AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Cyrille DUMAS
Laurent ROGER
Joseph NDAYRA
Mohamed BARRY
Wannes VOSSEN
Julien DESVEAUX
Thomas DUVIVIER
Thomas CAPRARO
Raphaël DUJARDIN
Jérémie BELMUDES
Frederic TARRERIAS
Cédric HARISMENDY
Hubert COMPAORE HARBOURE
Nattapong TIWAPORNCHAROENCHAI

Projet de sécurité

Groupe Défense

Le 13 décembre 2010

Présentation de l'équipe

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Jérémie Belmudes
Responsable

Architecture	**Système**	**Communication**
- *Thomas Duvivier* - *Nattapong Tiwaporncharoenchai* - *Thomas Capraro* - *Frederic Tarrerias* - *Raphael Dujardin*	- *Laurent ROGER* - Joseph Ndayra - Mohamed Barry - Cédric Harismendy - Hubert Compaore	- *Wannes Vossen* - Julien Desveaux - Cyrille Dumas

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Présentation Communication

BELMUDES Jeremie

VOSSEN Wannes

DUMAS Cyrille

DESVEAUX Julien

Sommaire

- La communication
- Politique de Sécurité
  - Généralités techniques
  - Politique de Communication
  - Politique de Comportement
  - Retour d'expérience
- Contrat de prestation de service
  - Description
  - Retour d'expérience

La communication

- Un double enjeu
  - Communication pour un travail efficace
    - Les réunions
    - Les écrits
  - Communication pour la sécurité

- Relation étroite avec la direction
  - Coordination des équipes
    - Au sien de l'équipe
    - Avec l'extérieur

Politique de Sécurité

- Politique de sécurité :

Objectifs:

- Plan d'actions.
  ➔ Limiter les fuites d'informations.
  ➔ Garantir l'image et fonctionnement de l'entreprise.

- **Généralités techniques.**
  ➔ Bonnes pratiques à appliquer par les administrateurs.

- **Politique de communication.**
  ➔ Bonnes pratiques de communication (électronique et physique).

- **Politique de comportement.**
  ➔ Bonnes pratiques liées au facteur humain (électronique et physique).

Généralités Techniques

- Généralités Techniques :

o Sécuriser son périmètre.

➔ Bâtir progressivement mais sur de bonnes bases.

➔ Délocaliser services mandataires (DMZ).

➔ Surveiller le trafic aux routeurs.

➔ Règles de filtrage contre les attaquants.

➔ Privilégier les communications mail HTTPS.

➔ Règles de filtrage contre les attaquants.

➔ Ne pas laisser fonctionner des services inutiles.

➔ Règles de filtrage contre les attaquants.

➔ Antivirus installés et mises à jours.

Généralités Techniques

- Généralités Techniques :

o Après une attaque …

➔ Utilisation de GHOST

➔ Utilisation disque dur iSATA de 1 To.

… reprise d'activité.

o Méthodes de chiffrements.

➔ Tentative de chiffrement du disque dur.

➔ Chiffrement des accès distants (via VPN).

➔ Chiffrement PGP pour certaines communications mails.

Politique de Communication

- Politique de communication:

o Dans l'entreprise.

➔ Electroniques : @aerodef.fr via Google Apps.

➔ Orales : discrètes.

o Avec nos collaborateurs de l'audit.

➔ Electroniques : @aerodef.fr via Google Apps.

➔ Orales : Interface : Groupe communication Aérodef.

o Avec l'équipe Attaque.

➔ Electroniques : contact@aerodef.fr via Google Apps.

➔ Orales : Interface : Groupe communication Aérodef.

➔ Eviter les attaque de social engineering.

Politique de Comportement

- Politique de comportement :

« Ce ne sont pas les murs qui protègent la citadelle,
mais l'esprit de ses habitants ». Thucydide (Vème siècle avant J.C)

➔ 40% des attaques sont causées par les utilisateurs des SI.

o Mots de passe.

➔ Changer très régulièrement.

➔ Charte composition : caractères alphanumériques : ex: **QS89ai37?**

➔ Ne pas partager les mots de passe.

➔ Ne pas les noter sur une feuille volante.

➔ Ne pas utiliser les mêmes mots de passes.

➔ Ne pas communiquer ses mots de passes par SMS ou mail.

Retour d’expérience

- Retours pratiques :

  - Politiques de sécurité en générale.

    ➔ Respectée sur le plan technique.

  - Politique de communication.

    ➔ Concluante au sein de l’entreprise et avec l’attaque.

    ➔ L’audit en communication directes avec nos équipes techniques pour des raisons efficacité.

  - Politique de comportement.

    ➔ Politique de mots de passe trop restrictive.

    ➔ Peu sûre d’être connue et appliquée par tous (peu de contrôle).

    ➔ Revoir et / ou faire signer la charte à l’avenir.

Contrat de prestation de service

- Description :
  - Contexte
    - ➔ Client d'AeroDef : Grand groupe du secteur aéronautique
    - ➔ Mission : Gestion du système d'information du client
  - Identification des besoins d'AeroDef pour remplir cette mission
  - Identification des tâches non réalisables dans les contraintes
    - ➔ Supervision
    - ➔ ToIP/VoIP
  - Diffusion de l'appel d'offre
    - ➔ Un pour chaque besoin

Contrat de prestation de service

- Description :
  - Réponse à l'appel d'offre
    - ➔ AssuranceTourix a présenté
      - Sa société
      - Ses compétences
      - Sa compréhension de la mission proposée
      - Sa solution avec un prix (59 600€f + 27 000€f)

    - ➔ La solution proposée (supervision)
      - Nessus : relève les faiblesses des machines
      - Netflow : métrologie
      - Syslog-ng : gestion des logs générés
      - Fully Automated Nagios : supervision avec envoi d'alertes
      - Prelude : détection d'intrusion sur réseau et machines
      - Analyse complémentaire

Contrat de prestation de service

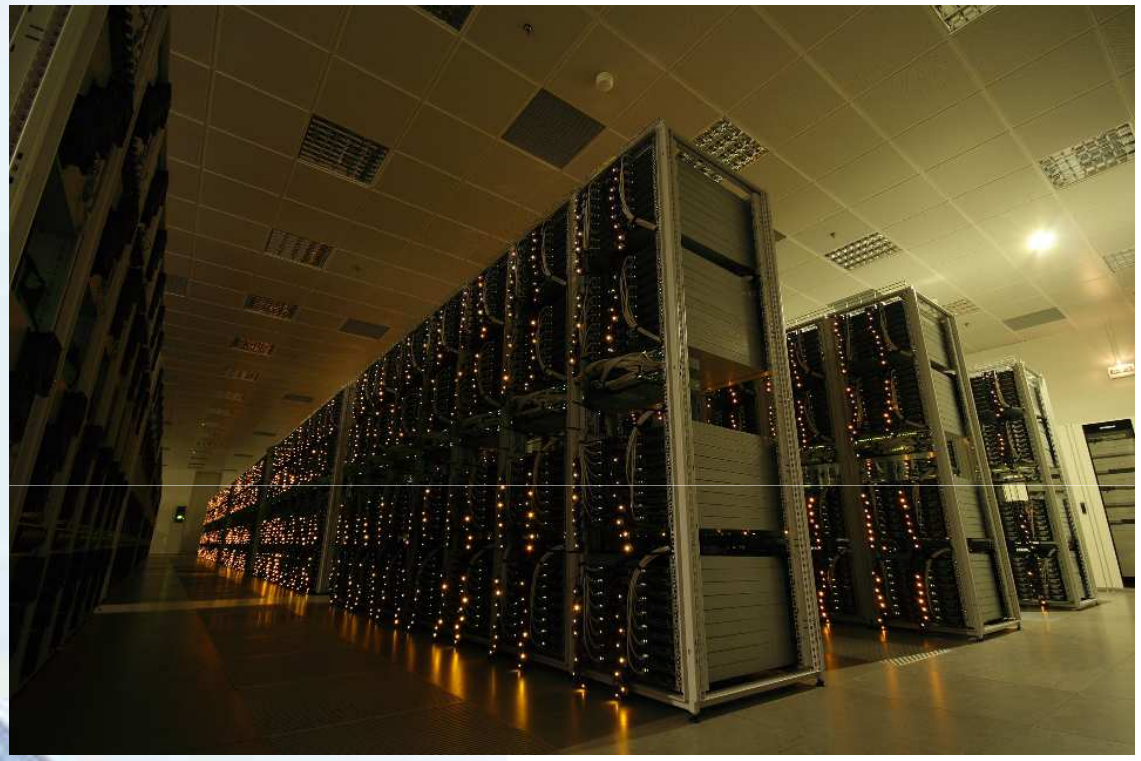
- Description :
  - La solution ToIP/VoIP:
    - ➔ PBX OpenSource Astérisk
    - ➔ SoftPhone (sur PC) Xlite
    - ➔ Cisco Phone 7965G
  - Solution satisfaisante
    - ➔ Réponse aux besoins
    - ➔ Coût acceptable
  - Rédaction du contrat
    - ➔ Négociation entre les deux parties (coûts et partage des informations)
    - ➔ Un contrat par prestation
  - Signature des contrat => réalisation de la prestiation

Contrat de prestation de service

- Retours pratiques :
  - Vision d’ensemble de la mission avant de prendre une décision
  - Relations avec un prestataire de service
  - Entente bénéfique pour les deux parties
  - Mise en situation réelle

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Présentation Architecture



Capraro Thomas
Dujardin Raphael
Tarrerias Frederic
Duvivier Thomas
Tiwaporncharoenchai Nattapong

Décembre 2010

Sommaire

- L'équipe
- Rôle de l'équipe
- Expression du besoin
- Présentation Architecture initiale
- Evolutions apportées
- Retour d'experience

L'équipe

- Capraro Thomas : Ingénieur inventaire
- Dujardin Raphael : Ingénieur documentation
- Tarrerias Frederic : Ingénieur translation
- Tiwaporncharoenchai Nattapong : Ingénieur filtrage
- Duvivier Thomas : Responsable de l'équipe

Rôle de l’équipe

- Etude et Conception de l'architecure
- Déploiement de l'architecture
- Optimisitation de l'architecture
- A l'écoute de l'utilisateur et de ses besoins
- Veille technologique

Expression du besoin

- Concevoir une architecture permettant une communication inter-services
- Permettre au parc d'accéder à internet
- Inclure l'audit et la telephonie dans l'architecture
- Permettre l'accès aux services offerts par l'entreprise depuis l'exterieur

Expression du besoin

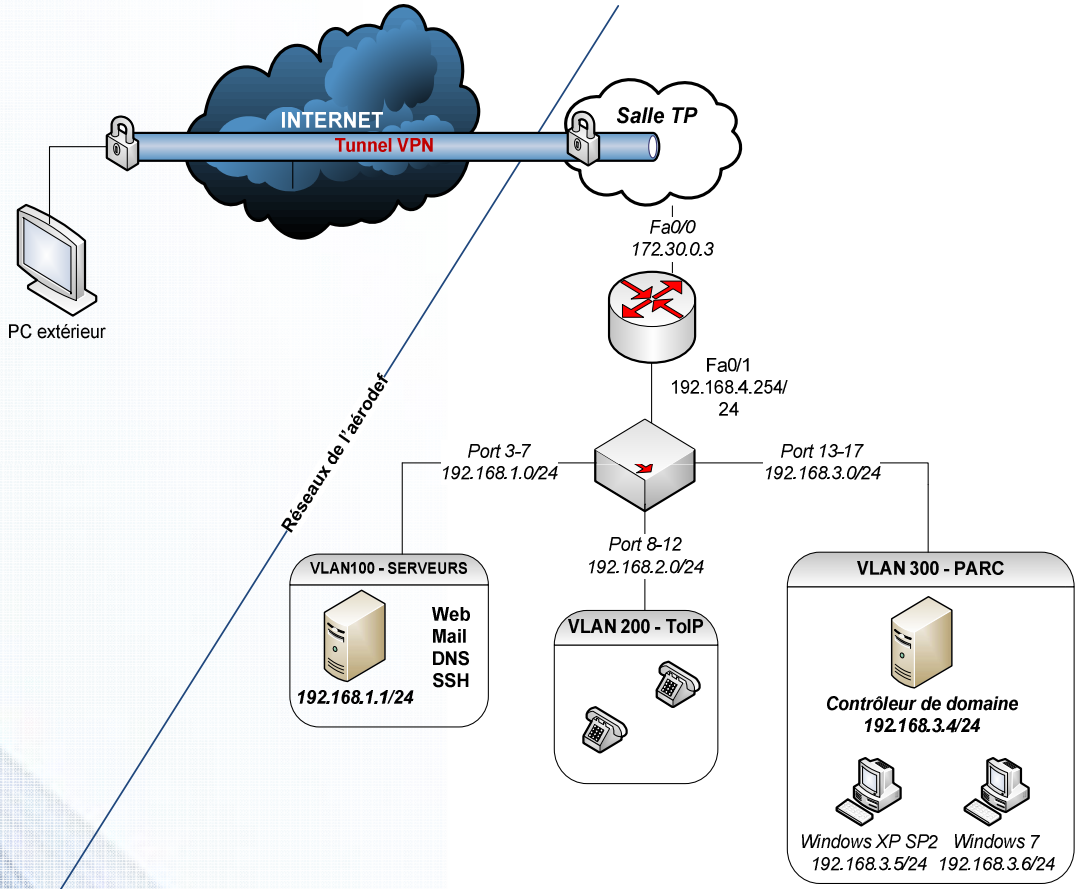
- Permettre l'accès à distance au LAN depuis l'extérieur
- Sécuriser et empêcher les compromissions de l'architecture
- Assurer la disponibilité et la qualité d'accès de l'architecture

Présentation architecture

- Pourquoi avoir choisi cette architecture ?

- Afin d'assurer :
  - La communication entre des machines dans le parc
  - L'administration des trafics
  - L'accès à distance sécurisé
  - L'évolutivité du réseau

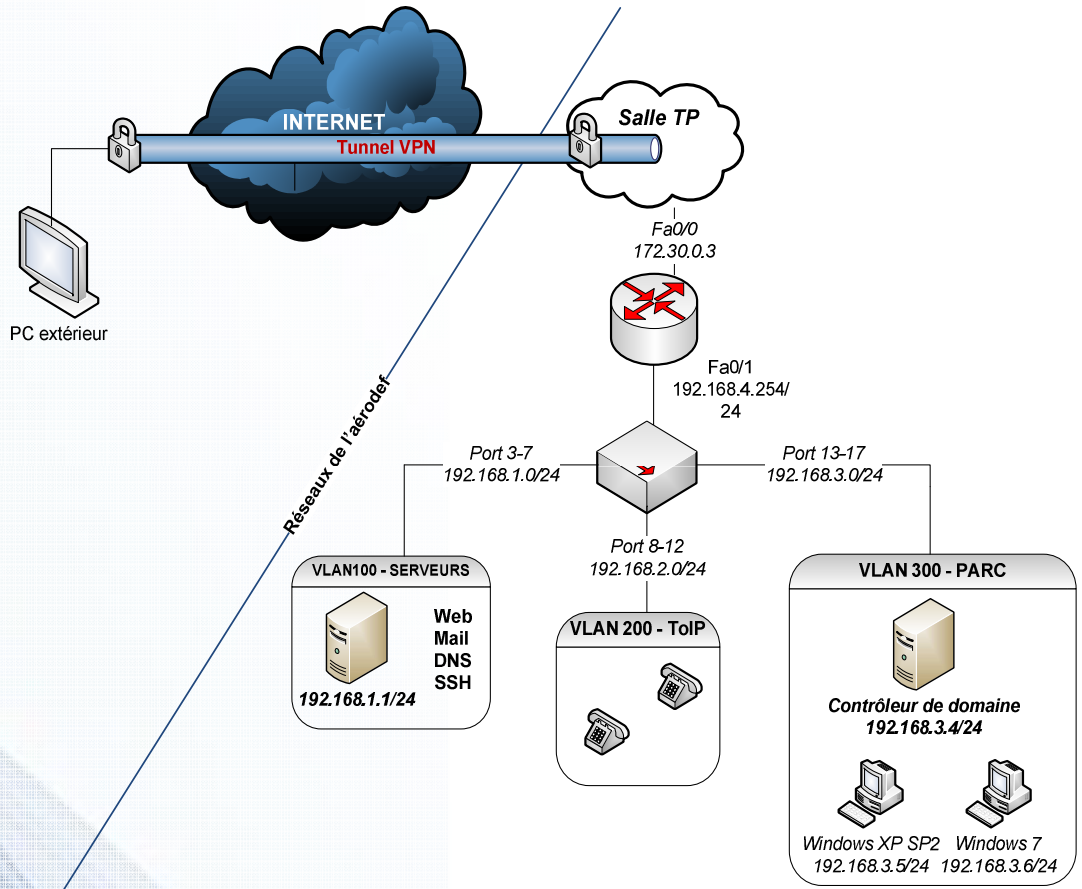
- Schéma architectutre globale



Présentation architecture

- Fonctionnalités de l'architecture
  - Découpage en sous-réseaux
  - Routage inter-vlans
  - Translation d'adresses
  - Liaison sécurisé VPN
  - Contrôle d'accès ACL

- Schéma architectutre globale



Evolution

Switchport statique

- But :
  - Minimiser les risques d'intrusion sur le parc
  - Avoir une vue globale des différents équipements
- Principe :
  - Association port => @MAC

ACL CBAC

- But :
  - Tirer partie du matériel à disposition
  - Firewall statefull matériel => prévention d’ attaques par déni de service
- Principe :
  - Eliminer les sessions orphelines
  - Inspection protocolaire

Deuxième adresse IP sur le serveur

- But :
  - Séparation des flux
  - Séparer les ports serveurs des ports client
  - Meilleur vision

- Principe :
  - Mise en place d'une IP secondaire sur l'interface
  - Mise en place d'ACL et de règle de PAT correspondant

Span port

- But :
  - Collaboration avec l'équipe Audit
  - Permettre l'analyse du trafic
- Principe :
  - Mise en place d'un monitor mode sur le switch

Fixation des seuils

- But :
  - Eviter que le routeur soit surchargé par du traffic excessif et inutile.
- Principe :
  - Mise en place de seuil associé à chaque interface, au delà d'une certaine limite, les paquets sont jetés.

Retour d'experience - Architecture

Objectifs :

Etude, Deploiement et Maintenance du SI.

- - Travail concentré en début de projet :
  - Etude et Déploiement.
- - Après :
  - Maintient en condition opérationnelle.
  - Contrôle d'accès.

Retour d'experience - Architecture (2)

Projet Riche en Enseignements :

- Projet de grande envergure :

  - Entreprise : 14 personnes
  - Equipe Achitecture : 5 personnes

--> Cohésion de travail nécessaire.

Retour d'experience - Apports

- Mise en pratique et approfondissements techniques :

Configurations avancées d'équipements :

- Routeurs
- Switchs
- Vlans, NAT, ACL, ...

Retour d'experience - Apports (2)

Service Architecture :

- Principal travail : Déploiement et Maintenance du SI.

- Importance du SI :
  - Dysfonctionnements : Retour rapide des utilisateurs.
    --> Résolution sous pression et avec précipitation

- Importance d'une connaissance exhaustive du SI :
  - Inventaire

Retour d'experience - Apports (3)

- Importance d'une planification structurée.

- Importance de la communication :
  --> Echange de point de vue
  --> Etude des différentes solutions envisageables.

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Présentation Systèmes

ROGER Laurent
NDAYRA Joseph
HARISMENDY Cédric
BARRY Mohamed
COMPAORE HARBOURE Hubert

Décembre 2010

Plan de présentation

- Définition des besoins
- Présentation du système initial
- 1ère confrontation
- 2ème confrontation
- 3ème confrontation
- Conclusion

Définition des besoins

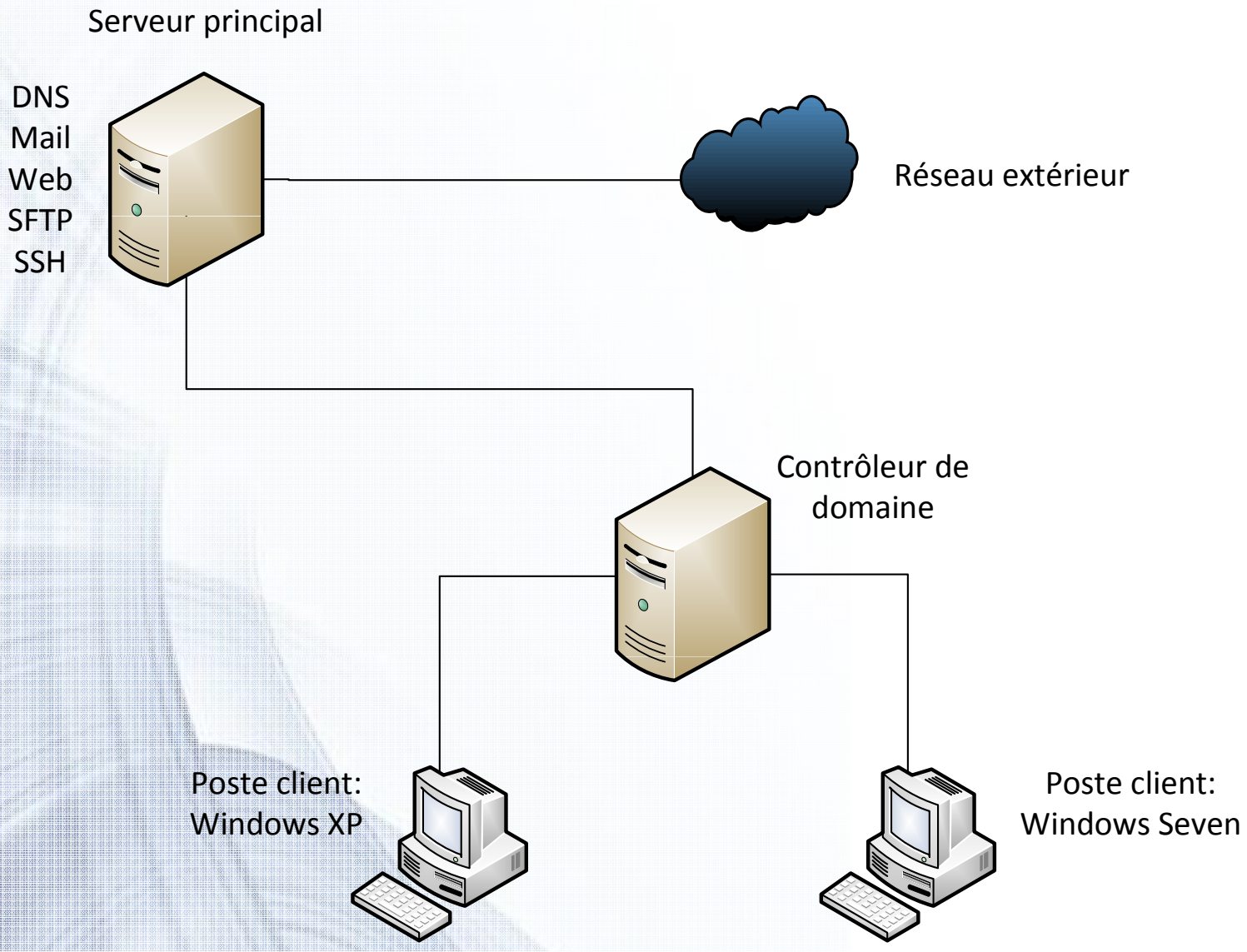
- **Parc informatique:**

  - Stations de travail pour les utilisateurs
  - Accès au réseau extérieur pour les utilisateurs

- **Services:**

  - Messagerie électronique pour le personnel
  - Site web de l'entreprise
  - Accès aux équipements à distance pour l'équipe Systèmes

Présentation du système initial



Présentation du système initial

- **Parc informatique:**

  - **Contrôleur de domaine**: Windows Server 2003

    - Active Directory: -> CompteXP
      -> CompteSeven

    - Antivirus: AVG Antivirus

  - **Windows XP SP2**
  - **Windows Seven**

    - Antivirus: AVG Antivirus
    - Internet Explorer 6 / 8

Présentation du système initial

- **Services:**
  - **Serveur principal**: Debian 5.0
    - DNS: Bind
    - Mail: Postfix + SquirrelMail (Webmail)
    - Web: Apache2 (HTTP/HTTPS)
    - SFTP: Vsftp
    - SSH: OpenSSH

Présentation du système initial

- **Services:**
  - **Quelques politiques et configurations:**

    - DNS: -> Résolution interne
      -> Zone interne: *aerodefense.stri*
      -> Transfert des requêtes externes à l'autorité supérieure
      -> Configuration d'un nom de domaine HTTP
      -> Configuration d'un nom de domaine Mail

    - Mail: -> Accès à la messagerie par Webmail

    - Web: -> Accès par les protocoles HTTP et HTTPS
      -> Affichage du site Internet
      -> Connexion espace sécurisé

Présentation du système initial

- **Services:**
  - **Quelques politiques et configurations:**

- SFTP: -> Connexion limitée aux comptes locaux
  -> Connexion impossible en *Super-utilisateur*
  -> Connexion impossible en *Anonymous*
  -> *Chroot* des utilisateurs dans leur répertoire

- SSH: -> Connexion limitée aux comptes locaux
  -> Connexion impossible en *Super-utilisateur*

1ère confrontation

- **Les besoins spécifiés par le groupe Attaque:**

  - **Sur le serveur de services :**

    - Service FTP disponible
    - Service Web disponible avec espace sécurisé

  - **Sur les postes de travail :**

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

1ère confrontation

- **Evolutions du système:**

  - **Sur le serveur de services :**

    - Mise en place d'une sauvegarde: SystemImager

  - **Sur le parc informatique:**

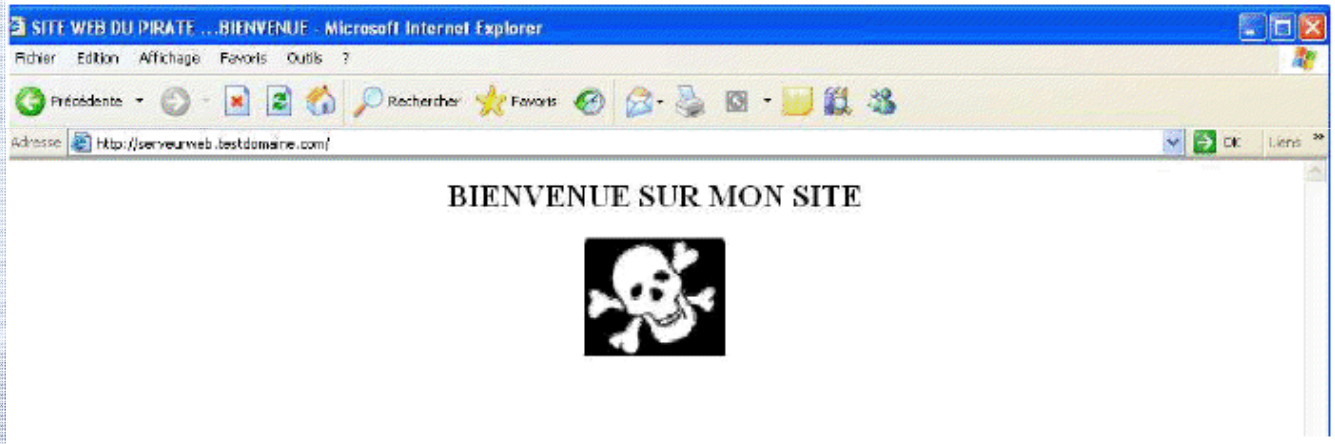
    - Installation des outils demandés

1ère confrontation

- **Les attaques survenues**

  - **DNS Spoofing :**

    - Accès Internet impossible
    - Redirection des requêtes HTTP



1ère confrontation

- **Les attaques survenues**

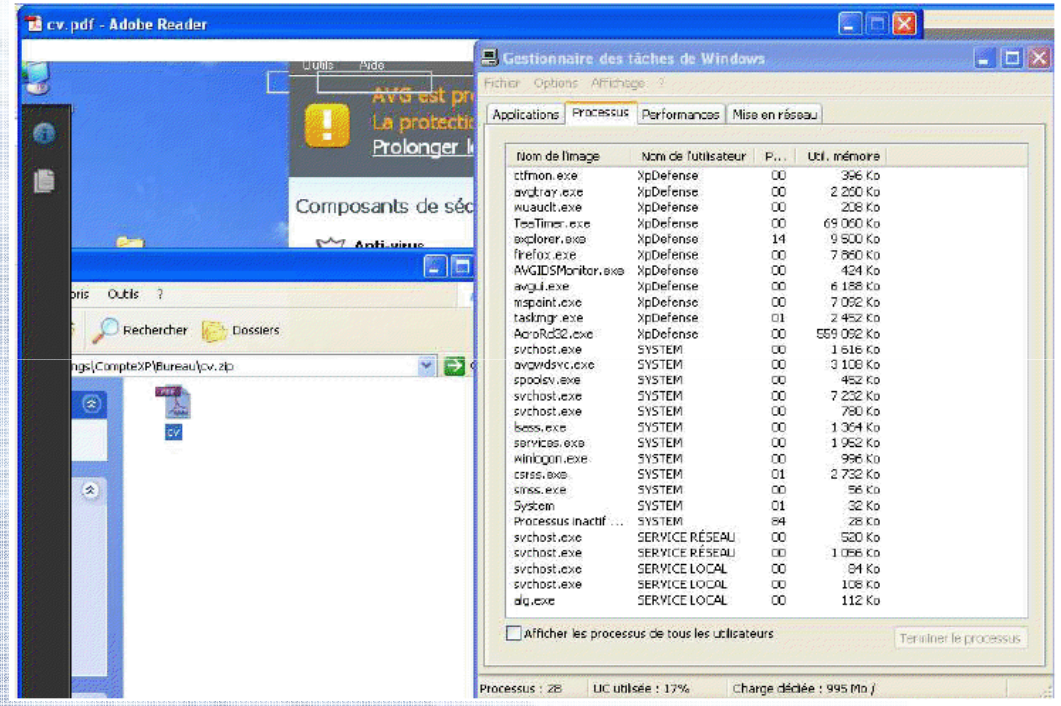
  - **Infection par code malveillant:**

    - Demande d'exécution d'un programme malveillant
    - Saturation charge système poste client

1ère confrontation

- Les attaques survenues

  - **Infection par code malveillant:**



1ère confrontation

- **Réflexion sur les attaques survenues**

  - **DNS Spoofing:**

    - Rendre le numéro d'identification des requêtes difficilement prédictible

    --> Solution trop contraignante techniquement, délai insuffisant

    - Chiffrage des flux DNS à l'aide de l'outil DNSSec

    --> Nécessite l'installation de DNSSec sur l'autorité supérieure

    → Mesures de protection contraignantes

1ère confrontation

- **Réflexion sur les attaques survenues**

  - **Infection par code malveillant:**

    - Attaque identifiée et prévenue par les outils de protection

    → Mesures de protection satisfaisante

2ème confrontation

- **Les besoins spécifiés par le groupe Attaque:**

  - **Sur le serveur de services :**

    - Service Web avec affichage de *news* dynamique

  - **Sur les postes de travail :**

    - Internet Explorer 6 ou 7
    - Adobe Reader 9.4
    - QuickTime 7.6.7

2ème confrontation

- **Evolutions du système**

  - **Sur le serveur de services :**

    - Mise en place de l'outil Fail2Ban: protection contre le « *brute-force* »

  - **Sur le parc informatique:**

    - Virtualisation des clients: VirtualBox
    - Service DHCP sur le contrôleur de domaine
    - Installation des logiciels demandés par le groupe Attaque

2ème confrontation

- **Les attaques survenues**

  - **DNS Spoofing**

  - **Intrusion dans le système de base de données:**

    - Accès et intrusion au service MySQL
    - Ecriture dans la base de données
    - Génération de news sur le site Aerodef

  - **Exécution d'un lien corrompu:**

    - Saturation de la mémoire physique des clients

2ème confrontation

- **Réflexion sur les attaques survenues**

  - **Intrusion dans le système de base de données:**
    - Hypothèse: faille de sécurité dans l'outil MySQL

    → Mise à jour générale du système

  - **Exécution d'un lien corrompu:**

    → Infection détectée et prévenue par les outils de défense

3ème confrontation

- **Evolutions du système**

  - **Sur le serveur de services :**

    - Mise à jour générale du système et des paquets

  - **Sur le parc informatique:**

    - Déploiement du service Terminal Server: Accès à distance

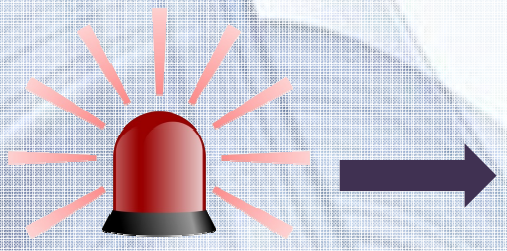
3ème confrontation

- **Les attaques survenues**

  - **DNS Spoofing**

  - **Intrusion générale dans le système:**

    - Accès et intrusion sur le serveur principal
    - Accès et intrusion sur le contrôleur de domaine
    - Modification de fichiers relatifs au site de l'entreprise
    - Accès à certains comptes de messagerie
    - Modification des accès sur les équipements et comptes e-mail



Situation catastrophique !

3ème confrontation

- **Les attaques survenues**

  - **Intrusion générale dans le système:**

    - Accès aux comptes mails du personnel Aerodef
    - Présence d'un compte utilisateur suspect sur le serveur
    - Reprise du contrôle du serveur à l'aide de Knoppix:

    → réinitialisation des comptes

    - Pas de sauvegarde pour le contrôleur de domaine

    → solution de sauvegarde Windows trop contraignante

3ème confrontation

- **Les attaques survenues**
  - **Au sujet de l'accès aux comptes mails Aerodef**
    - Détournement observé tardivement
    - Changement de mot de passe inefficace

→ Appropriation de messagerie puis transferts de mails

  - **Solution**
    - Utilisation de messagerie signée et chiffrée
    - Prendre davantage de prudence

Bilan technique

- Robustesse des équipements de détection et de prévention d'intrusion
- Solutions difficiles contre certaines attaques : **DNS Spoofing**
- Difficultés de prévenir les failles de sécurité du système et des outils
- Système de sauvegarde / reprise intéressant : **Systemimager**
- « *Boite à outils* » de secours nécessaire: **Knoppix**
- Facilité pour mettre un système en fonctionnement, difficultés pour le défendre !

Bilan personnel

- **Projet très enrichissant car**:
  - Simulation du fonctionnement d'une entreprise
  - Simulation d'un contexte critique
  - Gestion de projets, responsabilités (responsables d'équipe)
  - Apports techniques: solutions pour détecter et prévenir certaines attaques
  - Apports relationnel: relations interpersonnel, hiérarchiques

En conclusion

- Grand intérêt pour ce projet

- Projet composé :
  - d'organisation (répartition des tâches)
  - de technique (système d'information complet)

- Mise en conditions réelles :
  - trois confrontations

➔ **Une expérience en sécurité concrète et enrichissante !**

Merci de votre attention !

Des questions ?