PROJET

Sécurité des systèmes d'information

Philippe BEAUGENDRE
Guillaume COTTIN
Emmanuelle DANG
Ilias DJOUAI
Cécile FOSSEN
Youri JEAN-MARIUS
Vincent LARRIBAU
Fabien PEYRONNET

21 Décembre 2006

SOMMAIRE

Introduction....4
Gestion de projet....5
Gestion des équipes....5
Gestion des étapes....6
Gestion du planning....7
Déroulement du projet....9
Phase 0....9
Phase 1....15
Phase 2....18
Phase 3....20
Conclusion....22
Bilan du projet....23

Introduction

Le but de ce projet était de diviser la demi classe en trois groupes ayant des fonctions différentes. Chaque groupe était donc composé de 8 personnes, ce qui est un nombre conséquent quand il s'agit de travailler ensemble. Nous avons donc du apprendre à mieux communiquer afin que tous les membres du groupe soient constamment au courant de l'avancée des autres membres. Ce projet avait donc un grand aspect communication et gestion de projet. Il fallait synchroniser les membres d'un même groupe mais aussi synchroniser les groupes entre eux. Nous devions donc communiquer entre partenaires mais aussi entre concurrents puisque nous étions chargés de planifier les attaques en accord avec le groupe « Attaque » et le groupe « Audit ». Ce projet avait donc un aspect humain très important puisque malgré la concurrence qui nous liait au groupe « Attaque » nous devions faire au mieux pour ne pas les bloquer complètement.

Nous étions donc le groupe surnommé « Défense » et nous avons eu pour mission de concevoir un réseau et de le sécuriser de façon « basique » afin que nos collaborateurs (les autres groupes) puissent effectuer des opérations d'audit et d'attaque.

Tout au long du projet, nous sommes restés dans l'optique de ne pas instaurer de politiques de sécurité trop exigeantes afin de ne pas empêcher totalement le groupe des attaquants à obtenir des résultats.

Au premier abord nous avions défini le projet en 4 grandes étapes. Ces étapes étaient découpées par les interventions des groupes « Audit » et « attaque » sur notre réseau. En effet nous avions défini pour première étape tout ce qui consistait aux recherches préalables des technologies à utiliser, à l'inventaire du matériel disponible et pour finir le déploiement physique du réseau. Une fois cela effectué nous pensions passer à la seconde étape en laissant le groupe « Attaque » et le groupe « Audit » procéder à leur première intervention. Ainsi, le groupe « Audit » nous aurait fourni le premier bilan qui nous aurait permis d'apporter des modifications sur notre architecture. Serait alors venu le temps de procéder à une seconde attaque marquant le passage à la troisième étape. De même que précédemment nous aurions pu procéder à de nouvelles modifications sur le réseau. A partir de là, nous pensions laisser réaliser une ultime attaque sur le réseau afin de conclure par la dernière étape de remise à niveau du réseau. Malheureusement, tout n'a pas pu se dérouler ainsi, voici donc les vraies étapes qui ont été faites.

Gestion de projet

➢ *Gestion des équipes*

Pour une organisation du travail plus facile, nous avons choisi de diviser l'équipe en différents pôles, chacun chargé d'une mission pour mener à bien le projet ainsi que le déploiement de notre architecture.

La répartition des « missions » a été faite ainsi :

- **Pôle Interconnexion** : Ilias et Fabien qui ont été chargés de la partie sécurisation de l'architecture
- **Pôle Services** : Guillaume et Youri, chargés du déploiement des services
- **Pôle Utilisateurs** : Philippe et Vincent qui devaient déployer les postes clients
- **Pôle Communication** : Cécile et Emmanuelle qui s'occupaient de gérer le projet au sein de l'équipe et les relations avec les autres équipes

Tout au long du projet, il a été question pour le pôle Communication de veiller à garder une bonne entente au sein de l'équipe afin de ne pas laisser un tel projet changer les relations que nous avions en dehors de ce contexte.
Mais gérer différents pôles n'est pas chose facile surtout lorsqu'il s'agit de coordonner le travail de chacun. Pour cela nous avions instauré des « règles » à respecter afin de connaître l'avancement de chaque groupe. La gestion de projet dans cela consistait à faire respecter les règles et à rappeler aux membres qu'ils devaient faire ce qui leur était demandé.

Gérer un tel projet faisait également intervenir les deux autres équipes. Un « contrat » a été établi entre notre équipe et l'équipe « Audit » afin que ce qui leur était demandé nous soit délivré au moment adéquat et en bon éduforme.

➢ *Gestion des étapes*

Les différentes étapes du projet ont d'abord été décidées par notre pôle Communication puis discutées avec les autres équipes afin de mettre tout le monde d'accord et de faire en sorte que chaque équipe soit satisfaite.

Les dates des différentes attaques ont été convenues par rapport aux disponibilités de chaque équipe afin de leur donner le temps nécessaire entre chaque attaque.

Les échanges intergroupes se faisaient principalement par mail via le pôle Communication. Cela permettait d'en garder une trace et servait en même temps de confirmation.

♦ Communication avec l'équipe « Audit »

Avant de réellement commencer le projet en faisant intervenir les deux autres équipes, nous avons été « confronté » à l'équipe « Audit » afin de mettre en place des règles de confidentialité et les moyens qui nous permettraient d'échanger les informations relatives au projet.
Cette phase s'est révélée assez difficile au départ car il n'est pas évident de mettre tout le monde d'accord sur un sujet qui s'avère être délicat dès qu'on l'appelle « contrat ».

Finalement, nous avons trouvé un terrain d'entente et tout a été correctement respecté.

♦ Les attaques

Les étapes du projet correspondent aux différentes attaques. Les dates des attaques étaient convenues avec l'équipe « Attaque » qui nous tenait informés de leurs disponibilités aux dates convenues.

Il a toujours été question de respecter le travail de chaque groupe et permettre à chacun d'être prêt avant chaque attaque. A ce niveau là, il n'y a pas eu de malentendu ou de problème quelconque.

♦ Communication interpoles

La communication au sein de notre équipe consistait à avertir d'une manière formelle les autres pôles de l'avancée du projet et du travail qu'il fallait réaliser. Il fallait garder à l'esprit l'échéancier et permettre le bon déroulement du projet, c'est-à-dire sans trop prendre de retard et en réalisant les documents nécessaires.

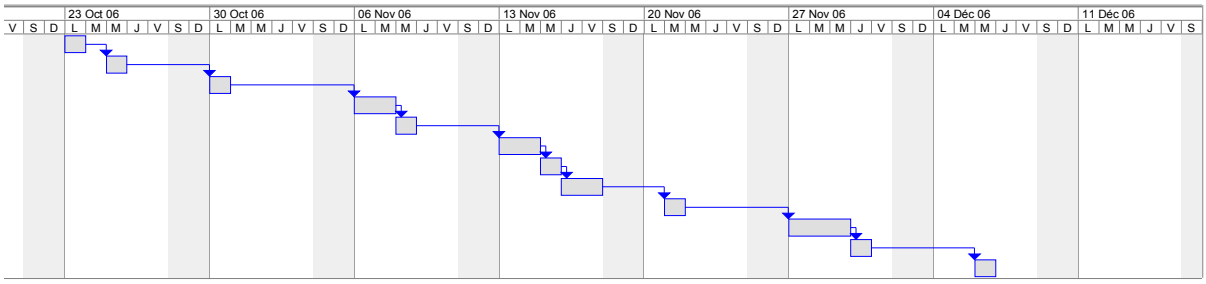
Encore une fois, il n'y a pas eu trop de problèmes à ce niveau là, si ce n'est que « rappeler à l'ordre » un certain nombre de personnes n'est pas toujours facile.

➢ *Gestion du planning*

En phase préliminaire du projet, il a été convenu de 5 attaques, la dernière devant avoir lieu le 30 novembre, ce qui nous aurait laissé le temps pour finaliser le projet.

Le planning suivant a donc été conçu :

N°	Nom de la tâche	Durée	Début	Fin
1	Réseau opérationnel	1 jour?	Lun 23/10/06	Lun 23/10/06
2	Premier audit	1 jour?	Mer 25/10/06	Mer 25/10/06
3	Première attaque	1 jour?	Lun 30/10/06	Lun 30/10/06
4	1er rapport audit + modifs	2 jours?	Lun 06/11/06	Mar 07/11/06
5	2ème attaque	1 jour?	Mer 08/11/06	Mer 08/11/06
6	2ème rapport audit + modifs	2 jours?	Lun 13/11/06	Mar 14/11/06
7	3ème attaque	1 jour?	Mer 15/11/06	Mer 15/11/06
8	3ème rapport audit + modifs	2 jours?	Jeu 16/11/06	Ven 17/11/06
9	4ème attaque	1 jour?	Mar 21/11/06	Mar 21/11/06
10	4ème rapport audit + modifs	3 jours?	Lun 27/11/06	Mer 29/11/06
11	5ème attaque	1 jour?	Jeu 30/11/06	Jeu 30/11/06
12	5ème rapport audit + modifs	1 jour?	Mer 06/12/06	Mer 06/12/06



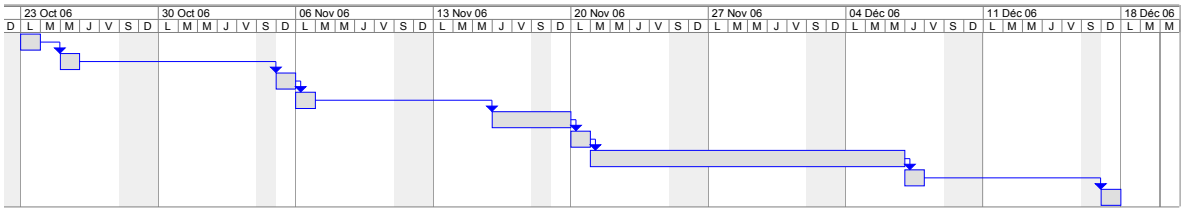
Malheureusement c'était sans compter les contretemps relatifs aux autres projets que nous avions en parallèle.
Le déploiement de l'architecture n'a pas pu permettre d'effectuer la première attaque à la date prévue.

Ce retard a entraîné la suppression de deux attaques.

Un planning final a donc été conçu selon 3 phases d'attaques :

- Une 1ère attaque sur notre réseau non sécurisé
- Une 2ème attaque avec une sécurité un peu plus renforcée
- Une 3ème attaque en permettant à l'équipe « Attaque » d'opérer de l'intérieur de notre réseau

N°	Nom de la tâche	Durée	Début	Fin
1	Réseau opérationnel	1 jour?	Lun 23/10/06	Lun 23/10/06
2	Premier audit	1 jour?	Mer 25/10/06	Mer 25/10/06
3	Bilan de sécu n°1 & 2	1 jour?	Dim 05/11/06	Dim 05/11/06
4	Première attaque	1 jour?	Lun 06/11/06	Lun 06/11/06
5	Bilan de sécu n°3 + modifs	3 jours?	Jeu 16/11/06	Dim 19/11/06
6	2ème attaque	1 jour?	Lun 20/11/06	Lun 20/11/06
7	Modifs	12 jours?	Mar 21/11/06	Mer 06/12/06
8	3ème attaque	1 jour?	Jeu 07/12/06	Jeu 07/12/06
9	Bilan de sécu n°4	1 jour?	Dim 17/12/06	Dim 17/12/06



Une organisation de la sorte nous a conduit à effectuer la dernière attaque le 7 décembre, les autres projets ne nous permettant pas de la mettre en place plus tôt.

Le projet s'est donc découpé comme suit :

- Phase 0 *(23 oct - 5 nov)* : le déploiement du réseau
- Phase 1 *(6-19 nov)* : de la 1ère attaque à la 2ème
- Phase 2 *(20 nov - 6 déc)* : de la 2ème attaque à la 3ème
- Phase 3 *(7-17 déc)* : après la 3ème attaque

Finalement, 3 attaques s'avéraient être suffisantes pour que chaque équipe puisse en tirer un bilan favorable.
Le but n'étant pas de sécuriser au maximum afin d'empêcher les attaquants de compromettre notre réseau, il en ressort pour chacun un résultat plutôt positif.

Déroulement du projet

Comme nous l'avons dit précédemment, le projet ne s'est pas déroulé exactement de la façon que nous avions pensée. Au final, nous constatons que nous avons tout de même réussi à laisser le groupe « Attaque » procéder à trois interventions ce qui est tout de même satisfaisant étant donné le travail que nous avions en dehors de tout ceci.

Voici donc comment se sont déroulées les différentes étapes de notre projet. Afin de mieux comprendre nous avons détaillé les étapes suivant les différents binômes de notre groupe.

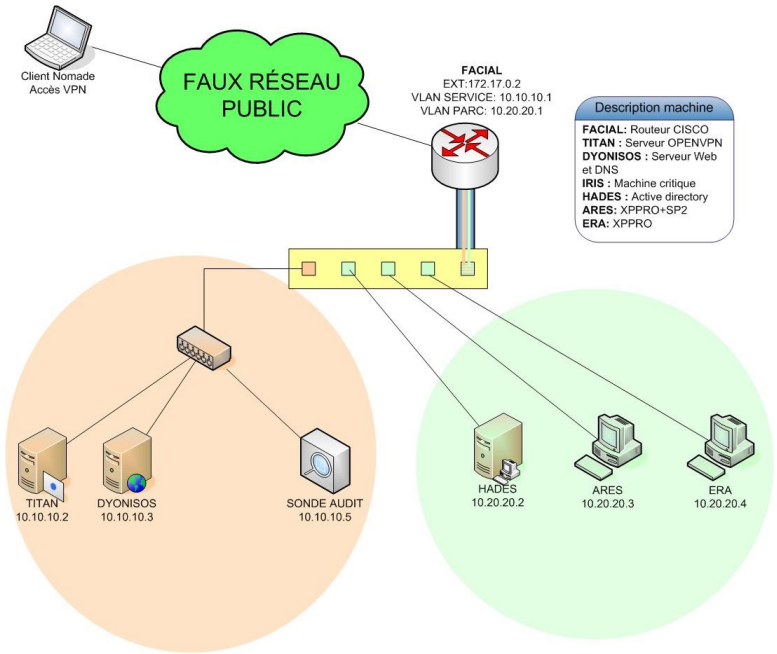
➢ *Phase 0*

La phase 0 consiste comme nous l'avons défini précédemment dans la recherche d'informations, le découpage du groupe en binômes et le déploiement de chaque pôle.

Nous avons commencé par procéder à la répartition des rôles de chacun afin de ne pas se lancer tous dans les mêmes recherches. Les binômes ont été présentés plus haut.

Une fois la répartition faite, chacun a fait des recherches de son côté sur les besoins propres à son rôle puis nous nous sommes réunis le mercredi 4 Octobre pour exposer les choix que nous avions faits à tous les membres de l'équipe. Nous avons ainsi pu nous conseiller les uns et les autres et ainsi définir l'architecture que nous voulions mettre en place ainsi que les logiciels que nous voulions utiliser.

L'architecture de notre réseau a donc été choisi comme suit :



Dès la seconde réunion du lundi 9 Octobre nous avons pu commencer les installations et les poursuivre le mardi et le mercredi suivant. Quelques problèmes sont survenus ce qui a fait que le lundi 16, le mardi 17 et le mercredi 18 les installations se sont à nouveau poursuivies et se sont terminées le mercredi 25 pour les binômes « Interconnexions » et « Utilisateurs » et le mardi 31 pour le binôme « Services ». Voici ce qui a été réalisé.

♦ Pôle Communication

Le pôle Communication a eu pour première tâche la rédaction des contrats aussi bien intergroupe et intra-groupe.

Pour chacun des deux contrats, il a été stipulé que la divulgation d'informations n'était pas permise, que la communication devait passer par les personnes concernées afin de ne pas parler à droite et à gauche sans avoir aucune trace de ce qui était dit. Il a aussi été fixé des délais à respecter (ce qui n'a malheureusement pas été toujours le cas malgré les précautions prises).

Au sein du contrat intra-groupe nous avons défini une politique de mot de passe ainsi qu'une politique de compte rendu qui a été appliquée à peu de choses près correctement. Il a aussi été imposé le nettoyage des postes après notre passage ce qui n'a malheureusement pas toujours été suivi ce qui a pu nous causer tord mais nous ne le savons pas de façon sûre pour le moment.

Au sein du contrat intergroupe, nous avions demandé une certaine fréquence de rapports qui n'a pas été respectée et qui leur aura causé du tord par la suite.

La signature de ces contrats n'a pas été évidente même si les pôles de communication des deux groupes se mettaient toujours d'accord, il apparaissait par la suite que le pôle communication du groupe « Audit » n'arrivait pas à convaincre les membres de leur équipe et devait revenir vers nous pour apporter de nouvelles modifications. Les contrats ont été remis pour la première fois le lundi 16 Octobre et ont été signés le jeudi 19 Octobre après de longs débats.

En ce qui concerne la signature du contrat intra-groupe, elle s'est effectuée dès la remise des contrats aux divers membres de l'équipe.

En parallèle de la rédaction de ces divers contrats, nous avons accompagné nos équipes dans la poursuite des installations le lundi 16, le mardi 17 et le mercredi 18 Octobre. Nous profitions de ces moments-là pour prendre des notes et récupérer des informations qui étaient susceptibles de nous être demandées par la suite par le groupe « Audit ».

Au cours du week-end du 21-22 Octobre nous avons reçu la première demande d'informations du groupe « Audit » à laquelle nous avons apporté une réponse dès le lundi suivant.

♦ Pôle Interconnexion

Le pôle Interconnexion a mis en place le routeur faisant l'interface entre le pseudo réseau public et le réseau local de Candide SA.

Le routeur est branché sur le Switch SW3550(SW1) sur un des ports attribués à la Défense du groupe 1. Ils ont tout d'abord mis à jour l'image de l'IOS du routeur (12.4.1a vers 12.8 advanced services).

Ils ont ensuite sécurisé les accès Telnet et console par un mot de passe respectant les règles de sécurité. Nous avons aussi ajouté un mot de passe pour le mode privilégié de l'accès au routeur.
Tous ces mots de passe ont été cryptés en AES.

Informations essentielles relatives à la première étape :

- Nom du routeur : Facial
- Type de router : Cisco 1841
- Adresse IP du routeur : 172.17.0.2

♦ Pôle Services

La phase 0 a représenté pour ce binôme un déploiement des machines et de leurs services de manière simpliste (pas de sécurisation des services). Voici donc leur démarche :

- **Inventaire du matériel qui était à leur disposition :**

Nous avons trois machines à disposition. Cependant une des machines a un problème matériel. Nous devons donc nous contenter de deux machines.

- **Choix du système d'exploitation et installation :**

Le choix du système d'exploitation s'est porté sur un Linux Debian Sarge pour nos services WEB, DNS, VPN et Base de données. Le service de messagerie sera déporté sur le serveur d'Active directory géré par le groupe utilisateurs. Après l'installation des deux machines sous linux nous procédons à la sécurisation du BIOS et le blocage du démarrage sur CD. Nous avons au final deux machines sous linux nommées **Dyonisos** et **Titan.**

- **L'adressage de nos machines**

L'adressage de nos machines correspond au plan d'adressage fixé lors d'une de nos réunions. Nous avons donc convenu que nos machines de services seraient isolées sur un VLAN évoluant par la suite comme une DMZ. Ce VLAN nommé Service à l'adresse réseau suivante 10.10.10.0 d'où

Titan 10.10.10.2
Dyonisos 10.10.10.3

- **Mise en place des services demandés**

Le serveur WEB + BD :
L'installation du serveur WEB a été réalisée sur Dyonisos par l'installation des packages suivants :

- Apache2
- PHP4
- MySQL
- phpMyAdmin

Le serveur DNS :
Le serveur DNS a été installé sur Dyonisos par l'installation de Bind9
Il répond aux demandes sur les noms suivants :

- www.candide-sa.com
- candide-sa.com
- mx de candide-sa.com

Le serveur VPN :
Titan a été dédié à l'accès VPN pour cela nous avons installé OpenVPN sur cette machine. Un seul certificat à été créé pour l'accès multiple des différents administrateur de chaque équipe. Cette machine réalise aussi une traduction d'adresse entre le réseaux local et le point a point établit avec l'utilisateur.

La messagerie d'entreprise :
Le service de messagerie a été déployé sur le serveur d'Active directory (Windows 2003 Serveur) par l'installation du logiciel Exchange 2003 lié à l'Active directory. La gestion de la messagerie est réalisée par le groupe utilisateurs.

Développement du site web :
Le site web à été développé en PHP et contient 3 pages :
Index.php => Page d'accueil
Société.php=>Page de présentation de la société
Livredor.php=>Page permettant de recueillir les impressions des internautes

- **La première attaque**

Lors de la première attaque nous avons remarqué que les attaquants remplissaient de manière anormale notre base de données correspondant à notre livre d'or par une boucle d'insertion de commentaires. Les conséquences pour notre société a été la perte des informations utiles (impressions de vrais internautes sur notre société) et un risque de chute de notre serveur de base de données. Heureusement le serveur a tenu le coup et nous avons pu vider la base.
Une autre attaque nous a permis de nous rendre compte que les utilisateurs étaient redirigés vers de mauvais sites web et que leurs mots de passe étaient récupérés. Les conséquences pour notre société ont été plus grave puisque certain de nos utilisateurs ont fournit leurs accès aux site web de nos partenaires (la société stri) et notre DNS n'était plus pris en compte.

♦ Pôle Utilisateurs

Cette première étape a été réalisée en LAN fermé chez une des personnes du groupe.

Nous avons tout d'abord installé un serveur de domaine et deux clients XP et nous avons réfléchi à un plan d'adressage pour notre architecture :

- Installation de Windows 2003 Server et mise en place du contrôleur du domaine candide-sa.com et du serveur DNS Interne sur la machine Hadès.
- Installation d'un client Windows XP non sécurisé et intégration dans le domaine. Machine Arès.
- Installation d'un client Windows XP « sécurisé » avec SP2 et intégration dans le domaine. Machine Era.

Nous avons alors établi un plan d'adressage que voici :

Nom	Adresse IP	Caractéristiques
HADES	10.20.20.2	Contrôleur de domaine, le DNS lui étant rattaché, ainsi qu'Exchange Server 2003
ARES	10.20.20.3	Client XP Pro sans service pack ni aucunes mises à jour
ERA	10.20.20.4	Client XP pro « sécurisé » : SP2 et mises à jour

Puis nous avons défini des règles de complexité sur les mots de passe avec expiration.

Nous avons ensuite créé deux comptes de domaine avec les droits administrateur, ainsi qu'un compte administrateur local identique sur chaque machine.

Nous avons également désactivé le « boot » sur disquette et CD et mis des mots de passe d'accès au BIOS des postes.

Nous avons ensuite transféré les machines pour les mettre en place en salle 213 en respectant le plan d'adressage défini.

Suite à cela, voici un récapitulatif des machines du réseau :

Nom de la machine	Adresse IP	Système d'exploitation	Description des services	Ports
FACIAL	Externe: 172.17.0.2	IOS CISCO 12.8 AS	Routage inter Vlan	
	VLAN Service: 10.10.10.1		Traduction d'adresse NAT	
	VLAN Parc: 10.20.20.1		Forward des ports	443,53,80,8080,25,110,143,12768
TITAN	10.10.10.2	Linux Debian	SSH	2222
			OPENVPN	443
			Traduction d'adresse NAT	
DYONISOS	10.10.10.3	Linux Debian	Apache 2.0 (web)	80
			PHP 4	
			Mysql	
			DNS (candide-sa.com)	53
			SSH	2222
HARES	10.20.20.2	Windows 2003 Serveur	Serveur de domaine (Active Directory)	
			Messagerie Exchange 2003	
			DNS interne	
			DHCP	
			VNC Serveur	5901
ADES	10.20.20.3	Widows XP PRO + SP2	Outlook 2003	
			VNC Serveur	
ERA	10.20.20.4	Widows XP PRO	Outlook 2003	
			VNC Serveur	5901
IRIS	none	none	Machine HS	

Bilan de cette phase : les interprétations et les conseils de l'audit

Pendant cette période de déploiement, le groupe « Audit » procédait lui aussi au déploiement de sa sonde sur notre réseau. Ils ont avant la première attaque pu nous communiquer deux bilans de sécurité. Le premier nous demandait de surveiller les logs de notre serveur Apache, ce conseil s'est conclu par le transfert automatique de nos logs sur la machine de l'audit.

Le second bilan de sécurité nous annonçait que les attaquants avaient tenté une attaque d'IP spoofing qui n'était pas prévue dans les créneaux d'attaques. Malheureusement, ils ne nous ont pas apporté de conseils quant à ces remarques.

➢ *Phase 1*

La phase a débuté à la suite de la première attaque. Celle-ci a eu lieu le vendredi 3 Novembre. Le pôle Communication avait convenu avec leur intermédiaire de cette date afin que tous les groupes soient prêts avant de passer aux choses sérieuses.

Suite à cette attaque le groupe « Audit » nous a transmis un bilan de sécurité dans lequel il nous résume tout ce qui a été fait ou tenté par le groupe « Attaque ». Ils nous ont ainsi avertis d'attaques sur notre serveur Web (que nous avions pu constater le jour même), d'exploitations SSL et d'attaques sur notre DNS. Là aussi aucune suggestion de contre-attaque ne nous a été fournie. Nous avons donc par nous même procédé à quelques modifications que voici :

♦ Pôle Interconnexion

Le pôle Interconnexion a réalisé la configuration finale du routeur.
Pour le moment le strict minimum a été mis en place au niveau de la sécurité. Aucune access-list n'a été mise en place. Nous nous contentons pour le moment d'une traduction d'adresse PAT (Port Address Translation).

Voici le détail de la configuration :

- Cryptage des mots de passe de manière à les masquer lors du show run.

```
password encryption aes
```

- L'interface WAN du routeur a été configurée en adresse « inside global »

```
interface FastEthernet0/0
 ip address 172.17.0.2 255.255.252.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
```

- L'interface LAN du routeur a été divisée en sub-interfaces afin d'assurer le routage inter-Vlans

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
```

- Les trois sous interfaces sont configurées chacune pour router le trafic venant d'un seul et unique VLAN. Le protocole CDP est désactivé pour améliorer la sécurité.

- Les interfaces FastEthernet0/1.1 et FastEthernet0/1.2 (considérées comme « inside local ») ont été respectivement configurées pour permettre l'accès au VLAN Service et au VLAN Parc. L'interface FE0/1.3 est dédiée à l'administration du switch.

```
!
interface FastEthernet0/1.1
 encapsulation dot1Q 117
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.2
 encapsulation dot1Q 118
 ip address 10.20.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 172.16.0.8 255.255.252.0
 no cdp enable
!
```

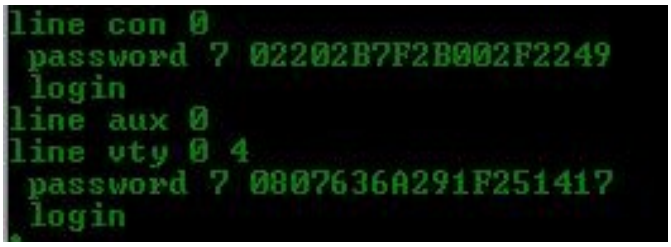
- Une translation d'adresses par ports a été mise en place. Il est cependant possible que nous revenions à une translation NAT statique adresse par adresse pour faciliter le travail de l'attaque.

- Nous avons aussi redirigé les ports suivants :
  - 80 pour le serveur web
  - 53 pour le dns
  - 443 pour openvpn
  - 22 pour le ssh de la sonde de l'audit

- Les adresses qui peuvent traverser le NAT sont 10.0.0.0/8 (à restreindre ultérieurement).

```
ip nat inside source list 1 interface FastEthernet0/0 overload
ip nat inside source static udp 10.10.10.3 53 172.17.0.2 53 extendable
ip nat inside source static tcp 10.10.10.3 80 172.17.0.2 80 extendable
ip nat inside source static tcp 10.10.10.2 443 172.17.0.2 443 extendable
ip nat inside source static tcp 10.10.10.5 22 172.17.0.2 12768 extendable
!
access-list 1 permit 10.0.0.0 0.255.255.255
```

- Enfin l'accès console et telnet ont été sécurisés.



♦ Pôle Services

Suite à la première attaque et à l'interprétation de l'audit nous avons réalisé les travaux suivants :

- **Sécurisation du Serveur WEB**

Suite à la tentative de DoS par le Wget nous avons installé le module modSecurity d'Apache dans lequel nous avons spécifié que nous bloquons les requêtes wget, les scripts et les demandes d'accès à un certain nombre de répertoires de notre serveur.

- **Sécurisation du DNS**

En prévision d'une attaque sur notre DNS, nous avons bloqué la récursivité sur notre DNS à des membres extérieurs à l'entreprise et nous avons bloqué le transfert de zone.

- **Ecriture d'une politique de sécurité sur l'utilisation de l'internet**

Suite à l'attaque par DNS Spoofing nous avons décidé de sensibiliser nos utilisateurs par l'écriture d'une politique de sécurité traitant de l'accès aux sites web de nos partenaires. Aussi il a été évoqué la possibilité d'établir des VPN avec nos partenaires afin d'avoir accès à leur site en local.

- **Développement d'un espace restreint sur le site WEB**

A la demande des « attaquants », nous avons développé un accès restreint à notre site avec un login et un mot de passe. De plus, nous avons modifié le type de certains champs dans la base de données afin de leur faciliter la tâche ☺.

♦ Pôle Utilisateurs

Le pôle Utilisateur a mis en place un serveur de mails : Exchange Server 2003, sur le contrôleur de domaine. Pour cela voici ce qu'il a du réaliser :

- Désinstallation du SP1 sur le serveur de domaine pour être compatible avec la version d'Exchange
- Installation de services nécessaires à Exchange :
  - IIS
  - NNTP
  - SMTP

- Installation d'Outlook
- Création des boîtes aux lettres à partir des comptes utilisateurs du domaine

Ils ont du procéder à la réinstallation du client XP sans sp2 de nom ERA. La machine avait des problèmes physiques donc ils ont installé ce client sur l'ancien poste IRIS qui n'était plus utilisé. Ce client conserve son nom ERA et son adresse IP.

Ils ont ensuite mis en place du service DHCP sur le serveur de domaine HADES : attribution automatique d'une adresse IP (plage d'adresse de 3 à 5).

➢ *Phase 2*

La phase 2 a débuté suite à la seconde attaque qui a eu lieu le mercredi 15 Novembre.
En ce qui concerne cette attaque nous n'avons rien reçu de la part du groupe « Audit ». Le binôme Communication a fait une demande une semaine après cette attaque au groupe « Audit » qui lui a expliqué qu'ils n'avaient pas tout a fait terminé. Ce que nous avons accepté. Ce binôme n'a pas réitéré sa demande car il a oublié à son tour suite au travail conséquent qui devait être réalisé à côté.

Malgré tout nous avions pu constater que les attaquants avaient réalisé une injection d'un javascript de redirection dans notre base de données via SQL (suite à la modification du type du champ dans la base de données de varchar à text).

Les conséquences d'une telle attaque peuvent être assez importantes pour notre société, nous ne pouvions plus récupérer les impressions de nos internautes mais ils risquaient en plus d'être à leur tour hackés à cause de cette redirection.

Nous avons donc procédé à quelques modifications que voici :

♦ <u>Pôle Interconnexion</u>

C'est lors de cette phase que la séparation du trafic entre le par cet la DMZ a été réalisée. Nous avons pensé à mettre en place un firewall mais nous avons opté pour une solution plus simple qui consiste à fermer tous les ports du routeur et à ouvrir seulement ceux qui sont nécessaires. Nous n'avons pas voulu non plus mettre en place un politique de sécurité trop importante afin de permettre à toutes les entités d'avoir des résultats convenables.

Nous avons réalisé ceci en utilisant des access-lists ainsi qu'une ACL étendue nommée en sortie de l'interface fastethernet 0/1.2. (versparc).

```
ip access-list extended versparc
 permit tcp any host 10.20.20.2 eq 8080
 permit tcp any host 10.20.20.2 eq smtp
 permit tcp any host 10.20.20.2 eq pop3
 permit tcp any host 10.20.20.2 eq 143
 permit tcp host 10.10.10.2 host 10.20.20.2
 permit udp host 10.10.10.2 host 10.20.20.2
 permit tcp host 10.10.10.2 10.20.20.0 0.0.0.255 eq 5901
 permit tcp host 10.10.10.3 host 10.20.20.2 eq www
```

Nous avons aussi ajouté des redirections de port de l'interface WAN vers les machines suivantes :

- facial:pop ->10.20.20.2:pop
- facial:imap ->10.20.20.2:imap
- facial:smtp ->10.20.20.2:smtp
- facial:8080 ->10.20.20.2:8080

```
ip nat log translations syslog
ip nat inside source list 1 interface FastEthernet0/0 overload
ip nat inside source static tcp 10.20.20.2 25 172.17.0.2 25 extendable
ip nat inside source static tcp 10.10.10.3 53 172.17.0.2 53 extendable
ip nat inside source static udp 10.10.10.3 53 172.17.0.2 53 extendable no-payload
ip nat inside source static tcp 10.10.10.5 80 172.17.0.2 80 extendable
ip nat inside source static tcp 10.20.20.2 110 172.17.0.2 110 extendable
ip nat inside source static tcp 10.20.20.2 143 172.17.0.2 143 extendable
ip nat inside source static tcp 10.10.10.2 443 172.17.0.2 443 extendable
ip nat inside source static tcp 10.20.20.2 8080 172.17.0.2 8080 extendable
ip nat inside source static tcp 10.10.10.5 22 172.17.0.2 12768 extendable
```

Quelques règles ont aussi été apportées concernant l'attaque de spoofing précédente :

- Activation d'Ip cef
- Vérification inverse de route

```
interface FastEthernet0/1.2
 encapsulation dot1Q 118
 ip address 10.20.20.1 255.255.255.0
 ip access-group versparc out
 ip verify unicast reverse-path
 ip nat inside
 ip virtual-reassembly
 no cdp enable
```

♦ Pôle Services

Cette phase a été orientée vers la maintenance de nos services.
Suite à la deuxième attaque nous avons réalisé les travaux suivants :

- **Sécurisation du code PHP pour lutter contre les injections SQL**

Suite à l'attaque nous avons amélioré notre code PHP afin de lutter contre les injections SQL.

- **Mise à jour de nos packages**

Nous avons fait une mise à jour de nos packages sur chacune de nos machines afin de lutter contre les nouvelles failles de sécurité de nos packages. Pour se faire nous avons ajouté à la *source list* un ensemble de sites traités et proposant des patchs de sécurité pour le noyau et application Linux Debian.

- **Création d'images de sauvegarde de nos machines**

Nous avons aussi réalisé une sauvegarde de nos machines en créant des images des disques à l'aide de l'outil Mondo Rescue.

♦ Pôle Utilisateurs

Nous avons mis en place le logiciel Kiwisyslog sur le contrôleur de domaine et les deux clients XP, et nous l'avons configuré pour que les logs de ces postes soient redirigés vers la machine de l'audit. De plus, pour des raisons de sécurité nous avons fait des images de nos clients XP. Nous n'avons pas pu réaliser d'image du contrôleur de domaine car il fallait une version spéciale de Norton Ghost.

La sécurité autour du service DHCP a été améliorée par la distribution d'adresses IP en fonction de l'adresse MAC du poste. Nous avons ensuite procédé à la réduction du nombre d'IP disponibles au nombre exact de machines du LAN.

Pour compléter cette sécurité nous avons désactivé le compte administrateur de domaine par défaut et création d'un remplaçant.

Enfin, nous avons réalisé une politique « d'utilisation et de sécurité » pour les employés de l'entreprise qui seraient amenés à utiliser les postes clients.

➢ *Phase 3*

La phase 3 a débuté le jeudi 7 décembre suite à l'ultime attaque. Cette attaque a eu des résultats très conséquents sur nos machines.

Nous avons reçu un dernier bilan de sécurité du rapport d'audit. Il s'avère que c'est le bilan que nous aurions du recevoir à l'étape précédente. Dans ce bilan nous avions pour la première fois des constatations de l'attaque ainsi que des recommandations !

Voici les conseils :

- Sécurisation renforcée du serveur Apache + modSecurity
- Pas de phpMyAdmin en http
- Passage de l'exchange sur la DMZ
- Installation d'un antivirus sur les postes Windows, passage d'un scan
- Installation de Core Force sur les postes XP
- Lecture et application de hardening windows 2003 for dummies
- Passage du serveur exchange du LAN à la DMZ

Malheureusement cela est arrivé un peu tard.

Cette dernière attaque a eu des conséquences très négatives sur notre réseau. Elle a paralysé toutes nos machines. Nous n'avions plus aucun accès à nos deux machines et le site web avait été modifié. Dans cette situation nous étions incapables de fournir un service fiable à nos utilisateurs et la société ne pouvait donc pas être présente sur le web, ce qui explique la chute du cours en bourse de nos actions. Cette attaque d'une extrême gravité a

nécessité une réparation rapide. La réparation ainsi que la récupération de nos logs (car le groupe « Audit » a tout perdu pendant cette attaque) correspond à la phase 3.

Suite à cette attaque fatale, nous avons suivi la démarche suivante pour tenter de restaurer nos services :

- **Récupération de l'accès à nos machines par un live CD**

Suite à l'attaque nous avons récupéré l'accès à nos machines par la modification à la main du mot de passe root grâce à un live CD.

- **Récupération des log puis envoi à l'audit**

Après la récupération de nos machines, nous avons envoyé tous nos logs au groupe « Audit » afin d'avoir leur interprétation.

- **Utilisation des CDs de sauvegarde**

Le moyen le plus rapide de remonter nos services a été de réinstaller nos machines via nos sauvegardes.

Conclusion

Les nombreuses attaques réalisées sur nos services, nous ont permis de comprendre qu'il faut anticiper les attaques afin de mieux nous protéger. Dans une vraie société l'installation des services ne doit en aucun cas se faire sans une réflexion sur la sécurité en externe comme en interne. Il est nécessaire de procéder à un maquettage de l'architecture choisie auquel on doit faire subir un ensemble de tests de hacking pour valider sa fiabilité et la disponibilité après une attaque.

L'analyse des logs, si un groupe d'audit n'a pas été embauché, est primordiale pour s'assurer du bon fonctionnement de son SI. L'expérience prouve que même avec une équipe d'audit, on ne peut leur décharger la totalité de cette analyse.

Bilan du projet

Ce projet nous a confronté à un problème auquel nous pouvons être amené à devoir résoudre prochainement. Il nous a également permis de nous rendre compte de ce qu'est le travail en équipe.

En tant qu'équipe « Défense », nous aurions pu prendre un mauvais départ, en faisant le maximum pour empêcher l'équipe « Attaque » de compromettre notre réseau. Mais dans une approche plus pédagogique, nous avons tenu à faire en sorte que tout le monde puisse retirer de ce projet quelque chose de positif. Nous avons mis en place une architecture « basique ». Cela a permis à l'équipe « Attaque » de mener à bien sa mission et de même pour le groupe « Audit ».

D'un point de vu technique, nous avons retenu les points suivants :

- Il est difficile de maîtriser du matériel qui nécessite une formation spécifique
- Il est difficile de respecter les règles de sécurité
- Faire le distinguo entre l'architecture du projet et une architecture réelle n'est pas évident
- Le drame provient souvent d'une erreur humaine
- Il n'est pas non plus facile de « penser à tout faire », même quand on est plusieurs

D'un point de vu relations humaines et communication, il nous est apparu que :

- Il n'y a pas eu de problème de communication à l'intérieur du groupe, ni avec les autres groupes du fait que l'on se connaissait déjà
- Chacun a fait de son mieux pour faire en sorte que le projet se déroule dans de bonnes conditions
- Il n'y a pas eu de réelle compétition, chacun était toujours prêt à aider l'autre

D'un point de vu gestion de projet, nous nous sommes rendu compte que :

- Il n'est pas forcément évident de diriger les personnes que l'on connaît
- Gérer un projet nécessite d'avoir une vision globale du projet tout en s'impliquant un minimum
- Il est souvent difficile de respecter les délais, car difficile de l'imposer à son équipe et encore plus à une autre équipe
- Il n'est pas facile de synchroniser plusieurs équipes entre elles car cela implique que chaque équipe respecte elle-même ses délais