AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Projet de sécurité des Systèmes d'Information

Rapport d'activité - Groupe Défense 2010

Master 2 STRI – Université Paul Sabatier

Mohamed BARRY
Jérémie BELMUDES
ThomasCAPRARO
Julien DESVEAUX
Cyrille DUMAS
Raphaël DUJARDIN
Thomas DUVIVIER
Harboure HUBERT COMPAORE
Cédric HARISMENDY
Joseph NDAYRA
Laurent ROGER
Frédéric TARRERIAS
Nattapong TIWAPORNCHAROENCHAI
Wannes VOSSEN

Référence : RAP12010

Sommaire

I - Introduction

Dans le cadre de l'enseignement en Réseaux Informatiques, l'IUP STRI propose à ses étudiants de mettre en œuvre, le temps d'un semestre, un projet d'envergure. Axé autour de la sécurité informatique, ce projet favorise l'apprentissage par la mise en situation pratique.

L'ensemble des 42 étudiants de Master 2 s'étant répartis en trois groupes, chacun de ces groupes se voit attribuer un rôle parmi les suivants :

- Le **groupe Défense** incarne une équipe technique responsable des systèmes informatiques dans une société de services. Leur objectif sera le déploiement de moyens informatiques de la société avec de fortes contraintes en sécurité.
- Le **groupe Audit** représente une société d'audit en sécurité informatique. Elle sera employée par le groupe Défense pour son expertise dans le domaine de la sécurité.
- Enfin, le **groupe Attaque** incarne une organisation de pirates informatiques dont l'objectif sera de compromettre la sécurité du système déployé par le groupe Défense.

A partir du lundi 27 Septembre et jusqu'au lundi 15 Novembre, les trois groupes vont, en autonomie, atteindre leurs objectifs respectifs. Toutefois, trois confrontations seront organisées au long du projet et au cours desquelles des scénarios d'attaque seront mis en place.

Le présent document est un compte rendu du déroulement du projet. Il s'attachera à relater et à commenter les évènements du point de vue du groupe Défense. Après avoir traité de l'aspect organisationnel, nous adopterons un plan chronologique jalonné par les trois confrontations.

II - Organisation du travail

1 - Structuration du produit

1.1 - Le besoin primaire

La société AeroDef.fr exerce une activité de consulting en aéronautique. Pour assister son activité, cette société souhaite mettre en place un réseau informatique. La société AeroDef.fr dispose déjà de matériels pour ce projet : un Routeur intégrant un module de ToIP, un Switch de niveau 3, un Serveur, trois postes informatiques, un point d'accès Wi-Fi. Il est également possible de faire usage des postes de Travaux Pratiques de la sale U2-212 mais ceux-ci seront régulièrement réinitialisés.

Etant donné le cadre pédagogique de ce projet, une attention toute particulière doit être portée aux notions de sécurité informatique. Le groupe défense doit veiller à garder un équilibre entre sécurité et utilisation, l'axe important étant la continuité de service.

1.2 - Les contraintes

L'une des principales contraintes pour ce projet est le très faible cloisonnement entre les étudiants des différents groupes : ces étudiants doivent collaborer à l'extérieur du projet, ils doivent communiquer, travailler dans les même salles et sur les mêmes infrastructures. Ce sont autant de risques pour la sécurité. Par exemple, nous avons été informés d'une tentative de récupération des mots de passe de sessions Windows auprès de l'administration en U3.

Une des conséquences de ce mélange est la possibilité pour les attaquants d'accéder à tout moment au matériel le plus sensible du système. Dans une situation réelle, cela rendrait impossible toute notion de continuité de service. Pour ce projet, il à été fait appel à la raison des uns et des autres et s'il est évident qu'il est inutile de débrancher un équipement pour provoquer un déni de service, nous pouvons nous poser la question de la légitimité d'autres opérations comme le détournement des flux entrant et sortant du réseau normalement destinés au fournisseur d'accès internet de l'entreprise, la compromission des périphériques et de messageries personnelles de l'étudiant.

1.3 - Les besoins consécutifs aux contraintes

1.3.1 La reprise d'activité

Etant donné les contraintes énoncées ci-dessus et en particulier l'accès physique aux équipements, la sauvegarde de l'existant et la possibilité de reprendre rapidement l'activité sont des problématiques de cœur. Un disque dur à été mis à disposition pour traiter ce problème.

1.3.2 La sécurisation contre l'accès physique

Lorsqu'un attaquant accède au matériel, ses possibilités sont décuplées. Il peut démarrer une machine à l'aide d'un live CD, démonter ses disques durs, intercepter toute les communications, ajouter des périphériques, positionner des Keyloggers matériels. Dans la mesure du possible, une sécurité contre l'accès physique doit être mise en œuvre.

1.3.3 La sécurisation contre les attaques man in the middle

De par son accès physique, l'attaque peut sans problème intercepter à très bas niveau et usurper tous les flux du réseau. Les attaques de type Spoofing sont par conséquent difficilement évitables, la solution étant de crypter l'ensemble des flux entrants et sortants du réseau.

1.3.4 La sécurisation contre le social engineering

Dès le départ, notamment au travers des retours d'expérience des années précédentes, nous avons identifié le social engineering comme principale menace pour ce projet. Afin d'éviter au maximum les vols d'informations et de mots de passe, une politique de sécurité a été rédigée. Cette politique s'adresse à la fois aux utilisateurs du système et aux administrateurs que nous sommes.

2 - Structuration des tâches

Afin d'organiser et d'optimiser le travail, nous avons défini trois types de taches dans ce projet qui permettront aux participants de se spécialiser dans l'une d'elle.

2.1 - Architecture

L'équipe d'Architecture est chargée du déploiement du réseau et de l'interconnexion des équipements du système. L'architecture se charge également des contrôles d'accès au réseau et intervient généralement sur les Routeurs et les Switch.

2.2 - Système

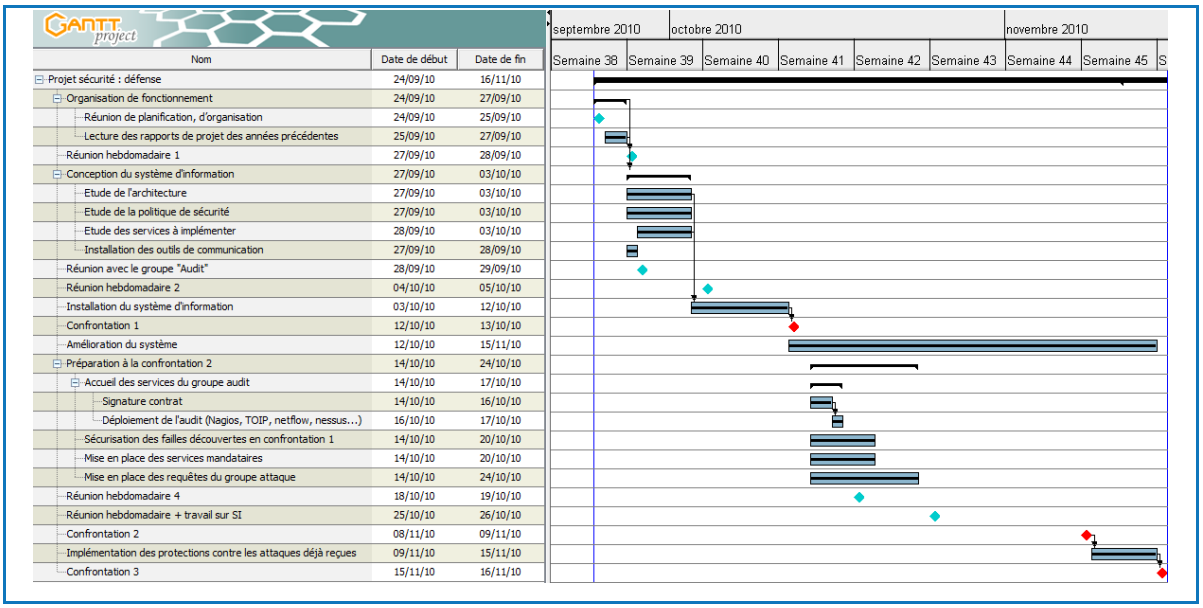
L'équipe Système est chargée de mettre en œuvre les différents services à l'utilisateur. Le système intervient principalement sur les postes client et les serveurs de la société.

2.3 - Communication

L'équipe de communication est chargée de la communication et de la qualité au sein et à l'extérieur du groupe. Elle a un rôle de coordination, de présentation de l'information. Elle est aussi chargée des aspects politique de sécurité et contractualisation des échanges.

2.4 - Planification du projet

Voici un diagramme de Gantt représentant l'évolution du projet dans le temps.

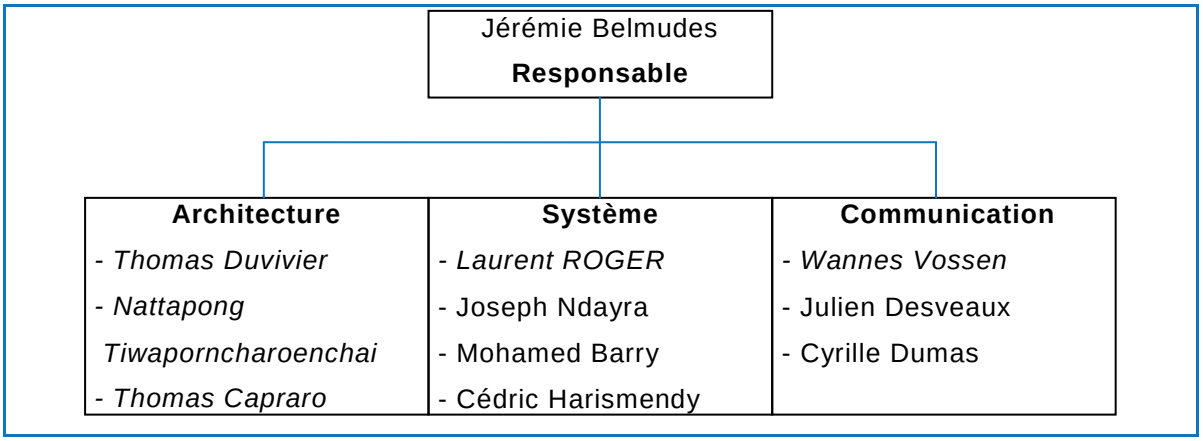


Nom	Date de début	Date de fin
Projet sécurité : défense	24/09/10	16/11/10
Organisation de fonctionnement	24/09/10	27/09/10
Réunion de planification, d'organisation	24/09/10	25/09/10
Lecture des rapports de projet des années précédentes	25/09/10	27/09/10
Réunion hebdomadaire 1	27/09/10	28/09/10
Conception du système d'information	27/09/10	03/10/10
Etude de l'architecture	27/09/10	03/10/10
Etude de la politique de sécurité	27/09/10	03/10/10
Etude des services à implémenter	28/09/10	03/10/10
Installation des outils de communication	27/09/10	28/09/10
Réunion avec le groupe "Audit"	28/09/10	29/09/10
Réunion hebdomadaire 2	04/10/10	05/10/10
Installation du système d'information	03/10/10	12/10/10
Confrontation 1	12/10/10	13/10/10
Amélioration du système	12/10/10	15/11/10
Préparation à la confrontation 2	14/10/10	24/10/10
Accueil des services du groupe audit	14/10/10	17/10/10
Signature contrat	14/10/10	16/10/10
Déploiement de l'audit (Nagios, TOIP, netflow, nessus...)	16/10/10	17/10/10
Sécurisation des failles découvertes en confrontation 1	14/10/10	20/10/10
Mise en place des services mandataires	14/10/10	20/10/10
Mise en place des requêtes du groupe attaque	14/10/10	24/10/10
Réunion hebdomadaire 4	18/10/10	19/10/10
Réunion hebdomadaire + travail sur SI	25/10/10	26/10/10
Confrontation 2	08/11/10	09/11/10
Implémentation des protections contre les attaques déjà reçues	09/11/10	15/11/10
Confrontation 3	15/11/10	16/11/10

3 - Structuration de l'équipe de projet

3.1 - Organigramme de l'équipe

L'organigramme suivant décrit l'attribution des tâches précédemment décrites à chacun des membres du groupe.



Cet organigramme n'est en aucun cas rigide et il n'exclut pas la possibilité pour un membre d'intervenir dans un domaine autre que celui qui lui a été assigné.

3.2 - Travail collaboratif

Une liste de diffusion et un espace de stockage partagé ont été fournis par Ph. Latu pour les communications relatives au projet. Nous étions toutefois libres de choisir d'autres modes de communication.

Etant donné que nous n'étions pas tout à fait sûrs de la fiabilité du système proposé : que les mots de passe administrateurs avaient été volés les années précédentes et que nous avions nous-mêmes accès à la liste de diffusion du groupe attaque, nous avons choisi de mettre en place une plateforme Google Apps associée à un nom de domaine.

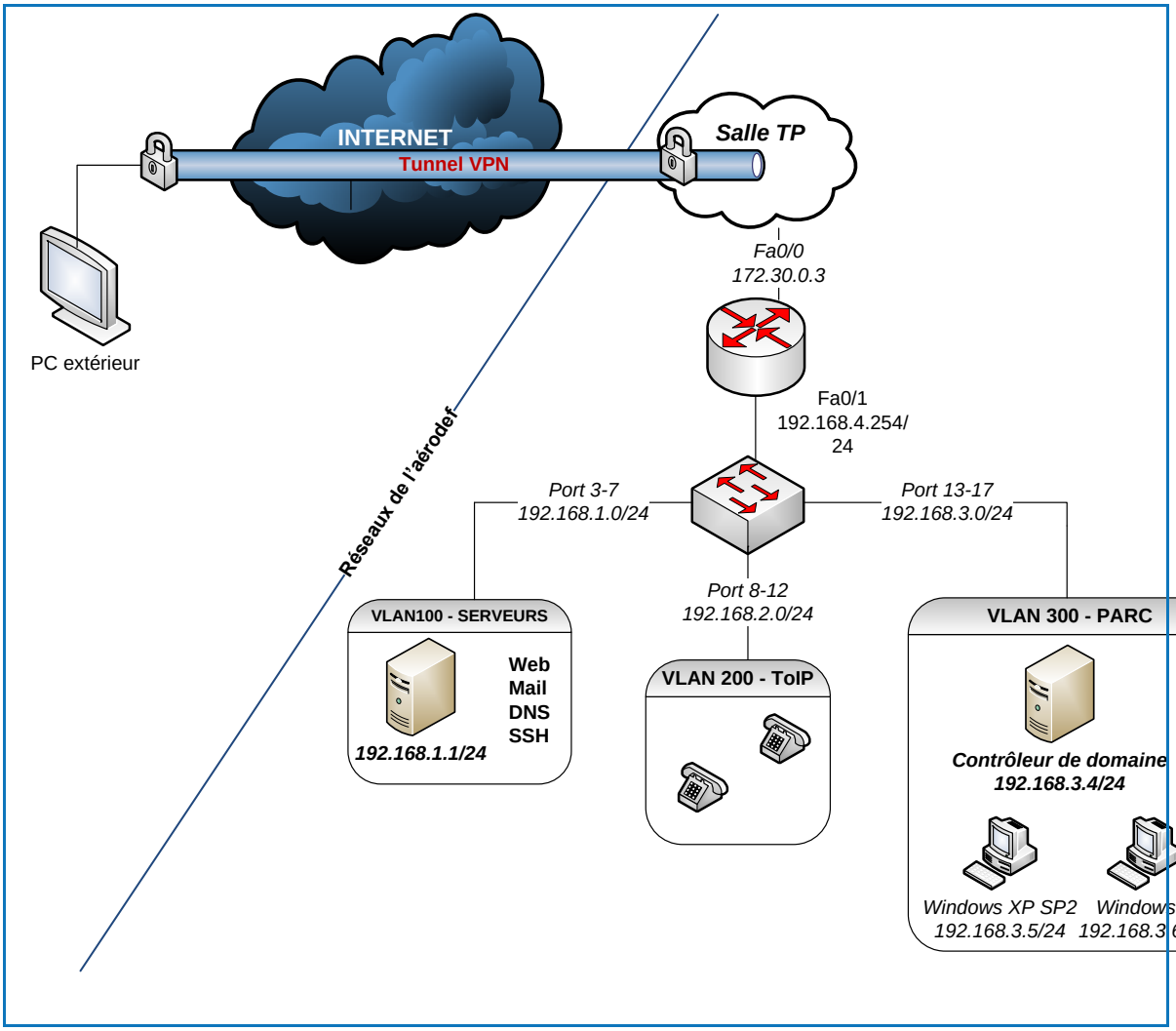
La plateforme Google Apps permet entre autres de gérer la partie mail d'un nom de domaine et de partager des documents à l'aide de Google Docs. L'utilisation d'une plateforme toute faite offre évidemment moins de possibilités que la mise en place d'un système personnalisé mais présente l'avantage de pouvoir être mise en place très rapidement et pour un coût minime (5€ pour le nom de domaine).

Chaque membre du projet dispose par conséquent d'une boite email accessible exclusivement en https à l'adresse https://mail.aerodef.fr. Les listes de diffusion conduite@aerodef.fr, système@aerodef.fr, architecture@aerodef.fr et communication@aerodef.fr permettaient d'envoyer des messages aux groupes décrits ci-dessus.

3.3 - Réunions

Des réunions de mise au point ont été organisées au moins toutes les semaines pour assurer une bonne communication dans le projet. A l'issue de chaque réunion, un compte rendu de réunion a été rédigé. Ce compte rendu reprend les principales décisions et objectifs fixés lors de la réunion.

III - Architecture



L'équipe architecture se charge de la mise en œuvre d'une architecture réseau répondant aux besoins de la société Aerodef. L'entreprise souhaite avoir un réseau local permettant la communication des machines dans le parc. Les services suivants ont été demandés : service web accessible depuis l'extérieur et depuis le parc, service de messagerie, l'accès à distance sécurisé et la résolution d'adresse. Les machines dans le parc devant pouvoir communiquer entre elles. Aussi elles doivent pouvoir bénéficier des services de l'entreprise. Un accès de tel groupe de travail vers tel service doit être défini et il sera restreint en cas de non permission. Dans le futur proche le client souhaiterait mettre en place la téléphonie IP au sein de l'entreprise. Il faut donc faire en sorte que le réseau soit évolutif. La sécurisation du réseau est indispensable tout au long de la conception et la mise en place de l'architecture.

Les machines du parc et celles pour les serveurs ont des rôles, des droits et des niveau de priorité différents. Afin de pouvoir gérer au mieux la charge du réseau et administrer des trafics, nous avons décidé de découper le réseau en plusieurs sous-réseaux.

Le découpage en sous-réseau virtuels ou Vlan permet tout d'abord de réduire la taille de domaine de diffusion. Ensuite il permet de créer un ensemble de logique isolé pour améliorer la sécurité. Nous avons choisi de mettre en place un VLAN de niveau 3 ou VLAN par adresse IP. Cela consiste à indiquer les adresses IP ou une plage d'IP qui appartiendront à tel ou tel VLAN.

Nous avons créé un premier sous-réseau regroupant tous les services proposés par l'entreprise afin de faciliter la maintenance et la surveillance. Quant aux machines de parc, ils se trouvent dans un deuxième sous-réseau où un contrôleur de domaine sera installé. Un troisième sous-réseau est prévu pour l'installation de la téléphonie IP ainsi que la supervision par le groupe audit.

Une fois les Vlan mis en place, il faut ensuite les interconnecter. Cela nécessite un lien Trunk, le lien d'interconnexion sur lequel plusieurs VLAN passeront. En revanche les trames seront marquées (taguées) pour que les commutateurs sachent à quel VLAN elles appartiennent. Le lien Trunk n'est pas simplement un multiplexage de communications, mais un multiplexage de réseaux virtuellement indépendants. Le routage de ces sous-réseaux sera assuré par notre routeur.

Une adresse IP privée de classe C a été choisie et implémentée. Nous considérons que le masque 24 nous paraît suffisant pour l'évolution éventuelle du Parc utilisateurs.

Voici le tableau récapitulant des Vlan :

VLAN	IP associée
Serveurs	192.168.1.0/24
ToIP	192.168.2.0/24
PARC	192.168.3.0/24

Un accès VPN nous a permis d'accéder à notre architecture depuis notre domicile. Un VPN repose sur un protocole de tunnelisation et aux algorithmes de cryptographie. Les données seront donc chiffrées à l'entrée et déchiffrées en sortie du tunnel. Ces données sont normalement incompréhensibles pour toute personne située entre les deux extrémités du VPN. Parmi des protocoles de tunnelisation, nous avons choisi le protocole SSH pour établir la liaison VPN puis qu'il offre la possibilité d'établir des connexions de type TCP. De plus le logiciel OpenSSH est facile à configurer.

La société ne possède qu'une seul adresse IP publique par conséquent, il est impossible d'assurer la connexion à Internet des machines de l'entreprise. Afin de résoudre ce problème sans acheter autant d'IP publique que le nombre de machines, la translation d'adresse par allocation de port dynamique semble la solution la plus appropriée.

Nous avons besoin de la translation d'adresse statique pour les services proposés par l'entreprise et la translation d'adresse dynamique pour les machines souhaitant aller sur Internet.

Dans un premier temps, le service web est le seul service que nous avons eu à mettre en place. Ce service doit être toujours accessible depuis l'extérieur et depuis le réseau local, il est nécessaire que le site ait une adresse IP fixe. Suite à la contrainte d'adresse IP publique insuffisante, nous devons faire correspondre l'adresse IP privé du serveur Web avec l'adresse

publique à laquelle nous appartenons en ajoutant le numéro de port pour ce type de service. Ci-dessous la table de correspondance pour le NAT statique.

IP interne	IP externe	Service
192.168.1.1 :80	172.16.30.3 :80	Web
192.168.4.254 :22	172.16.30.3 :22	SSh

La communication en interne entre les collaborateurs de la société Aerodef en dehors des horaires de travail est parfois indispensable. De plus nous souhaitons être certain que l'information de la société reste toujours secrète et à l'abri de la concurrence. Nous avons acheté un nom de domine pour la société. Ensuite nous avons intégré notre domaine dans GoogleApps service gratuit permettant d'importer un domaine existant et de bénéficier les services de Google. Grâce à cela, nous pouvons créer autant de compte de courrier électronique que nécessaire. Nous pouvons également bénéficier du service de partage de fichier ce qui nous permet d'avoir toujours la dernière version des documents collaboratif.

1 - Evolution

1.1 - Switchport

Tout au long du projet il a été envisagé que l'équipe attaque puisse avoir accès à la salle et ainsi pouvoir connecter physiquement une machine malveillante aux équipements d'Aérodef. Afin de minimiser au maximum ce type de rixes il a été décidé de mettre en place sur notre switch du switchport statique :

```
Switch# configuration terminal
Switch(config)# interface fastethernet 0/x
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

Une fois ces 2 commandes effectuées on va spécifier le type de protection sur le port :

- Soit on passe en mode sticky (Le port va enregistrer le 1er équipement qui se connecte et se bloque sur l'@MAC) :

```
Switch(config-if)# switchport port-security mac-address sticky
```

- Soit on configure manuellement la ou les adresse(s) qui seront autorisé à se connecter sur le port.

```
Switch(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

Les ports ont étés configurés suivant le tableau suivant :

#1	#3	#5	#7	#9	#11	#13	#15	#17	#19	#21	#23
#2	#4	#6	#8	#10	#12	#14	#16	#18	#20	#22	#24

Port	VLAN	Equipement	@MAC
#1	1	*Routeur*	-
#2	1	-	Port Bloqué
#3	Serveur : 100	Zeus	0012.7955.C96F
#4	Serveur : 100	-	Port Bloqué
#5	Serveur : 100	-	Port Bloqué
#6	Serveur : 100	-	Port Bloqué
#7	Serveur : 100	-	Port Bloqué
#8	Audit : 200	-	Port Bloqué
#9	Audit : 200	Téléphone IP	Pas encore rattaché au Switch
#10	Audit : 200	Téléphone IP	Pas encore rattaché au Switch
#11	Audit : 200	PC Audit	0018.F355.8088
#12	Audit : 200	*Serveur Audit*	-
#13	Parc : 300	-	Port Bloqué
#14	Parc : 300	Controleur de domaine	0018.F309.7385
#15	Parc : 300	Client Windows 7	Pas encore rattaché au Switch
#16	Parc : 300	Machine Debian qui virtualise plusieurs Clients	Pas encore rattaché au Switch
#17	Parc : 300	-	Port Bloqué
#18	1	-	Port Bloqué
#19	1	-	Port Bloqué
#20	1	-	Port Bloqué
#21	1	-	Port Bloqué
#22	1	-	Port Bloqué
#23	1	-	Port Bloqué
#24	1	*SPAN*	-

1.2 - Inspect

Le routeur mis à disposition gère les CBAC. Afin de maximiser la sécurité de l'architecture nous avons décidé de mettre en place différentes règles les mettant à profit. Il faut savoir que les ACL CBAC offrent la possibilité de distinguer dans un flot de paquets ceux qui appartiennent à une session en cours de ceux qui viennent se heurter aux parois du routeur et n'appartiennent pas à une session valide. Le routeur est alors transformé en un véritable firewall à conservation d'état (stateful). Le déploiement de telle ACL aide à combattre les attaques de déni de service par saturation de la pile TCP/IP.

Ces ACl offrent diverses possibilités :

- Ouverture dynamique de règles autorisant le retour d'un traffic ayant débuté dans une zone de confiance.
- Inspection protocolaire
- Surveillance des numéros de séquence TCP

- Paramétrage de l'expiration des sessions
- Dispositif d'alerte
- Blocage de trafics suspects.

```
ip inspect max-incomplete high 20000000
ip inspect max-incomplete low 10000000
ip inspect one-minute high 100000000
```

Nous appliquons tout d'abord quelques commandes afin de nous prémunir contre les attaques par déni de service qui consistent à ouvrir des connexions TCP à moitié et à les laisser dans cet état. Les commandes ip inspect max-incomplete high 20000000 et ip inspect max-incomplete low 20000000 sont complémentaires. Il s'agit ici de demander au routeur d'éliminer les connexions (à moitiés ouvertes) lorsque leur nombre dépasse 20000000 et d'arréter de les supprimer lorsqu'il en reste que 10000000. Les deux commandes suivantes sont similaires mais se basent sur le nombre de connexions (à moitiés ouvertes) par minutes.

```
ip inspect udp idle-time 15
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 1
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 100000 block-time 0
ip inspect name fw1 icmp audit-trail off
ip inspect name fw1 udp audit-trail off
ip inspect name fw1 tcp audit-trail off
```

Puis viennent les commandes qui introduisent la liste des protocoles à inspecter. Ces informations peuvent être redirigées vers un serveur de type syslog.

1.3 - Deuxième adresse IP sur le serveur

Afin d'avoir une meilleur vision du trafic et des différents flux circulant sur le réseau il à été décider d'associer une deuxième adresse ip sur le serveur (Zeus). Ainsi lors de la translation d'adresse et du PAT les ports serveur et clients sont entièrement dissocier.

Configuration de l'interface :

```
interface FastEthernet0/0
 ip address 172.30.0.5 255.255.255.248 secondary
```

Règles ACL :

```
access-list 111 permit tcp any host 172.30.0.5 eq www
access-list 111 permit tcp any host 172.30.0.5 eq 443
access-list 111 permit tcp any host 172.30.0.5 eq smtp
access-list 111 permit tcp any host 172.30.0.5 eq 22
```

Règle NAT :

```
ip nat inside source static 192.168.1.1 172.30.0.5
```

1.4 - Span port

Lors du contrat passé avec le groupe Audit il à été spécifié la mise en place d'un span port sur notre switch. Il s'agit de rediriger les paquets vers ce port afin qu'ils puissent en analyser le contenu avec un outil de type Wireshark installé sur un PC connecté au port monitor.

Configuration:

```
Switch(config)#monitor session 1 source interface fastethernet 0/1
both
Switch(config)#monitor session 1 destination interface
fastethernet 0/24
```

1.5 - Rate-limit

Etant donné le faible trafic circulant sur notre réseau il nous a semblé judicieux de limiter la bande passante sur l'interface relié au serveur principal de la société afin d'éviter que le routeur soit saturer par du trafic excessif et inutile.

Dans la pratique la commande rate-limit s'utilise comme ceci :

```
Router(config-if)#rate-limit {input | output} access-group bps
burst-normal burst-max conform-action conform-action exceed-action
```

{input | output} : on doit spécifier dans quel sens le traffic sera limité.

access-group : numero de l'ACL concernée.

bps : vitesse maximale. burst-normal et burst-max : vitesse et vitesse max en rafale (nous utiliserons les valeurs par défaut).

conform-action : indique ce que l'on fait quand le traffic est conforme à la limitation.

exceed-action : indique ce que l'on fait quand le traffic dépasse la limitation.

Ce qui donne dans notre cas :

```
rate-limit input access-group 112 512000 64000 128000 conform-action
continue exceed-action drop
```

Ainsi les paquets non conformes seront supprimés.

IV - Système

1 - Les besoins

L'entreprise AeroDef nécessite pour le fonctionnement interne de ses employés des éléments suivants :

- Parc informatique destiné aux employés AeroDef avec accès au réseau extérieur,
- Service de messagerie électronique interne pour les employés AeroDef,
- Site Web de l'entreprise pour les clients AeroDef.

Ces éléments seront détaillés par la suite dans la présentation du système.

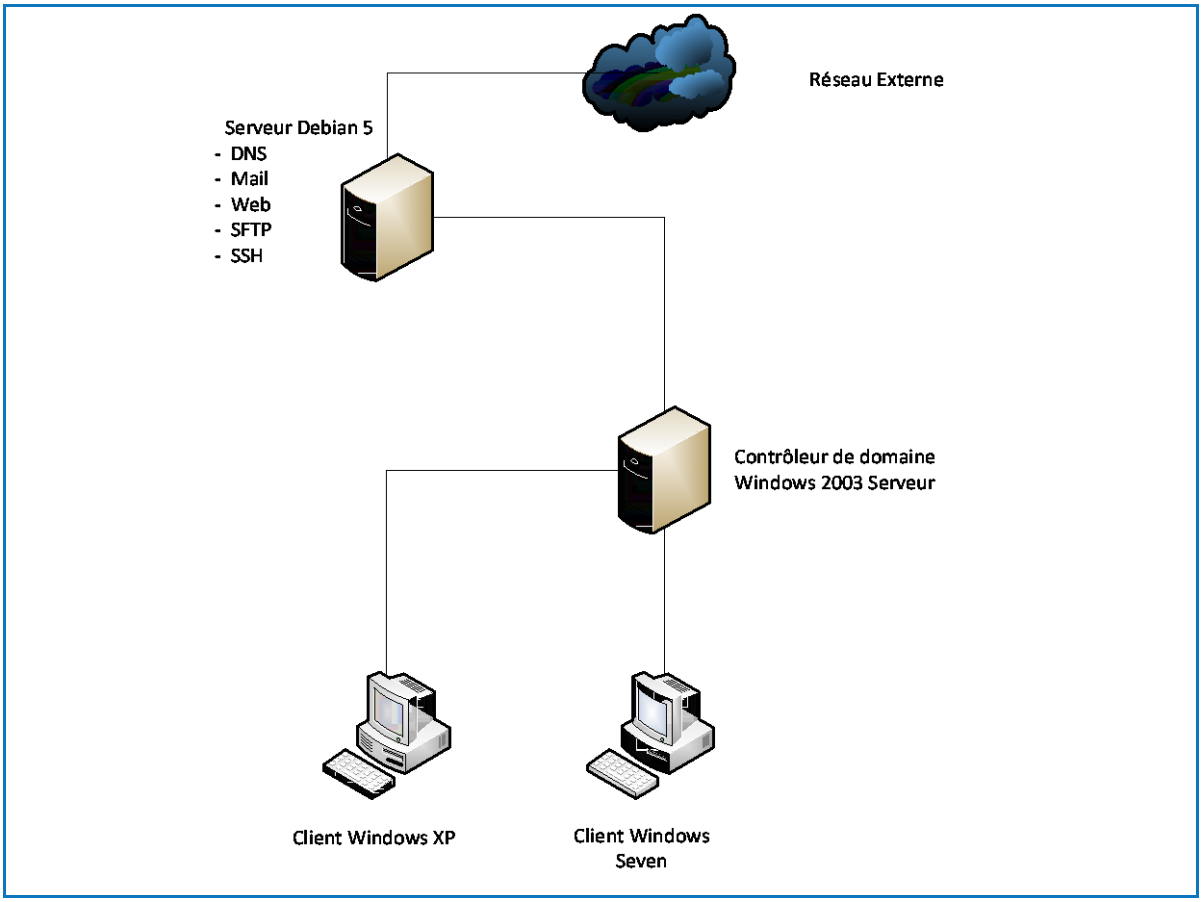
2 - Présentation du système

Le système de l'entreprise AeroDef est découpé en deux parties distinctes :

- Le parc informatique,
- Les services.

Ce découpage nous a permis d'isoler la partie réservée aux employés AeroDef de celles des administrateurs.

Voici la topologie initiale du système de l'entreprise :



2.1 - Les Services

Afin de répondre au mieux aux différents besoins explicités précédemment, nous décidons dans un premier temps de déployer les services suivants :

- DNS : Le service de résolution de nom de domaine effectuera la résolution des équipements interne à l'entreprise. Concernant les requêtes à destination de noms extérieurs au réseau local, le service contactera alors l'équipement de hiérarchie supérieur pour la résolution d'adresse, et transmettra les réponses aux équipements internes.
- Mail : Le service de courrier électronique prévoira un compte de messagerie interne à tous les employés de l'entreprise, accessible depuis un Web mail.
- Web : Pour ses clients et ses employés, l'entreprise doit être en mesure de proposer une interface Web avec système d'authentification. Ce site doit également posséder un espace sécurisé à l'aide du protocole HTTPS.
- SFTP : Le transfert de fichiers sur le serveur doit pouvoir s'effectuer, notamment pour l'ajout des fichiers relatifs au site Web, de façon sécurisée. Nous optons pour cela pour le protocole SFTP.

- SSH : Les différents serveurs doivent être accessibles à distance de façon sécurisée. Nous choisissons donc d'installer le service SSH qui garantit un accès distant avec un flux chiffré.

Disposant d'un nombre restreint d'équipements physiques, ainsi que d'un serveur à grande capacité de stockage (4x160 Go) le choix des différents équipements utilisés pour mettre en place ces services fut porté sur un unique serveur. En effet le faible taux d'utilisation des services et du réseau en interne nous permet de mutualiser les services sur un seul équipement.

Le serveur de service disposera donc du système d'exploitation Debian 5, reconnu pour sa fiabilité, son accessibilité et sa communauté d'utilisateurs très active.

2.1.1 DNS

Le service DNS utilise le protocole bind, la zone AeroDefense.stri a été définie pour l'ensemble du domaine interne de l'entreprise.

Les différents équipements définis dans le DNS sont les suivants :

- Zeus : il s'agit du serveur de service principal responsable entre autres du DNS
- Mail : le service mail est indiqué dans le DNS
- Web : le service web est également indiqué dans le DNS
- Contrôleur de domaine : l'entité responsable de la gestion du parc informatique

L'ensemble des équipements ci-dessus sont donc joignables à l'aide de leur nom d'hôte sur le réseau interne AeroDef.

La définition des services Web et Mail nous permet d'acquérir l'url www.aerodefense.stri pour le site de l'entreprise, et des adresses e-mail de type compte@mail.aerodefense.stri.

2.1.2 Mail

Le service Mail utilise l'agent SMTP/POP3 Postfix pour l'envoi et la réception de courriers électroniques sur le réseau interne. Nous n'avons pu ouvrir ce service en dehors du périmètre AeroDef en raison d'une restriction fixée par l'entité responsable du réseau sur le Campus Universitaire.

Le service mail, configuré dans le DNS, nous permet d'obtenir des adresses e-mail avec notre nom de domaine. Pour consulter leur messagerie le service de Webmail SquirrelMail a été installé sur le serveur. Nous avons opté pour cette solution car elle nous permet de nous affranchir de la lourdeur d'installation et de la restriction d'un client de messagerie local.

2.1.3 Web

Pour offrir aux utilisateurs, un service web, nous avons utilisé le service Apache2. L'accès au site peut se faire à l'aide des protocoles HTTP et HTTPS. Dans un premier temps le site permet les fonctions suivantes :

- Affichage de la page d'accueil,

- Connexion sur un espace sécurisé.

Le service PHP et une base de données MySQL ont également été installés pour ce faire.

2.1.4 SFTP

Le transfert de fichiers sur le serveur doit pouvoir s'effectuer de façon sécurisée. Nous utilisons donc le protocole SFTP, extension du protocole FTP mais disposant d'un chiffrement SSL pour le flux de données.

Les paramètres configurés pour ce service sont les suivants :

- Connexion possible uniquement avec les comptes locaux,
- Connexion impossible en super-utilisateur,
- Connexion impossible en anonyme,
- Chroot pour les utilisateurs dans leur dossier respectif.

Ce service a été déployé à l'aide de l'outil vsftp.

2.1.5 SSH

Le service SSH est primordial sur un équipement serveur, nous permettant un accès distant et sécurisé à l'aide d'un tunnel SSL sur ce dernier.

Les paramètres configurés pour ce service sont les suivants :

- Connexion possible uniquement avec les comptes locaux,
- Connexion impossible en super-utilisateur.

2.2 - Le parc informatique

Le parc informatique de l'entreprise est constitué des éléments suivants :

- Contrôleur de domaine : Equipement responsable de l'administration des équipements du parc informatique. Sur cet équipement seront définis les différents comptes d'accès pour les utilisateurs. Il permet également de relayer les requêtes DNS des équipements du parc à destination du serveur DNS de l'entreprise.
- Poste de travail Windows XP SP2 : Equipement utilisateur
- Poste de travail Windows Seven : Equipement utilisateur

L'intérêt d'utilisateur deux types de systèmes d'exploitation pour les stations de travail est de caractériser leur différences notamment par la suite lors des confrontations.

2.2.1 Contrôleur de domaine

Il s'agit d'un équipement fonctionnant à l'aide du système d'exploitation Windows Server 2003. Sur ce dernier ont été installés les services suivants :

- Active directory : il s'agit de l'annuaire utilisateurs. Deux types de comptes ont été créés :
  - CompteXP : compte utilisateur pour la station Windows XP SP2,
  - CompteSeven : compte utilisateur pour la station Windows Seven.
- AVG antivirus : Antivirus contre les fichiers malveillants.

2.2.2 Windows XP SP2

La station a été installée avec une configuration standard.

Les outils suivants ont été installés :

- AVG Antivirus : Antivirus contre les fichiers malveillants,
- Internet explorer 6 : Navigateur Internet.

V - Communication

1 - Politique de sécurité

1.1 - Rapport

La politique de sécurité de la société AeroDef est disponible en annexe de ce document.

Dans cette partie, nous justifierons si la politique de sécurité fut appliquée avec succès. Dans le cas négatif, nous citerons les points transgressés.

Le réseau de notre entreprise a subi des attaques tout au long des confrontations et vraisemblablement en dehors. La politique de communication a été généralement appliquée bien que parfois, les responsables du groupe audit venaient directement communiquer avec nos responsables architecture et système. Ce qui n'était pas convenu d'après la politique de sécurité.

Afin de contrôler nos communications, nous nous sommes rendu compte que l'attaque avait réussi à récupérer certains mots de passes. Ainsi, on peut donc constater que nos politiques de sécurité concernant la clause « Les périphériques » et la clause « Les mots de passe » n'ont pas été respectées.

En effet, la clause « Les périphériques » traitait un ensemble de directives et de bonnes pratiques concernant la formation des utilisateurs et leur sensibilisation sur les conséquences de leurs actions.

Bien souvent par facilité, certains équipiers venaient se connecter à leur messagerie personnelle depuis un poste de salle de TP. Généralement, ces postes étaient au préalable remis à zéro avec une nouvelle image. Mais cela ne garantit pas l'intégrité des machines (keylogger physique par exemple).

L'interdiction de se connecter à la messagerie de l'entreprise depuis l'université fut globalement respectée.

En ce qui concerne la politique des mots de passe qui était plutôt restrictive, une majorité ne l'aurait pas nécessairement appliquée. Le fait est que nous n'avons pas fait lire et signer la politique de sécurité à tous les membres de l'entreprise. Nous avons seulement énoncé à l'oral les grandes lignes, ce qui était insuffisant.

En pratique, nous avons réinitialisé nos comptes de messagerie de l'entreprise trois fois, afin de diminuer les risques d'être infiltré.

La clause de longueur et composition des mots de passes ne furent pas contrôlés. Ainsi, le mot de passe être plus facile à trouver par attaque en « force brute » ou même via « dictionnaire ».

Certains d'entre nous se sont d'ailleurs très peu connecté dans d'autres salles (comme en U3) avec leurs comptes de messageries personnelles.

L'attaqua a semble-t-il réussi à infiltrer notre messagerie de l'entreprise à cause de manquement à la politique de mots de passes. Certains auraient sans doute mis le même mot de passe pour différents services, ce qui aurait été à l'origine de l'infiltration dans notre entreprise.

Enfin, les mots de passe serveurs ont été communiqués par mail à l'équipe système, utilisateurs ayant leur messagerie potentiellement corrompue.

1.2 - Bilan

Pour être efficace et protectrice, la politique de sécurité doit être lue, approuvée et signée par tous les utilisateurs. Les utilisateurs doivent avant tout comprendre les risques et les raisons pour chaque clause. Le fait est qu'ils ne doivent pas se sentir trop restreints et surtout connaître son existence. La politique de sécurité doit être un mode de comportement, pour la pérennité de l'entreprise.

Dans notre cas, nous pouvons conclure qu'il est très difficile de faire appliquer une politique de sécurité. Aussi il ne faut pas se reposer sur celle-ci pour se sécuriser, mais plutôt mettre en place des moyens techniques pour ce faire.

2 - Le contrat passé avec l'audit

2.1 - Le contexte de l'appel d'offre

Dans le cadre du déploiement et de la sécurisation du système d'information d'une grande entreprise du secteur aéronautique, AeroDef (le groupe Défense), ayant été choisi pour la réalisation de ce projet, a décidé de faire appel à un prestataire de services : AssuranceTourix (le groupe Audit). Ce projet va se décliner en deux volets : la supervision système et réseau du système d'information de la grande entreprise du secteur aéronautique et le déploiement de la téléphonie sur IP (ToIP) dans ce même système d'information.

Pour se faire, AeroDef a diffusé (fictivement) un appel d'offre sur le marché auquel AssuranceTourix a répondu. Après discussion et négociation entre ces deux sociétés, deux contrats ont été rédigés : un portant sur la supervision du réseau et un autre portant sur la ToIP.

2.2 - Réponse à l'appel d'offre

Ce document a été fourni par AssuranceTourix et avait pour but d'une part, présenter la solution que proposait cette société et d'autre part, faire une estimation des coûts à la charge d'AeroDef.

Ainsi, AssuranceTourix a présenté à AeroDef sa société avec les qualifications et les compétences qu'elle offrait, une présentation de la mission proposée par AeroDef (afin de montrer qu'ils avaient bien compris la teneur du projet) et une présentation de l'entreprise AssuranceTourix.

Puis, cette entreprise a proposé une solution permettant la supervision. En effet, elle propose de mettre en place les outils suivants :

- Nessus : outils informatiques signalant les faiblesses de machines.
- Netflow : outil de métrologie (avec NFDump et NFSen).
- Syslog-ng : permet de collecter des informations et évènements sur les équipements du système d'information.
- FAN (Fully Automated Nagios) : outil de supervision de système d'information, d'analyse et d'envoi d'alerte.
- Prélude : système de détection d'intrusion (IDS) hybride travaillant sur le réseau comme sur les machines clientes, c'est-à-dire Network IDS et Host IDS.

Enfin, AssuranceTourix se propose de faire une analyse complémentaire afin de proposer des améliorations à AeroDef.

Le coût total proposé par AssuranceTourix pour cette prestation de service est 59 600€ fictifs. Cette estimation prend en compte les différents coûts humains et matériels dont cette entreprise a besoin.

AeroDef, au vu de la réponse à l'appel d'offre, a décidé de faire appel à AssuranceTourix pour cette mission car AssuranceTourix a su proposer des solutions satisfaisantes et un coût acceptable.

2.3 - Les contrats

Les deux contrats ont été exclusivement rédigés par AeroDef, en outre AssuranceTourix a pu soumettre des modifications, pour notamment protéger ses intérêts, qui ont été prises en compte dans les contrats.

Ils se sont principalement articulés autour de sept articles :

- Article 1 : Partage des informations, il spécifie les informations que les deux parties étaient prêtes à partager.
- Article 2 : Clause de confidentialité, il précise les conséquences d'une divulgation non désirée d'une information à un tiers (et notamment au groupe attaque).

- Article 3 : Moyens mis à disposition au Prestataire, ce sont tous les moyens qu'AeroDef a fourni à AssuranceTourix afin de bien mener cette prestation de service à son terme.
- Article 5 : Frais, ce sont les frais à la charge d'AeroDef
- Article 6 : Communication, cet article précise les moyens de communications à disposition des deux parties.
- Article 7 : Modification du contrat, permet une modification après la signature du contrat.

Les deux groupes présentés en introduction du contrat ont signé ce dernier à sa fin.

VI - Première confrontation

1 - Acquisition d'expérience

Cela fait maintenant plusieurs années que les Master 2 STRI réalisent un projet de sécurité. Chaque année, un rapport comme celui-ci est rédigé et ces rapports sont mis à disposition des nouvelles promotions. La lecture de ces rapport permet de mieux estimer les tenants et aboutissants du projet mais aussi de s'approprier une partie des expériences vécues par nos prédécesseurs. Ainsi nous avons décidé de répartir la lecture de l'ensemble des rapports depuis 2004 entre les différents membres de groupe avec rédaction d'un compte rendu des points les plus importants. Ces points ont été présentés et discutés lors de la réunion du 29 Septembre 2010 :

- L'ARP/DNS Spoofing a bien fonctionné pour les années précédentes.
- Le Social Engeneering est le principal danger.

Afin de se protéger des vols de mots de passe par social engineering, il est possible d'utiliser le cryptage des communications et les alertes SMS.

2 - Démarche itérative par paliers

Lors de notre seconde réunion le 27 Septembre, suite à la lecture des rapports des années précédentes, nous avons défini un système « idéal » prenant en compte toutes nos connaissances en sécurité informatique telles que le cloisonnement, la redondance et l'utilisation de proxys. Toutefois, une telle configuration est coûteuse en ressources, à la fois humaines et matérielles. Les délais étant réduits, nous avons décidé d'adopter une démarche itérative, c'est-à-dire que nous avons commencé par rendre opérationnel un noyau simple que nous améliorerons par la suite en fonction du temps et du retour d'expérience.

3 - L'audit

La prise de contact entre les groupes de défense et d'audit c'est faite le 28 Septembre. Au cours de cette réunion, les modalités de communication entre les groupes ont été fixées. A la

demande de l'Audit et en raison de leur politique de sécurité interne, toute communication électronique entre les groupes doit être chiffrée et signée.

Les groupes Audit et Défense doivent travailler ensemble à la sécurisation du système d'information AeroDef.fr mais ces groupes constituent deux entités différentes qui, dans le contexte professionnel, auraient des objectifs et des intérêts différents. Il est par conséquent important que la collaboration entre ces groupes soit contractualisée et clairement définie.

A l'issue de leur première réunion, les groupes Audit et Défense ont décidé de mettre en scène une contractualisation suite à un appel d'offre. Ainsi, le groupe défense à soumis un appel d'offre au groupe Audit. Cet appel d'offre comportait toutefois les différents points que le groupe audit souhaitait aborder. Suite à la réponse du groupe Audit, le groupe Défense à rédigé un Contrat qui a été discuté et signé avec le groupe Audit.

4 - Déroulement de la confrontation

Il a était convenu avec le groupe Attaque de débuter la première confrontation le lundi 11 octobre 2010. La première confrontation a pris du retard car la sécurisation de notre réseau n'était pas optimale, d'autant plus que certains points restaient à régler avec le groupe audit à la réunion le matin même de 8h30 à 8H55.

La confrontation a débuté lundi 11 octobre 2010 à partir de 10H30. Une liste de logiciels avec des versions précises avait été préalablement transmise au groupe communication. Il avait été demandé d'installer ces logiciels sur nos postes Windows.

Poste Windows XP	Poste Windows Seven
VLC 0.9.4	VLC 0.9.4
VNC 4.1.2	VNC 4.1.2
Open Office 3.2	Open Office 3.2
Acrobat reader 9.3.4	Acrobat reader 9.3.4

Le début de la confrontation fut marqué par l'envoi d'un premier mail à 10h36 :

Aux alentours de 10H45, il a été constaté au niveau du routeur un trafic très important. Comme il nous l'a été demandé par l'attaque, nous avons installés les logiciels sur nos machines clientes. D'ailleurs Un membre du groupe Attaque nous a proposé de nous transmettre une clef USB contenant la version d'Adobe Reader 9.3.4, version présentant une grosse faille de sécurité et difficilement trouvable sur le net depuis la sortie de la version 9.4.

Cela nous a laissé de fortes présomptions que l'attaque va tenter de se servir des failles de sécurité de ces logiciels pour réaliser leur exploit comme par exemple faire de l'injection de code malveillant.

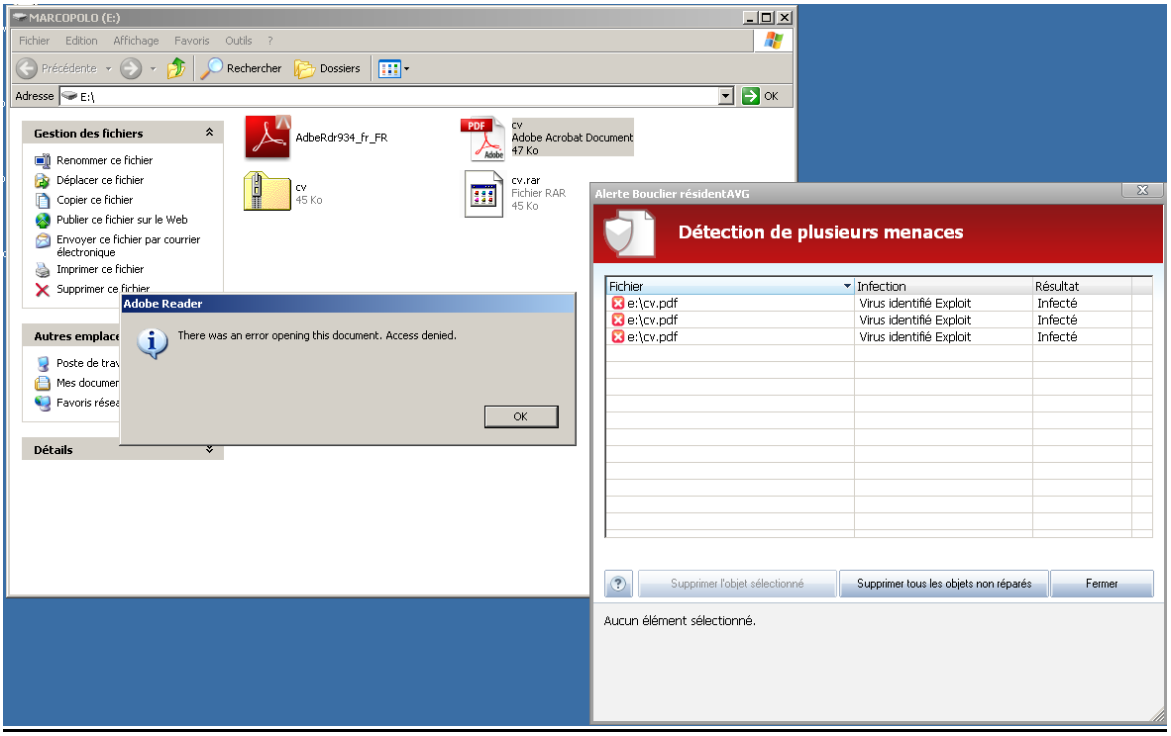
Les nombreuses tentatives d'installation du poste Windows SEVEN ne nous ont pas laissé le temps d'installer un antivirus. Ce dernier ne disposait pas de défenses particulières au niveau du poste mis à part la mise à jour du système effectuée.

En ce qui concerne le poste XP, il disposait d'un antivirus AVG mis à jour, d'une mise à jour du service pack 3, et la désactivation des dossiers de partages.

A 11h17, nous avons reçu un de leur mail nous informant qu'ils allaient nous transmettre une clef USB contenant un document PDF qu'il fallait ouvrir et laisser ouvert. Après réception de la clef USB, nous avons suivi leurs recommandations et laissé mis la clef USB sur le poste XP.

4.1 - Premier volet d'attaque

Première capture d'écran :



A 11h23, moment même où nous insérons la clef USB, notre antivirus AVG détecte la présence de menaces se situant dans le fichier PDF "CV.pdf".

Nous avions vu juste, l'équipe attaque cherche à exploiter la faille de sécurité de la version Adobe Reader 9.3.4 recensée par le lien suivant mis à jour le 5 Octobre 2010 : http://www.adobe.com/support/security/advisories/apsa10-02.html

"A critical vulnerability exists in Adobe Reader 9.3.4 and earlier versions for Windows, Macintosh and UNIX, and Adobe Acrobat 9.3.4 and earlier versions for Windows and Macintosh. This vulnerability (CVE-2010-2883) could cause a crash and potentially allow an attacker to take control of the affected system. There are reports that this vulnerability is being actively exploited in the wild."

Nous décidons donc de désactiver l'antivirus 15 minutes (temps maximum de désactivation de l'antivirus), afin de pouvoir lancer le document PDF, sous les recommandations de Ph Latu.

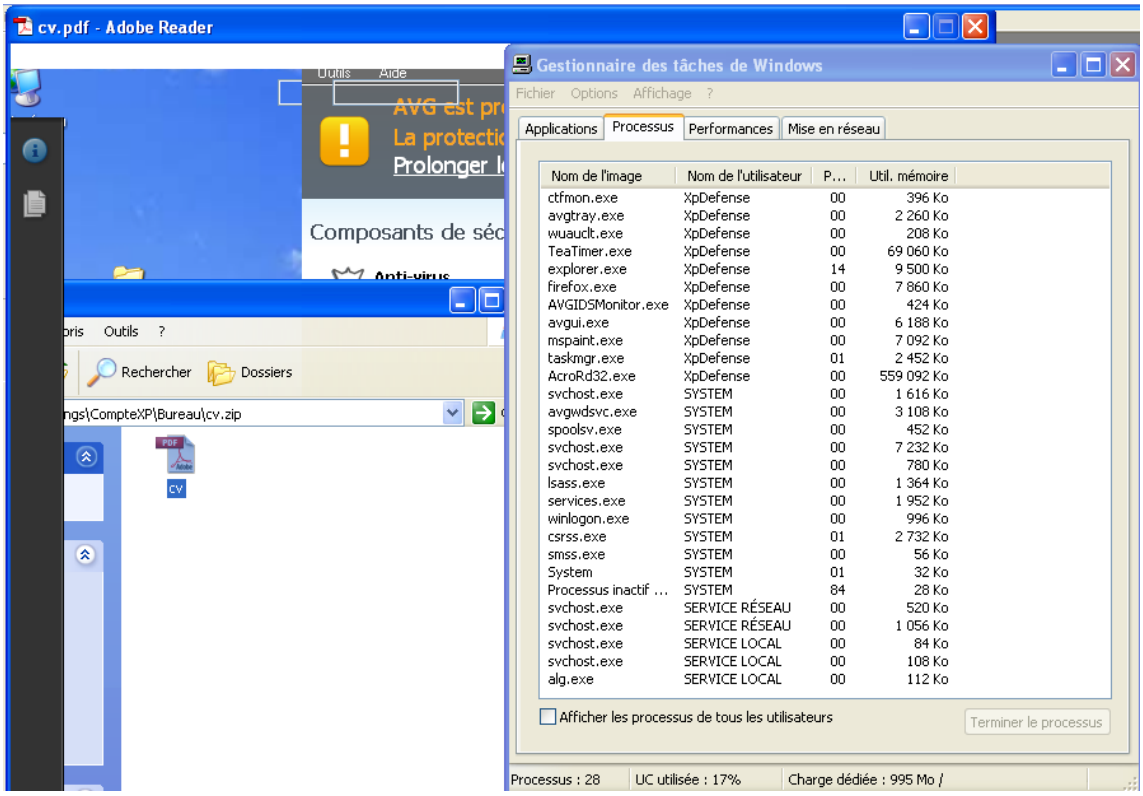
A 11h42, après désactivation de notre antivirus, on lance donc l'exécution du PDF avec les droits administrateurs. Il s'en suit un blocage de notre poste XP (écran figé).

Pour en avoir le cœur net, on observe les processus et on constate bien que l'espace mémoire utilisé par le programme Adobe Reader "AcroRd32.exe" est anormalement élevé. En

effet, pour un document PDF de 47Ko comme indiqué dans la première capture d'écran, l'occupation mémoire tourne aux environs de 26360Ko (tests à l'appui).

On observe ici pour le même programme, une occupation mémoire de 559092Ko soit plus de 21 fois l'occupation normale dans les mêmes conditions.

Seconde capture d'écran :



4.2 - Second volet d'attaque

A 11h45, nos postes de travail SEVEN et XP n'arrivent plus à joindre de site Internet. Peu après, on constate que chaque ouverture de navigateur Web nous redirige vers une page élaborée par le groupe Attaque.

5 - Présentation de l'architecture

5.1 - Les besoins

Durant ce projet nous avons mis en place une architecture correspondant à ce que l'on peut trouver dans une entreprise. Cependant, nous l'avons déjà évoqué, le nombre d'équipements que nous avons à disposition est assez limité.

Pour que notre architecture corresponde à ce que l'on peut retrouver dans une entreprise nous avons séparé les postes de travail et le serveur. Comme dit précédemment le nombre

d'équipements est limité donc nous allons mettre en place des VLANs pour simuler cette séparation.

L'équipe Audit travaille avec nous pour nous permettre d'effectuer une surveillance de notre architecture donc nous lui avons aussi créé un VLAN.

Pour simuler le fonctionnement d'une entreprise notre architecture devait être accessible depuis l'extérieur, donc nous avons mis en place des filtrages au niveau de notre routeur qui permettent de laisser passer seulement les flux autorisés. Tout comme dans le cas réel nous devons nous protéger de l'extérieur mais nous devions aussi effectuer un filtrage au niveau interne de notre architecture. Ceci pour permettre d'une part de réguler le trafic et donc pour que notre architecture ne soit pas inutilisable lors d'une trop grande activité, et d'une autre part pour nous protéger aussi de l'intérieur au cas où une de nos machines serait compromise.

Cependant durant ce projet des scénarios seront mis en place pour simuler des tentatives d'attaques de l'architecture. Pour répondre à cela nous avons du souvent baisser le niveau de notre filtrage pour que ces scénarios puissent être réalisés.

Coté système, toujours dans le but de simuler le réseau d'une entreprise, nous avons du mettre en place diverses installations toujours présentes dans certaines entreprise. Certaines installations assez vielles nous ont posé des problèmes mais dans le cadre des scénarios d'attaques nous devions mettre en place une protection sans devoir mettre à jour les installations.

5.2 - Architecture à la première confrontation

- Global+aerodef
- Réponse au besoin
- COnnexion vpn
- Mail AeroDef
- Vlan
- Trunk
- nat
- (Inventaire des équipements)

6 - Présentation du système

6.1 - Les besoins du groupe attaque

Le groupe Attaque nous a fait parvenir les besoins suivants pour les tests d'intrusion :

- Sur le serveur de services :

- Service FTP disponible
- Service Web disponible avec espace sécurisé

- Sur les postes de travail :

- VLC 0.9.4

- VNC 4.1.2
- Open Office 3.2
- Acrobat reader 9.3.4

6.2 - Les mesures de sécurité

Pour prévenir cette première confrontation nous avons effectué une sauvegarde du serveur de services à 'laide de l'outil SystemImager. Cet outil permet de transférer des partitions systèmes sur un serveur spécifique, et de les restaurer en l'état actuel à tout moment.

Sur les équipements clients ont été installés les logiciels suivants :

Poste Windows XP	Poste Windows Seven
VLC 0.9.4 VNC 4.1.2 Open Office 3.2 Acrobat reader 9.3.4	VLC 0.9.4 VNC 4.1.2 Open Office 3.2 Acrobat reader 9.3.4

6.3 - Attaques subies

Les attaques suivantes ont pu être réalisées :

- DNS Spoofing : Le service DNS a été compromis à l'aide d'une station tiers répondant plus vite aux requêtes DNS destinées à notre service DNS. Cet incident à des conséquences sur l'accès au réseau extérieur notamment à l'aide d'un navigateur. L'ensemble des requêtes http ayant été relayées sur un serveur auxiliaire
- Infection par code malveillant : Après désactivation de nos antivirus et exécution d'un programme sur les postes utilisateurs à la demande du groupe Attaque, nous avons relevé une importante charge système sur le poste Windows XP :

Cette première confrontation à eu un impact sur :

- Le parc informatique : L'attaque par DNS Spoofing a empêché la navigation Internet pour les utilisateurs. L'attaque par exécution de code malveillant ayant gravement détérioré la station de travail Windows XP.

6.4 - Réflexion sur les attaques survenues

DNS Spoofing : Pour se prémunir de ce type d'attaque les solutions sont les suivantes :

- Rendre les numéros d'identifications des requêtes difficilement prédictibles
- Chiffrage des flux DNS à l'aide de l'outil DNSSec

La première solution est difficilement réalisable car elle suppose les changements des identifiants dans les champs des trames DNS. Cette opération nécessite des connaissances et des délais supérieurs pour être mise en œuvre.

Nous ne pouvons également utiliser le chiffrage de flux DNS en raison de l'utilisation d'une autorité externe au projet pour la résolution des requêtes extérieurs. Cet équipement, qui n'est pas de notre propriété, devrait également être configuré avec DNSSec.

Ne pouvant mettre en œuvre l'un des deux solutions, nous n'avons pas pu déterminer une solution pour se prémunir contre ce type d'attaque.

- Exécution de code malveillant : Notre antivirus ayant détecté et empêché l'exécution du code malveillant, avant qu'il ne nous soit demandé de le désactiver, cette protection est donc considérée comme étant suffisante.

7 - Déroulement de la confrontation

Compte rendu Cyrille

8 - Retour d'expérience

Architecture / Système

Objectifs pour la prochaine confrontation

VII - Seconde confrontation

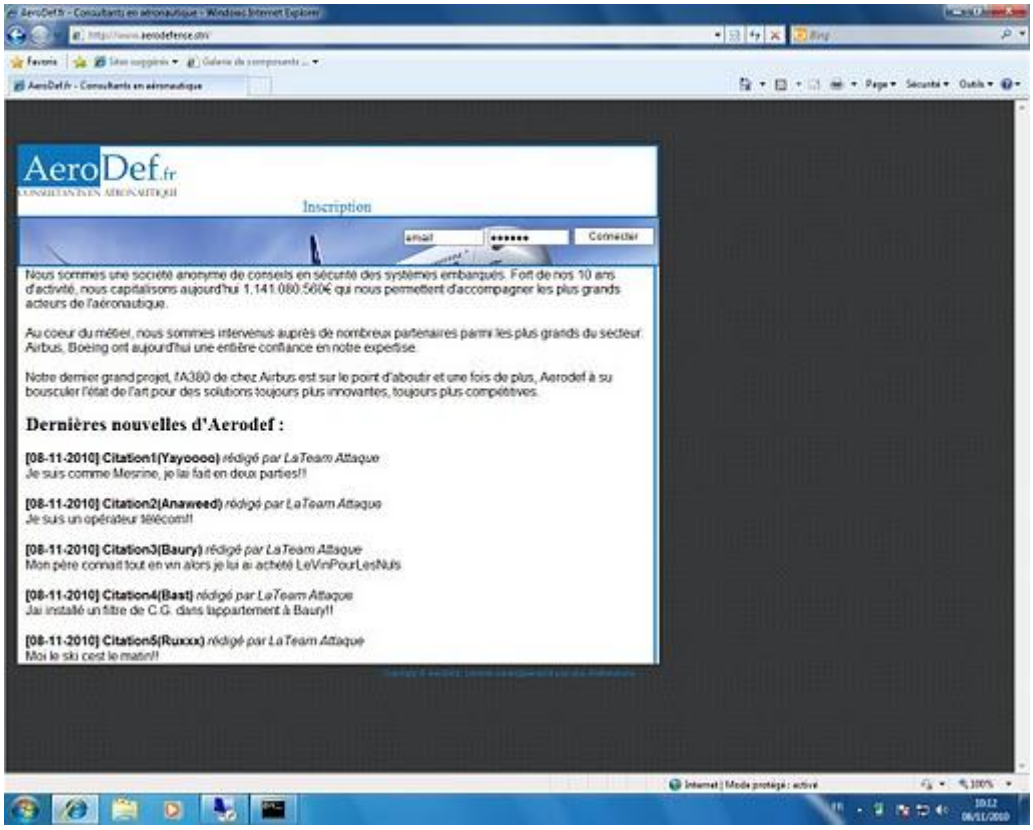
1 - Déroulement de la confrontation

Il a était convenu avec le groupe Attaque de débuter la seconde le lundi 8 novembre 2010. La seconde première confrontation s'est déroulée dans un contexte où l'architecture défense de notre entreprise s'est davantage développée depuis la première confrontation.

1.1 - Premier volet d'attaque

La confrontation a débuté à 8h00. A 8h57, nous avons reçu un premier mail de l'attaque nous demandant d'aller sur le site web de notre entreprise.

Première capture d'écran :



Nous avons ainsi pu constater à 9h09 que notre site Web avait été manipulé par l'attaque.

1.2 - Second volet d'attaque

Une liste de logiciels avec des versions précises avait été ensuite transmise au groupe communication dans un mail à 9h10. L'attaque nous a ensuite recommandé de les télécharger sur le site le site Oldversion.com à 9h21.

Poste Windows XP	Poste Windows Seven
QuickTime 7.6.7 Adobe Reader 9.4 IE 6 ou 7 au choix	Rien à signaler

La suite de la confrontation fut marquée par l'envoi d'un premier mail à 10h36 :

L'attaque souhaite ré-exécuter l'attaque PDF.

A 10h21, un autre mail nous a été envoyé. Il s'agissait de simuler un cas dans lequel une secrétaire clique sur un lien reçu dans un email, rentrez ce lien : http://172.16.48.73:8081/ en URL dans IE sur une machine XP. Ensuite, la secrétaire va boire un café 15 mn. Pendant ce temps, l'explorateur IE est toujours sur ce lien.

A 12h20, nous installons IE6, lançons http://172.16.48.73:8081/ et attendons 15 minutes.

A 12:23, la plage IP de l'attaque est bloquée par le routeur (Défense en profondeur). Il faut la débloquer le firewall pour que l'attaque puisse agir.

A 12:25, le firewall est débloqué et nous relançons la requête de la secrétaire.

A 12:26, sur le poste de la secrétaire, la fenêtre de IE s'est fermée (ou a été fermée).

2 - Présentation du système

2.1 - Les évolutions des services et des équipements

2.1.1 Sur le serveur de services :

L'outil Fail2Ban est installé sur le serveur de service principal. Cet outil prévient les attaques de type « brute-force » en analysant les fichiers logs des différents services de l'équipement. Si plusieurs tentatives infructueuses sont relayées dans ces fichiers, l'outil prend l'initiative de « bannir » l'adresse IP en cause pendant un certain temps grâce à l'ajout d'une règle Iptables.

Le site Web possède désormais la gestion dynamique de l'affichage de news. L'usage d'un fichier htaccess a permis une configuration spécifique du site web. Effectivement l'url est transformée grâce aux règles RewriteRule, ainsi les pages PHP apparaissent comme des pages statiques HTML (variables cachées).

2.1.2 Sur le parc informatique:

Le contrôleur de domaine est désormais configuré comme serveur DHCP pour toutes les stations présentes dans le parc informatique.

Nous avons également opté pour la vitalisation des clients à l'aide de l'outil VirtualBox. Ceci nous permettant une remise en état beaucoup plus rapide des stations utilisateurs. L'usage des machines virtuelles a été très limité : l'hôte ne supportait pas la machine virtuelle au-delà de 512 Mo de mémoire alléguée.

2.2 - Attaques subies

- DNS Spoofing : n'ayant pu nous protéger auparavant de cette attaque, le groupe Attaque a réédité l'attaque de DNS Spoofing paralysant ainsi notre accès au réseau extérieur.
- Intrusion Base de données : Le groupe Attaque est parvenu à accéder à notre service de base de données pour générer des news. Nous émettons l'hypothèse qu'ils aient exploité une faille récente du service MySQL pour s'introduire dans notre Système ou que l'attaque ait récupéré le mot de passe en question.
- Intrusion dans la base de données et génération d'une nouvelle.
- Exécution d'un lien malveillant : A la demande du groupe Attaque nous avons installé un certain nombre d'outils, désactivé certains outils de protection (Antivirus) puis cliqué sur un lien corrompu reçu dans un mail. Ceci eut pour conséquences un ralentissement brutal de la machine ainsi que la saturation de la mémoire physique de cette dernière.

2.3 - Réflexion sur les attaques subies

- DNS Spoofing : Nous supposons que cette attaque fut une diversion destinée à nous confondre et concentrer nos efforts sur d'autres aspects moins critique.
- Intrusion Base de données : La découverte d'une récente faille de sécurité de MySQL nous a poussés à effectuer une mise à jour générale du système. Il est important de notifier que l'attaque n'est pas dûe à une faille du site selon notre analyse.
- Exécution d'un lien malveillant : Cette attaque a pu être détectée et empêchée à l'aide d'outils de protection comme l'antivirus mais également le routeur qui effectue une analyse des flux.

VIII - Troisième confrontation

1 - Déroulement de la confrontation

Il a était convenu avec le groupe Attaque de débuter la dernière confrontation le lundi 15 novembre 2010. La troisième confrontation s'est déroulée très rapidement après la seconde confrontation.

Afin de ne plus renouveler les pertes de temps qui ont prolongés la seconde confrontation, nous avons conclu une liste de logiciels à installer au préalable avec l'équipe d'attaque dans un mail du 8 novembre à 13h23.

Une liste de logiciels avec des versions précises avait été ensuite transmise au groupe communication dans un mail à 9h10. Il avait été demandé d'installer ces logiciels sur notre poste Windows XP. L'attaque nous a ensuite recommandé de les télécharger sur le site le site Oldversion.com à 9h21.

Poste Windows XP (SP2)	Poste Windows Seven
QuickTime 9.6.7 Adobe Acrobat Reader 9.4 Internet Explorer 6.	Rien à signaler

Dans un second mail du 10 novembre 2010 à 00h13, l'attaque nous propose de pouvoir se connecter directement sur notre réseau pour simuler une machine corrompue dans le parc informatique du groupe attaqué. Il suffit pour cela que nous leur laissions un port sur notre commutateur.

1.1 - Volet d'attaque

9h30 : Il est constaté que les mots de passe administrateur du serveur ont été dérobés depuis un certain temps. La messagerie est compromise ainsi que tous les serveurs.

10h10 : exécution de fichiers PDF corrompus sur notre machine XP.

2 - Présentation Système

2.1 - Les besoins du groupe Attaque

Pour cette troisième confrontation, le groupe Attaque nous a seulement fait parvenir un fichier PDF corrompu, nous demandant de l'exécuter sur un des clients.

Nous avons observé leur confiance absolue à leur future attaque.

2.2 - Les évolutions des services et des équipements

2.2.1 Sur le serveur de services

Une mise à jour générale du système a été effectuée la veille de la confrontation afin d'éviter l'exploitation d'éventuelles failles de sécurité dans des versions d'outils obsolètes.

2.2.2 Sur le parc informatique

Le service Terminal Server a été installé afin de pouvoir configurer le contrôleur de domaine à distance.

2.3 - Attaques subies

- DNS Spoofing : Cette attaque n'ayant pas pu être prévenu fut une nouvelle fois reproduite.
- Intrusion générale dans le système : Le groupe Attaque est parvenu à accéder au serveur principal de services ainsi qu'au contrôleur de domaine, à en prendre le contrôle et à réinitialiser l'ensemble des accès.
- Disposant d'une sauvegarde relativement ancienne, nous avons préféré reprendre le contrôle du serveur de services à l'aide de l'outil Knoppix et ainsi réinitialiser tous les mots de passe. Nous avons grâce à cela détecté la présence d'un compte utilisateur suspect présent la veille de l'attaque.

Ne disposant pas de sauvegarde pour le contrôleur de domaine (solution lourde à mettre en œuvre pour le temps imparti) nous n'avons pu reprendre le contrôle du contrôleur de domaine.

2.4 - Observation ultérieure à l'attaque.

Les comptes de messagerie personnelle ainsi que ceux utilisés pour la gestion de ce projet furent corrompus. Effectivement, nous avons observé la création de transfert de mails vers un mail de l'attaque sur certaines de nos messageries personnelles et celles d'Aerodef. Même après changement des mots de passe, le transfert restait effectif.

Nous supposons que l'intrusion dans le système fut possible grâce à l'accès à la messagerie par laquelle nous nous échangions les mots de passe systèmes.

2.5 - Réflexion sur les attaques survenues

Cette confrontation fut la plus dramatique pour notre groupe, en effet l'accès aux comptes de messagerie ainsi que l'intrusion découlant sur notre système a permis au groupe Attaque de causer d'importants dégâts dans le système de la société AeroDef.

Cette seule attaque a permis entre autres : un déni de service général, la perte de l'accès à certains équipements, et l'impossibilité de communiquer (comptes mails corrompu). Voici les différentes possibilités de vols auxquels nous avons pensé :

- usurpation d'équipements réseau (U3),
- usurpation d'équipements réseau (Wifi),
- usurpation de service de messagerie en ligne (Gmail, Yahoo, ...). Effectivement, il nous a paru après coup s'être connecté à ces messageries en salle de TP U3 et avoir rencontré des problèmes de connexion.

Cette attaque a également perturbé la coordination entre le personnel AeroDef, en effet subissant plusieurs attaques instantanément, la perte d'accès à nos équipements et l'ignorance de la cause de cette intrusion nous a déstabilisés.

Nous supposons que celle-ci fut préparée de longue date avec soin afin de causer le maximum de dégâts possibles comme ce fut le cas.

Pour autant très intéressante, malgré sa gravité, cette confrontation nous a permis de comprendre la complexité d'entretenir la sécurité d'un périmètre et de réagir rapidement aux diverses attaques.

IX - Bilans et retours d'expérience

1 - Equipe Architecture

1.1 - 1er Jalon

Au cours des premières réunions, notre équipe s'est réunie afin de définir l'architecture et les services qui seront mis en œuvre. Nous avons ainsi débattu des systèmes et des solutions pouvant être retenues, leurs avantages et leurs inconvénients.

A la suite de cela, nous avons établi une architecture mettant en œuvre un ensemble de services. Nous avons alors configuré les différents équipements réseaux (Routeurs, Switchs) et les services associés (Filtrage, Vlans, ...).

1.2 - 1ère confrontation

Par manque de temps, les règles de filtrage n'ont pas pu être approfondies à temps, ce qui a eu pour effet une paralysie du SI à la confrontation. La correction de cet incident s'est alors faîte avec précipitation et sous pression des utilisateurs mécontents.

A la suite de cela, nous avons inspecté les différents flux transitant sur le parc informatique.

Suite à une attaque DNS Spoofing, nous avons étudié les solutions envisageables.

Nous avons également décidé pour la suite du projet :

- de compléter l'inventaire du parc informatique pour une vision exhaustive du SI.
- d'approfondir le filtrage sur les flux.

1.3 - 2eme Jalon

Nous avons mis en place les solutions décidées à la première confrontation. Une étude approfondie du filtrage Inspect a été nécessaire afin d'établir les règles de filtrage. Aussi un inventaire complet des équipements et des services a été effectué.

Nous avons ensuite effectué les opérations nécessaires au maintien en service du SI, notamment l'affinage des logs du routeur qui avait pour effet une baisse de performance de l'équipement.

Nous avons également mis en place les services nécessaire au groupe Audit (SPAN, Ouverture de port : Modification des règles de filtrage, ...).

1.4 - 2ème confrontation

Notre parc informatique a été là encore victime d'une attaque DNS spoofing.

Nous également avons inspecté les différents flux transitant puis avons bloqué les tentatives de Denis de service en filtrant la plage d'adresse IP de l'équipe attaque.

Avec succès puisque aucun Denis de service ne s'est produit. Les logs eux se sont abondamment remplis.

1.5 - 3ème Jalon

Nous avons effectué les opérations nécessaires au maintien en service du SI.

1.6 - 3ème confrontation

Notre parc informatique a été encore victime d'une attaque DNS spoofing.

Durant cette confrontation, un ensemble de service système ont été corrompu. Aucune défaillance particulière n'a été décelée au niveau de notre architecture réseau.

1.7 - Retour Expérience Général

Cette expérience fut enrichissante avec la configuration des équipements, les recherches associées et le travail d'équipe mis en œuvre pour parvenir à l'objectif fixé.

Notre travail fut principalement concentré en début de projet lors de la mise en place de l'infrastructure, à la suite de quoi l'activité principale s'est concentrée sur la maintenance de l'existant.

A noter qu'aucun déni de service sur notre Architecture n'a été efficace.

Les problèmes techniques qui furent toutefois rencontrés durant la mise en place du système d'information, ont mis en évidence l'importance de ce dernier et les conséquences de son dysfonctionnement.

Notamment les réactions rapides des utilisateurs et la correction des problèmes sous pression et avec précipitation.

De plus, notre groupe Architecture étant composé de personnes appartenant à des groupes de TD différents, nous avons eu du mal à nous concerter afin de mettre en commun les idées, débattre du travail à effectuer et des améliorations à mettre en œuvre.

Chaque tâche était alors attribuer à la volée à plusieurs personnes mettant en œuvre un travail d'équipe mais supprimant l'implication de chacun à long terme sur une tâche précise.

Nous avons ainsi remarqué l'importance d'une planification structurée qui définit l'objectif et l'attribution de chaque opération.

Ce projet a également mis en évidence l'importance de la communication pour un travail efficace.

Notamment au sein de l'entreprise entière où l'échange d'information sur l'avancée du travail furent peu nombreux.

Cette expérience fut donc riche en enseignement de par les caractéristiques de ce projet de grande envergure.

Nous avons ainsi remarqué l'importance d'une planification structurée qui définit l'objectif et l'attribution de chaque opération.

Ce projet a également mis en évidence l'importance de la communication pour un travail efficace.

Notamment au sein de l'entreprise entière où l'échange d'information sur l'avancée du travail furent peu nombreux.

Cette expérience fut donc riche en enseignement de par les caractéristiques de ce projet de grande envergure.

2 - Cédric Harismendy

Ce projet sécurité a été l'occasion de se confronter à de réels enjeux, tels qu'on pourrait les rencontrer en milieu professionnel.

En effet, le mode de fonctionnement collectif a permis de travailler en équipe et de façon réfléchie. Cette façon de faire permet un réel investissement et une implication accrue. De plus, l'autogestion a induit toute une phase de réflexion préliminaire intéressante.

L'organisation en plusieurs groupes de travail participe également à une meilleure cohérence. Malgré tout, il est vrai que de cette façon, il est parfois un peu difficile d'avoir une vue d'ensemble claire de toutes les activités.

Aux vues des différentes confrontations, il s'est avéré que notre travail a bien été efficace techniquement. En effet, les différentes attaques à l'encontre de notre système n'ont pas réellement affecté son bon fonctionnement, à l'exception du DNS Spoofing par exemple.

Par contre, l'utilisation du social engineering par l'équipe adverse a lui été bien plus performant. Malgré le fait d'avoir pris des précautions et d'y avoir pensé en amont, nous avons bien pu nous rendre compte de notre négligence sur ce point.

Malgré les résultats mitigés de toute cette organisation, il n'empêche que cela nous a permis d'en tirer des enseignements importants. En effet, il a été démontré de façon claire que les menaces qui semblent les moins dangereuses peuvent être les plus redoutables. Cependant cela s'avérera au final, pour notre futur, une bonne expérience et une prise de conscience efficace.

D'un point de vue plus personnel, ce projet a été enrichissant. Il m'a bien entendu permis de voir à quel point une cohérence et une rigueur dans les impératifs de sécurité étaient nécessaires. Il a également montré que la collaboration dans la mise en place du système était très importante, et qu'il fallait réellement communiquer entre les différentes entités.

3 - Cyrille Dumas

Ce projet sécurité m'a permis de me projeter dans un vrai contexte d'entreprise avec sa structure et ses objectifs. Ce fut une expérience très enrichissante de pouvoir manipuler sur du long terme et pas seulement l'espace d'un TP. Le coté enjeu mélangé avec l'aspect interactif avec les autres groupes était une motivation supplémentaire à celle même de faire de la sécurité.

Outre l'aspect technique, cela nous a permis de développer certaines qualités humaines que nous n'avons pas l'habitude de voir en milieu universitaire. Il s'agit des fonctions de management et de gestion de projet. Cela nous a permis de prendre conscience de son importance, et les responsabilités qui en découlent.

4 - Harboure Hubert Compaore

Le travail qui nous a été demandé dans le cadre de l'équipe défense était de mettre en place un système informatique d'une société.

Ceci était une expérience fructueuse pour ma part car elle me mettait dans la peau d'un membre du service informatique d'une structure en l'occurrence la société « Aero Defense ».

Ce qui est particulièrement enrichissant parce que nous nous retrouverons certainement dans cette situation dans notre vie professionnelle à venir. Nous serons prêts à donner notre avis sur une architecture ou une solution système donnée à la lumière de notre petite expérience.

En plus de ces rencontres de discussion et de confrontation d'idées au sein du groupe je peux souligner comme expériences acquises la notion de responsabilité dans le fonctionnement de ce qui m'était confié et aussi de tirer des leçons des pratiques de sécurité que nous avons mis en place face aux velléités de l'équipe attaque.

5 - Jérémie Belmudes

Très motivé par ce projet et le domaine de la sécurité, je me suis beaucoup investi dès le départ dans l'organisation du projet. Souhaitant m'orienter dans le domaine de la sécurité des systèmes d'information, je vois ce projet comme un tremplin.

C'était pour moi une première expérience en qualité de responsable de projet. Nous avons eu de nombreux projets tout au long de la formation STRI. Ici les groupes étaient constitués de 14 personnes, il n'est pas facile de gérer l'activité d'autant de personnes. Il est donc indispensable de savoir répartir les tâches. La création de sous-groupes gérés par un responsable a facilité les dialogues.

Lorsque des problèmes/conflits internes ou externes subviennent, c'est à la charge du responsable de les régler. On doit être diplomate et savoir faire des choix et surtout les faire appliquer. Dans mon cas, je n'ai rencontré que très peu de ces cas. La cohésion du groupe était très satisfaisante.

La part technique du projet n'était pas aisée non plus. Effectivement, le temps disponible pour la mise en place du système est court. Il faut choisir des implémentations simples, rapides et sûres. Il est conseillé de ne pas vouloir trop en faire.

En définitive ce projet, m'a montré la difficulté de mettre en place un système d'information complet et qui plus est sécurisé. Cela implique des configurations du système d'exploitation, de chaque service offert et surtout une rigueur dans l'utilisation du système, utilisation décrite dans la politique et charte de sécurité.

6 - Julien Desveaux

Faisant parti du service communication de la société AeroDef, je peux dire que ce projet m'a apporté une vision de la prestation de service proche de celle du monde du travail. Outre le fait de ma progression technique, le service communication devait avoir une vision globale de la mission en plus des réalisations techniques à faire. Ainsi, je pense que ce projet m'a préparé à ma future intégration au monde du travail.

7 - Laurent Roger

Ce projet fut le plus enrichissant de la formation car il nous a permis de mettre en place dans un contexte concret, les nombreuses connaissances que nous avons acquis sur :

- L'administration des réseaux
- L'administration Systèmes
- La gestion de projet
- La relation interpersonnelle au sein d'une entreprise

Ces paramètres combinés, nous ont permis de simuler le fonctionnement d'une véritable entreprise dans un cas critique.

Cette expérience nous a permis de prendre en compte la difficulté de la gestion de la sécurité d'un système au quotidien, l'anticipation sur les différentes failles de sécurité, ainsi que l'analyse régulière de la fiabilité d'un Système.

Les confrontations fréquentes furent une véritable source de connaissances techniques et de comportement à acquérir, tant le contexte critique au quotidien est enrichissant. Nous avons ainsi pu mettre en évidence notre manque de rapidité de réaction face à certaines attaques, le déni de certaines règles de sécurité primordiales (sauvegarde équipements fréquentes, social engineering) au profit d'autres.

Au contraire, nous avons pu tester la robustesse de certains outils, et valider la mise en place de certaines politiques de sécurité.

Responsable du service Systèmes, j'ai pu découvrir le métier de chef d'équipe avec toutes les responsabilités qu'il incombe ; la gestion et la communication des tâches au sein de l'équipe, et les relations avec les membres et les supérieurs.

8 - Mohamed Barry

Ce projet qui a été conduit en équipe a ressorti des aspects très positifs :

Concernant les aspects techniques du déploiement, nous avons pu mettre en place un système informatique réel regroupant en son sein tous les services qu'une société a besoin pour son réseau informatique. Ce qui nous a permis de voir en pratique la conception de réseaux informatiques LAN dans une entreprise et tous ce qui peux y avoir comme problèmes à confronter.

Sur le plan relationnel, ça été une collaboration de l'ensemble de l'équipe, nous nous sommes repartis en 3 groupes bien hiérarchisés : système, architecture, communication.

Sur l'aspect de la communication, les réunions de groupe ont été très intéressantes, car nous a permis de mieux repartir les taches nécessaires et trouver des solutions aux différents problèmes qui surgissaient. Ce qui a permis de faire un travail très cohérent. La solution de messagerie externe pour l'intégrité de nos données a été plus ou moins efficace. Elle nous a facilité l'organisation, la communication et le partage de nos documents mais malheureusement a subi une attaque qui a eu des conséquences très néfastes sur notre système.

Sur l'aspect de l'intégrité et confidentialité de notre système, il faut tout de même signaler des dérives de pratique du groupe attaque qui ont outrepassé le cadre réel du projet en volant les mots de passe de certains nos comptes personnels et en transférant l'ensemble de nos messages personnels sur un compte de messagerie. Ils sont à avertir que cette pratique est dangereuse, et peux entrainer une poursuite en justice.

9 - Wannes Vossen

Ce projet introduit quelques nouveautés par rapport à ce à quoi nous avions été habitués en STRI.

Pour commencer, à quatorze dans un groupe, les enjeux de la communication sont démultipliés. Par groupes de trois ou quatre, nous avons l'habitude de guider l'ensemble du projet d'une main commune. Chacun est alors présent à chaque réunion et les problèmes de

fond sont discutés jusqu'à ce qu'un accord soit trouvé. Cette façon de procéder n'est pas forcément la plus efficace mais du point de vue pédagogique, elle permet à chacun d'avoir une vision complète sur le thème traité.

Dans ce projet, une telle approche aboutit à de très longues discutions. Nous en avons fait l'expérience lors de nos premières réunions, lorsqu'il s'agissait de fixer nos objectifs. Une fois que chacun c'est vu attribuer sa tâche, les échanges entre membres se sont fait de manière de plus en plus ciblée et chacun a su prendre des initiatives dans son domaine.

Il ne faut pas non plus que chacun travaille dans son coin. Un mal entendu ou un oubli de communication est vite arrivé et peut avoir des répercussions sur l'efficacité du travail.

La taille du groupe pose aussi un problème quand à la responsabilité de chacun. La part de responsabilité, pour la réussite du projet, d'un membre parmi quatorze n'est pas aussi significative que celle qu'il aurait eue dans un groupe de trois personnes. Il n'y a aucune autorité entre étudiants et la participation de chacun dépend par conséquent de son bon vouloir.

Une deuxième particularité de ce projet, est la compétition, la méfiance et la séparation qui est introduite entre les trois groupes d'attaque, de défense et d'audit.

Du point de vue pédagogique, cela permet d'aborder le thème des « communications officielles entre entités distinctes aux intérêts contradictoires » à l'aide de procédures, de contrats et de politiques de comportement. Nous avons eu tout le loisir de constater la difficulté de cette tâche, d'être suffisamment méfiant sans pour autant passer notre temps à nous méfier. Du point de vue humain, la méfiance et le partage de responsabilités ont introduit quelques tentions, bien que nous ayons la plus part du temps su faire la part des choses.

Ensuite, ce projet se caractérise par la très grande autonomie laissée à chaque groupe. Les consignes sont larges et il est difficile de se positionner par rapport aux attentes de l'enseignement.

En ce qui concerne l'aspect de la sécurité informatique, nous l'avions descellé dans les rapports des années passées mais en avons quand même fait les frais : la plus grande menace est le social engineering. Le contexte de ce projet s'y prêtait particulièrement puisque nous avons côtoyé nos attaquants au jour le jour, qu'ils avaient un accès légitime à toutes nos installations et que nous avons partagé avec eux les mêmes infrastructures. Cela reste toutefois un bon avertissement quant à la facilité d'un vol d'informations, même quand on sait que quelqu'un s'y attèle.

En conclusion, l'autonomie, la durée, l'envergure du projet ont demandé un investissement particulièrement soutenu. Ce projet aura été riche en enseignements et en expériences nouvelles, pas toujours agréables mais probablement très utiles.