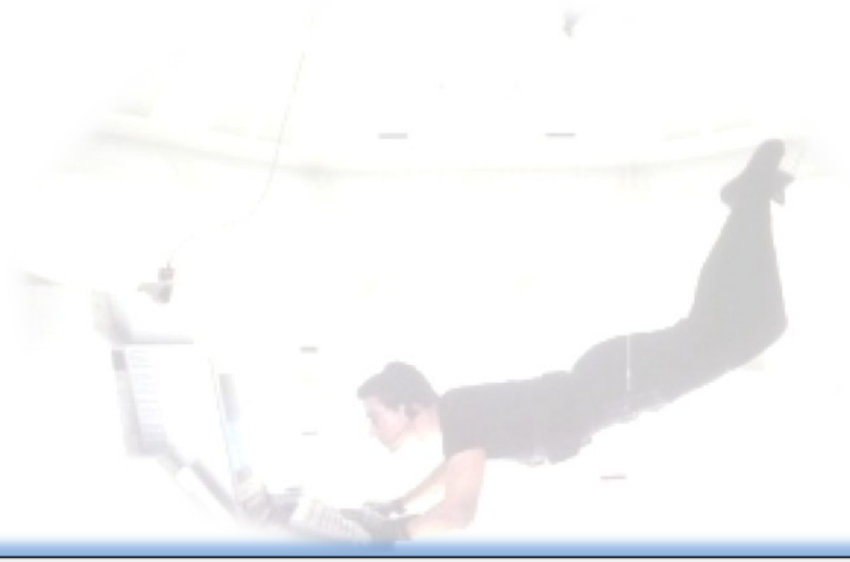
Projet Sécurité

Groupe Attaque

Compte-rendu de l'attaque de la société Candide SA

Sommaire

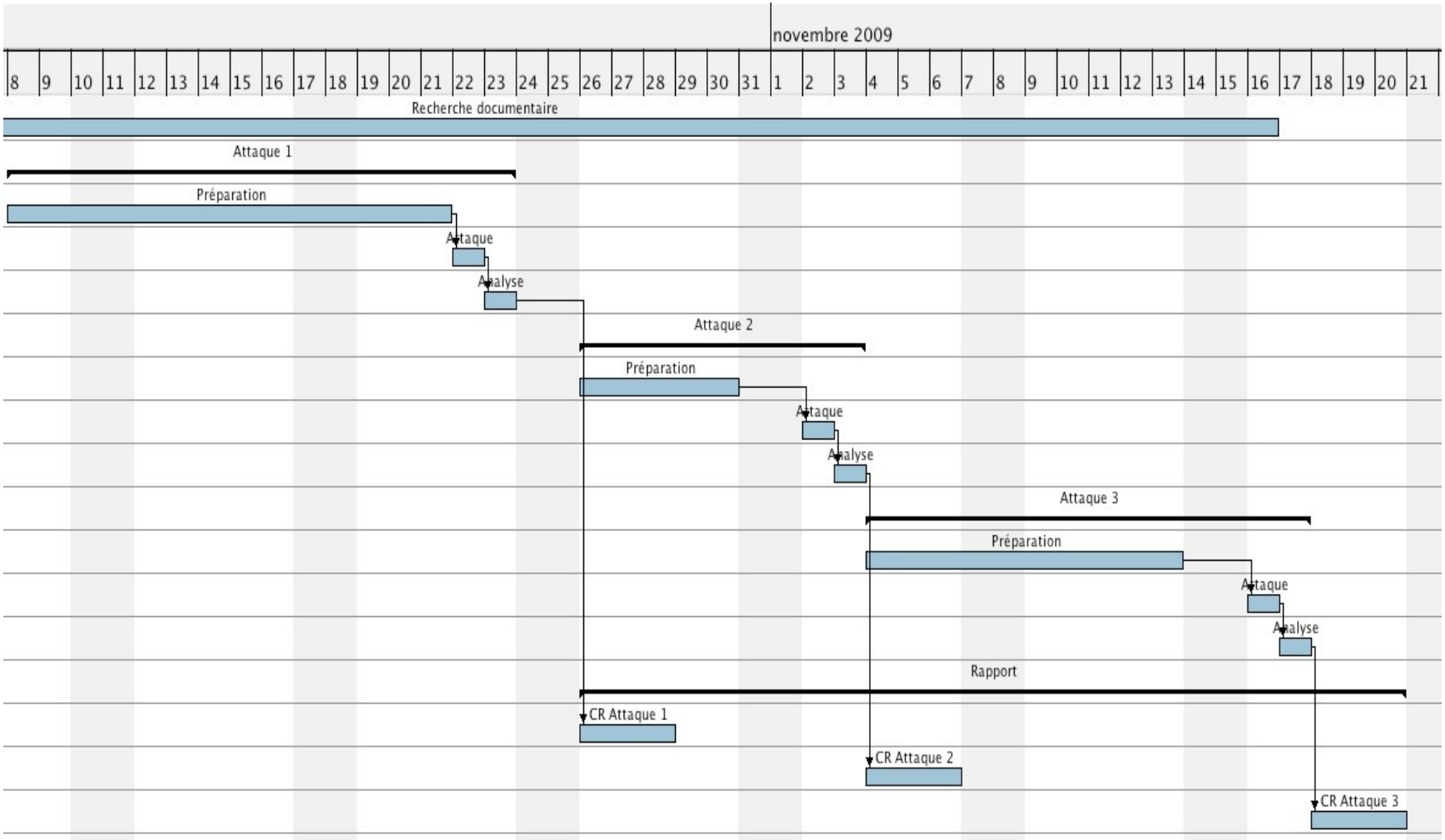
- Introduction
- Planification - Organisation
- Architecture
- Projets transversaux
- Première confrontation
- Deuxième confrontation
- Troisième confrontation
- Bilan



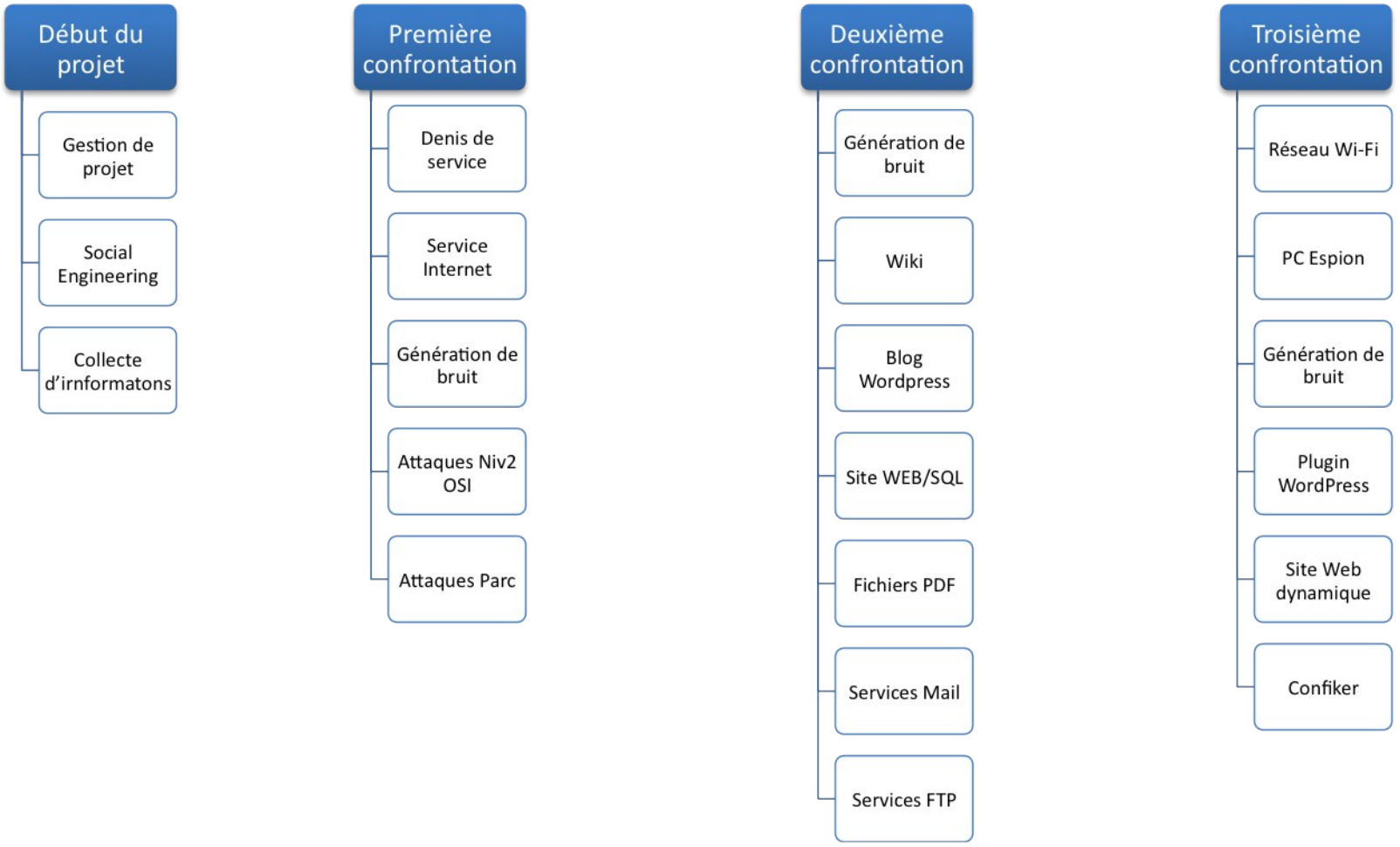
Introduction

- Sensibilisation à la sécurité des SI
- Approfondissement des enseignements
- Mise en pratique des enseignements
- Gestion de projet
- Travail en équipe
- Innovation du mode d'enseignement !

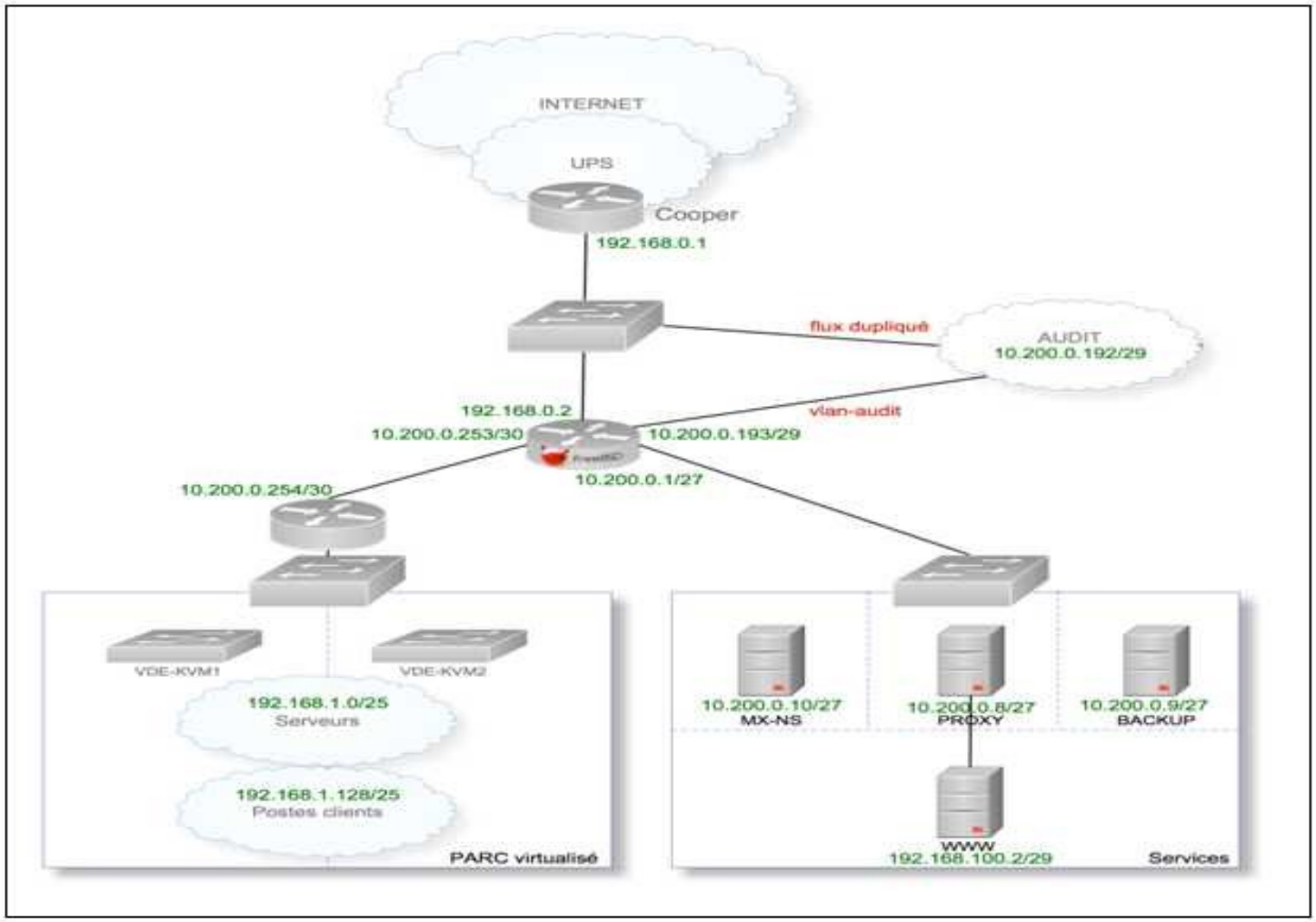
Planification



Organisation

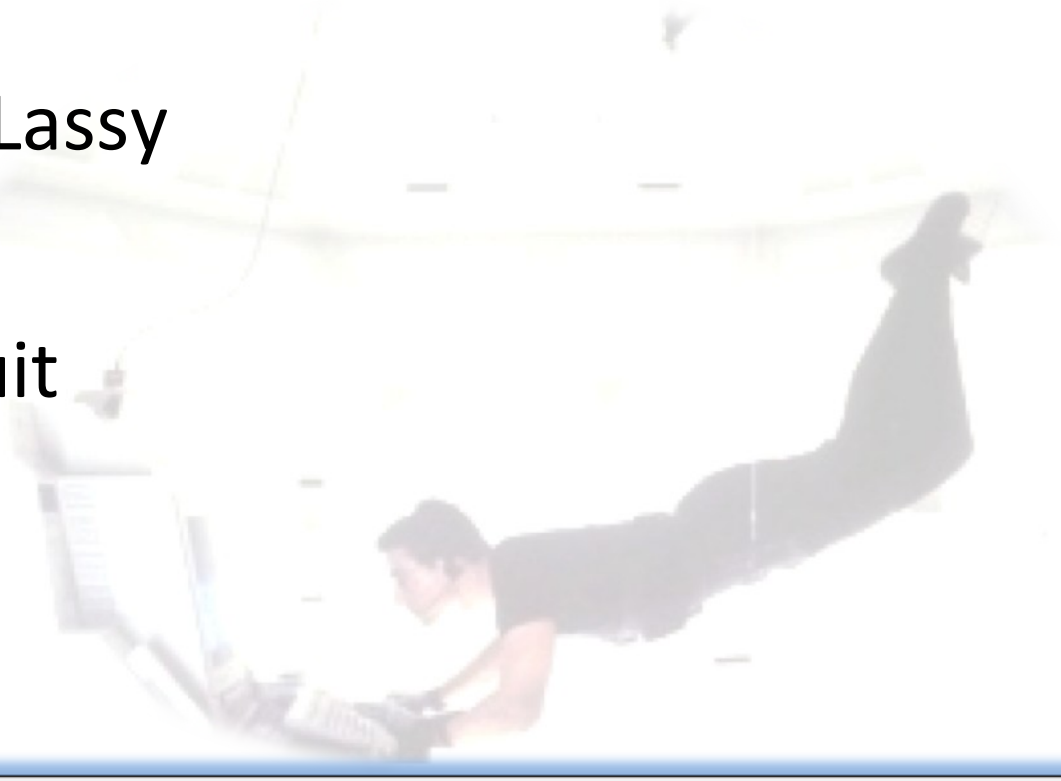


Architecture CANDIDE S.A



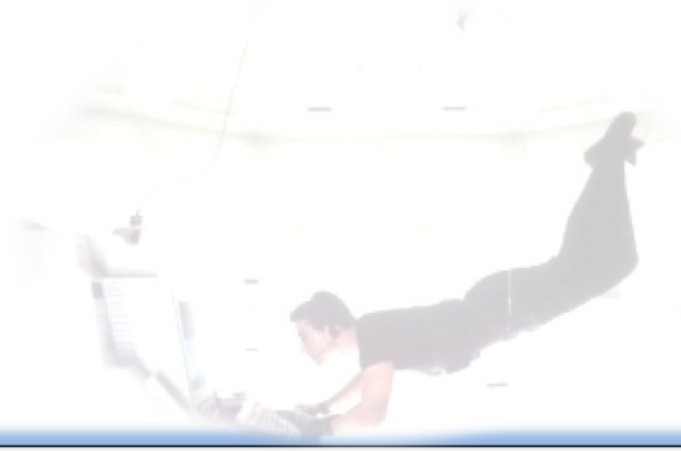
Projets transversaux

- KeyLogger
- Machine espion : Lassy
- Génération de bruit
- Ingénierie sociale



Projets transversaux - KeyLogger

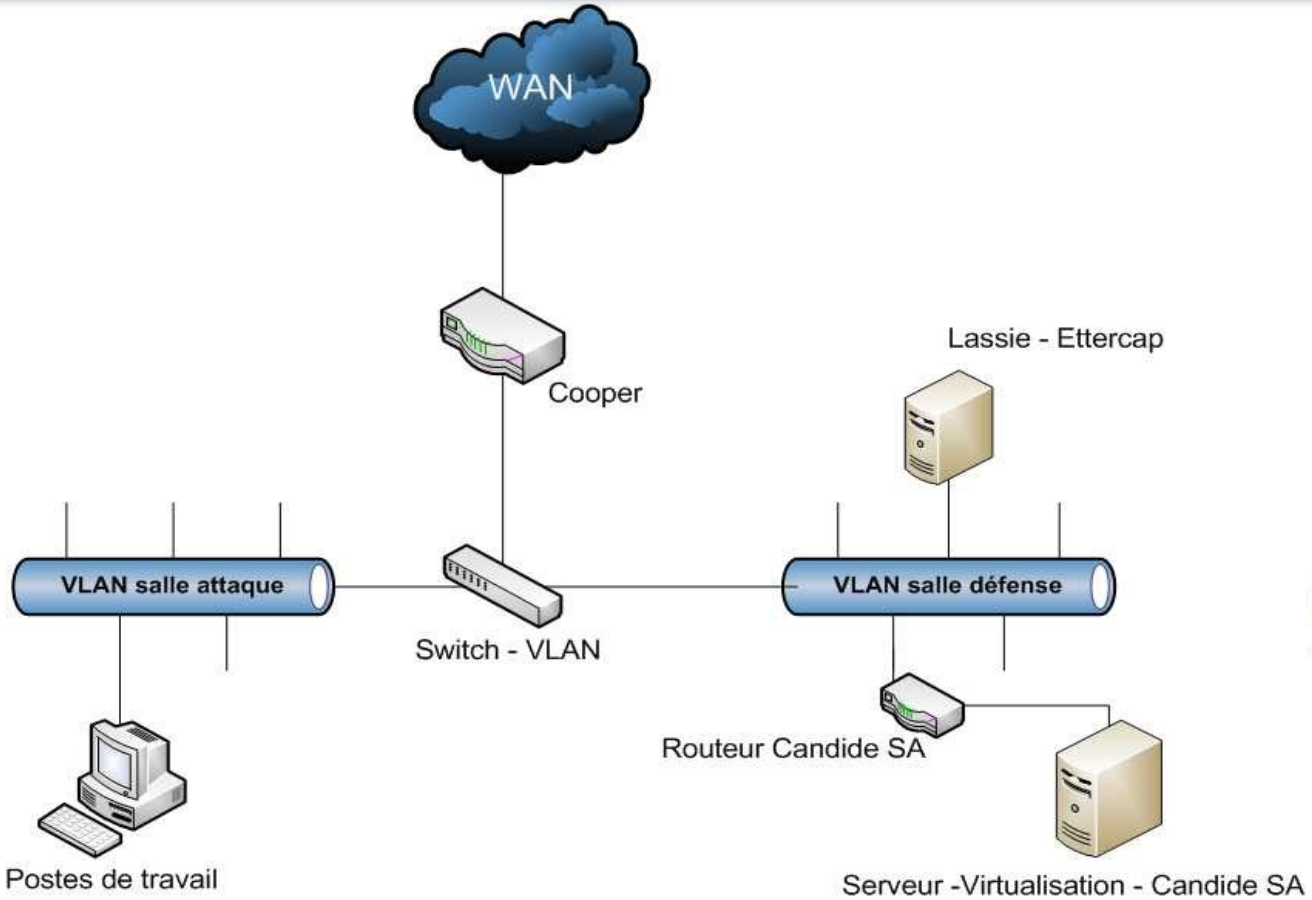
- Module complémentaire (.xpi) de Firefox
- Installation: U2 – 212/211
- Durée de vie: durée du projet
- Récupération des logs par FTP
- Ratio d'efficacité ≈ 20%



Projets transversaux - KeyLogger

- ≈ 40 comptes mails récupérés (L3, 1 Enseignant STRI et 1 M2 Groupe Défense et 1 M2 Audit)
- Comptes M2
  - Comptes secondaires
  - 1 document de Candide SA **récupéré**
  - 1 compte-rendu de réunion – Audit/Défense
- Bilan:
  - Semi-échec (volume d'informations volées)
  - **Contexte professionnel** ➔ **critique**

Projets transversaux - Lassy



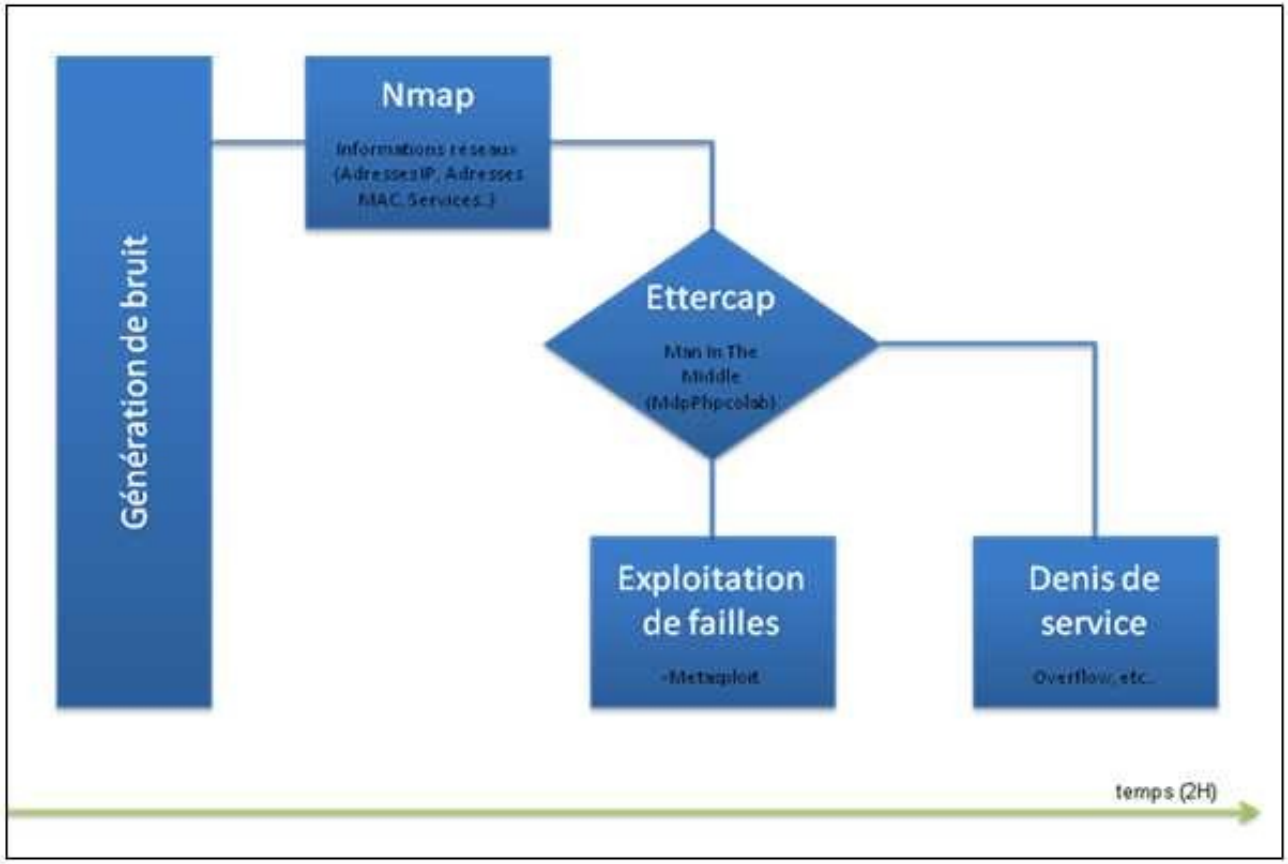
- Machine espion
- Faux plafond
- Switch commun

Projets transversaux - Lassy

- OS : Linux
- Problème de VLAN résolus
- Possibilité Man in The Middle, Wireshark…

- Bilan:
  - Semi-échec (très peu d'informations récupérées)
  - **Contexte professionnel ➔ hyper critique**

Première confrontation



Denis de service

Services internet

Génération de bruit

Attaques Niveau 2 OSI

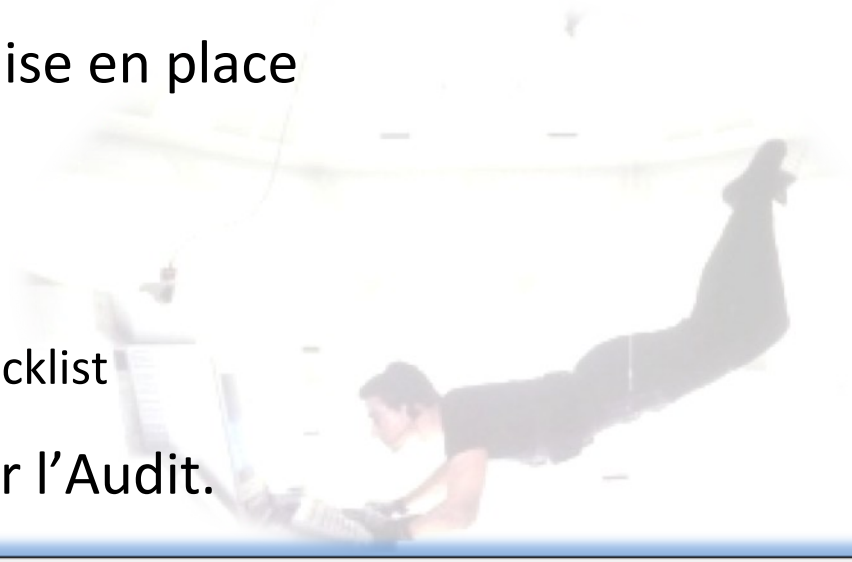
Applicatif/ Système

Deuxième confrontation

Deuxième confrontation

Génération de bruit

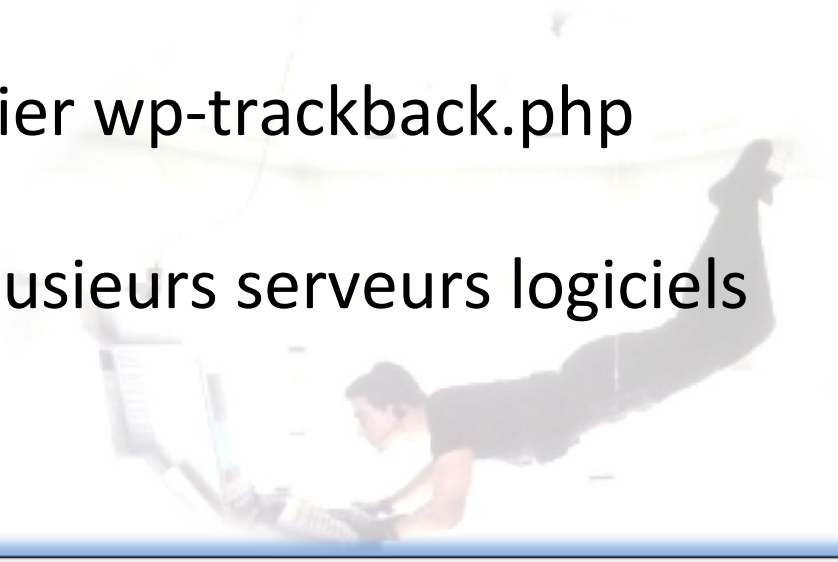
- Script PHP: fausse authentification gestion EDT de Candide SA
- Exécuté sur 10 machines
- Avantage:
  - Facilité de développement / mise en place
- Améliorations:
  - Alterner les couples login/mdp
  - Modification adresse IP ➔ éviter blacklist
- Bilan: Evaluation de l'efficacité par l'Audit.



Deuxième confrontation

WordPress

- Système de blog géré en PHP
- Failles courantes, même si rapidement corrigées
- Exemple d'exploitation : fichier wp-trackback.php
- Résultat de l'exploitation : plusieurs serveurs logiciels H.S.



Deuxième confrontation

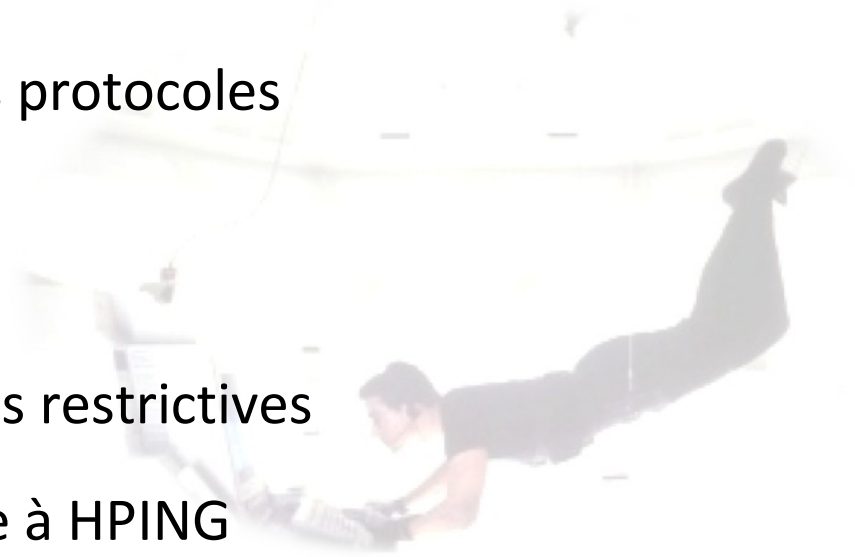
Mail Bombing

- Mise en place: XMAS 2000
- Difficultés trouvées
  - Antivirus
  - Pas d'accusé de réception du serveur smtp
  - Disponibilités
- Bilan
  - Différents outils Mail bombing détection et filtrage des messages indésirables facile

Deuxième confrontation

HPING

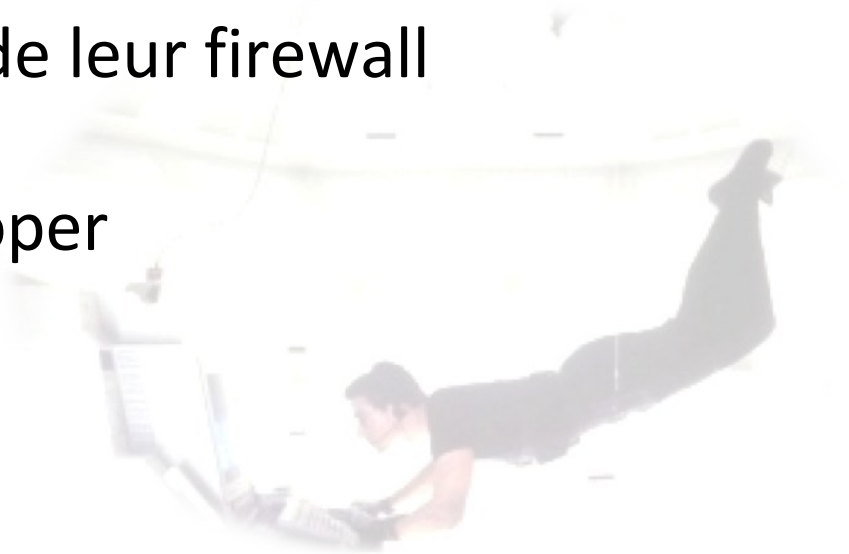
- Outil pour tester la sécurité des réseaux
  - Test de firewall
  - Port scanning
  - Test de réseaux avec différents protocoles
- Blacklister une adresse
  - Configuration de la défense très restrictives
  - Modifier l'adresse source grâce à HPING



Deuxième confrontation

HPING

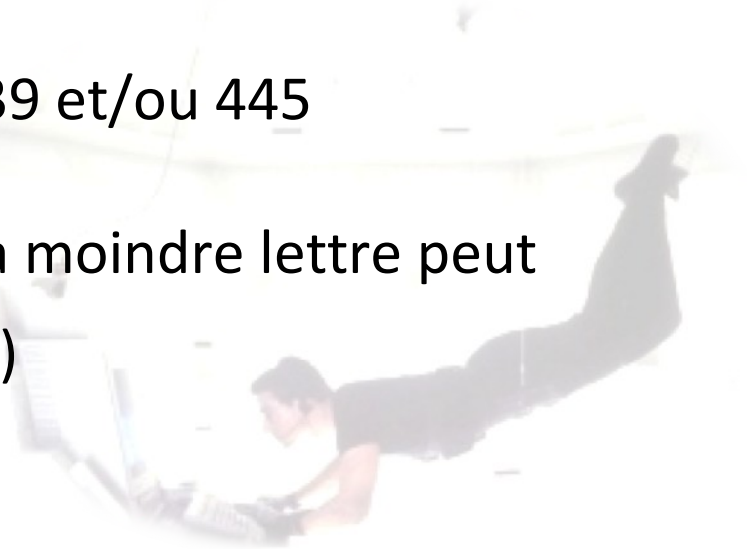
- Bilan
  - Fonctionnement des commandes
  - Modifications des règles de leur firewall
  - Utilisation de NAT sur cooper



Deuxième confrontation

Winnuke2

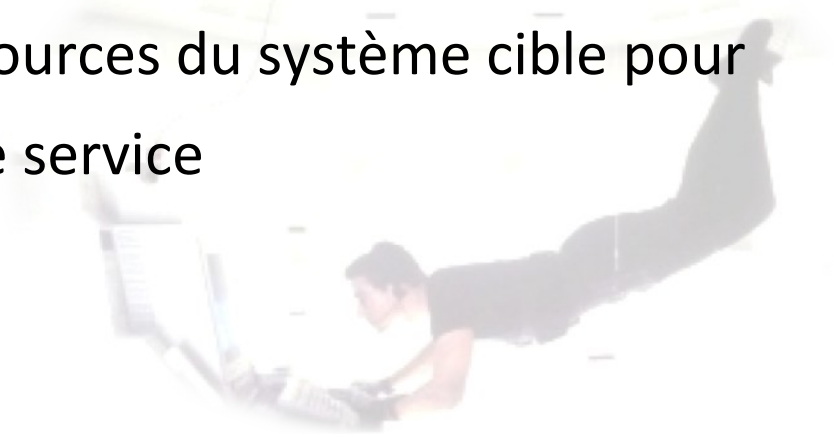
- But
  - Créer un dénis de service sur des machines Windows NT, 2000 et XP (après winnuke → Patch)
  - Connexion en TCP sur les ports 139 et/ou 445
  - 139, port utilisé par NetBIOS → la moindre lettre peut faire bugger windows (écran bleu)
- Résultat



Deuxième confrontation

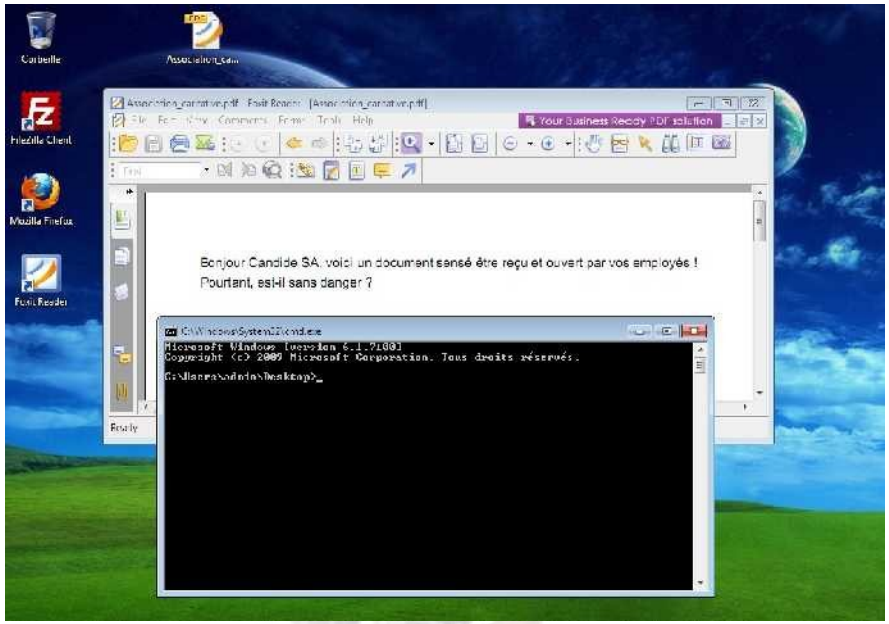
Jolt2

- But
  - Vise les systèmes Windows 2000 et NT
  - Envoyer un grand nombre de paquets IP fragmentés
  - Utiliser un maximum des ressources du système cible pour le ralentir et créer un dénis de service
- Résultat

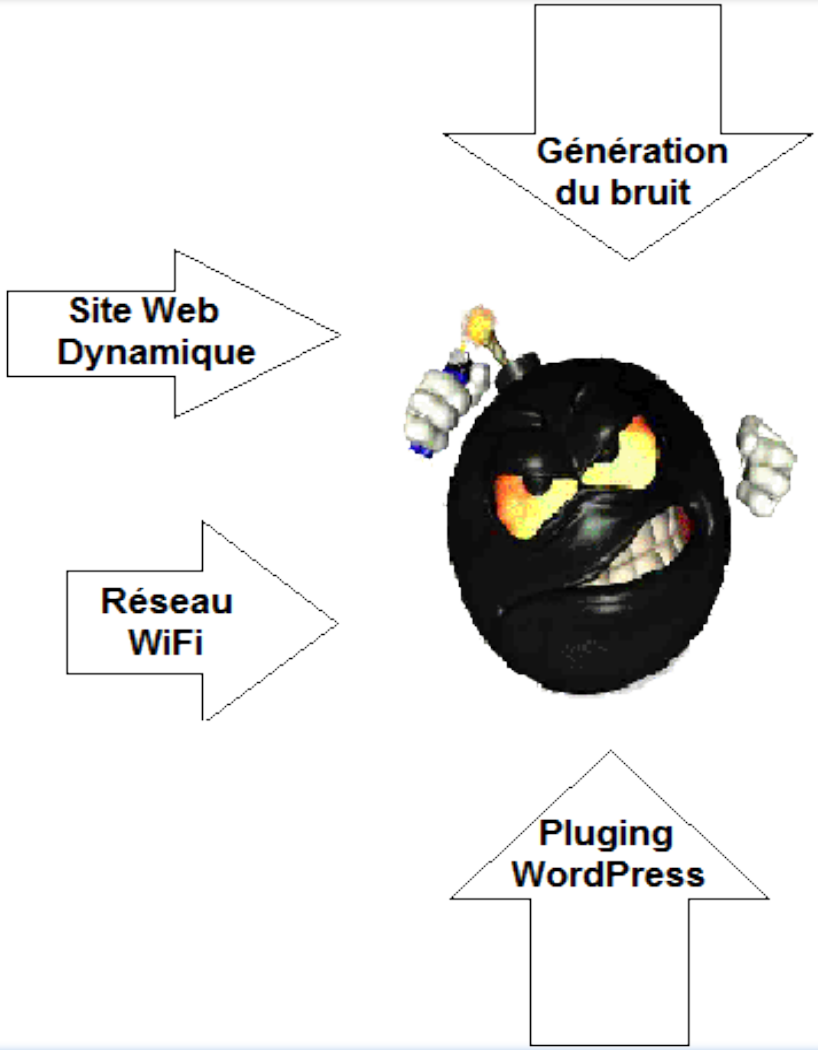


Les fichiers PDF

- Présentation
  - Le format « Portable Document Format »
  - Librairie java iText 5
  - Foxit Reader
- Résultats obtenus
- Bilan
  - Pédagogie



Troisième confrontation



- Réseau WiFi
- Intrusion PC Lassy
- Génération de bruit
- Plugin WordPress
- Site Web dynamique
- Confiker

Bilan

- De plus en plus de paquet/logiciel sécurisés
- Groupe défense très compétent !
- Manque d'implication dès le départ
- Gestion de projet
- Expérience de travail collaboratif