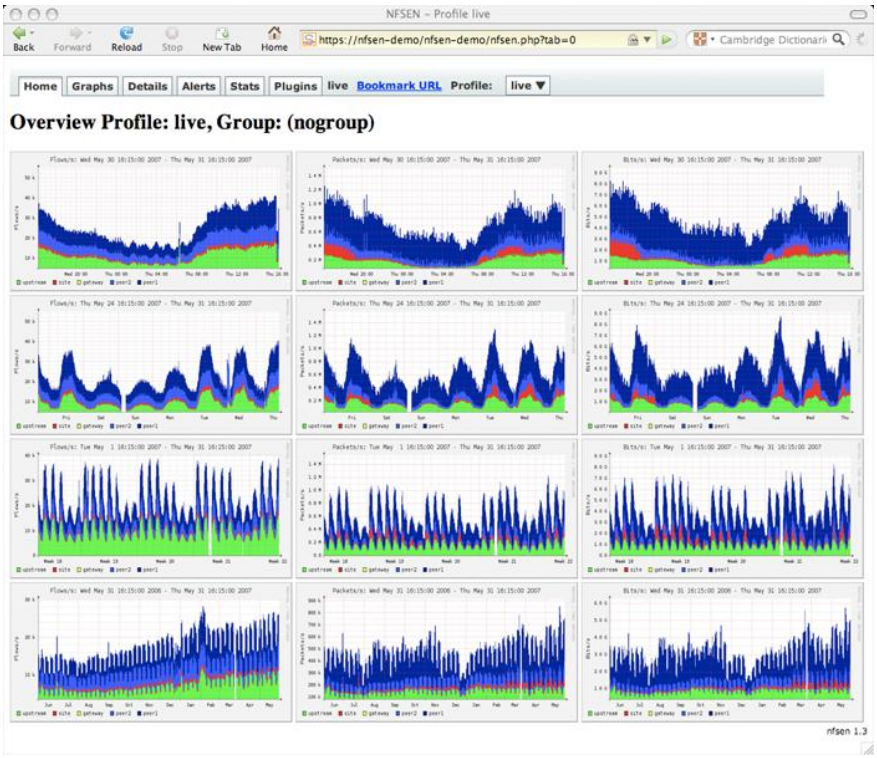


Figure 15 - Analyse Netflow

2. SPAN

Le commutateur d'entrée est un CISCO, il est possible de réaliser du SPAN, et donc dupliquer toutes les requêtes entrantes et sortantes vers une sortie reliée à la sonde SNORT. Nous avons donc installé une seconde carte réseau sur notre serveur afin de pouvoir collecter les informations à travers SNORT, PRELUDE et des analyses TSHARK lors des confrontations.

Le SPAN (Switched Port Analyzer) est une fonction des commutateurs Ethernet Cisco qui permet de recopier sur un port donné le trafic destiné à un ou plusieurs autres ports. Un analyseur de réseau connecté au port SPAN peut surveiller le trafic provenant de l'un des ports du commutateur. Cette fonction permet d'effectuer des analyses de trafic sans perturber le fonctionnement.

3. Gestion des logs

a. Syslog-ng et log-rotate

Les journaux, ou logs dans le jargon, servent à enregistrer tous les évènements qui surviennent sur un système. Historiquement, le service syslog a été développé pour la branche Unix des systèmes BSD. Depuis, ce service a été très largement adopté. On le retrouve sur tous les systèmes Unix, GNU/Linux et surtout sur les équipements réseau de nombreux constructeurs. Le protocole syslog est décrit dans le document RFC3164 "The BSD Syslog Protocol".

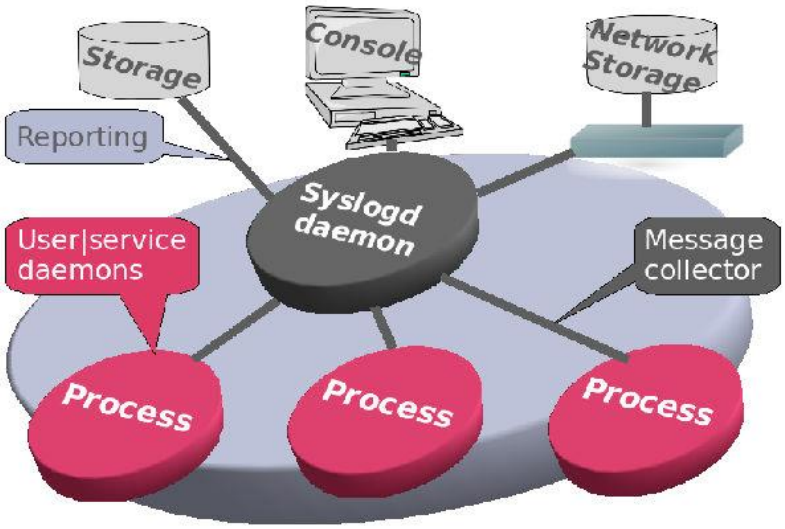


Figure 16 - Daemon Syslogd

Syslog-ng (new generation) est une implémentation étendue du protocole standard de gestion des journaux système. Il est largement utilisé dans la centralisation des logs provenant de différents systèmes d'infrastructures hétérogènes. Syslog-ng peut travailler en mode serveur (réception des logs) ou agent (envoi des logs). Chaque machine serveur peut ainsi envoyer ses logs systèmes vers un serveur central. Syslog-ng est flexible et simple a configurer. Il propose des fonctionnalités puissantes de filtrage de contenu permettant de répartir les logs dans des fichiers et répertoires propres à chaque système.

"logrotate" est un outils de gestion de fichiers de logs. Il permet d'archiver, d'organiser et de sauvegarder les journaux systèmes automatiquement. L'outil est modulable et permet aux administrateurs consciencieux de conserver une trace précise, structurée et hiérarchisée de l'activité de leurs machine dans le respect des lois (comme par exemple : garder une profondeur de logs d'un an ET ne pas conserver de logs de plus d'un an, etc).

L'outil est essentiellement composé d'un script de rotation des logs (logrotate) et de ses fichiers de configuration ("/etc/logrotate.conf" et "/etc/logrotate.d/*").

Le déclenchement du script est effectué par le cron (cron, fcron ou vixie-cron). Lorsque le script est appelé, il examine les fichiers de logs qui ont été spécifié dans "/etc/logrotate.conf" ou "/etc/logrotate.d/*", et y applique le traitement définit dans le fichier de configuration (compression, numérotation, archivage, etc…).

Dans notre projet, nous centralisions l'ensemble de nos log serveurs mais également ceux de la société AeroDef (uniquement syslog.log). Nous analysions régulièrement l'état de ces logs (quotidiennement) dans un premier temps » à la main » puis à travers le logiciel Splunk qui nous a facilités **considérablement** les recherches d'évènements particuliers.

Il aurait été intéressant de nous donner l'intégralité de leur log système de la société AeroDef afin de déceler toutes les intrusions ou effets non désirés sur leur SI. Pour certains raisons, le fichier auth.log (analyse d'authentification sur le système) n'a été donné en audit qu'en fin de projet.

b. Splunk

L'éditeur Splunk propose une approche novatrice dans la gestion et l'exploitation des logs. L'objectif est d'améliorer la lisibilité des très nombreuses remontées de logs issues d'éléments actifs du réseau.

Splunk indexe tout ou partie des logs informatiques à partir de n'importe quelle source, en temps réel (équipements réseaux, journaux d'évènements, enregistrements de fichiers, modification de configurations/paramétrages d'OS, connections VPN, …).

Quelque soit la source ou le format, Splunk est capable d'indexer sans modules complémentaire à acquérir, à développer ou à maintenir.

Dans un deuxième temps, l'application permet de rechercher les logs, de générer des rapports, et de surveiller ou d'analyser en temps réel les informations issues de la collecte. Ceci à travers toute l'infrastructure IT.

Splunk favorise les dépannages rapides et les investigations sur les incidents. Offre de puissantes analyses statistiques et de corrélation de logs. Fournit également une interface utilisateur interactive afin d'alerter, surveiller, permettre du reporting (permet de mettre à jour des compteurs d'évènements, de calculer des métriques et de spécifier des laps de temps définis) et des analyses.

Splunk offre la possibilité de recherches en temps réel ou rétroactive. L'assistant de recherche propose par exemple :

- une barre de recherche ainsi qu'une aide contextuelle afin d'exploiter au mieux toute la

puissance du langage de recherche

- une interaction avec les résultats de recherche en temps réel.
- la possibilité de zoomer ou dézoomer sur une échelle de temps particulière dans l'optique de dégager rapidement des tendances, des pointes ou des anomalies.
- de naviguer dans les résultats et éliminer le « bruit ».

Il est possible de convertir des recherches en alertes déclenchant l'envoi automatique de mails, de notifications RSS, ou d'exécution de scripts.

Il est également prévu de pouvoir ajouter du sens aux logs en identifiant, nommant, marquant des champs et des données.

Splunk permet aussi d'ajouter des informations à partir de sources externes (bases de données de management, systèmes de gestion des configurations, annuaires utilisateurs).

Le générateur de rapport permet de créer rapidement des graphiques et des tableaux de bord qui indiquent les tendances significatives, les hauts et les bas, les résumés des valeurs premières et la fréquence des occurrences sans demander aucune connaissance approfondie des commandes de recherche.

Cette outils nous a été d'une aide **CRUTIALE** pour l'analyse de log système du fait que nous pouvons effectuer très rapidement des recherches très précises sur des mots clés, des sources,… On aurait dû le mettre en place dès le début du projet afin d'explorer l'ensemble des fonctionnalités offertes par ce système. Il nécessite néanmoins une machine robuste et du temps pour le paramétrage des fonctionnalités divers. **Logiciel à suivre car il se révéla à la hauteur de nos attentes.**

4. Supervision avec FAN – Full Automated Nagios

Dans le cadre de notre audit de sécurité de la société AéroDef, il nous a semblé judicieux pour la pérennité de leur système d'information de mettre en place un outil de supervision. La supervision a pour but d'une part de contrôler l'état de fonctionnement d'un élément informatique (ordinateur, serveur, Switch, etc.), d'un service (web, dns, sql, etc.), mais également d'envoyer des alertes (appelée « trap ») sans avoir à faire une collecte d'information sur l'élément informatique, mais envoyées automatiquement en cas de problème.

Il faut savoir également que l'outil de supervision sert uniquement à détecter les différents problèmes. Il ne va en aucun cas régler le problème par lui-même. Il va uniquement servir à l'utilisateur à détecter les problèmes éventuels sur les éléments qu'il supervise.

De plus, l'outil de supervision aura différentes vocations :

- Surveiller les éléments du réseau via une interface web.
- Etre alerté des éventuels disfonctionnements.
- Présentation des informations à divers niveaux d'abstraction.

Le monde informatique étant en constante évolution dans l'ensemble de ces domaines, la solution de supervision a été en constante évolution durant la totalité du projet afin de répondre

pleinement aux différents besoins du client d'une part, mais également de s'adapter aux évolutions de leur architecture d'autre part.

a. Présentation des outils

Afin de réaliser la fonction de supervision de l'ensemble du parc AéroDef, nous avons mis en place divers outils avec des fonctionnalités différentes. Etant donné du court délai disponible pour réaliser le projet, et en prenant en compte la complexité de mise en œuvre des différents outils, nous avons choisi de mettre en place une solution automatisée, la distribution FAN (**F**ully**A**utomated**N**agios). Cette distribution linux est basée sur CentOS et a pour but de proposer une solution globale dédiée à la supervision. Elle contient les outils de supervision suivants :

L'outil **Nagios** et certains de ses plugins : cœur de la supervision, élément centralisateur des données remontées par les agents.

L'outil **Centreon** : surcouche à l'outil Nagios. Offre une interface web intuitive à l'utilisateur lui permettant de gérer plus facilement son parc d'éléments à superviser.

L'outil **Nagvis** : permet d'avoir une cartographie complète de l'architecture réseau (position géographique, position des services, etc.).

L'outil **Nareto** : propose une interface de haut niveau à Nagios permettant d'organiser l'ensemble des éléments à superviser sous la forme d'une arborescence (inutilisé dans le cadre du projet).

L'outil **Apache** : serveur web qui est nécessaire au fonctionnement de l'ensemble des outils.

L'outil **Mysql** : Historisation des données remontées par les agents.

En complément de tous ces outils, nous avons utilisé deux protocoles de supervision différents. Les protocoles de supervision ont pour but d'instaurer un dialogue entre la machine « manager » qui stocke et traite les informations, et les différents « agents » d'où proviennent les informations. Voici

ci-dessous les protocoles plus en détail :

- Le protocole **SNMP** : permet à la machine « manager » d'interroger les différents agents, afin d'aller récupérer les informations désirées dans les différentes MIB.

- Le protocole **NRPE** : permet à la machine « manager » de demander l'exécution d'un code à distance sur « l'agent », une fois ce code exécuté, le résultat est retourné à la machine « manager ».

Afin de bien comprendre le fonctionnement de la supervision, voici ci-dessous un schéma explicatif sur la supervision et plus particulièrement sur l'outil Nagios.

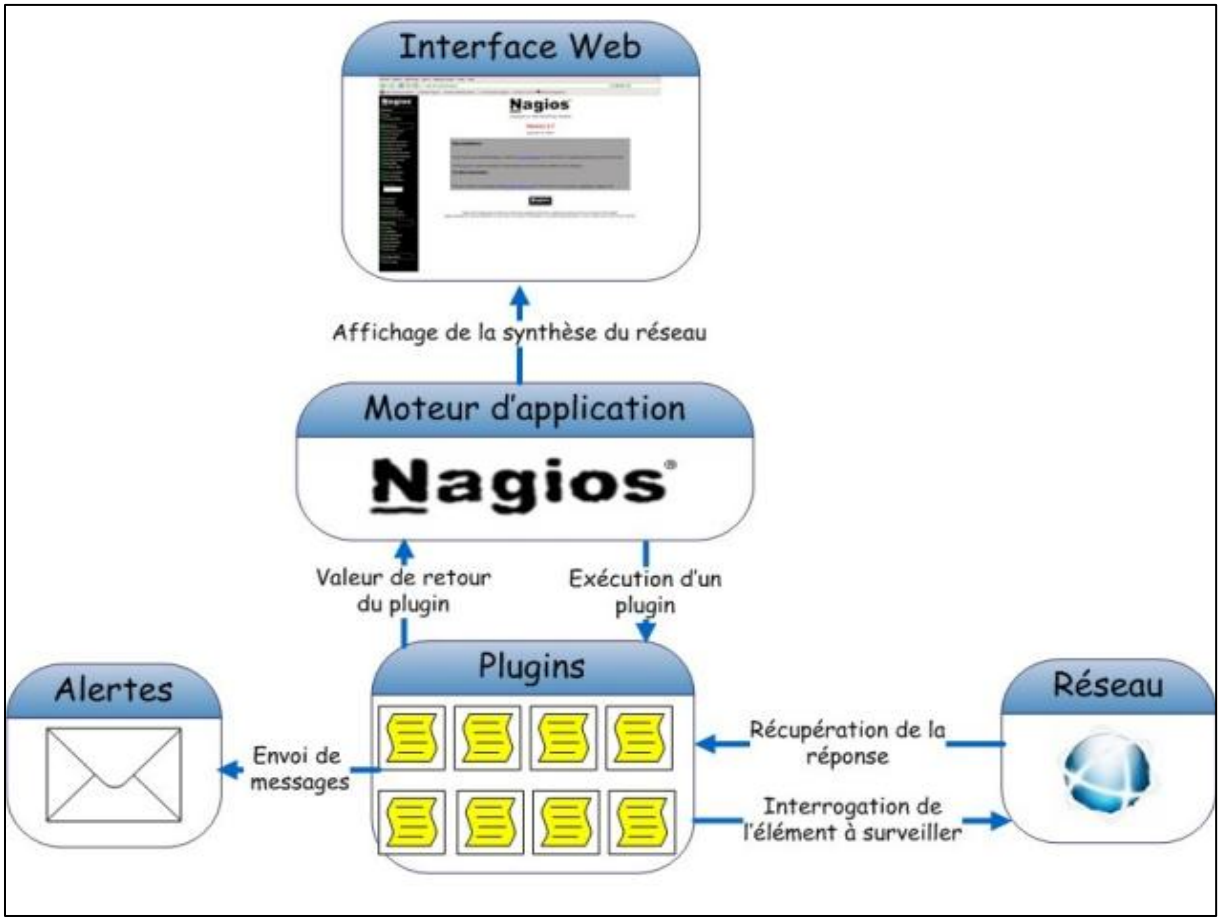


Figure 17 - Schéma général de la Supervision et Nagios

1. Nous avons tout d'abord l'outil Nagios qui est l'élément centralisateur. Il exécute différents plugins en fonction de l'information à récupérer ou de l'action à effectuer.
2. Le plugin va ensuite interroger le ou les différents agents en passant par l'intermédiaire du réseau.
3. Le ou les différents agents renvoient ensuite la réponse au plugin.
4. Le plugin va avoir ensuite deux choix possibles. Le premier étant de lever une alerte si nécessaire, ou alors de simplement renvoyer la valeur de retour au moteur d'application Nagios.
5. La valeur de retour est ensuite stockée, analysée, et mise en forme par l'outil Nagios.
6. L'outil Nagios met à disposition de l'utilisateur les résultats sous différentes formes

(graphique, textuelle, etc.) via une interface web.

b. Méthodologie de déploiement

La méthode employée pour surveiller une architecture se met toujours en place en respectant le même schéma.

Nagios/Centreon offre la possibilité de créer des modèles d'hôtes et de services. Nous avons donc conçu des templates pour chaque type de machines. A ces modèles d'hôtes sont associés des modèles de services.

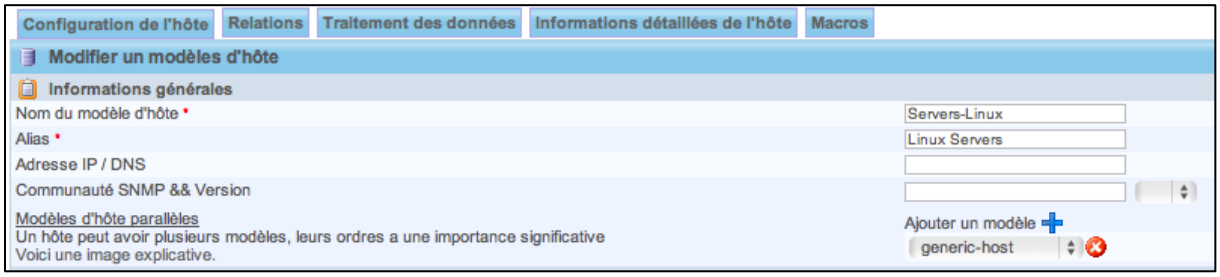
Dans les prochains paragraphes nous présenterons une coupe verticale du processus de déploiement de la supervision sur l'architecture du client.

Les modèles d'hôtes :

Dans cette partie nous allons montrer, à l'aide de captures d'écran, comment créer un modèle d'hôte sur Centreon. Pour cette démonstration nous créons un modèle de machine de type serveur Linux.

L'interface de création des modèles d'hôtes se trouve dans la partie configuration/Hôtes/Modèles de Centreon.

La première chose à faire est donc de définir un modèle de machine dont tous les serveurs linux hériteront.

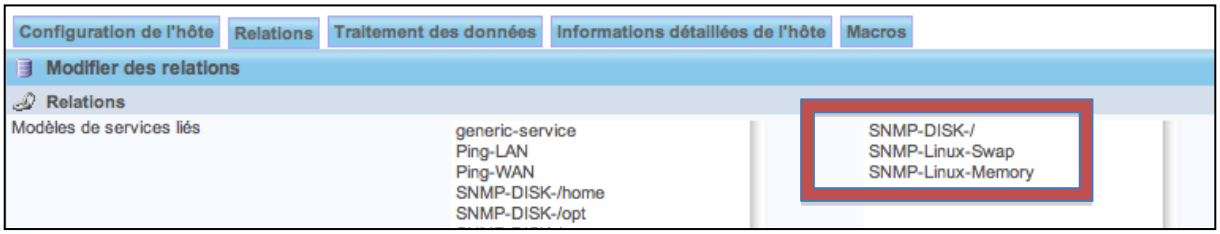


L'onglet configuration de l'hôte va permettre de renseigner le nom de notre modèle. C'est tout ce que nous allons faire dans cette partie.

La suite du déploiement passe par la création de modèle de services que nous allons associer au modèle d'hôte que nous venons de créer. Ainsi toutes les machines qui hériteront du modèle

d'hôtes auront automatiquement les services associés au modèle qui leur seront également associés.

Voici les services qui sont associés automatiquement à un modèle :



Dans le prochain paragraphe nous allons présenter comment ajouter d'autres services au modèle d'hôte.

Les modèles de services :

Pour ajouter un modèle de service, il faut aller dans la partie configuration/services/modèles.

Voici comment se présente le formulaire de configuration du service :

Dans les informations générales on renseigne le nom du service ainsi que son alias. Mais la partie la plus intéressante est la commande de vérification : C'est dans cette partie qu'est spécifié le plugin utilisé pour aller chercher l'information recherchée. Dans cet exemple on cherche à avoir le taux d'utilisation du cpu. On utilise donc le plugin check_snmp_centreon_load_average.

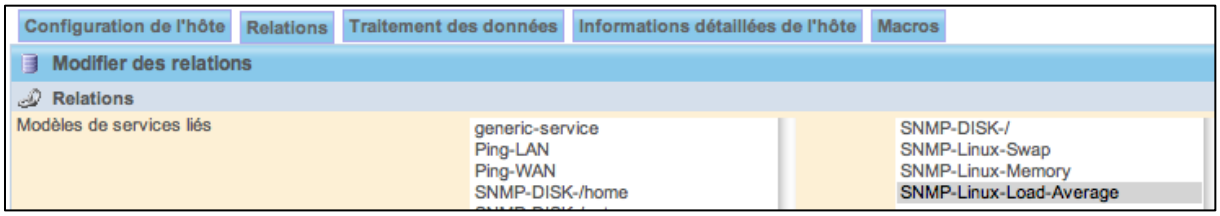
La ligne arguments renseigne les arguments nécessaires à la requête pour fonctionner.

- $USER2$: variable contenant la communauté utilisée
- 4,3,2 : seuil au-dessus duquel la commande renvoi un warning
- 6,5,4 : seuil au-dessus duquel la commande renvoi un critical

Notre service est configuré, il faut maintenant l'associé au modèle d'hôte Serveur-Linux. Pour

cela, il faut aller dans l'onglet « relations » et ajouter Serveurs-Linux à la liste « Lier aux modèle de l'hôte » :

Assurons-nous que le service apparaît maintenant dans l'interface de configuration du modèle de l'hôte :

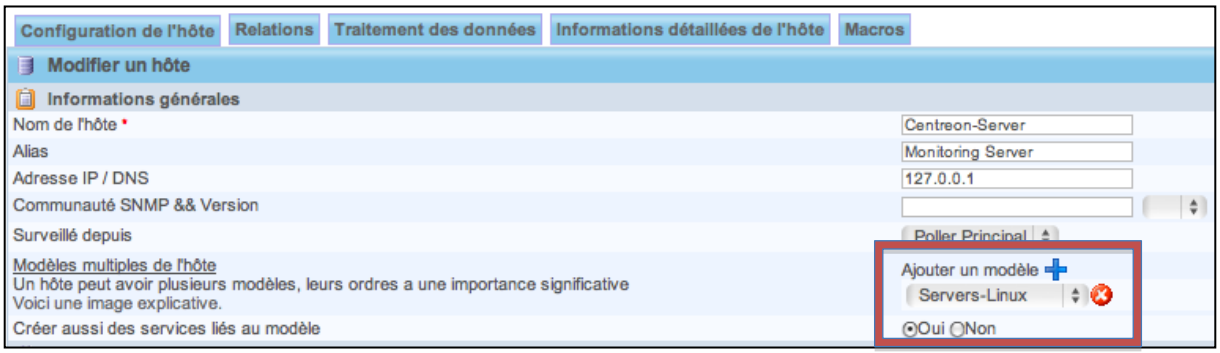


On aperçoit bien en bas à droite de la capture ci-dessus le nom du nouveau service en gris.

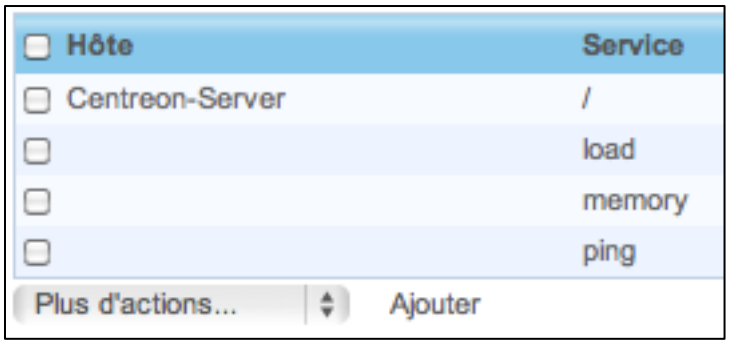
La création d'un hôte :

Le modèle server-Linux est créé et configuré selon nos souhaits. Pour autant à ce niveau là, aucun serveur linux n'est surveillé.

Mais grâce au travail sur les modèles cela sera grandement facilité. Il suffit de créer une machine, lui donné un nom, un alias, renseigné son @IP et surtout l'associé au groupe des Servers-Linux et le tour est joué.



On voit sur la capture ci-dessus que nous avons ajouté la machine Centreon-Server au modèle Server-linux et décidé de créer les services associés au modèle.



Les services associés à notre serveur Centreon sont créés automatiquement.

Les ajouts de plugins :

Il se peut que les plugins initialement prévus dans la FAN ne répondent pas à une de nos problématiques. Heureusement, Nagios possède une communauté active de personnes qui développent des plugins en perl ou en bash. Ces plugins sont ensuite téléchargeables via des sites web.

Vous pouvez trouver de nombreux plugins à l'adresse suivante : http://exchange.nagios.org/

Les plugins doivent être placés dans le répertoire /usr/lib/nagios/plugins. Il faut ensuite créer une nouvelle commande ou nous spécifierons la syntaxe de la requête d'utilisation du plugin. Une fois la commande créée il faut l'utiliser dans un service que nous associerons à l'hôte à surveiller.

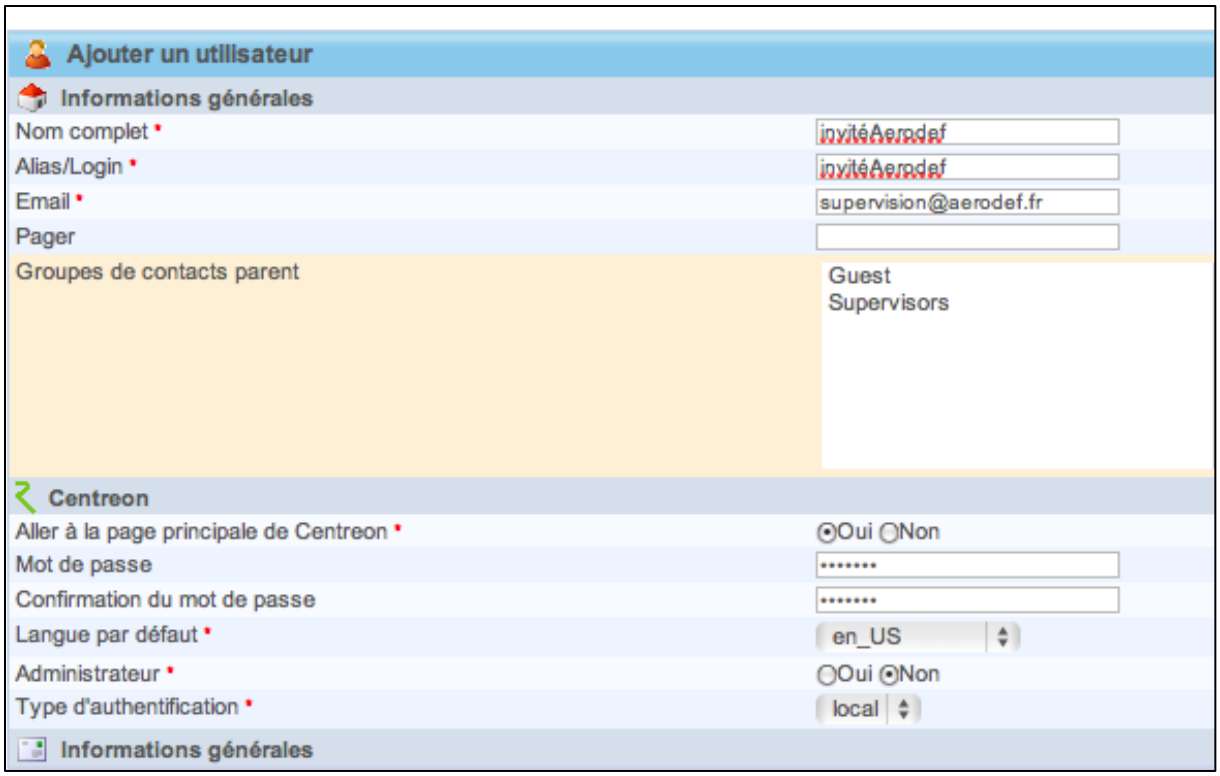
On peut ainsi configurer nos services pour qu'ils renvoient exactement l'information souhaitée et de la manière désirée.

La prochaine étape aurait été de développer nous-même nos propres plugins mais le temps nous manquait.

Les utilisateurs :

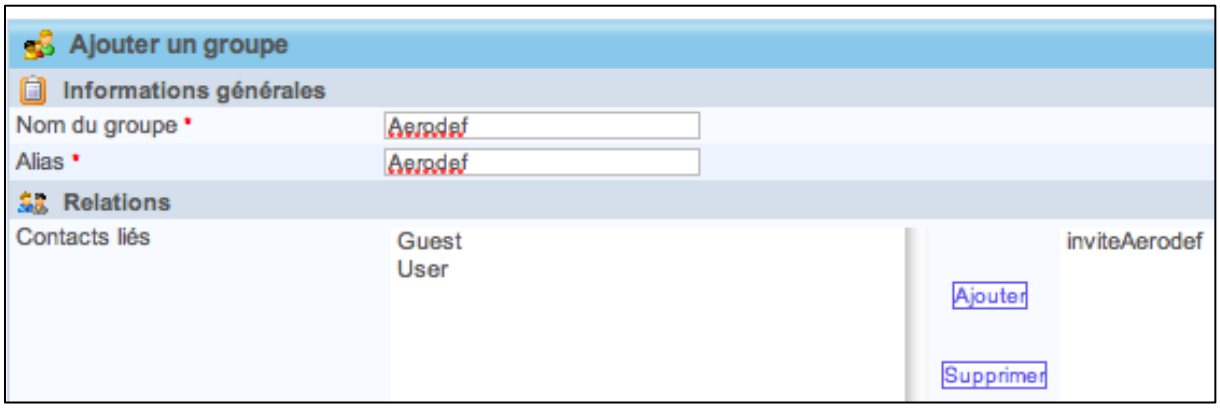
La finalité de ce système de supervision réseau est de mettre en place une solution pour le client. Nous avions donc dans l'idée de permettre au personnel d'Aérodef de consulter la plateforme Centreon. Nous devions donc créer des utilisateurs ayant des droits restreints et un visu sur seulement une partie de l'architecture. Les lignes qui suivent vous présentent comment nous avons procédé.

Nous créons donc un utilisateur inviteAerodef. L'interface de création des utilisateurs se trouve dans configuration/utilisateur.



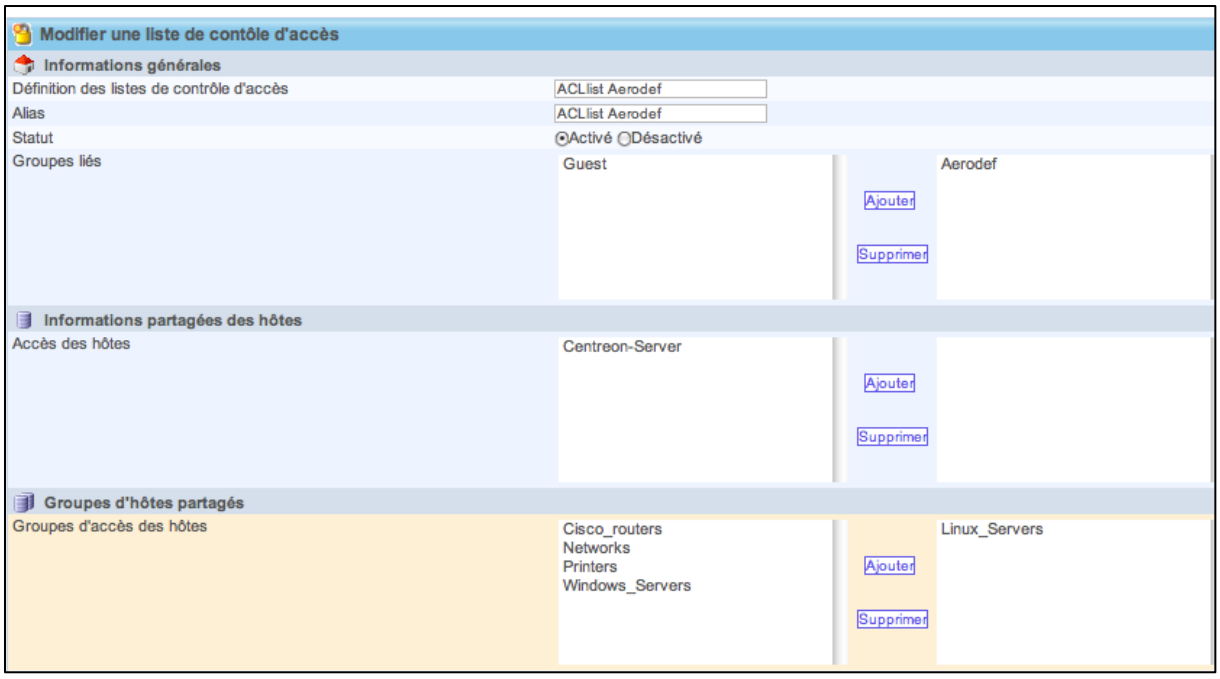
Il faut ensuite placer cet utilisateur dans un groupe d'accès. Nous avons décidé de créer de nouveaux groupes plutôt que d'utiliser les groupes existants.

Nous créons donc un groupe d'accès « Aerodef » et ajoutons notre nouvel utilisateur à sa liste de contacts liés. Le menu de création de groupe d'accès se situe dans administration/ACL/Access Groups.



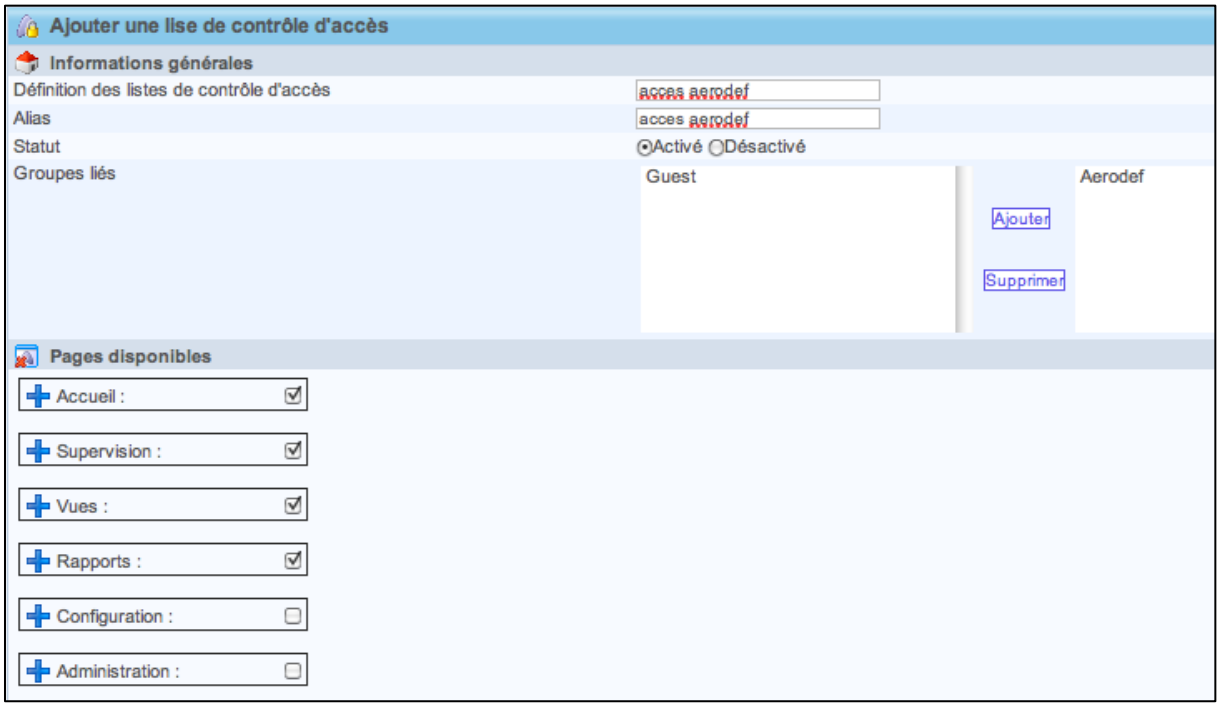
A ce groupe nous allons permettre l'accès seulement aux onglets accueil, supervision, vues, rapports. Pour cela rendons nous dans administration/ACL/Resources Access.

On crée ensuite une nouvelle liste de contrôle d'accès. Dans cette liste nous spécifierons le groupe d'utilisateurs et les machines impactés par les ACL.

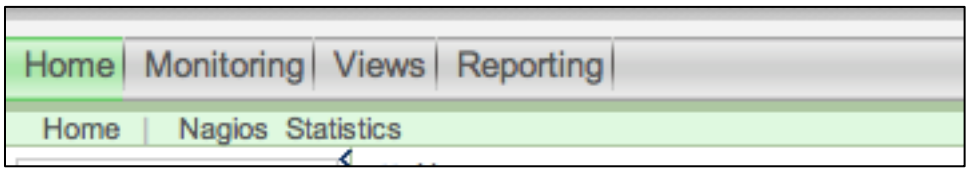


Nos ACL vont s'appliquer sur le groupe d'accès Aerodef et sur les Servers-Linux.

Il nous reste plus qu'à créer les règles d'accès dans administration/ACL/Menus Access. Dans cette partie on renseigne les onglets accessibles par le groupe d'accès aerodef. Vous voyez dans la capture ci-dessous que nous leur permettons d'accéder uniquement aux onglets mentionnés un peu plus haut dans le rapport.



Connectons-nous maintenant avec l'utilisateur inviteAerodef :



Comme le montre la capture ci-dessus seul les 4 premiers onglets sont visibles.

Nagvis :

Nagvis est un addon de visualisation pour Nagios qui permet de générer des vues métier de la supervision. Il est très facile à installer, à utiliser et très intuitif avec Nagios et son système de Drag and Drop.

Cet outil permet de réaliser une cartographie des éléments à superviser au sein d'un système d'information. Une fois la carte du système d'information conçue, il faut récupérer les hôtes et les services supervisés dans Nagios et les placer sur la map.

Nagvis a été mis en place pour avoir une vue simple et globale de l'architecture et pour connaître l'état de chaque élément à superviser. Son avantage est qu'il permet aux chefs d'avoir un résumé de l'état de fonctionnement du système d'information de l'entreprise AéroDef.

Nous avons donc décidé de ne pas représenter sur cette carte tous les services supervisés dans Nagios, mais plutôt de sélectionner les plus importants à destination les chefs.

Voici les hôtes et les services supervisés :

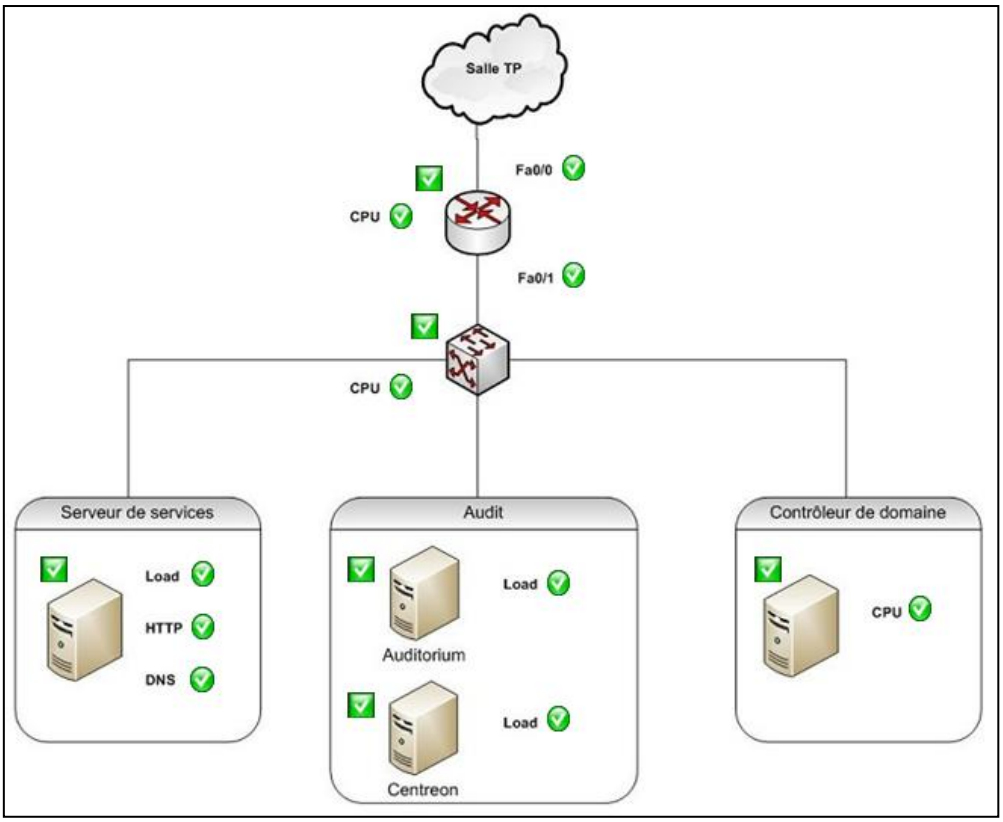


Figure 18 - Nagvis au sein d'Aérodef

Légende :

Représente les hôtes.

Représente les services.

La couleur verte signifie que l'élément fonctionne correctement. Le jaune signifierait qu'un élément est en état de warning et le rouge un problème majeur sur l'élément.

c. *Surveillance de l'architecture AeroDef :*

Après avoir abordé la partie concernant la méthodologie de déploiement, nous allons maintenant l'appliquer à l'architecture de la société AéroDef. En effet, dans cette partie, nous évoquerons les différents équipements qui ont été supervisés, mais également les différentes informations récoltées sur chaque équipement.

Les éléments « réseau » :

- Le Routeur CISCO :
  - Etat du routeur (UP/DOWN)
  - Ping
  - Etat des différentes interfaces (ex : f0/0 : UP/DOWN)

- Charge CPU (en pourcentage)
- Charge mémoire (en pourcentage)

- Le Switch CISCO :
  - Etat du Switch (UP/DOWN)
  - Ping
  - Etat des différentes interfaces (ex : f0/0 : UP/DOWN)
  - Charge CPU
  - Charge mémoire

Les éléments « système » :

- Le serveur de service (serveur Linux):
  - Etat du serveur (UP/DOWN)
  - Ping
  - Charge CPU (en pourcentage)
  - Charge Mémoire (en pourcentage)
  - Espace disque (espace libre / espace utilisé)
  - Service HTTP (UP/DOWN)
  - Service SSH (UP/DOWN)
  - Service DNS (est-ce le bon serveur Dns qui répond ?)

- Le contrôleur de domaine (serveur Windows):
  - Etat du serveur (UP/DOWN)
  - Ping
  - Charge CPU (en pourcentage)
  - Charge Mémoire (en pourcentage)
  - Espace disque (espace libre / espace utilisé)

Remarque : les différents postes clients n'étant pas d'une importance capitale dans le fonctionnement de l'architecture de la société AéroDef, nous avons choisi de ne pas les superviser afin de ne pas surcharger le réseau, et d'avoir une supervision plus étoffée des différents équipements réseaux et serveurs.

Maintenant que nous avons passé en revue les procédures de mises en place et les différents équipements que nous avons supervisé, nous allons maintenant aborder dans cette partie les résultats que nous avons pu obtenir grâce aux différents outils mis en place.

d. Résultats obtenus :

Interface « supervision_réseau » :

Afin de permettre au responsable réseau de la société AéroDef d'avoir une vue d'ensemble sur ses équipements, nous lui avons créé une interface spécifique. Cette interface est accessible via internet (login/mot de passe).

Elle contient l'ensemble des éléments de supervision liés aux équipements réseaux. Cette interface a la particularité d'être uniquement consultable. En d'autres termes, l'utilisateur peut uniquement consulter les différentes données (valeurs, graphes, etc.) mais en aucun cas changer les configurations de supervision.

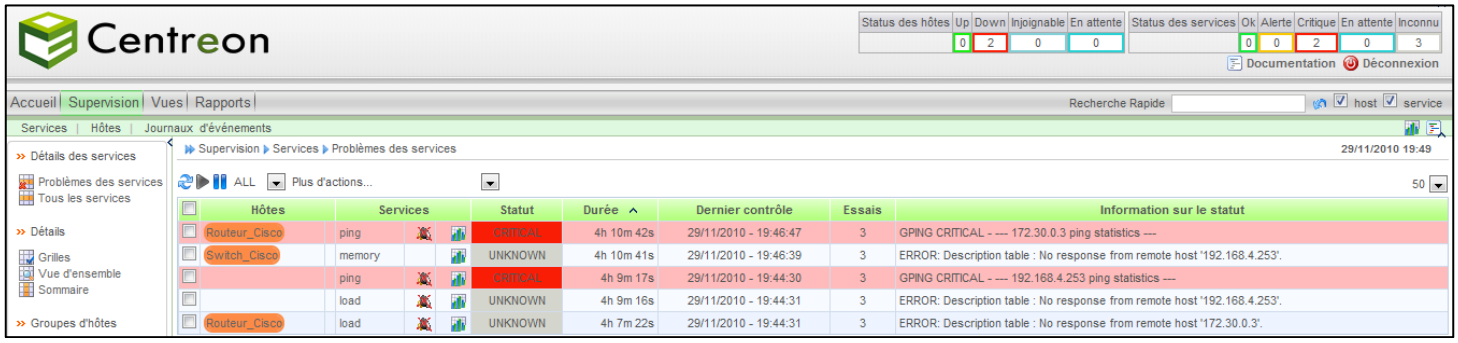


Figure 19 - Interface "supervision_réseau"

Interface « supervision_serveur » :

Sur le même principe, nous avons également créé une interface spécifique pour le responsable des différents serveurs de la société AéroDef. Cette interface possède les mêmes caractéristiques que l'interface réseau, à la différence que celle ci contient les informations relatives aux différents serveurs.

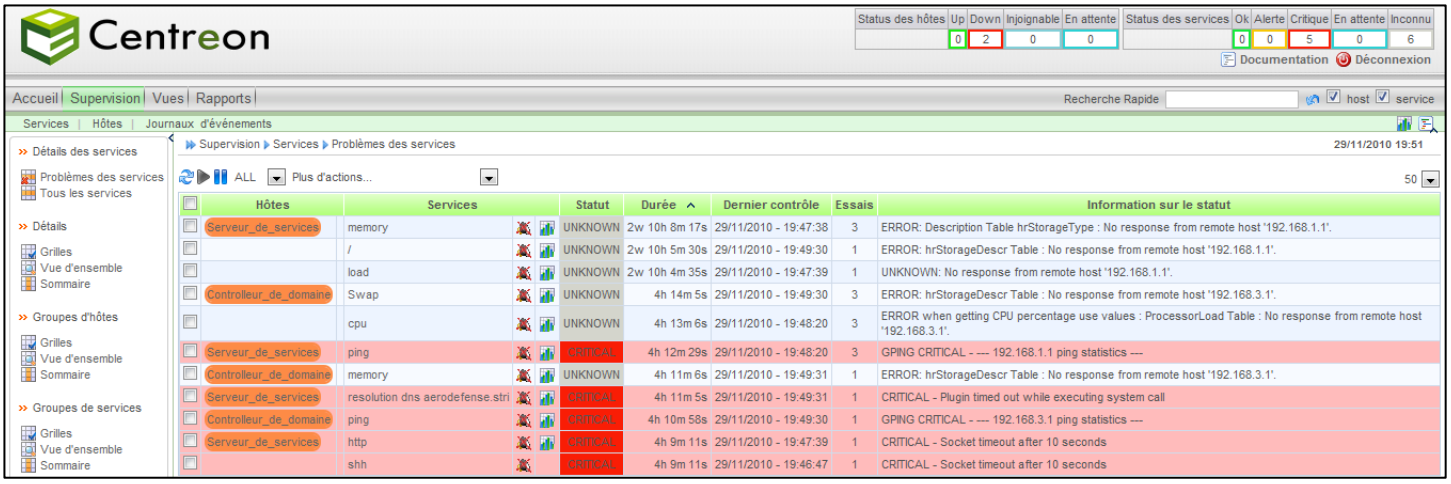


Figure 20 - Interface "supervision_serveur"

Détection du problème de « mauvais serveur DNS » :

Grâce au plugin NRPE concernant le serveur DNS, nous avons pu détecter qu'un mauvais serveur (autre que celui de la société AéroDef défini dans les paramètres) répondait aux requêtes DNS. L'outil de supervision a permis ici de détecter une attaque par « dnsspoofing ».

Services resolution dns aerodefense.stri sur l'hôte Serveur_de_services [Debian]	
Services	
Etat des services	CRITICAL
Information sur l'état	Domain aerodefense.stri was not found by the server
Données de performence	
Tentative actuelle	3 / 3
Type d'état	Hard
Dernier contrôle du type	Active
Dernier contrôle	15/11/2010 - 08:34:41
Prochaine planification de contrôle actif	15/11/2010 - 08:39:41
Latence	0.897 seconds
Durée de la vérification	0.05447 seconds
Changement du dernier état	07/11/2010 - 22:01:25
Durée de l'état actuel	1w 10h 34m 55s
Dernière notification du service	
Numéro de notification actuel	0
Est ce que ce service est oscillant ?	Non
Pourcentage de changement d'état	0 %
Dans la planification d'arrêt ?	Non
Dernière mise à jour	15/11/2010 - 08:36:20

Figure 21 - Problème "mauvais serveur DNS"

Détection du problème « surcharge du routeur » :

Concernant le routeur, les outils de supervision ont permis de détecter, pendant une période assez significative (hors fonctionnement nominal), une montée de la charge CPU. Cette anomalie peut être liée à une utilisation intensive du réseau (cas normal), ou alors à une surcharge volontaire du routeur par une attaque (cas anormal).

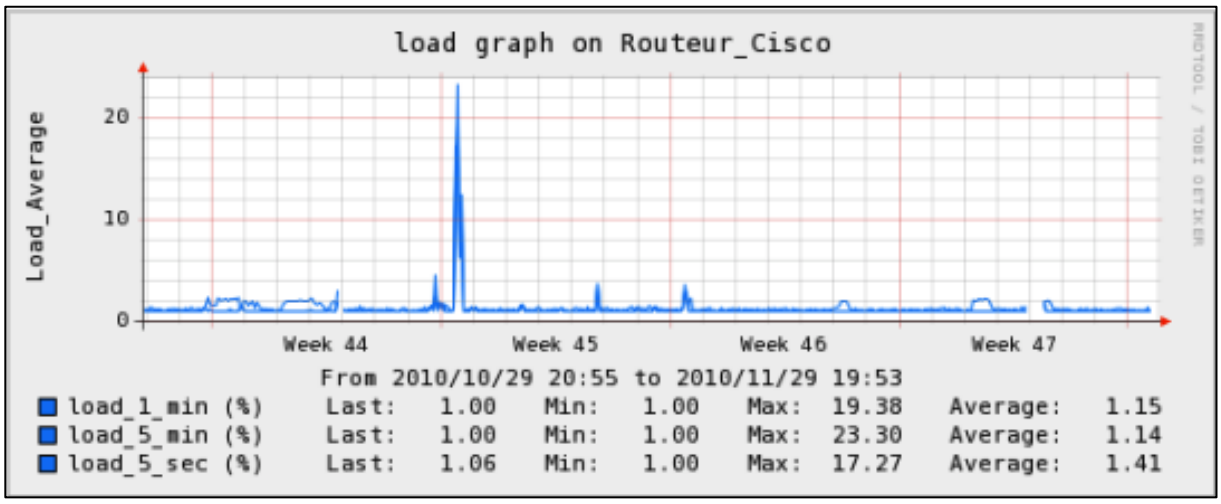


Figure 22 - Problème "surcharge du routeur"

Détection du problème « serveur de service DOWN » :

Pour finir, après une attaque de vol d'identité sur le serveur de service, celui-ci est devenue injoignable et hors service. Au niveau de la supervision, nous avons constaté plusieurs alertes qui sont apparues, et nous avons pu contacter le responsable d'AéroDef concerné.

Hôtes		Statut	Adresse IP	Dernier contrôle	Durée	Information sur le statut
Auditorium		UP	192.168.2.1	15/11/2010 - 09:50:54	5h 47m 4s	PING OK - Packet loss = 0%, RTA = 166.74 ms
Centreon		UP	127.0.0.1	15/11/2010 - 09:49:59	1w 18h 33m 19s	PING OK - Packet loss = 0%, RTA = 0.23 ms
Controlleur_de_domaine		UP	192.168.3.1	15/11/2010 - 09:50:25	5h 47m 1s	PING OK - Packet loss = 0%, RTA = 4.98 ms
Nessus		DOWN	192.168.2.102	15/11/2010 - 09:50:54	26m 24s	CRITICAL - Host Unreachable (192.168.2.102)
Routeur_Cisco		UP	172.30.0.3	15/11/2010 - 09:46:46	1w 32m 27s	PING OK - Packet loss = 0%, RTA = 1.66 ms
Serveur_de_services		DOWN	192.168.1.1	15/11/2010 - 09:49:58	6m 46s	(Host Check Timed Out)
Switch_Cisco		UP	192.168.4.253	15/11/2010 - 09:48:22	1w 32m 32s	PING OK - Packet loss = 0%, RTA = 1.29 ms

Figure 23 - Problème "serveur de service DOWN"

e. *Problèmes rencontrés*

Durant le projet de sécurité, le groupe supervision a été confronté à différents problèmes de sources différentes. Cette partie a pour but de retracer les différents problèmes et les solutions qui ont été mises en place pour les résoudre.

1er problème : connaissance de l'architecture AéroDef :

Le premier problème auquel nous avons été confrontés concerne la connaissance non exhaustive de l'architecture AéroDef. La mise en place de la supervision a débuté dès le commencement du projet. Mais, à ce moment-là, l'architecture d'AéroDef n'était pas complètement mise en place et plusieurs éléments nouveaux à superviser se sont petit à petit intégrés.
Afin d'aborder ce problème le plus efficacement possible, nous avons tout d'abord demandé à l'équipe AéroDef de nous tenir informé (le plus rapidement possible) des nouveaux équipements installés. Par la suite, nous avons organisé plusieurs réunions, cf. annexe 11, avec les différents responsables concernés, afin d'avoir une liste la plus complète possible sur les équipements qu'ils souhaitaient superviser, mais également le type de supervision pour chaque équipement (ex : charge CPU, PING, etc.).

2ème problème : installation des agents

Concernant l'installation des agents, la tâche n'a pas été facile à exécuter. La société AssuranceTourix étant une société de sous-traitance, elle n'avait pas directement accès au différentes machines et équipements de l'architecture d'AéroDef.
Pour installer les différents agents, nous avons dans un premier temps effectuer des tests sur nos propres machines pour s'assurer du bon fonctionnement et déterminer la phase d'installation et de configuration, puis dans un deuxième temps créer différents tutoriaux (cf. partie annexe 12) que nous avons fait parvenir à la société. Enfin, pour effectuer toutes les opérations de modification et de mise à jour, nous avons directement échangé avec les différents responsables concernés de la société AéroDef.

3ème problème : autorisation du Firewall :

Pour s'échanger les différentes informations, le «manager» et les différents « agents » ont besoin de dialoguer par l'intermédiaire des différents protocoles de supervision (SNMP et NRPE). Il a fallut donc contacter la personne responsable du Firewall afin qu'elle débloque les différents ports de communication (port SNMP : 161 – dialogue supervision / 162- trap ; port NRPE : 5666).

4ème problème : surcharge du réseau et des log :

L'une des grosses difficultés liées à la supervision, concerne la configuration. En effet, les protocoles de supervision sont des protocoles nécessitant beaucoup de ressources. De ce fait, ils ont entrainé des ralentissements général du réseau, mais également une « pollution » des logs.
Pour résoudre ce problème, nous avons allongé les intervalles d'interrogation des différents

équipements.

5ème problème : différence d'utilisation entre SNMP et NRPE :

Il existe différents protocoles pour faire de la supervision (cf : 2. Présentation des outils), le protocole SNMP et le protocole NRPE. Chacun possède une installation, une configuration et une utilisation très différente l'une de l'autre.
Pour résoudre ce problème, chaque équipement réseau a été supervisé grâce au protocole SNMP (en natif sur les équipements). En ce qui concerne les serveurs (Windows et Linux), nous avons mis en place et configuré les deux protocoles pour avoir le plus de choix possible et avoir une supervision la plus complète possible. De plus, cela a entrainé plusieurs configurations sur chaque serveur d'une part, mais également sur la machine « manager » d'autre part.

En débutant ce projet de sécurité, l'ensemble du sous-groupe « supervision » n'avait qu'une connaissance très générale de la supervision par l'intermédiaire des différents cours de M1 STRI.

Afin d'avoir une connaissance plus étoffée de ce domaine, l'une des premières étapes a été de se documenter sur l'ensemble des protocoles, des outils, etc. Cette première phase a permis à chacun des membres du groupe d'avoir une connaissance beaucoup plus riche dans ce domaine incontournable des réseaux informatiques et des télécommunications.

Outre les nombreuses connaissances techniques apportées par ce travail, nous avons également énormément appris en gestion de projet et travail en équipe. Ce projet nous a permis de nous mettre en exemple de situation réelle et de faire face aux différents problèmes que nous pourrons rencontrer plus tard. Notamment les divergences d'opinions dans des groupes important en nombre de personne, la difficulté de ne pas avoir la machine à disposition mais de devoir passer par un intermédiaire en exécutant toujours une procédure particulière pour effectuer une action (ex : installation de paquet).
De plus, nous avons pu également aborder les différents problèmes de communications entre le client et la société prestataire de service.

Pour conclure, malgré les nombreux problèmes auxquels nous avons du faire face en travaillant sur ce projet, celui-ci nous a permis d'enrichir nos connaissances techniques d'une part, de travailler sur un projet concret sur du long terme, avec des équipes conséquentes, mais également d'aborder différents aspects liés au projet hors compétences techniques (gestion du projet, planification, réunions, aspects humains, etc.)

5. IPS / IDS

La sécurisation des systèmes informatiques revêt aujourd'hui un caractère important du fait de la multiplicité des virus, des chevaux de Troie, et bien d'autres vulnérabilités auxquelles un système d'information est exposé.

D'où l'idée de la mise en place d'un outil de détection d'intrusion s'avère très importante. Appelé aussi IDS (Intrusion Detection System), un système de détection d'intrusion est un logiciel capable de remonter les différentes anomalies dans le trafic du réseau. Son rôle est de surveiller, contrôler et détecter les attaques menées à l'encontre du réseau.

Un IDS journalise les événement grâce à un fichier log (source d'informations et vision des menaces courantes), averti le système via un message SNMP et amorce certaines actions sur le réseau ou sur l'hôte.

Il existe deux principaux types d'IDS :

– HIDS (Host IDS) : Basé dans un ordinateur

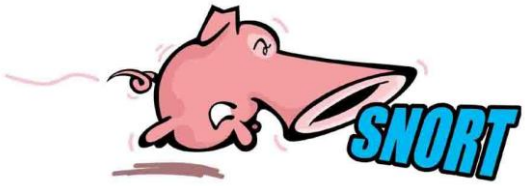
- Permet de surveiller le système et les applications
  - – Les journaux systèmes
  - – de contrôler l'accès aux appels systèmes
  - – de vérifier l'intégrité des systèmes de fichiers
- Le HIDS à accès à des composants non accessibles sur le réseau
  - – Exemple : la base de registre de Windows
- Ne surveille qu'un seul hôte

– NIDS (Network IDS) : Un sonde placée dans le réseau

- Surveille l'ensemble du réseau
- Capture et analyse tout le trafic
- Recherche de paquets suspects
  - Contenu des données
  - Adresses IP ou MAC source ou destination
  - …
- Envoi d'alertes

Dans le cas de notre groupe, nous serons amenés à étudier et analyser les techniques de sécurisation du parc informatique et de leur apporter notre expertise par la proposition d'une solution IDS hybride (NIDS couplée à des HIDS) : Prelude. Cette solution utilise un IDS bien connu dans le domaine : SNORT.

a. SNORT



Snort est un système de détection d'intrusion libre (ou NIDS) publié sous licence GNU GPL. En effet, ce système de détection d'intrusion léger peut « logger » les paquets arrivant sur notre réseau et peut être utilisé sur les petits réseaux, alors que sur les plus grands (Gigabit Ethernet), snort devient peu fiable. À l'origine écrit par Martin Roesch, il appartient actuellement à Sourcefire.

Les règles sont quotidiennement mises à jour avec l'apparition de nouvelles attaques. Snort est disponible pour Unix comme pour Windows.

Snort peut être lancé en quatre modes:

- mode sniffer:	**Snort va lire le trafic réseau et le montrer à l'écran.**
- mode packet logger:	Snort va enregistrer le trafic réseau sur un fichier.
- mode IDS:	Le trafic réseau correspondant aux règles de sécurité sera enregistré. (mode utilisé dans notre tutorial)
- mode IPS:	Aussi connu sous le nom de snort-inline (IPS= Intrusion Prevention System)

Intérêts d'un IDS :

Plusieurs fois, il est beaucoup trop facile pour les pirates informatiques d'analyser notre réseau pour les services vulnérables qui pourraient être en cours d'exécution ou scanner les ports qui sont disponibles.

Par conséquent, il ne faut pas ignorer la sécurité quand la mise en place de la détection d'intrusion est si facile à faire.

Snort permet de surveiller notre réseau interne. En effet, la majeure partie des problèmes de sécurité viennent en fait de l'intérieur de notre réseau et dans ce cas, cet outil est gratuit et disponible sur la plupart des plates-formes.

Sans IDS, comment détecter une attaque ?

- **Firewalls ?**
  - La plupart des attaques sont des attaques sur des flux applicatifs.
- **Logs systèmes ?**
  - Trop verbeux.
  - Ne remonte pas tout.
  - Éparpillés sur des dizaines de serveurs.
  - Plutôt adapté au « post mortem ».
- **Pourquoi chercher à détecter des attaques ?**

- Pour bloquer un attaquant avant qu'il ne réussisse
- Savoir ce qui est attaqué (et donc ce sur quoi mettre des moyens en terme de protection).
- Pour analyse « Post mortem ».

Quand dois-je utiliser snort :

Snort peut être utilisé à tout moment si on désire prendre des mesures de sécurité de base qui nous permettent d'enregistrer et d'analyser le trafic sur notre réseau. Avec un pare-feu ce devrait être un autre élément fondamental de notre réseau de sécurité.

Plateformes qui fonctionnent avec SNORT :

x86	Sparc	M68k/PPC	Alpha	Other	
X	X	X	X	X	Linux
X	X	X			OpenBSD
X			X		FreeBSD
X		X			NetBSD
X	X				Solaris
	X				SunOS 4.1.X
				X	HP-UX
				X	AIX
				X	IRIX
			X		Tru64
		X			MacOS X Server

Où positionner son IDS ?

Il existe plusieurs endroits où il est possible de placer un IDS. Le schéma suivant illustre un réseau local ainsi que les trois positions que peut y prendre un IDS :

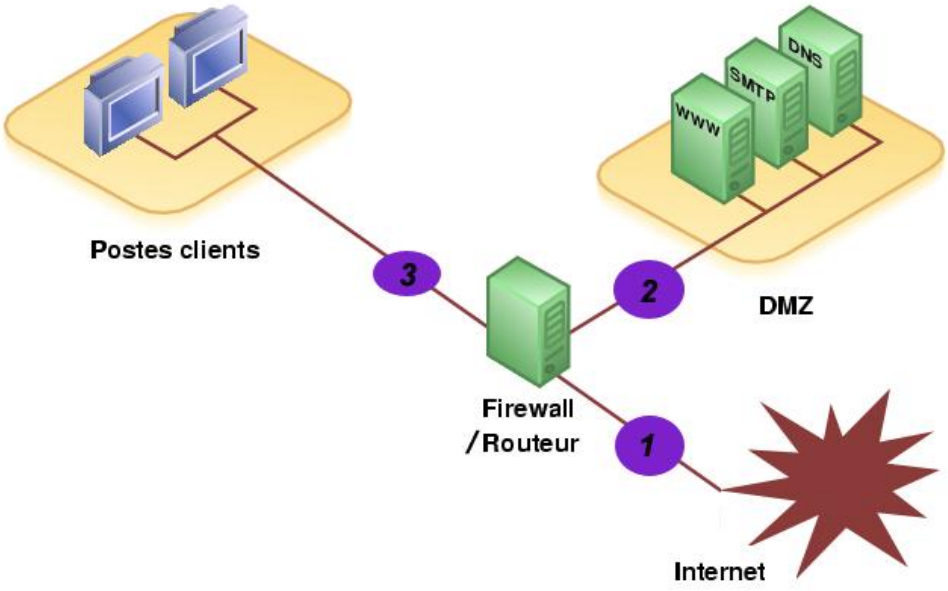


Figure 24 - Intégration d'un IDS

Position (1) :

Sur cette position, l'IDS peut détecter l'ensemble des attaques provenant de l'extérieur, avant le firewall. Ainsi, beaucoup) d'alertes seront remontées dans les logs ce qui les rendra plus difficile à analyser.

Position (2) :

Si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter mais difficile à interpreter.

Position (3) :

L'IDS peut ici rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur.

Idéalement, on placerait des IDS sur les trois positions puis on délèguerait la consultation des logs à l'application "acid" qui permet d'analyser les alertes et d'en présenter clairement les résultats via une interface web complète. Si une seule machine peut être déployée, autant la mettre sur la position 2, crutiale pour le bons fonctionnement des services.

Avantages/Inconvénients

SNORT	
Avantages	**Inconvénients**

• Open Source,
• Large communauté d'utilisateurs
  ○ Beaucoup de contributions
  ○ Beaucoup de documentations
• Bonne base de signatures
  ○ Mise à jour
  ○ Modifiable
• Nouvelles règles très régulièrement proposées
• Nombreux plugins, frontends, consoles de management, ...
• Mise en oeuvre basique rapide
• Beaucoup de documentations
• Fichiers d'alertes très complets (header des paquets, lien vers description de l'attaque...)
	• Technologie complexe
	• Nécessite un degré d'expertise élevé
	• Long à optimiser
	• Réputer pour générer de fausses alertes
	• Encore immature
	• Configuration essentiellement par édition de fichiers texte
	• De nombreuses fonctionnalités payantes

b. Le SIEM Prelude

Prelude est un SIEM (Security Event Information Management). Ces solutions ont pour objectif d'effectuer des corrélations entre les alertes remontées par les IDS du réseau (ici SNORT) et les diverses sources d'informations collectées sur le réseau (informations provenant du système de supervision du réseau, des firewalls, des routeurs, etc...). Voici l'architecture retenue pour ce projet :

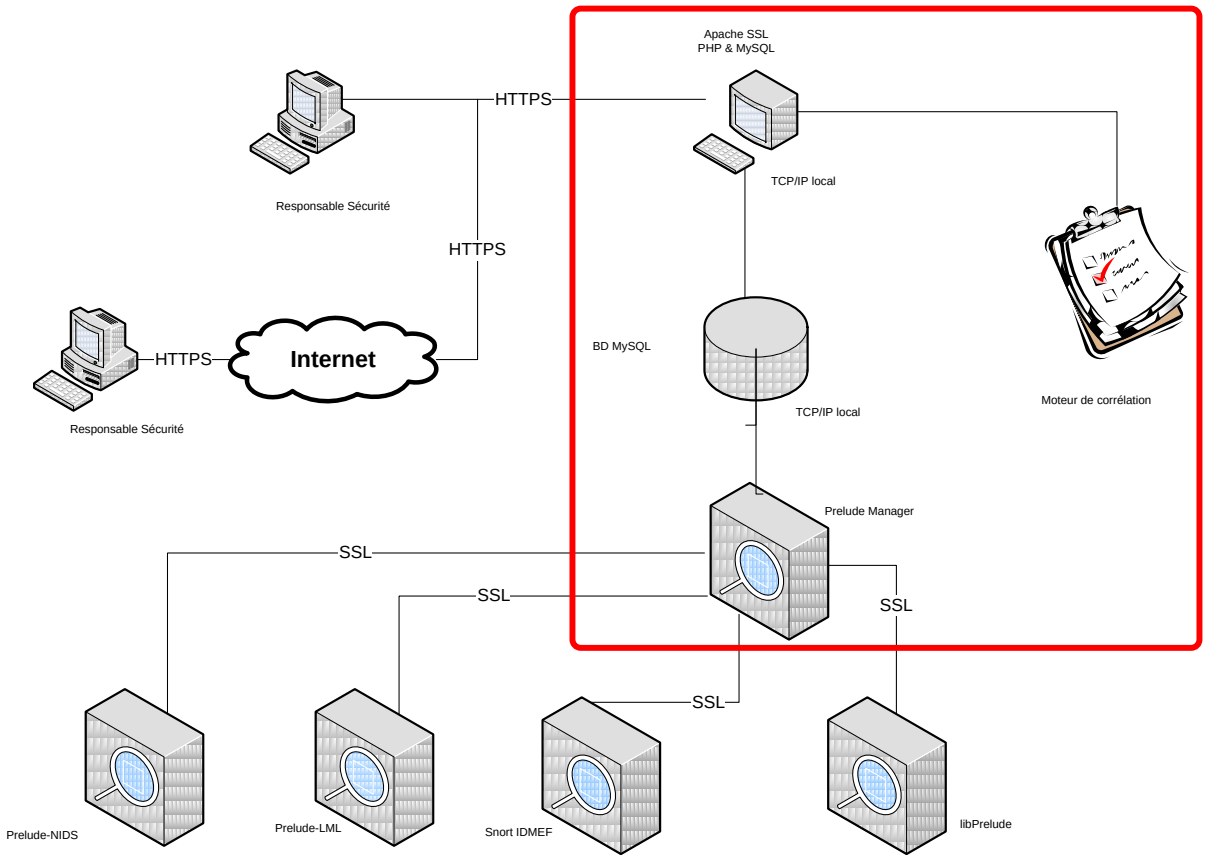


Figure 25 - Architecture Prelude

En effet, Prelude est un système de détection d'intrusions et d'anomalies distribué sous licence GPL. Nous disposons d'une seule machine virtuelle afin d'installer les divers composants de Prelude. Nous allons maintenant vous expliquer l'utilité de ces différents composants dans l'architecture décrite précédemment :

- Le ***manager*** permet de gérer des sondes installées sur le parc de machines, en effet il accepte les connexions des différents capteurs et collecte les différentes alertes.

- Le ***moteur de corrélation*** sert, quant à lui, à analyser les différentes alertes remontées par les sondes (NIDS et HIDS) afin d'en augmenter le niveau de pertinence ainsi que de faire ressortir parmi ces dernières les attaques menées contre le système d'information. En effet, il ne fournit au « Responsable de la Sécurité » que les événements utiles.

- La ***base de données de journalisation*** des alertes après que l'analyse par le moteur de corrélation soit réalisée.

- Le ***serveur web d'administration graphique*** sécurisé (https) est une interface de visualisation des alertes journalisées dans une base de données qui permet aux administrateurs du système d'information de posséder un outil leur permettant de déceler plus rapidement les tentatives d'intrusions.

Voici quelques avantages de Prelude en tant qu'IDS :

- Interopérabilité avec tout système envoyant des évènements (logiciel ou matériel)
- facilité d'ajout de nouvelles signatures d'application
- respect des standards (IDMEF, CEF, etc.) afin de permettre sa connexion à des outils tiers
- capacité à évoluer avec l'infrastructure
- corrélateur ouvert pouvant accéder à d'autres systèmes ou sources d'informations
- console de management centralisé multi-niveaux
- déploiement non intrusif
- protection des échanges par connexions chiffrées entre les agents
- collecter des informations sous tous formats (logs et autres)
- corrélateur d'évènements en temps réel

c. Module Apache mod_security

Mod_security est un module permettant de contrôler finement les échanges entre le serveur Apache et le client. Il filtre et journalise ces échanges. Ce module nous aidera donc à stopper les injections de type SQL, le cross-site scripting et d'autres attaques web par l'intermédiaire de données corrompues.

Apache permet déjà de filtrer les requêtes HTTP mod_security va beaucoup plus loin en travaillant également sur les réponses HTTP et en permettant une analyse beaucoup plus étendue des requêtes. Il est également capable de filtrer les flux HTTPS et corriger les URL mal formées.

Pour cela, ce module s'intègre avant le traitement normal des requêtes par Apache.

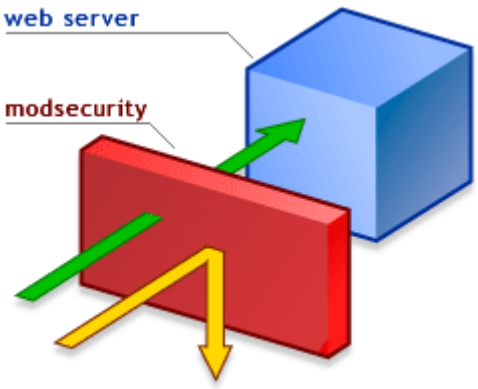


Figure 26 - Principe du module "modsecurity"

Ce module permet de filtrer beaucoup de choses intéressantes :

- Détecter les injections SQL

- Bloquer l'accès aux fichiers passwd, shadow
- Interdire les commandes systèmes (ls, wget, etc…)
- Interdire la méthode TRACE
- Empêcher une attaque transversale de répertoire
- Bloquer le bot DTS Agent

- Interdire le HTML et le Javascript dans les requêtes
- Etc…

La configuration de celui-ci est très simple, il suffit d'ajouter les règles souhaitées dans la configuration de nos « virtualhost » d'Apache. (ex : « SecFilter "delete[[:space:]]+from" » => empêche les delete).

Ce module Apache est donc très intéressant à mettre en œuvre mais il faut cependant faire attention à sa configuration pour ne pas qu'il bloque certaines requêtes censées être autorisées.

Contexte du projet :

L'entreprise Aerodef disposant d'un serveur web Apache avec un site internet mis en ligne à disposition des attaquants, nous leur avons demandé de mettre en place ce module avant d'améliorer la sécurité de leur site WEB afin d'empêcher les différentes attaques présentées dans le paragraphe précédent.

Sur ce point Aerodef ne nous a pas écouté ou n'a tout simplement pas eu le temps de mettre ce module en place. Nous n'avons pas eu plus d'informations à ce sujet.

La détection d'intrusion est actuellement au stade d'expérimental. L'investissement nécessaire vis à vis des résultats obtenus n'est pas des plus satisfaisants :

- grand nombre de faux positifs
- les faux négatifs sont très dangereux

Les HIDS, IDS installés sur les machines du parc informatique ne remontent pas

d'informations suffisamment pertinentes et donc ce ne peuvent pas être considérés comme des solutions fiables.

D'autre part le mécanisme alerte / action des Intrusions Prevention System, c'est à dire que le déclenchement d'une alerte entraine une action sur le Système d'information, par exemple la reconfiguration des règles du pare-feu de l'entreprise se révèle être un mécanisme assez dangereux. Effectivement, si l'IPS lève à tort une alerte concernant une machine du parc informatique le pare-feu est alors reconfiguré pour bloquer cette machine identifiée comme appartenant à un botnet.

En outre, les SIEM ont pour objectif d'effectuer des corrélations entre les alertes remontées par les IDS du réseau et les diverses sources d'informations collectées sur le réseau (informations provenant du système de supervision du réseau, des firewalls, des routeurs, etc...). Ce sont des logiciels assez imposants autant en configuration qu'en maintenance et dont les résultats qu'ils délivrent ne sont pas encore éprouvés. Tout comme la détection d'intrusion, les SIEM sont encore au stade d'expérimentation, bien que des solutions commerciales existent.

Malgré tout, il est utile de suivre les évolutions dans le domaine de la détection d'intrusion et en cela d'intégrer un IDS dans son réseau local. L'objectif étant alors de s'en servir comme source d'informations supplémentaires pour la surveillance du réseau d'entreprise tout en gardant un recul sur ce type de système

6. Nessus

Nessus est un outil de sécurité informatique. Il signale les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres :

- les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles (lecture de fichiers confidentiels par exemple), des dénis de service...
- les fautes de configuration (relais de messagerie ouvert par exemple)
- les patchs de sécurité non appliqués, que les failles corrigées soient exploitables ou non dans la configuration testée
- les mots de passe par défaut, quelques mots de passe communs, et l'absence de mots de passe sur certains comptes systèmes. Nessus peut aussi appeler le programme externe Hydra pour attaquer les mots de passe à l'aide d'un dictionnaire.
- les services jugés *faibles* (on suggère par exemple de remplacer Telnet par SSH)
- les dénis de service contre la pile TCP/IP

La séquence des opérations est la suivante (liste non exhaustive):

- détection des machines vivantes sur le réseau
- « scan » des ports avec un des quatre ports scanners internes, ou un scanner externe.

- récupération d'informations
  - type et version des divers services
  - Connexion (SSH, Telnet ou rsh) pour récupérer la liste des packages installés

Le logiciel client standard peut exporter les données sous divers formats. Outre les failles, Nessus présente également diverses informations utiles à un auditeur comme la version des services ou de l'OS.

Dans le cadre du projet, la société AeroDef ne souhaitait pas que l'on utilise ce logiciel car elle le jugeait trop agressif et pouvait entrainer des disfonctionnements sur leur SI. De ce fait, aucun scan n'a été réalisé sur leur réseau, ce qui aurait permis d'identifier de nombreuses failles.

VI. VOIP et Téléphonie

1. Installation du serveur Astérisk

a. Récupération de la dernière version d'Asterisk

Il est important de télécharger la toute dernière version d'Asterisk pour éviter au maximum tous risques d'attaques concernant d'éventuelles failles de sécurité.

La dernière version d'Asterisk se récupère à l'adresse suivante :
http://www.asterisk.org/downloads/asterisk/releases/asterisk-1.6.2-current.tar.gz

Pour charger sur la distribution Debian le fichier Tar.gz d'Asterisk, on réalise la commande suivante :

```
wget http://www.asterisk.org/downloads/asterisk/releases/asterisk-1.6.2-current.tar.gz
```

Il faut ensuite décompresser l'archive à l'aide de la commande suivante :

```
tar zxvf asterisk-1.6.2-current.tar.gz
```

b. Installation d'Asterisk

On peut à présent installer notre serveur Asterisk.

```
./configure
make menuselect (optionnel)
make
make install
make config
make samples
```

Remarque:

L'inconvénient d'installer Asterisk directement depuis un fichier taz.gz (et non pas via un package) est qu'AUCUNE dépendance est gérer. Il faut installer au préalable tous les paquets nécessaires au bon fonctionnement d'Asterisk.
Voici l'ensemble des paquets à installer (avant l'installation d'Asterisk) :

```
apt-get install libncurses5-dev bison libssl-dev libcap-dev libnewt-dev zlib1g-dev procps gcc g++ make binutils doxygen
```

Le serveur Asterisk se lance à l'aide de la commande suivante :

```
/etc/init.d/asterisk start
```

Ensuite, une commande CLI dédié au serveur est disponible. Elle va permettre d'obtenir de nombreuses informations comme le nombre de personnes enregistrés, les appels en cours, etc …

Voici la commande pour lancer la console CLI :

```
asterisk –rvvvvvvvvv
```

-*r :* reload
- *v* : mode verbose. Plus il ya de « v », plus le serveur sera « parlant »

2. Configuration du serveur Astérisk

a. Création de deux comptes SIP pour Xlite

La création d'utilisateur SIP se réalise dans le fichier sip.conf (*/etc/asterisk/sip.conf*)

```
[general]
context=default          ; Default context for incoming calls
allowoverlap=no
bindport=5060     // Mise en écoute du serveur sur le port 5060 (SIP)
bindaddr=0.0.0.0 // Le serveur écoute sur toutes les interfaces
```

```
srvlookup=yes
qualify=yes
nat=yes

[Tristan]
type=friend
host=dynamic       // Allocation dynamique d'une adresse IP
username=Tristan  // Nom d'utilisateur
secret=tristan_VOIP   // Mot de passe
callerid="Tristan" <100>  // Identifiant d'appel
language=fr
context=local  // Context local ➔ Voir fichier extensions.conf

[Goulven]
type=friend
host=dynamic
username=Goulven
secret=goulven_VOIP
callerid="Goulven" <101>
langage=fr
context=local

[Mederic]
type=friend
host=dynamic
username=Mederic
secret=mederic_VOIP
callerid="Mederic" <102>
langage=fr
context=local

[Laurent]
type=friend
host=dynamic
username=Laurent
secret=laurent_@udit
callerid="Laurent" <103>
language=fr
```

Il faut également définir un plan de numérotation. Celui-ci se gère dans le fichier extentions.conf (*/etc/asterisk/extentions.conf*)

```
; extensions.conf - the Asterisk dial plan
[general]
;
static=yes
writeprotect=no
;autofallthrough=no
;extenpatternmatchnew=no
;
clearglobalvars=no
```

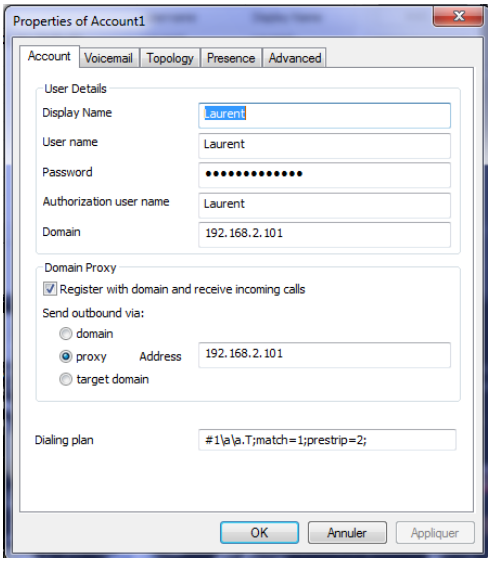
```
;priorityjumping=yes
;userscontext=default
[globals]
CONSOLE=Console/dsp                    ; Console interface for demo
;CONSOLE=DAHDI/1
;CONSOLE=Phone/phone0
IAXINFO=guest                          ; IAXtel username/password
;IAXINFO=myuser:mypass
TRUNK=DAHDI/G2                         ; Trunk interface


[local]   // Context " local"

exten => 100,1,Dial(SIP/Tristan) // Si on compose le N°101 alors on appel l'utilisateur Tristan
exten => 101,1,Dial(SIP/Goulven)
exten => 102,1,Dial(SIP/Mederic)
exten => 103,1,Dial(SIP/Laurent)
exten => 104,1,Dial(SIP/Thomas)
exten => 105,1,Dial(SIP/Nat)
exten => 106,1,Dial(SIP/Lise)
```

b. Configuration de Xlite

Une fois la déclaration des utilisateurs SIP réalisé sur l'Asterisk, il ne reste plus qu'a configurer le softphone Asterisk.



Display Name : Nom affiché sur l'interface Xlite
User name : Numéro de l'utilisateur
Password : Mot de passe du compte utilisateur
Authorization user name : Nom de l'utilisateur
Domain : Adresse IP du serveur Asterisk **: 192.168.2.101**

Proxy : Adresse IP du serveur Asterisk : **192.168.2.101**

Une procédure de configuration des téléphones Xlite a été remise à l'équipe Défense afin qu'elle puisse configurer plus facilement ce softphone sur leurs équipements.

Vérifier le bon enregistrement d'un client Xlite

Pour vérifier l'enregistrement d'un client SIP, on utilise la CLI. Voici la commande à exécuter :

sip show peers

```
auditor@asterix: ~
asterix:/home/auditor# asterisk -r
Asterisk 1.6.2.13, Copyright (C) 1999 - 2010 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for detail
s.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
  == Parsing '/etc/asterisk/extconfig.conf': Parsing /etc/asterisk/extconfig.con
f
  == Found
Connected to Asterisk 1.6.2.13 currently running on asterix (pid = 1960)
Verbosity is at least 9
Core debug is at least 9
    -- Remote UNIX connection
asterix*CLI> sip show pee
peers  peer
asterix*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
Goulven/Goulven            (Unspecified)    D   N      5060     UNKNOWN
Laurent/Laurent            (Unspecified)    D   N      5060     UNKNOWN
Lise/Lise                  (Unspecified)    D   N      5060     UNKNOWN
Mederic/Mederic            (Unspecified)    D   N      5060     UNKNOWN
Nat/Nat                    (Unspecified)    D   N      5060     UNKNOWN
Thomas/Thomas              (Unspecified)    D   N      5060     UNKNOWN
Tristan/Tristan            192.168.2.8      D   N      17056    OK (112 ms)
7 sip peers [Monitored: 1 online, 6 offline Unmonitored: 0 online, 0 offline]
asterix*CLI>
```

On constate sur cette capture d'écran que l'utilisateur « Tristan » est connecté au serveur Asterisk avec l'adresse IP 192.18.2.8

c. Passage du serveur Asterisk sous un autre user

Pour réaliser cela, il suffit de taper les commandes suivantes :
(Un groupe et un utilisateur Asterisk ont été crée automatiquement lors de l'installation de ce dernier)

```
/etc/init.d/asterisk stop
chown --recursive asterisk:asterisk /var/lib/asterisk
chown --recursive asterisk:asterisk /var/log/asterisk
chown --recursive asterisk:asterisk /var/run/asterisk
chown --recursive asterisk:asterisk /var/spool/asterisk
chown --recursive asterisk:asterisk /usr/lib/asterisk
chown --recursive asterisk:asterisk /dev/dahdi
chmod --recursive u=rwX,g=rX,o= /var/lib/asterisk
chmod --recursive u=rwX,g=rX,o= /var/log/asterisk
chmod --recursive u=rwX,g=rX,o= /var/run/asterisk
chmod --recursive u=rwX,g=rX,o= /var/spool/asterisk
chmod --recursive u=rwX,g=rX,o= /usr/lib/asterisk
chmod --recursive u=rwX,g=rX,o= /dev/dahdi
chown --recursive root:asterisk /etc/asterisk
chmod --recursive u=rwX,g=rX,o= /etc/asterisk
cp /etc/asterisk/asterisk.conf /etc/asterisk/asterisk.conf.org
vi /etc/asterisk/asterisk.conf
# Modifiez la ligne suivante :
#
# astrundir => /var/run
#
# par
#
# astrundir => /var/run/asterisk
#
#--------------------------------------------------
cp /etc/init.d/asterisk /etc/init.d/asterisk.org
#--------------------------------------------------
vi /etc/init.d/asterisk
#
# Modifiez la ligne suivante :
#
# #AST_USER="asterisk"
# #AST_GROUP="asterisk"
#
# par
#
# AST_USER="asterisk"
```

 # AST_GROUP="asterisk"
#
#--
chmod g+w /etc/asterisk/voicemail.conf
chmod g+w,+t /etc/asterisk
/etc/init.d/asterisk restart

d. Filtrage des flux de la TOIP

L'un des problèmes essentiels inhérents aux protocoles de signalisation réside dans le filtrage des flux. Très souvent, les entreprises utilisent des mécanismes de translations d'adresses (NAT), lesquels sont incompatibles avec les traitements appliqués sur les flux multimédias.

Le problème de la VOIP est que les trames RTP n'ont pas de numéros de port prédéfinis. Les numéros de port du RTP sont totalement aléatoires et changent à chaque nouvelle communication. Il est donc très difficile de passer les pare feux pour un flux RTP.

Fort heureusement il existe plusieurs solutions pour palier à ce problème.

Il est possible de fixer une plage de port RTP sur l'Asterisk. On peut par exemple définir sur l'asterisk une plage de port entre 3000 et 3100. Toutes les communications RPT entre l'asterisk et le téléphone se réaliseront dans cette plage. Il ne reste plus qu'a autoriser cette plage de ports sur pare feu. C'est la solution que nous avons mis en œuvre en TP.

Une autre solution beaucoup plus poussé et intéressante consiste à utiliser un filtrage applicatif.

Présentation général du filtrage applicatif de données

Pour opérer les modifications d'adresses IP et de ports requises par la translation d'adresse, le boitier NAT doit impérativement connaitre le format et la syntaxe des protocoles sous-jacents. Les protocoles utilisés dans les couches basses de la communication réseau sont généralement classiques. Pour l'adressage IP, il s'agit du protocole IP (couche de niveau réseau); pour le port, il s'agit du protocole TCP ou UDP (couche de niveau transport). La majorité des flux sont donc reconnus et peuvent être traités .On peut généraliser cette idée. En connaissant les spécificités d'un protocole, on peut opérer exactement les mêmes modifications que celles effectués avec le NAT pour l'adresse IP et le port. Même si le problème est plus complexe, puisqu'il existe de nombreux protocoles, cette solution demeure parfaitement fonctionnelle. Ainsi, le boitier NAT ne supporte plus uniquement les fonctionnalités de NAT classiques, mais est en plus capable d'analyser les flux pour déterminer quels sont les protocoles utilisés. En connaissant la syntaxe de ces protocoles, le boitier peut effectuer toutes les modifications nécessaires.

La réponse apportée dans ce cadre est donc une solution de filtrage de tous les protocoles utilisés par les applications qui posent des problèmes de NAT.

Les passerelles de niveau applicatif

Une nouvelle gamme de passerelles multimédias a été mise au point pour permettre la reconnaissance des flux. Appelées ALG (Application Layer Gateway), ces passerelles sont proposées dans un grand nombre de solutions commerciales, embarquées le plus souvent au sein d'un pare-feu. Les flux sont filtrés, et, s'ils sont reconnus, les modifications nécessaires au bon fonctionnement du NAT sont opérées parallèlement à l'autorisation accordée à ces flux de traverser le pare-feu.

C'est dans cet esprit que le projet libre Netfilter sous Linux propose la reconnaissance d'un très grand nombre de protocoles, des couches basses aux couches les plus hautes. Les modules de reconnaissance sont également disponibles pour le protocole H.323 (modules ip_conntrack_h323 et ip_nat-H323), ainsi que pour le protocole SIP (module SIP et NAT ip_conntrack_sip et ip_nat_sip). Deux modules sont nécessaires, le premier (ip_conntrack) réalisant le suivi de connexion (car les flux utilisent des ports dynamiques qui doivent être détectés durant la communication) et le second (ip_nat) réalisant la translation d'adresse.

La Technologie Netfilter est accessible par défaut dans toutes les distributions actuelles de Linux, par le biais de la commande iptables. Elle est fournie avec un ensemble de filtres pour la reconnaissance des protocoles les plus standards.

L'application n'a pas à modifier la structure des paquets envoyés. Le pare-feu se charge en émission (du réseau local vers le réseau Internet) de les rendre valides et en réception (du réseau Internet vers le réseau local) de les distribuer au terminal adéquat.

Le NAT à une tache beaucoup plus lourde à accomplir puisqu'il doit filtrer des protocoles complexes, de niveau applicatif, ce qui réclame des ressources de traitement importantes.

Dans notre cas, si nous devions utiliser ce principe il faudrait mettre en place sur le pare feu de la défense le module « *ip_conntrack_sip* ». Ce module aura pour but d'aller lire dans le champ SDP des trames SIP les numéros de ports RTP défini pour la communication. Le module n'aura plus qu'à ouvrir dynamiquement les ports RTP en conséquence.

Source: Livre « *Téléphonie sur IP* » de Laurent Ouakil et Guy Pujolle

e. Etude pour 40 postes

Le groupe défense nous a demandé d'évaluer la métrologie et le coût concernant le passage à l'échelle de cette solution pour 40 postes.

Les équipements

Concernant les postes téléphoniques à proprement dit, le cout restera intact puisque nous utilisons le softphone gratuit Xlite.
Le serveur Asterisk ne subira également aucune modification hardware car 515 Mo de RAM suffisent largement à le faire fonctionner même avec 40 postes téléphoniques.

Le réseau

Le point crucial dans l'étude réside dans le niveau de bande passante à allouer dans notre LAN et WAN afin que les communications téléphoniques ne soient pas dégradées.
Le LAN de la défense est un réseau à 100 Mbits/s. On décide d'utiliser le codec *G711* sur l'ensemble du parc téléphonique lors d'un appel en interne.
En effet, le codec *G711* nécessite un débit utile de 64 kbit par seconde.
Supposons que 40 personnes appellent en même temps (ce qui est très peu probable), cela donne un débit de :
40*64= 2,560 Mbit/s.
Un réseau de 100Mbits est donc largement suffisant pour accueillir le codec G711 sans rencontrés de saturation.
Ce codec a l'avantage de ne pas compresser la voix. La qualité audio est donc optimale.

Par contre, en ce qui concerne les appels externes, le débit maximal n'est pas le même. On ne connait pas le débit du lien WAN de la défense (aucune information à ce sujet). On suppose que celui-ci est de 2 Mbits et qu'on utilise un trunk SIP vers un opérateur SIP pour réaliser les appels externes. On constate qu'avec l'utilisation du codec *G711*, on pourrait ne pas émettre 20 appels en simultanées : 2,560 Mbit/s de requis pour 2Mbits de bande passante.
Pour résoudre ce problème, il est recommandé d'utiliser le codec *G729* pour les appels externes. Ce codec a la particularité d'utiliser une bande passante faible tout en conservant une qualité audio convenable (moins bonne que celle du *G711*). Il utilise seulement 8 Kbit/s par appel, soit 320Kbit/s pour 40 appels vers l'extérieur. Les 2Mbit/s de lien WAN sont donc suffisant dans ce cas de figure.
Bien sûr, cette étude est fondée uniquement sur des suppositions. Dans un cas réel, il faudrait réaliser une étude sérieuse afin de connaitre le nombre d'appel par jour des employés et déterminer la durée moyenne que passe l'employé au téléphone. Grâce à toutes ces informations, il est possible de calculer l'erlang. L'erlang est une unité de mesure d'intensité du trafic téléphonique. Elle mesure le nombre de sessions de communication et leur durée sur une période donnée. 1 erlang correspond à l'occupation maximale sur une ligne ne permettant qu'une communication téléphonique.

3. Listes des attaques réalisables et solutions pour les contrer

a. Les attaques réalisables

Déni de Service (DOS)

Le Déni de service (DoS) sur VoIP qui consiste à lancer une multitude de requêtes, « flooding SIP », « TCP syn » ou « UDP », (par exemple, demandes d'enregistrement et d'appels...) jusqu'à saturation des services VoIP. Ces types d'attaques ciblent souvent les serveurs, les passerelles, les proxys ou encore les téléphones IP qui voient leurs ressources sont rapidement épuisées par ces requêtes dont l'objectif est de perturber voire mettre hors service le système ciblé.

Manipulation du stream RTP et SIP :

1. La manipulation du contenu multimédia et des signaux est une attaque qui permet d'injecter un fichier son dans un flux RTP par le biais d'une attaque « RTP Insertsound ».

2. Raccrochage (BYE) : Une autre attaque également répandue consiste à envoyer des commandes « BYE » au téléphone afin de mettre fin à la conversation en cours...

Relecture

Attaque par « relecture » ou « Détournement d'enregistrement » de sessions autorisées obtenues grâce à une analyse de trame par un « sniffer » sur le réseau ou par interception de trafic. Cette attaque se déroule au niveau du protocole SIP, elle utilise la commande « Register » qui sert à localiser un utilisateur par rapport à son adresse IP. Le pirate peut alors rejouer ces sessions de « register » valide en modifiant uniquement l'adresse IP de destination en sa faveur...Cette attaque est due au fait que le protocole SIP transite une partie des informations en clair, il est donc possible de mettre en place du SIPS qui intègre des mécanismes d'authentification et assure l'intégrité des données.

Man In the Middle :

Le « Man in the Middle » (figure 3 : exemple d'échange protocolaire) (MITM) est une des attaques les plus connues ; elle permet à l'assaillant de se positionner entre le client et le serveur afin d'intercepter les flux ciblés qui sont échangés. Le pirate usurpe alors l'adresse MAC (spoof MAC) de ces 2 parties par l'empoisonnement du cache ARP des switches (ex: Ettercap + plugin «chk_poisoning ». Autre exemple : arpspoof (dsniff) ou arp-sk) afin d'être transparent dans ces échanges.

Envoi de requêtes ARP falsifiées. Répondant aux requêtes ARP en se faisant passer pour la cible ou les cibles. Emettant de messages ARP gratuitous.

Les données transitent alors au travers du système pirate. Dans le cas de la ToIP cette technique est utilisée pour « l'Eavesdropping » («Oreille indiscrète ») lui permettant ainsi d'écouter et d'enregistrer les conversations entre les interlocuteurs mais aussi de récupérer un ensemble d'informations confidentielles. Cette technique est aussi utilisée pour d'autres protocoles (SSL, DNS, SSH...).

Ecoute et analyse des flux RTP :

Capture de l'échange des trames SIP d'usage avant l'établissement de l'appel, avec en prime le début de la conversation via le protocole de transport, à savoir RTP.

Récupération et cassage des comptes :

Le mode d'authentification des téléphones IP reste somme toute assez basique, puisque certains flux sont en clairs et puisque le challenge est réalisé avec un hash simple en "MD5" et pas de chiffrement... Ce qui renforce l'importance de la politique de mot de passe.

1. Récupération des trames :

Il est facile quand on a capturé les bonnes trames de récupérer les credentials d'un compte SIP, les requêtes REGISTER comportent le numéro d'extension et un hash MD5.

La capture en live de ces sessions d'enregistrement qui se reproduisent par défaut toutes les 3600 secondes est très aisée.

2. Cassae des comptes :

Une suite d'outil existe pour faciliter la vie en extirpant ces informations du fichier de capture.

Puis, on utilise un outil pour lancer un bruteforce sur le hash en utilisant soit l'entrée standard *stdin* ou un dictionnaire.

Usurpation de numéro :

En SIP, les équipements bénéficient d'une réelle intelligence embarquée contrairement aux MGCP par exemple... il est donc possible de demander à un téléphone « d'afficher » lors d'un appel à son destinataire un numéro de téléphone différent du sien. En interne, cela n'a que peu d'effet. Pourtant, une personne pourrait prétendre appeler depuis le centre de sécurité ou le bureau du directeur... et demander l'exécution d'actions particulières par exemple. De l'extérieur, être discret, se faire passer pour quelqu'un autre, ou encore afficher systématiquement pour tous les appels sortants, un numéro tiers pirate (modification sur passerelle ou IPbx). Lorsque les destinataires tenteront de recontacter leurs collègues et/ou partenaires en faisant « BIS » ou rappeler dans l'historique des appels, ils tomberont systématiquement sur le numéro (payant) qui était affiché (ex : 1,4€ par appel).

b. Les attaques Réalisées par nos soins

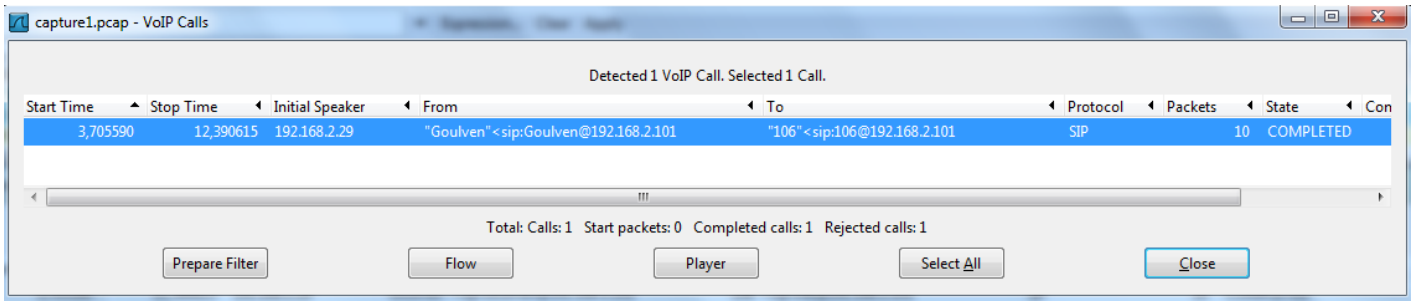
Les captures, effectuées ci-après, ont directement été réalisées sur le serveur Asterisk. Nous aurions pu effectuer ces captures en effectuant au préalable un ArpSpoofing. Cependant, il nous aurait fallu les autorisations de la part d'AeroDef ce qui aurait considérablement allongé les délais de réalisation des démonstrations d'attaques. En effet, le contrat de Voip/Toip ayant été réalisé très tardivement par la société AeroDef, nous ne pouvions plus attendre.

Ecoute et analyse des flux RTP

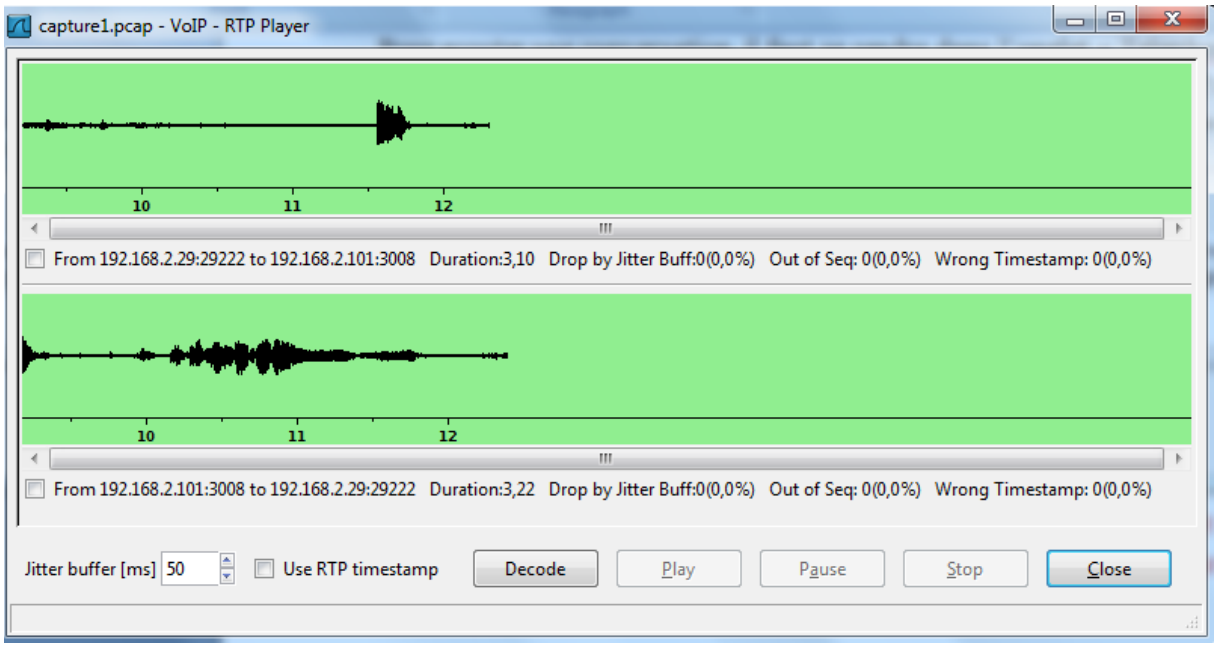
Une fois une communication SIP entre deux téléphones récupérés, il est très facile d'utiliser le logiciel Wireshark pour écouter la conversation.
En effet, Wireshark est capable d'analyser les trames RTP et d'identifier les différents flux de communication.

Ensuite, on peut sélectionner la communication qui nous intéresse et demander à Wireshark de reconstituer la conversation ainsi capturée.
Pour écouter une conversation, il faut se rendre dans l'onglet « *Telephony* » et cliquer sur « *VoIP Calls…* ». Une nouvelle fenêtre s'ouvre listant l'ensemble des conversations VOIP qui ont pu être capturé.

Voici un exemple réalisé en séance de TP :



Dans cette capture, on constate qu'une conversation entre Goulven et le poste 106 a été capturé. Pour l'écouter, il suffit de cliquer sur « *Player* » et un lecteur audio s'ouvre offrant la possibilité d'écouter la conversation.



Récupération et cassage des comptes

Nous avons capturé les paquets envoyés lors de l'établissement de communication entre deux softphone. Nous essayons de récupérer de trouver des comptes analysables.

kami@kami-laptop:~$ sudo sipdump -p/media/TRISTAN/capture recup.dump

SIPdump 0.2 (MaJoMu | www.codito.de)

---

* Using pcap file '/media/TRISTAN/capture' for sniffing

* Starting to sniff with packet filter 'tcp or udp'

* Dumped login from 192.168.2.101 -> 192.168.2.9 (User: 'Mederic')

* Exiting, sniffed 1 logins

On constate ici que nous avons obtenu des informations concernant le softphone utilisé par l'utilisateur « Mederic ».

Nous allons alors tenter de déchiffrer le mot de passe à l'aide d'un dictionnaire disponible sur le site www.authsecu.com. Cependant, le mot de passe que nous avons paramétré est relativement complexe et ne peut se trouver dans un dictionnaire. Cette tentative se solde par un échec.

```
kami@kami-laptop:~$ sudo sipcrack -w francais-divers.txt recup.dump

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------
* Found Accounts:
Num     Server          Client          User    Hash|Password

1       192.168.2.9     192.168.2.101   Mederic
c1c5056882fb8a35e7219571e8eb8c89

2       192.168.2.9     192.168.2.101   Mederic
c1c5056882fb8a35e7219571e8eb8c89

3       192.168.2.9     192.168.2.101   Mederic
c1c5056882fb8a35e7219571e8eb8c89

* Select which entry to crack (1 - 3): 1

* Generating static MD5 hash... 5844aebb38e6df795ca1e5ba8280553c
* Loaded wordlist: 'francais-divers.txt'
        * Starting bruteforce against user 'Mederic' (MD5:
'c1c5056882fb8a35e7219571e8eb8c89')
* Tried 46832 passwords in 0 seconds

* Tried all passwords, no match
```

Nous essayons alors de déchiffrer le mot de passe via la technique de bruteforce. Cependant, cette technique demande une puissance de calcul très importante puisqu'elle teste les nombreuses possibilités de mot de passe et s'avère très longue. Cette tentative se solde également par un échec.

```
kami@kami-laptop:~$ sudo sipcrack -s recup.dump

SIPcrack 0.2  ( MaJoMu | www.codito.de )

----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password


1       192.168.2.9     192.168.2.101   Mederic
c1c5056882fb8a35e7219571e8eb8c89

2       192.168.2.9     192.168.2.101   Mederic
c1c5056882fb8a35e7219571e8eb8c89

3       192.168.2.9     192.168.2.101   Mederic
c1c5056882fb8a35e7219571e8eb8c89


* Select which entry to crack (1 - 3): 3


* Generating static MD5 hash... 5844aebb38e6df795ca1e5ba8280553c

* Type your passwords:

        * Starting bruteforce against user 'Mederic' (MD5:
'c1c5056882fb8a35e7219571e8eb8c89')
```

Le mot de passe que nous avons paramétré s'avère trop complexe pour pouvoir être déchiffré rapidement. On comprend, ici, l'intérêt d'une politique de mot de passe complexe, qui a été recommandée par le service communication dans la charte des utilisateurs.

c. Les parades aux attaques:

Usurpation de numéro :

Des solutions existent en matière de détection d'attaque (IDS/IPS) et/ou de modification suspicieuse sur le protocole ARP avec « Arpwatch » ou « snort », ou mécanisme basique dans le monde du switching comme le « port security » qui limite le nombre d'adresses MAC utilisables par port, ou encore du « 802.1x »...

Parefeu statefull :

Implémenter des pare-feux Statefull « nouvelle génération » avec une reconnaissance protocolaire plus avancée (ADN applicatif...).

Sécurisation des protocoles SIP et RTP :

Sécurisation des protocoles SIP et RTP par l'utilisation de PKI (Public Key Infrastructure) et la mise en place du « SIPS », « SRTP », « SRTCP » utilisant le « DTLS » RFC 4347...

WAN :

Côté WAN, ne jamais exposer son IPBX par une IP Public même « natée », ni en DMZ publique et/ou directement à l'extérieur même un module spécifique à cet usage est proposé, privilégier le mode VPN SSL ou IPSEC par le biais du firewall.

4. Les problèmes rencontrés

a. Communication avec Aerodef

La communication avec Aerodef s'est révélée relativement compliquée. En effet, l'appel d'offre envoyée par Aerodef ne comportait que des informations techniquement faibles. Lors de notre réponse à l'appel d'offre, nous ne possédions pas de schéma détaillé de l'infrastructure. Malgré nos multiples relances pour obtenir un ce schéma (Nat/Pat, Vlans etc...), nous n'avons obtenu qu'un schéma global sans véritable information susceptible de nous intéresser. A ce jour, nous ne possédons d'ailleurs pas ces informations. De plus, Aerodef a mis deux semaines à répondre à notre réponse à l'appel d'offre entrainant un ralentissement dans nos recherches et mise en place de solutions de VOIP.

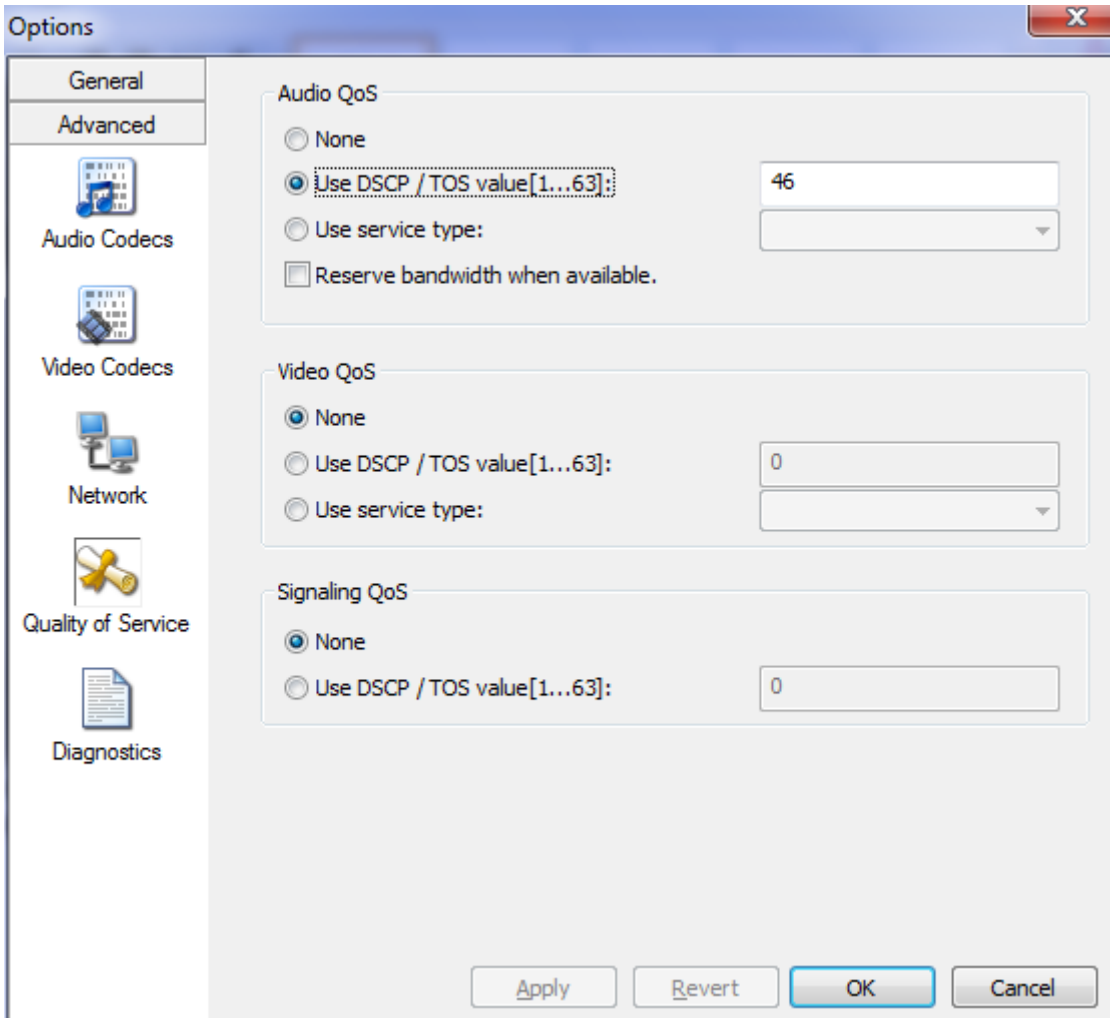
b. Les problèmes techniques

Le softphone Xlite

Le softphone Xlite installé sur l'ordinateur ne permet pas de transmettre directement le trafic voix dans des trames 802.1Q avec l'identifiant du vlan voix approprié (niveau 2 du modèle OSI). Cependant il a été choisi puisqu'il est capable de marquer le champ TOS (ou DSCP) d'un paquet IP (niveau 3 du modèle OSI).

Configuration X-lite pour Tag Vlan

Afin de dissocier les paquets du VLAN « voix » et du VLAN « data », il nous est nécessaire de pouvoir marqué les paquets de Xlite. Pour réaliser ce marquage, il faut aller dans les options puis sélectionner la partie « avancée » et enfin la sous-partie « Qualité de service ». Dans cette partie, on peut paramétrer un champ TOS, champ qui permet de marquer les paquets de la communication, comme vous pourrez le voir ci-après.



Cependant, pour que cela fonctionne, il faut que les paquets puissent être taggués dans VLAN « voix » ensuite par le switch. Cependant, nous n'avons pas trouvé de documentation sur les switchs permettant cela.

C'est pourquoi nous avons utilisé le stratagème présenté au point 3 sur les switchs CISCO.

Configuration des switchs

Nous avions demandé au client Aerodef de bien vouloir nous laisser des accès sur leurs switchs afin de nous permettre de mettre à jour leurs configurations. Le but de ces mises à jour de configurations étaient de permettre le taggage des paquets voix dans le vlan voix.

Malheureusement à ce jour nous n'avons obtenu aucune réponse tant positive que négative. Cependant, à force de persistance, nous avons tout de même obtenu du service réseau d'Aerodef de faire entrer, par un de leur technicien, les commandes présentées dans la figure ci-après dans leurs switchs.

Configuring Ports to Carry Voice Traffic in 802.1Q Frames

Beginning in privileged EXEC mode, follow these steps to configure a port to carry voice traffic in 802.1Q frames for a specific VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mls qos**	Enable QoS for the entire switch.
Step 3	**interface** interface-id	Specify the interface connected to the IP phone, and enter interface configuration mode.
Step 4	**mls qos trust cos**	Classify ingress traffic packets with packet CoS values. For untagged packets, use the port default CoS value.
Step 5	**switchport voice vlan** *vlan-id*	Instruct the Cisco IP Phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP Phone forwards the voice traffic with an 802.1Q priority of 5. Valid VLAN IDs are from 1 to 4094.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** interface-id **switchport** or **show running-config interface** *interface-id*	Verify your voice VLAN entries. Verify your QoS and voice VLAN entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Figure 27 - Commandes de taggage des paquets voix dans vlan voix

Les paquets voix reçus par le switch sont alors directement taggués dans le bon vlan, ici la vlan voix d'Aerodef. Les paquets data quant à eux ne subissent aucune modification et sont taggué suivant la configuration définie par Aerodef dont nous ignorons tout.

Configuration des téléphones CISCO

Lors des séances de TP, nous avions également à disposition 4 téléphones CISCO *7965*.
Malheureusement, ces téléphones IP fonctionnent de base avec le protocole propriétaire *Skinny Call Control Protocol* (SCCP) de Cisco.
Dans un premier temps, nous avons effectué des recherches documentaires pour réaliser une communication en Skinny entre l'Asterisk et le téléphone CISCO. Asterisk gère ce protocole et la configuration se réalise dans le fichier « *skinny.conf* ». Par contre, la configuration de ce fichier est très lourde et assez complexe. Nous n'avons trouvé aucune explication claire à ce sujet.

Après réflexion, on a décidé d'abandonner cette solution et d'essayer de modifier le firmware des téléphones afin qu'ils puissent interpréter le protocole SIP.

Officiellement, il est possible de modifier le firmware du téléphone grâce au Cisco Unified Communications Manager (UCM). L'UCM est le logiciel édité par Cisco qui permet de gérer des appels VOIP. C'est l'UCM qui est capable d'injecter le nouveau firmware dans le téléphone CISCO.

Sans UCM normalement aucune mise à jour n'est possible. Or, nous ne possédons pas d'UCM en salle de TP.
Après des recherches sur internet, certains articles évoquent la possibilité de mettre à jour le téléphone en SIP sans passé par l'UCM.
(http://www.markholloway.com/blog/?p=549)

Cette manipulation se réalise avec un serveur DHCP &TFTP. Nous avons réalisé ces deux serveurs sous la distribution Debian.
Le DHCP doit fournir une adresse IP au téléphone et également indiqué au téléphone l'adresse IP du serveur TFTP. Une fois que le téléphone récupère l'adresse IP du serveur TFTP, il récupère le nouveau firmware présent sur le serveur.
Pour information, le firmware « SIP » est présent sur le site de Cisco.

Une fois les deux serveurs configuré, il faut réaliser une séquence de touche particulière afin que le téléphone démarre et récupère le nouveau firmware. C'est lors de ce démarrage que nous avons rencontré des problèmes.
Le téléphone récupère bien le firmware. Une fois le téléchargement du firmware arrivé à 100% le téléphone redémarre et recommence à nouveau le téléchargement du firmware. Le téléphone tourne en boucle en récupérant à chaque fois le firmware.
Nous n'avons malheureusement pas réussi à résoudre ce problème.

VII. Les étapes du projet

Dans cette partie, nous présenterons les attaques qui ont eu lieu durant ce projet que nous avons pu identifier avec les informations que nous avons :

- Fichier syslog.log du serveur Zeus
- Netflow
- SPAN

1. Première confrontation

Lors de la première confrontation nous n'étions pas opérationnels. En effet, nous n'avons eu accès à la salle que le vendredi en fin d'après-midi (18h00). Cela ne nous a donc pas permis de mettre en place 100% de nos services.

Durant cette confrontation, le réseau a été soumis à deux types d'attaques :

- Exploit PDF sur des postes clients
- DNS Spoofing

a. Exploit PDF

L'utilisation d'exploit est très difficile dans un univers de production. En effet, cela fonctionne très bien sur une maquette car nous contrôlons l'ensemble des paramètres (numéro de version, machine,…). Dans ce cas-là, l'antivirus à directement détecté la menace.

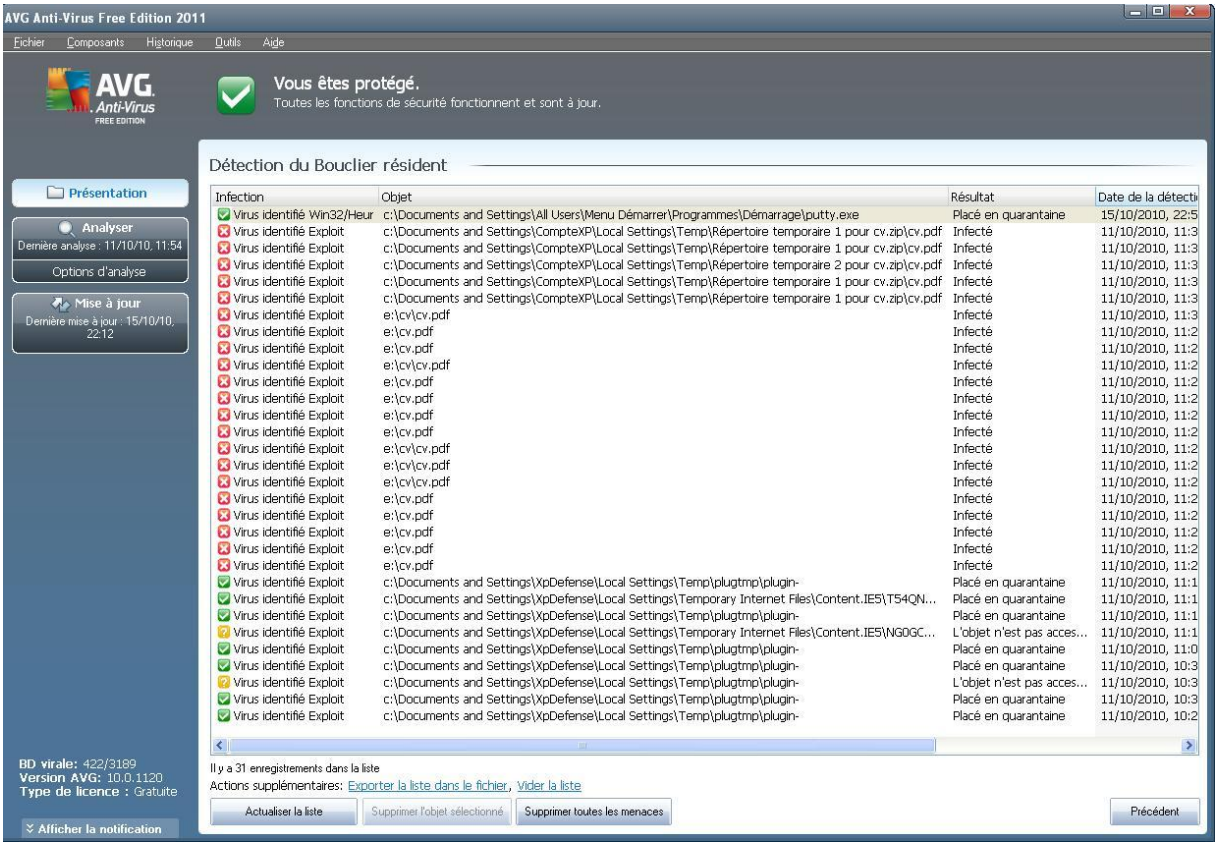


Figure 28 - Détection par AVG du PDF

Le fichier PDF malicieux étant trop chargé en exploit ce qui a eu pour conséquence de « détruire la machine » (elle n'a pu être redémarrée par la suite) au lieu de pouvoir récupérer la main dessus.

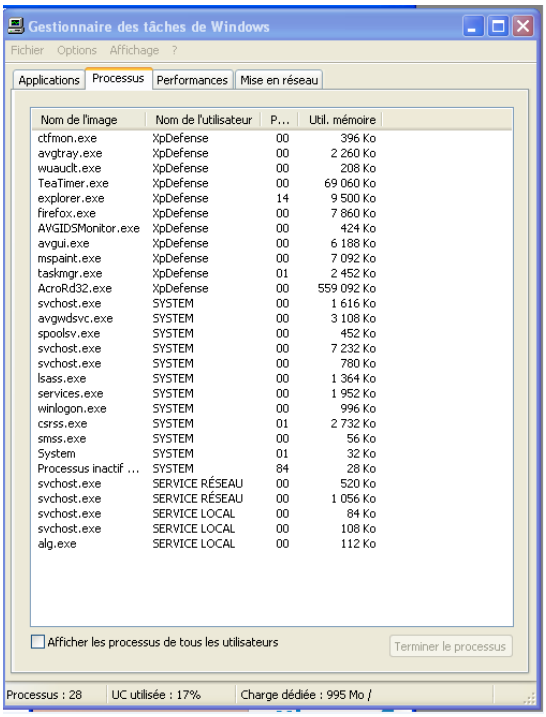


Figure 29 - Gestionnaire de tâche de la machine attaquée

b. DNS Spoofing

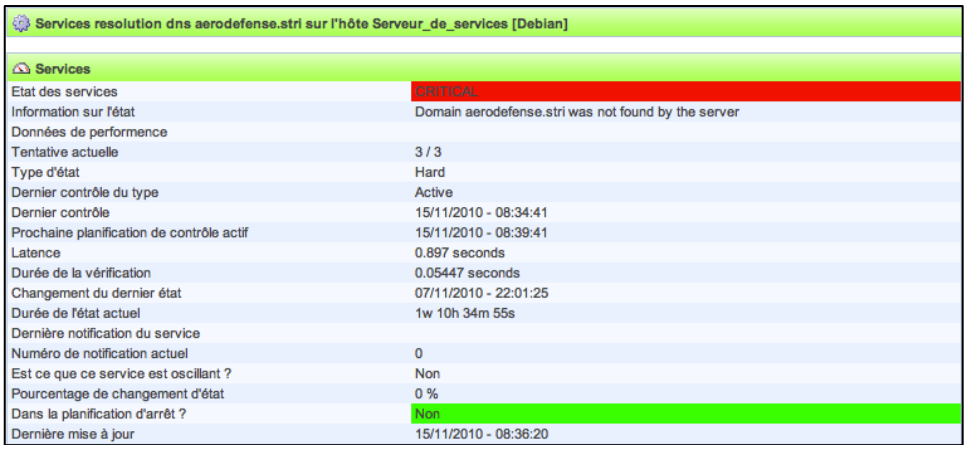
Nous avons été soumis à une attaque de DNS Spoofing durant cette confrontation. Afin de réaliser cette attaque dans le cadre d'une société il faut se placer très précisément dans le réseau. En effet, le principe de cette attaque est que le serveur pirate répond plus rapidement que le vrai serveur.

Dans le contexte d'une société, il faut que le serveur pirate se trouve :

- Soit dans le réseau de l'entreprise ➔ difficile à réaliser si le pirate n'appartient pas à l'entreprise
- Soit en sortie du réseau de l'entreprise dans l'infrastructure de l'opérateur

Le fait que le groupe attaque se trouve sur le même LAN à donc permit de rendre possible cette attaque.

Grâce au plugin NRPE concernant le serveur DNS, nous avons pu détecter qu'un mauvais serveur (autre que celui de la société AéroDef défini dans les paramètres) répondait aux requêtes DNS. L'outil de supervision a permis ici de détecter une attaque par « dns spoofing ».



Services resolution dns aerodefense.stri sur l'hôte Serveur_de_services [Debian]

Services	
Etat des services	CRITICAL
Information sur l'état	Domain aerodefense.stri was not found by the server
Données de performence	
Tentative actuelle	3 / 3
Type d'état	Hard
Dernier contrôle du type	Active
Dernier contrôle	15/11/2010 - 08:34:41
Prochaine planification de contrôle actif	15/11/2010 - 08:39:41
Latence	0.897 seconds
Durée de la vérification	0.05447 seconds
Changement du dernier état	07/11/2010 - 22:01:25
Durée de l'état actuel	1w 10h 34m 55s
Dernière notification du service	
Numéro de notification actuel	0
Est ce que ce service est oscillant ?	Non
Pourcentage de changement d'état	0 %
Dans la planification d'arrêt ?	Non
Dernière mise à jour	15/11/2010 - 08:36:20

Figure 30 - Détection de l'attaque DNS Spoofing

L'attaque se traduit de la manière suivant :

Oct 11 11:45:25 192.168.2.254 2635: Oct 11 11:45:42.495: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.3.1:1030) -- responder (172.30.0.1:53)
Oct 11 11:45:25 192.168.2.254 2636: Oct 11 11:45:42.583: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.3.1:1030) -- responder (172.30.0.4:53)
Oct 11 11:45:25 192.168.2.254 2637: Oct 11 11:45:42.635: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.3.1:1030) -- responder (192.175.48.6:53)
Oct 11 11:45:25 192.168.2.254 2638: Oct 11 11:45:42.687: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.3.1:1030) -- responder (192.175.48.42:53)
Oct 11 11:45:31 192.168.2.254 2639: Oct 11 11:45:48.079: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.3.1:1030) sent 170 bytes -- responder (172.30.0.1:53) sent 674 bytes
Oct 11 11:45:31 192.168.2.254 2640: Oct 11 11:45:48.079: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.3.1:1030) sent 274 bytes -- responder (172.30.0.4:53) sent 0 bytes
Oct 11 11:45:31 192.168.2.254 2641: Oct 11 11:45:48.079: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.3.1:1030) sent 73 bytes -- responder (192.175.48.6:53) sent 521 bytes
Oct 11 11:45:31 192.168.2.254 2642: Oct 11 11:45:48.079: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.3.1:1030) sent 73 bytes -- responder (192.175.48.42:53) sent 521 bytes
Oct 11 11:45:47 192.168.2.254 2645: Oct 11 11:46:03.867: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.2.1:37975) -- responder (172.16.64.1:53)
Oct 11 11:45:52 192.168.2.254 2646: Oct 11 11:46:09.071: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.2.1:37975) sent 70 bytes -- responder (172.16.64.1:53) sent 325 bytes
Oct 11 11:45:59 192.168.2.254 2647: Oct 11 11:46:16.203: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.2.1:47316) -- responder (172.16.64.1:53)
Oct 11 11:45:59 192.168.2.254 2648: Oct 11 11:46:16.207: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.2.1:40004) -- responder (172.16.64.1:53)
Oct 11 11:46:00 192.168.2.254 2649: Oct 11 11:46:17.207: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.2.1:60356) -- responder (172.16.64.1:53)
Oct 11 11:46:01 192.168.2.254 2650: Oct 11 11:46:18.211: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.2.1:59061) -- responder (172.16.64.1:53)
Oct 11 11:46:02 192.168.2.254 2651: Oct 11 11:46:19.211: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.2.1:47043) -- responder (172.16.64.1:53)
Oct 11 11:46:03 192.168.2.254 2652: Oct 11 11:46:20.215: %FW-6-SESS_AUDIT_TRAIL_START: Start dns session: initiator (192.168.2.1:34770) -- responder (172.16.64.1:53)
Oct 11 11:46:04 192.168.2.254 2653: Oct 11 11:46:21.359: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.2.1:47316) sent 31 bytes -- responder (172.16.64.1:53) sent 278 bytes
Oct 11 11:46:04 192.168.2.254 2654: Oct 11 11:46:21.359: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.2.1:40004) sent 41 bytes -- responder (172.16.64.1:53) sent 118 bytes
Oct 11 11:46:05 192.168.2.254 2655: Oct 11 11:46:22.383: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.2.1:60356) sent 41 bytes -- responder (172.16.64.1:53) sent 118 bytes
Oct 11 11:46:06 192.168.2.254 2656: Oct 11 11:46:23.407: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.2.1:59061) sent 41 bytes -- responder (172.16.64.1:53) sent 118 bytes
Oct 11 11:46:07 192.168.2.254 2657: Oct 11 11:46:24.431: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.2.1:47043) sent 41 bytes -- responder (172.16.64.1:53) sent 118 bytes
Oct 11 11:46:08 192.168.2.254 2658: Oct 11 11:46:25.455: %FW-6-SESS_AUDIT_TRAIL: Stop dns session: initiator (192.168.2.1:34770) sent 41 bytes -- responder (172.16.64.1:53) sent 118 bytes

Dans la partie en verte, il s'agit du vrai serveur DNS qui nous répond ➔ 172.30.1.3 :53
Dans la partie en rouge, il y a la mise ne place du DNS Spoofing, le serveur mis en place par le groupe attaque répond à nos requêtes ➔ 172.16.61.1 :53

Pour illustrer cela, une simple commande dig sur Google effectuer depuis notre serveur Auditorium ; et c'est toujours le serveur pirate qui nous répond (172.16.64.1 :53) :

```
Auditorium:/home/auditor# dig www.google.fr
; <<>> DiG 9.7.1-P2 <<>> www.google.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3511
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.fr.              IN      A
;; ANSWER SECTION:
www.google.fr.         3600    IN      A       172.30.0.4

;; Query time: 3 msec
;; SERVER: 172.16.64.1#53(172.16.64.1)
;; WHEN: Mon Oct 11 11:50:13 2010
;; MSG SIZE  rcvd: 47
```

Le DNS Spoofing est une attaque qui nous a fortement perturbés durant l'ensemble du projet en particulier durant la dernière confrontation car elle a été répétée à chaque fois.

La solution

c. Recommandations émises

Après la première confrontation nous avons émis plusieurs recommandations auprès des différents interlocuteurs.

En effet, nous avons constaté que les mots de passe avaient une faible sécurité : 5 caractères. Nous leur également suggéré de mettre en place le module Apache mod_security afin de se prémunir d'attaque possible.

Nous leur avons également demandé de surveiller les ports ouverts sur le routeur :

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-10-10 22:09 CEST
Interesting ports on 172.30.0.3:
Not shown: 987 closed ports
PORT    STATE    SERVICE
22/tcp  open     ssh
23/tcp  open     telnet
25/tcp  open     smtp
53/tcp  open     domain
80/tcp  open     http
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
```

445/tcp filtered microsoft-ds
1025/tcp filtered NFS-or-IIS
1720/tcp open   H.323/Q.931
3001/tcp filtered nessus
5060/tcp open   sip
5061/tcp open   sip-tls

2. Seconde confrontation « La revanche »

Pour cette confrontation, le réseau de la société AeroDef a été coupé le vendredi soir suite à une mauvaise manipulation de nos clients. L'accès n'a peut-être rétabli que le lundi matin. Nous n'avons pu détecter que très peu d'incident mis à part, une nouvelle attaque de DNS Spoofing.

Durant cette confrontation, les attaques ont visés le site web de la société. N'ayant pas d'IDS opérationnel à ce moment-là, nous ne pouvions en aucun cas détecter les modifications par SQL injection.

Lors de la dernière confrontation, nous avions émis auprès du responsable système la nécessité d'installer le mod Apache Secure sur leur serveur mais le conseil n'a pas été suivi et 3 semaines plus tard, les conséquences ne se sont pas fait attendre : site web de la société AeroDef a été defaced.

3. Troisième confrontation – « Ultimate Fighting »

Dans cette troisième confrontation, la société AeroDef a perdu son serveur Zeus. En effet, après quelques analyses des logs fournis après coup, nous avons constaté que de nombreux accès frauduleux avaient eu lieu.

Nous n'avons pas pu sur le coup et même durant l'ensemble du projet authentifié ces authentifications du fait que l'intégralité des logs du serveur ne nous a pas été fournie en particulier auth.log. Seul syslog.log nous a été fourni!!!

Nous avons donc identifié un compte administrateur n'ayant jamais été utilisé par AeroDef. Le compte « mohamed » est donc un compte avec les accès root qui n'aurait jamais dû exister vu qu'il n'y jamais servi.

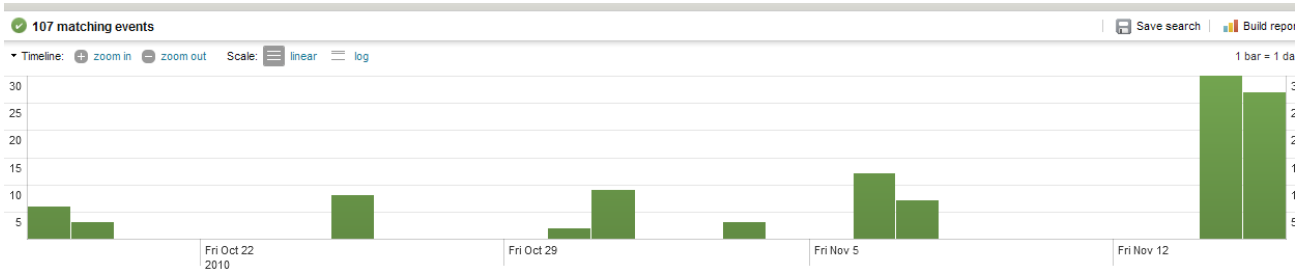


Figure 31 - Analyse des logs sur le serveur Zeus avec le compte "mohamed"

En effet, les accès de ce compte a été récupéré par le groupe attaque afin de commettre des actions non autorisées. Cela aurait pu être évité deux 2 manières :

- Installation de Fail2Ban ➔ bannir les IP qui font du brute-force
- Fournir TOUS les fichiers de logs à l'analyse.

D'autre part, nous avons également constaté que de nombreux échecs d'authentifications avaient eu lieu tout au début du projet réalisé avec du brute-force en ssh :

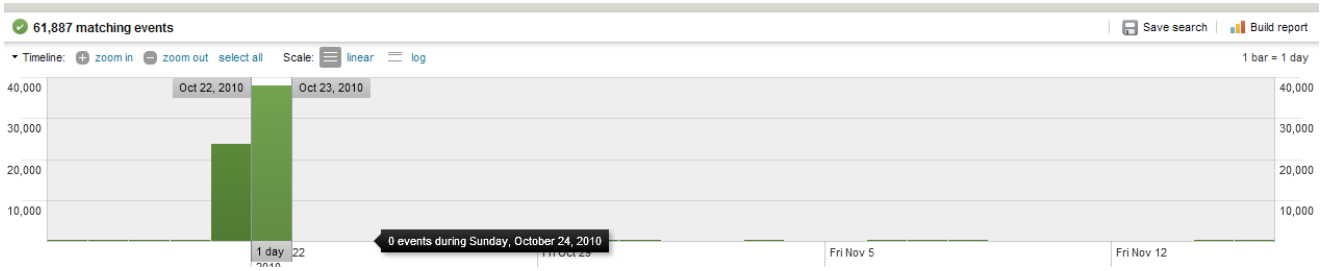


Figure 32 - Authentifications échouées (plus de 40000 en 1 seule journée)

Cette analyse grâce à l'outil Splunk se révèle très rapide. Une recherche dans les logs sur la machine Zeus avec les paramètres auth et failure :

host="zeus" auth failure

Résultat en quelques secondes, nous avons détecté de très nombreuses authentifications échouées mais après coup.

4. Cas de la téléphonie

A vrai dire, il n'y a pas vraiment d'analyse à réaliser concernant les confrontations pour la téléphonie IP puisque l'infrastructure n'a subi aucun dommage. Cependant elle n'était pas assez conséquente pour attiser le moindre intérêt concernant d'éventuelles attaques. Ceci étant dû au retard de contractualisation et au contact technique obtenu tardivement.

En effet, l'appel d'offre de VOIP/TOIP, nous a été transmis par Aerodef le 03/10/10 nous y avons

alors répondu le 18/10/10. Cependant, l'équipe Aerodef n'a établi le contrat que le 04/11/10 soit 11 jours avant la fin du projet (15/11/10).

Conclusion

Le projet "Sécurité des systèmes d'information" de l'année 2010 / 2011 s'est présenté comme les années précédentes. Trois groupes se sont confrontés. Un groupe Défense, un groupe Audit et un groupe Attaque. Un aspect nouveau cette année a été l'intégration d'un service VoIP / ToIP par le groupe Audit au sein de l'entreprise de la Défense.

Ce projet a commencé par une étude des services à implémenter et / ou à surveiller. Une fois ce travail réalisé il a fallu s'organiser, créer une hiérarchie, attribuer un rôle à chacun et mettre en place un outil de collaboration ainsi que des communications sécurisées. Cette étape préliminaire fut primordiale et nous a permis d'avoir une base solide et une bonne cohésion au sein du groupe.

Ensuite nous avons pu commencer l'établissement des contrats avec le groupe Défense. Durant tout le long de ce projet les communications entre l'Audit et la Défense furent assez chaotiques. Ceci a entaché l'avancement du projet de retards conséquents, notamment concernant la VoIP qui a de ce fait été restreinte à un service basique sans sécurisation conséquente.

Nous avons utilisé un seul serveur physique sur lequel a été virtualisé des machines dédiées aux différents services fournis (supervision, VoIP / ToIP, IDS...). De la même manière il a été nécessaire de virtualiser des équipements réseaux afin de faire communiquer ces machines avec le réseau local de l'entreprise Défense. Cette installation nous à causer quelques soucis et nous avons dû migrer certains services vers la machine physique (pour exemple : le problème de redirection du port SPAN vers la machine virtuelle de l'IDS).

Les trois confrontations se sont déroulées en crescendo, la première se résumant à un simple DNS spoofing associé à un exploit PDF qui a tout de suite été détecté par l'anti-virus du poste client. Lors de la seconde confrontation l'Attaque a réitéré le DNS spoofing et a mené à bien une attaque de type "website defacement". Il est à noter que la Défense aurait pu contrer cette tentative en appliquant les recommandations que l'Audit avait émises. Finalement, la dernière confrontation s'est révélée ravageuse envers le SI de la Défense. Effectivement, outre un DNS spoofing récurrent, le groupe Défense a tout bonnement perdu le contrôle d'un de ses serveurs.

Afin de tirer un bilan, ce projet nous a permis d'appréhender les divers problèmes de sécurité que rencontre un Système d'Information proposant des services courants : accès internet, site web d'entreprise, mise à disposition d'un environnement logiciel sujet à des failles de sécurité, etc.... Les difficultés auxquelles nous nous sommes confrontés ont été aussi diverses que variées : allant de la communication entre les entités Audit et Défense jusqu'aux nombreux problèmes techniques rencontrés. Ce projet à l'issue de la fin de la formation STRI tombe à point nommé en permettant d'appliquer du point de vue pratique les connaissances engrangées jusque-là.

Table d'illustration

Sources

- **Virtualisation système et enseignement par Ph. LATU**

  http://www.linux-france.org/prj/inetdoc/telechargement/vm.pdf

- **Virtualisation de réseaux avec KVM par Serge BORDERES,** Centre d'Etudes Nucléaires de Bordeaux-Gradignan

- **http://www.nagios.org/ (site officiel NAGIOS)**

- **http://www.centreon.com/ (site officiel CENTREON)**

- **http://www.nagvis.org/ (site officiel NAGVIS)**

- **http://fannagioscd.sourceforge.net/ (site officiel NAGVIS)**

- **http://blog.nicolargo.com/nagios-tutoriels-et-documentations(tutoriel supervision)**

- **http://www.labo-microsoft.org/articles/network/snmp/ (tutoriel installation snmp)**

- **Livre « Téléphonie sur IP » de Laurent Ouakil et Guy Pujolle**

- **Installation + utilisation NESSUS**
  http://www.nessus.org/documentation/

Annexe 1 : RAO de supervision.

Disponible Ici

Annexe 2 : RAO Voip/Toip.

Disponible ici

Annexe 3 : Contrat complet de supervision.

Disponible ici

Annexe 4 : Contrat complet de Voip/Toip.

Disponible ici

Annexe 5 : Charte de l'utilisateur du système d'information.

Disponible ici

Annexe 6 : Mise en place des mails

chiffrés.

Disponible ici

Annexe 7 : GoogleDocs.

Disponible ici

Annexe 8 – Script automatisation du serveur

Extrait du fichier « /etc/network/interface » :
post-up /root/script/post-up.sh

Script «post-up.sh »

```
#!/bin/bash

#Activation du routage
echo 1 > /proc/sys/net/ipv4/ip_forward

#creation du tap0
tunctl -t tap0 &

#Creation du bridge br0
brctl addbr br0

#interconnexion sur le bridge de l'interface eth0 et tap0
brctl addif br0 eth0
brctl addif br0 tap0


#configuration des interfaces
ifconfig br0 192.168.2.1 netmask 255.255.255.0 up
ifconfig tap0 192.168.2.2 netmask 255.255.255.0 up
#ifconfig eth0 192.168.2.3 netmask 255.255.255.0 broadcast 192.168.2.255 up
ifconfig eth0 up

#definition de la route par dÃ©faut
route add default gw 192.168.2.254 br0

#Démarrage du vde_switch
vde_switch -s /root/vde.ctl -tap tap0 &

#Démarrage du pool de serveurs virtuels
#/root/script/start_pool_machine.sh
```

Script machine virtuelle :
Le démarrage des machines se fait à l'aide du script suivant :

```
#!/bin/bash

vm=$1
memory=$2
```

```
port=$3

if [[ -z "$vm" || -z "$memory" || -z "$port" ]]
then
        echo "ERREUR : parametre manquent"
        echo "Utilisation : $0 <fichier image> <quantitÃ© mÃ©moire ne mo> <port commutateur
[2..32]>"
        exit 1
fi

macaddress="52:54:00:12:34:$port"

echo -e "$RedOnBlack"
echo "~> Machine virtuelle      : $vm"
echo "~> MÃ©moire RAM           : $memory"
echo "~> Port commutateur       : $port"
echo "~> Adresse MAC           : $macaddress"
#echo "~> Adresse IP           : $ip"
tput sgr0

kvm \
 -name $vm \
 -m $memory \
 -hda /root/img/$vm \
 -boot c \
 -k  fr\
 -usb -usbdevice tablet \
 -localtime \
 -net vde,vlan=0,sock=/root/vde.ctl,port=$port \
            -net nic,vlan=0,model=virtio,macaddr=$macaddress >/dev/null \
```

Annexes 9 – Mise en place de Syslog-ng et log-rotate

Dans le fichier */etc/syslog-ng/syslog-ng.conf*, on rajoute les lignes comme suit :

Définition de notre serveur comme source du service :

```
#Source
source net {
      udp(ip(192.168.2.1));
      };
```

Définition des fichiers de stockage des logs pour chaque équipement de destination du service Syslog-ng :

```
# Destination

#Cisco Gateway
destination d_cisco_gateway {
      file("/var/log/cisco.log");
      };

#Serveur ZEUS
destination d_serveur_zeus {
      file("/var/log/zeus.log");
      };
```

Définitions de filtres pour spécifier les ip des destinations et le niveau de criticité des logs qui doivent être retenus :

```
# Filtre
#Cisco Gateway
filter f_cisco {
      host(192.168.2.254) and level(info,notice,warn,crit,err);
      };

# Serveur ZEUS
filter f_serveur_zeus {
      host(192.168.1.1) and level(info,notice,warn,crit,err);
      };
```

Associations des source + destination + filtre pour faire fonctionner le service pour chaque destinataire :

```
#Cisco
log {
        source(net);
        filter(f_cisco);
        destination(d_cisco_gateway);
};

#Serveur zeus
log {
        source(net);
        filter(f_serveur_zeus);
        destination(d_serveur_zeus);
};
```

Lancement du daemon :

```
sudo /etc/init.d/syslog-ng restart
```

logrotate

Il est possible de configurer les options appliquées par défaut à tous les fichiers dans le logrotate.conf, toutefois on peut également changer leurs valeurs lors de la définition de l'archivage d'un fichier.

```
vim /etc/logrotate.conf

# see "man logrotate" for details
# rotate log files weekly
weekly
# frequence de rotation des fichiers (chaque semaine)


# keep 4 weeks worth of backlogs
rotate 4
# conservation de 4 archives = 4 semaines ici

# create new (empty) log files after rotating old ones
create
# creation d'un nouveau fichier vide de log lors d'une rotation

# uncomment this if you want your log files compressed
#compress
# fichier de logs non compresses

# packages drop log rotation information into this directory
include /etc/logrotate.d
```

```
# Inclusion des scripts propres aux logs


# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}
# rotations concernant wtmp et btmp
```

Tous les logs définis dans les fichiers de configurations (apache2, aptitude, dpkg, …) du répertoire "*/etc/logrotate.d*" sont inclus dans *logrotate.conf* via la directive "**include**".

```
ls /etc/logrotate.d/
apache2  aptitude  dpkg       exim4-paniclog  rsyslog.disabled  zeus
apt      cisco     exim4-base  fail2ban        syslog-ng
```

Par exemple pour les logs du serveur zeus

```
vim /etc/logrotate.d/zeus

/var/log/zeus.log {
   rotate 15
   daily
   compress
   delaycompress
}
```

Annexes 10 – Mise en place de NetFlow

Installation de la machine de collecte :

Cette installation suppose que le serveur possède déjà un serveur WEB apache ainsi que PHP d'installer.

Nfdump :

On installe le paquet nfump ainsi que toutes ses dépendances :

```
Aptitude install nfdump
```

Nfsen :

Il faut d'abord installer les prés requis suivant ainsi que leurs dépendances :

```
Aptitude install rrdtool libmail-perl librrdtool-oo-perl
```

Téléchargement de nfsen :

```
Wget http://ovh.dl.sourceforge.net/project/nfsen/stable/nfsen-1.3.5/nfsen-1.3.5.tar.gz
```

Décompression de l'archive :

```
Tar –xzvf nfsen-1.3.5.tar.gz

Mv nfsen-1.3.5/  /usr/local/src/
```

Ensuite pour poursuivre l'installation il faut configurer le fichier nfsen.conf :

```
Cd nfsen-1.3.5/etc/

Cp nfsen-dist.conf nfsen.conf
```

Enfin il faut éditer le fichier nfsen.conf :

```
Vim nfsen.conf
```

Ici il faut renseigner le répertoire web (/var/www), puis le mail de contact ainsi que le chemin pour accéder à nfdump.

Création d'un utilisateur et d'un groupe nfsen :

```
useradd -m nfsen

passwd nfsen

groupadd nfsen

usermod -G nfsen nfsen
```

Création d'un groupe nfsenadmin afin de rajouter l'utilisateur apache :

```
groupadd nfsenadmin

usermod -a -G nfsenadmin nfsen

usermod -a -G nfsenadmin www-data
```

Ensuite on créer l'arborescence WEB pour nfsen :

```
Mkdir –p /var/www/nfsen
```

Puis il ne reste plus qu'à exécuter le script d'installation :

```
Cd /usr/local/src/nfsen-1.3.5/

./install.pl etc/nfsen.conf
```

Ensuite il faut démarrer le daemon nfsen :

```
/usr/local/src/nfsen-1.3.5/bin/nfsend start
```

Enfin l'installation est terminée et l'interface WEB nfsen est accessible depuis l'adresse suivante :

http://IP-du-server/nfsen

Ensuite il convient de sécuriser l'accès à « nfsen » en bloquer l'accès au dossier « /var/www/nfsen » grâce à un .htaccess.

Il est possible aussi de n'autoriser l'accès au serveur web que seulement en HTTPS.

Pour finir il suffit de rajouter les sources Netflow

Annexe 11 – Compte rendu de la réunion du 25 Octobre 2010 entre la supervision et les responsables des serveurs.

Annexe 12 – Tutoriel d'installation du protocole SNMP sur un serveur LINUX et WINDOWS

	GroupeAUDIT	**Compte rendu réunion Lundi 25 Octobre**
	Sous-Groupe : Supervision	**Date : 28 Octobre 2010**

Sujet :

Mise en place d'outils de supervision au sein de la société AéroDef afin de permettre la surveillance de leurs différents serveurs.

Contenu :

La société AéroDef possède deux serveurs différents. Un premier serveur (sous Débian) a pour rôle d'héberger les différents services de la société (DNS, HTTP, POSTFIX, etc.). Un deuxième serveur (sous Windows server 2003) servant de contrôleur de domaine (Active Directory).

Voici ci-dessous la liste des différents indicateurs que cette société souhaitera contrôler au travers de l'outil de supervision proposé par l'entreprise Assurancetourix :

Serveur de service :

- **Hardware :**
  - Charge CPU (réalisable)
  - Charge mémoire (réalisable)
  - Espace disque (réalisable)
  - Nombre d'utilisateurs (réalisable)

- **Services :**
  - DNS (en cour d'étude)
  - HTTP/ HTTPS (en cour d'étude)
  - SFTP (en cour d'étude)
  - SSH (en cour d'étude)
  - POSTFIX (en cour d'étude)
  - SPAMASSASSIN (en cour d'étude)
  - MYSQL (en cour d'étude)

Serveur de contrôleur de domaine :

- **Hardware :**
  - Charge CPU (réalisable)
  - Charge mémoire (réalisable)
  - Espace disque (réalisable)
  - Nombre d'utilisateur (réalisable)

- **Services :**
  - (en cour d'étude)

Analyse du réseau :

- Surveillance du réseau (en cour d'étude)

Courbe du chef (un voir deux indicateurs les plus importants):

- Continuité de service (en cour d'étude)

	Groupe AUDIT	**Tutoriel d'installation SNMP sur Serveur Linux**
	Sous-Groupe : Supervision	**Date : 28 Octobre 2010**

Description :

Ce tutoriel a pour but d'installer le service SNMP sur un serveur avec une distribution LINUX DEBIAN. Une fois les paquets installés et la configuration réalisée, le serveur Nagios pourra dialoguer avec le serveur linux pour récupérer les informations se trouvant dans la MIB par l'intermédiaire du protocole SNMP.

Procédure d'installation :

1. Installation du paquet snmp :
- *Apt-getinstallsnmpd*

2. Configuration du fichier « snmpd.conf » :
- *Vim /etc/snmp/snmpd.conf*
- Une fois dans le fichier, modifier les lignes correspondantes pour obtenir le résultat suivant :

Remarque : Cette configuration permet de renseigner l'adresse IP du serveur Nagios, mais également la communauté utilisée pour dialoguer entre le serveur et les agents.

3. Configuration du fichier « snmpd » :
- *Vim /etc/default/snmpd*

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid
@IP'
```

- Une fois dans le fichier, remplacer '@IP' par l'adresse IP de votre interface d'écoute.

4. Relancer votre démon SNMP
- #/etc/init.d/snmpd restart

Cas d'erreur :

En cas de non compréhension du tutoriel ou en cas d'erreur, contacter directement le contact

	Groupe AUDIT	**Tutoriel d'installation SNMP sur Serveur Windows**
	Sous-Groupe : Supervision	**Date : 28 Octobre 2010**

Description :

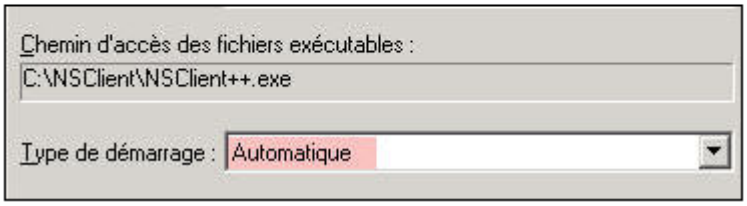
Ce tutoriel a pour but d'installer le service SNMP sur un serveur avec une distribution Windows Server. Une fois le logiciel installé et la configuration réalisée, le serveur Nagios pourra dialoguer avec le serveur Windows pour récupérer les informations se trouvant dans la MIB par l'intermédiaire du protocole SNMP.

Procédure d'installation :

1. Téléchargement de NSCLIENT++ :
- Télécharger le NSCLIENT++ et décompresser le dossier à l'endroit voulu pour l'installation.

2. Installation de NSCLIENT ++ :
- Lancez une invite de commande
- Allez dans c:\NSClient (si le NSCLIENT décompresser se trouve sur le disque c).
- Tapez les commandes suivantes :

3. Configuration de NSCLIENT++ :
- Ouvrir la mmc **service.msc** et configurer pour tout d'abord l'autoriser à interagir avec le bureau, puis faire un démarrage automatique (cf. fenêtre ci-dessous) :



- Editer le fichier **NSC.ini** afin de configurer la connexion entre le serveur Nagios et votre contrôleur de domaines. Pour se faire, il faut décommenter tous les modules de la section **[MODULES]** à l'exception de **checkWMI.dll** et **RemoteConfiguration.dll**.

```
[modules]
;# NSCLIENT++ MODULES
;# A list with DLLs to load at startup.
;  You will need to enable some of these for NSClient++ to work.
; ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
; *                                                               *
; * N O T I C E ! ! ! - Y O U   H A V E   T O   E D I T   T H I S *
; *                                                               *
; ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
FileLogger.dll
CheckSystem.dll
CheckDisk.dll
NSClientListener.dll
NRPEListener.dll
SysTray.dll
CheckEventLog.dll
CheckHelpers.dll
;CheckWMI.dll
;
; RemoteConfiguration IS AN EXTREM EARLY IDEA SO DONT USE FOR PRODUCTION ENVIROMNEMTS!
;RemoteConfiguration.dll
; NSCA Agent is a new beta module use with care!
NSCAAgent.dll
; LUA script module used to write your own "check deamon" (sort of) early beta.
LUAScript.dll
; Script to check external scripts and/or internal aliases, early beta.
CheckExternalScripts.dll
; Check other hosts through NRPE extreme beta and probably a bit dangerous! :)
NRPEClient.dll
; Extreamly early beta of a task-schedule checker
CheckTaskSched.dll
```

- Il faut ensuite aller dans la section **[SETTING]** (toujours dans le même fichier) pour configurer le mot de passe :

```
;# PASSWORD
;  This is the password (-s)
access the daemon remotly.
password=Ton_Password
```

Remarque : Il s'agit de la communauté, donc nous reprendrons ici la communauté configurée sous Nagios : **aerodef**.

- Toujours dans la même section **[SETTING]**, décommenter la ligne **allowed_hosts**. Il faut ensuite rajouter l'@IP du serveur Nagios avec lequel on souhaite communiquer :

```
;# ALLOWED HOST ADDRESSES
;  This is a comma-delimited list of IP
;  If leave this blank anyone can access
;  The syntax is host or ip/mask so 192.1
allowed_hosts=Adresse IP de Nagios
```

Remarque : L'@ip du serveur nagion est : **192.168.2.103**.

- Décommenter la ligne (si elle est commentée) du port avec lequel NSCLIENT va communiquer (par défaut le numéro de port est **12489**):

```
;# NSCLIENT PORT NUMBER
;  This is the port the NSClientListener.dll will listen to.
port=12489
```