Université Paul Sabatier
TOULOUSE III

Projet de sécurité des systèmes d'information

Groupe 1 : Équipe défense

ALVAREZ Irène
MUNOZ Aurélie
ANDRE Michael
REUTER Ivan
CAPECCHI Kevin
SAYSSET François



Plan de la présentation

- Présentation du sujet
- Organisation de l’équipe
- Planification du projet
- Gestion du projet
- Groupe interconnexion
- Groupe systèmes et services
- La communication
- Conclusion

Présentation du sujet

Groupe défense

- Mise en place d'un système d'information et de services
- Mise en œuvre d'une politique de sécurité par étapes

Le groupe analyse

- Collecte d'informations
- Analyser et identifier des actions

Le groupe attaque

- Chercher et exploiter des failles de sécurité
- Intrusions et/ou de compromissions (piratage, dénis de service…)

→ **Objectifs :** techniques, organisationnels

Organisation de l'équipe

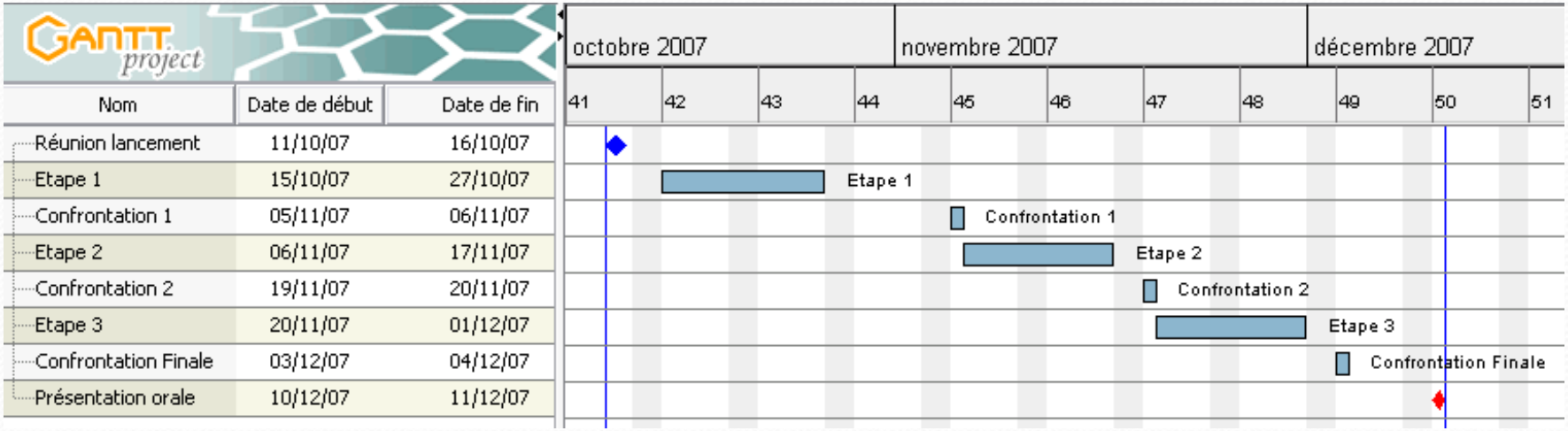
- **Interconnexion**
  - 2 personnes (Michael et Kévin)
  - Conception de l'architecture du réseau de l'entreprise
  - Mise en place et maintenance des équipements réseau
  - Sécurisation de l'architecture
- **Systèmes et Services**
  - 2 personnes (Ivan et Irène)
  - Déploiement des OS et des services
  - Maintenance et sécurisation des services

Organisation de l'équipe

- **Communication**
  - 1 personne (Aurélie)
  - Intermédiaire avec les autres groupes du projet
  - Elaboration du contrat d'audit
- **Gestion de projet**
  - 1 personne (François)
  - Planification des tâches du projet
  - Gestion et coordination des groupes internes

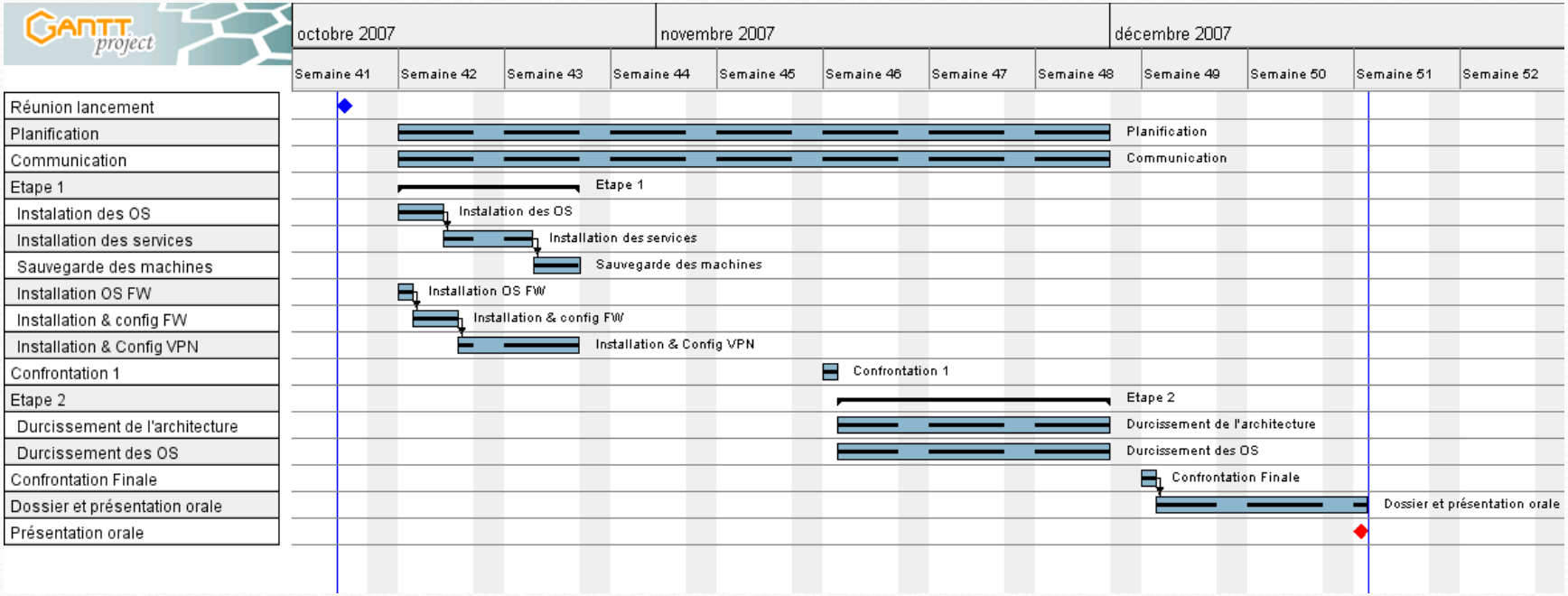
Planification du projet

- Planification préliminaire



Planification du projet

- Planification pratique



Gestion du projet

- Mise en place d'outils de communication
  - Liste de diffusion
  - Site Web (http://projet-seurite.neuf.fr)

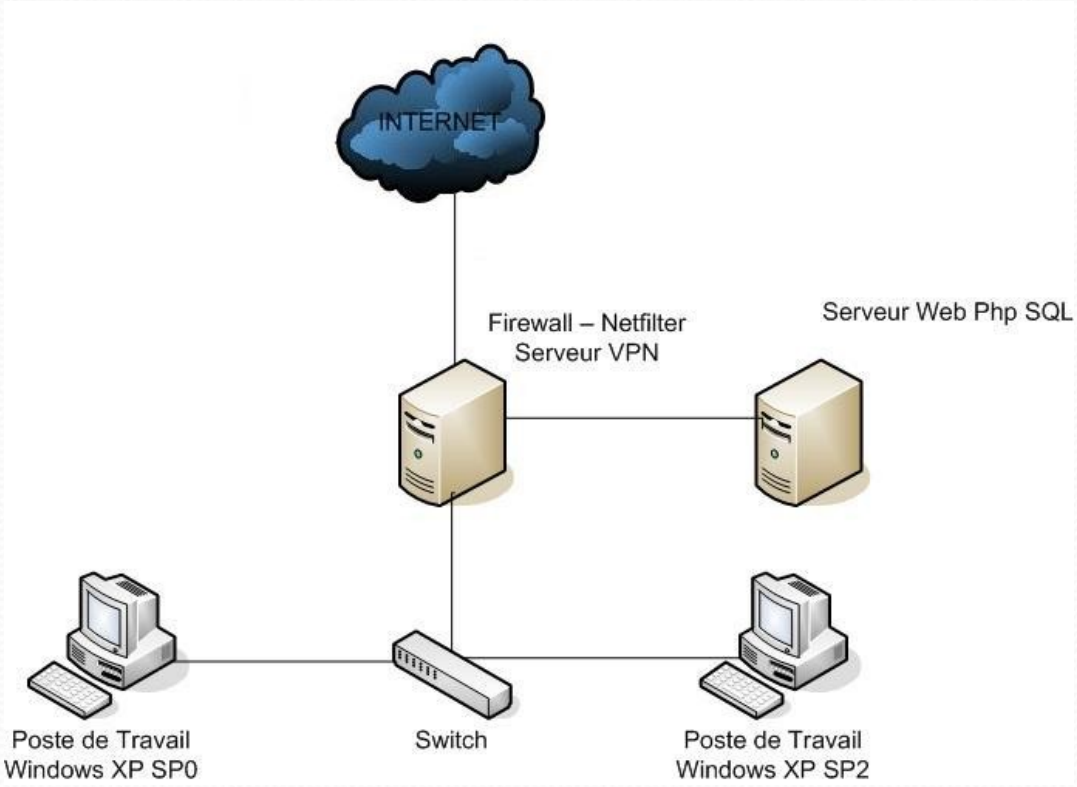
- Rapport régulier
  - Après la finition d'une tâche (ou fin de séance)
  - Après les confrontations

Groupe interconnexion

- Rôle du groupe
  - Proposer une architecture complète permettant d'offrir un service au réseau public
  - Mettre en place une solution défensive afin de prémunir des attaques l'infrastructure de l'entreprise
  - Proposer des évolutions à la défense mise en place

Groupe interconnexion

- Le choix de l'architecture défensive



Groupe d'interconnexion

- Le choix du pare-feu
  - Une gestion simple et efficace
  - Services nombreux et faciles à implanter
  - Sauvegarde de l'intégralité des paramètres du système
  - La solution PfSense.

Limites à ce choix: possibilité d'avoir une console en super-utilisateur sans avoir à se loguer

Solution : Virtualisation pour verrouiller l'accès à la machine

Groupe d'interconnexion

- Les évolutions

  Au début le pare-feu est un
  - translateur d'adresses
  - serveur VPN

  Le pare-feu sépare le réseau local et la zone de service.

  1er évolution
  - configurer un proxy
  - ouverture des ports pour le service DNS de notre serveur de la DMZ.
  - accès à l'intégralité de l'architecture au groupe Audit
  - Modification du fichier de configuration des logs pour conserver une copie locale.

Groupe d’interconnexion

- 2ème évolution
  - durcissement des règles de transit par ajout d’un analyseur de paquet
  - Élimination de toute possibilité de faire du point à point entre la machine et un hôte distant
  - Priorité du trafic de type HTTP et HTTPS

  Les autres services possédant une bande passante limitée à 2%.

Groupe systèmes & services

- Rôle du groupe
  - Mettre en place des postes clients et un serveur web
  - Collaborer avec le groupe audit pour les accès systèmes
  - Proposer des évolutions des systèmes mis en place

Groupe systèmes & services

- Mise en place de 2 postes clients
  - 1 sous Windows XP SP0 sans antivirus ni MAJ
  - 1 sous Windows XP SP2 avec antivirus et MAJ
- Mise en place d'un serveur Web sous Debian
  - Enlever tous les services inutiles et protéger au démarrage
  - Installation et configuration d'Apache
  - Installation et configuration de PhP/MySQL
  - Création d'un livre d'or en PhP/MySQL comme site Web

Groupe systèmes & services

- Première confrontation
  - Exécuter un script java et visite d'un site avec Active-X
  - Tentatives d'injection SQL sans succès
- Après la première confrontation
  - Ghost du poste client sur lequel le script java a été lancé
  - Vidage de la base SQL qui a été un peu remplie
  - Installation et configuration d'un service DNS
  - Désactivation des autorun USB sur les postes client + installation antivirus sur poste XP SP0

Groupe systèmes & services

- Seconde confrontation
  - Tentative d'éxécution d'un virus sans réussite
  - Signer le livre d'or
- Après la seconde confrontation
  - Vidage de la base SQL qui a été un peu remplie

Groupe systèmes & services

- Bilan
  - Le serveur Web n’a pas réussit à être attaqué
  - L’injection SQL n’a pas fonctionnée, BD intègre
  - Juste un ghost d’un poste client par sécurité
  - Mission services et systèmes accomplie !